Neusoft

东软集成安全网关软件 V4.2 用户使用指南

版权所有

本软件和相关文档的版权归沈阳东软系统集成工程有限公司所有，任何侵犯版权的行为都将被追究法律责任。未经版权所有者的书面许可，不得将本软件的任何部分或全部及其用户手册以任何形式、采用任何手段 (电子的或机械的，包括照相复制或录制)、为任何目的，进行复制或传播。

版权所有 © 2001-2014 沈阳东软系统集成工程有限公司。所有权利保留，侵权必究。

沈阳东软系统集成工程有限公司不对因使用本软件及其用户手册所造成的任何损失承担任何责任。

东软联系信息

网站：http://www.neusoft.com

电子信箱：neteyeservice@neusoft.com

服务电话：4006 — 556789

目录

前言 1
文档约定 2
相关手册 2

1 快速向导 3
1.1 部署模式 4
1.1.1. 透明模式 4
1.1.2. 路由模式 4
1.2 使用向导进行初始化配置 5
1.2.1 登录 5
1.2.2 设置系统语言 / 主机名 / 系统时间 6
1.2.3 配置透明模式（二层） 7
1.2.4 配置路由模式（三层） 12
1.2.5 重置密码 19
1.2.6 导入 License 19
1.3 使用 WebUI 进行初始化配置 20
1.3.1 登录 20
1.3.2 WebUI 概述 20
1.3.3 重置密码 21
1.3.4 设置系统语言 / 主机名 / 系统时间 22
1.3.5 配置透明模式 23
1.3.6 配置路由模式 23
1.3.7 导入 License 26
1.4 使用 CLI 进行初始化配置 27
1.4.1 CLI 基本信息 27
1.4.2 设置系统语言 / 主机名 / 系统时间 28
1.4.3 重置密码 29
1.4.4 配置透明模式 29
1.4.5 配置路由模式 31
1.4.6 导入 License 34
1.4.7 使用 SSH 登录 35
1.4.8 使用 Telnet 登录 36

2 功能概述 37
2.1. 系统配置 38
2.2. 网络配置 39
2.3. 数据包处理流程 40
2.4. 路由 42
2.4.1. 三层单播路由 （缺省路由和策略路由） 42
2.4.2. 三层多播 （多播和 DVMRP） 44
2.4.3. 二层多播 （IGMP Snooping） 45
2.5. 地址转换 （NAT） 46
2.6. 服务质量 （QoS） 47
2.7. 防火墙策略 48
2.8. 攻击防御 51
2.9. 统一威胁管理 （UTM） 52
2.9.1. 应用控制 53
2.9.2. HTTP 控制 54
2.9.3. DNS 控制 55
2.9.4. 客户端防护 56
2.9.5. 服务器防护 58
2.10. 虚拟专用网 （VPN） 60
2.10.1. IPSec VPN 60
2.10.2. SSL VPN Web 入口页面 61
2.10.3. SSL VPN 隧道 62
2.11. 高可用性 （HA） 63
2.12. 虚拟系统 / 网络 （Vsys/Vnet） 64
2.13. 监控 / 日志 65
2.14. 报表 65

3 系统配置 67
3.1 WebUI 主页 68
3.2 系统概述 69
3.2.1 基本配置步骤 69
3.2.2 配置参数说明 70
3.3 标题信息 71
3.3.1 概述 71
3.3.2 基本配置步骤 71
3.4 资产汇总 72
3.5 版权信息 73
3.6 系统时间 74
3.6.1 概述 74
3.6.2 基本配置步骤 75
3.6.3 配置参数说明 76
3.7 License 77
3.7.1 概述 77

3.7.2 基本配置步骤 78
3.7.3 配置参数说明 80
3.8 系统升级 81
3.8.1 概述 81
3.8.2 基本配置步骤 81
3.8.3 配置参数说明 83
3.9 安装升级包管理 84
3.10 增强升级包管理 85
3.11 访问服务 86
3.11.1 基本配置步骤 86
3.11.2 配置参数说明 87
3.12 SNMP 88
3.12.1 概述 88
3.12.2 基本配置步骤 89
3.12.3 配置参数说明 90
3.13 管理用户 91
3.13.1 概述 91
3.13.2 基本配置步骤 93
3.13.3 配置参数说明 94
3.14 网络用户 95
3.14.1 概述 95
3.14.2 基本配置步骤 96
3.14.3 配置参数说明 97
3.15 用户认证 98
3.15.1 概述 98
3.15.2 基本配置步骤 99
3.15.3 配置参数说明 101
3.16 WebAuth 配置 102
3.16.1 概述 102
3.16.2 基本配置步骤 103
3.16.3 配置参数说明 105
3.16.4 范例：用户认证 106
3.17 备份恢复 111
3.17.1 概述 111
3.17.2 基本配置步骤 111
3.18 技术支持 113
3.18.1 概述 113
3.18.2 基本配置步骤 113
3.19 集中管理 114
3.19.1 概述 114
3.19.2 基本配置步骤 114
3.20 诊断工具 115
3.20.1 Ping 115

3.20.2 Traceroute 115
3.20.3 Debug 116
3.21 报警配置 118
3.21.1 概述 118
3.21.2 基本配置步骤 119
3.21.3 配置参数说明 122
3.22 日志维护 124
3.22.1 概述 124
3.22.2 基本配置步骤 125
3.22.3 配置参数说明 126
3.23 证书 127
3.23.1 概述 127
3.23.2 基本配置步骤 128
3.23.3 范例：自动生成证书 131
3.23.4 本地证书参数 135
3.23.5 CA 证书参数 136
3.24 对象 137
3.24.1 IP 地址 137
3.24.2 服务 139

4 网络配置 141
4.1 接口概述 142
4.1.1 工作模式 142
4.1.2 接口属性 142
4.2 以太网接口 146
4.2.1 概述 146
4.2.2 基本配置步骤 146
4.2.3 范例：以太网接口 152
4.3 以太网通道 154
4.3.1 概述 154
4.3.2 基本配置步骤 154
4.4 冗余接口 157
4.4.1 概述 157
4.4.2 基本配置步骤 157
4.5 虚拟接口 161
4.5.1 概述 161
4.5.2 基本配置步骤 161
4.6 VLAN 接口 164
4.6.1 概述 164
4.6.2 基本配置步骤 164
4.6.3 范例：VLAN 接口 165
4.7 环回接口 168
4.7.1 概述 168

4.7.2 基本配置步骤 168
4.8 PPPoE 接口 170
4.8.1 概述 170
4.8.2 基本配置步骤 170
4.8.3 配置参数说明 172
4.9 隧道接口 174
4.9.1 概述 174
4.9.2 基本配置步骤 174
4.9.3 配置参数说明 175
4.10 ARP 176
4.10.1 概述 176
4.10.2 基本配置步骤 176
4.10.3 配置参数说明 177
4.11 CAM 178
4.11.1 概述 178
4.11.2 基本配置步骤 178
4.11.3 配置参数说明 179
4.12 安全域 180
4.12.1 概述 180
4.12.2 基本配置步骤 180
4.12.3 范例：安全域应用 182
4.12.4 配置参数说明 183
4.13 DNS 主机 184
4.13.1 概述 184
4.13.2 基本配置步骤 184
4.13.3 配置参数说明 184
4.14 DNS 代理 185
4.14.1 概述 185
4.14.2 基本配置步骤 185
4.14.3 配置参数说明 186
4.15 DNS 缓存 187
4.15.1 概述 187
4.15.2 基本配置步骤 187
4.15.3 配置参数说明 188
4.16 DHCP 服务器 189
4.16.1 概述 189
4.16.2 基本配置步骤 189
4.16.3 DHCP 范例 191
4.16.4 配置参数说明 195
4.17 DHCP 作用域 196
4.17.1 概述 196
4.17.2 基本配置步骤 196

4.17.3 配置参数说明 198
4.18 DHCPv6 199
4.18.1 概述 199
4.18.2 基本配置步骤 200
4.18.3 DHCPv6 范例 201
4.18.4 配置参数说明 206
4.19 STP 208
4.19.1 概述 208
4.19.2 基本配置步骤 210
4.19.3 范例：STP 应用 211
4.19.4 配置参数说明 218
4.20 邻居发现 219
4.20.1 概述 219
4.20.2 基本配置步骤 220
4.20.3 ND 范例 221
4.20.4 配置参数说明 226

5 路由 229
5.1. 概述 230
5.1.1 单播. 231
5.1.2 三层多播. 234
5.1.3 二层多播. 235
5.2. 基本配置步骤 236
5.2.1 单播. 237
5.2.2 三层多播. 241
5.2.3 二层多播. 243
5.3. 基础范例 245
5.3.1 单播. 246
5.3.2 三层多播. 250
5.3.3 二层多播. 252
5.4. 高级范例 254
5.4.1 范例 1：创建带有负载均衡的静态路由 255
5.4.2 范例 2：创建策略路由策略 257
5.4.3 范例 3：静态多播路由应用 261
5.4.4 范例 4：动态 DVMRP 多播路由应用 264
5.4.5 范例 5：IGMP Snooping 和静态多播 CAM 表项应用 266
5.4.6 范例 6：IGMP Snooping 和动态多播 CAM 表项应用 269
5.5. 参数说明 271
5.5.1 单播路由参数 272
5.5.2 单播策略路由参数 273
5.5.3 三层动态多播 （DVMRP）参数 274
5.5.4 三层静态多播参数. 275
5.5.5 二层动态多播参数 （IGMP Snooping） 276

5.5.6 二层静态多播 CAM 条目参数 277

6 地址转换 279
6.1 地址转换概述 280
6.1.1 NAT 规则创建和选择 280
6.1.2 SNAT 规则 281
6.1.3 DNAT 规则 285
6.1.4 MIP 规则 288
6.1.5 导入 / 导出 289
6.2 基本配置步骤 290
6.2.1 创建 SNAT 规则 290
6.2.2 创建 DNAT 规则 293
6.2.3 创建 MIP 规则 295
6.3 范例 296
范例 1：一对一 SNAT 296
范例 2：多对一 SNAT （启用 NAPT） 298
范例 3：一对一 DNAT 300
范例 4：一对多 DNAT （启用 NAPT） 302
范例 5：MIP 304
范例 6：DNAT 和 DNS 重写 306
6.4 配置参数说明 308
6.4.1 源地址转换规则参数 308
6.4.2 目的地址转换规则参数 309
6.4.3 地址映射规则参数 310

7 服务质量 311
7.1. 基本概念 311
7.2. 基本配置步骤 312
7.2.1 创建普通 QoS 防护配置 313
7.2.2 创建每 IP/ 用户 QoS 防护配置 313
7.2.3 创建 QoS 策略 314
7.3. 范例 318
7.4. 配置参数说明 321
7.4.1. QoS 策略 321
7.4.2. QoS 防护配置 322
7.4.3. 每 IP/ 用户 QoS 防护配置 323

8 策略 325
8.1 概述 326
8.1.1 IP-MAC 绑定 326
8.1.2 访问策略 327
8.1.3 缺省访问策略 327
8.1.4 多播策略 327

8.1.5 会话策略 328
8.2 基本配置 329
8.2.1 配置 IP-MAC 绑定 329
8.2.2 创建访问策略. 331
8.2.3 配置缺省访问策略 334
8.2.4 创建多播策略. 334
8.2.5 创建会话策略. 336
8.3 范例. 338
范例 1：创建 IP-MAC 绑定策略. 339
范例 2：创建访问策略. 341
范例 3：安全域间多播策略的应用. 343
范例 4：创建基于目的 IP 的会话策略 347
8.4 配置参数说明. 349
8.4.1 IP-MAC 绑定策略参数 349
8.4.2 访问策略参数. 350
8.4.3 多播策略参数. 352
8.4.4 会话策略参数. 353

9 攻击防御 355
9.1. 基本概念. 356
9.1.1. 攻击目的. 356
9.1.2. 攻击威胁类型 356
9.1.3. 应对措施. 356
9.2. 攻击类型 / 方式 / 解决措施 357
9.2.1. DoS 防御 358
9.2.2. 探测防御. 360
9.2.3. TCP 逃避控制. 362
9.2.4. IP 选项校验. 363
9.2.5. ICMP 攻击防御. 365
9.3. 基本配置步骤 367
9.3.1. DoS 防御 367
9.3.2. 探测防御. 368
9.3.3. TCP 逃避控制. 368
9.3.4. IP 选项校验. 369
9.3.5. ICMP 攻击防御. 370
9.4. 配置参数说明 371
9.4.1. DoS 防御参数. 371
9.4.2. ICMP 防御参数. 372
9.4.3. IP 选项校验参数 373
9.4.4. 探测防御参数 373
9.4.5. TCP 逃避控制. 374

10 统一威胁管理 375
10.1. 概述 376
10.1.1. 出口控制 377
10.1.2. 客户端防护 378
10.1.3. 服务器防护 382
10.1.4. 应用场景 383
10.2. 基本配置步骤 384
10.2.1. 出口控制 385
10.2.2. 客户端防护 397
10.2.3. 服务器防护 421
10.2.4. 通知消息 432
10.2.5. 概要信息页面 433
10.3. UTM 范例 434
范例 1：UTM 出口控制典型应用 435
范例 2：UTM 客户端防护典型应用 447
范例 3：UTM 服务器防护典型应用 458
10.4. 配置参数说明 469
10.4.1. 概要信息 470
10.4.2. 出口控制 471
10.4.3. 客户端防护 481
10.4.4. 服务器防护 485
10.4.5. 防病毒 492
10.4.6. 反垃圾邮件 497
10.4.7. IPS 504
10.4.8. 通知消息 512
10.5. UTM 缺省设置 514
10.5.1. 缺省防病毒防护配置 515
10.5.2. 缺省反垃圾邮件防护配置 518
10.5.3. 反垃圾邮件规则集 518
10.5.4. 缺省 IPS 防护配置 520
10.5.5. 攻击签名规则 521
10.5.6. HTTP 协议限制缺省设置 522
10.5.7. SMTP 协议限制缺省设置 523
10.5.8. POP3 协议限制缺省设置 524
10.5.9. IMAP 协议限制缺省设置 524
10.5.10. DNS 协议限制缺省设置 525
10.5.11. （Web 防护）信息泄露防护 526
10.5.12. （Web 防护）注入攻击防御 528

11 虚拟专用网 529
11.1 概述 529
11.1.1 网段到网段 IPSec 手动密钥隧道 531
11.1.2 网段到网段自动密钥隧道 535

11.1.3. 远程访问 IPSec VPN 540
11.1.4. SSL VPN Web 入口页面访问 541
11.1.5 SSL VPN 隧道访问 543
11.1.6 NAT 环境下网段到网段 IPSec VPN (隧道模式） 544
11.1.7 高可用环境下的 VPN. 546
11.2 基本配置 547
11.2.1 网段到网段手动密钥隧道 （范例 1） 547
11.2.2 网段到网段 IPSec 自动密钥隧道 （范例 2） 547
11.2.3 远程访问 IPSec 自动密钥隧道 （范例 3） 548
11.2.4 SSL VPN Web 入口页面访问 （范例 4） 549
11.2.5 SSL VPN 隧道 （范例 5） 550
11.3 范例 551
范例 1. 网段到网段的手动密钥隧道 552
范例 2. 基于路由的网段到网段自动 IKE 560
范例 3. 远程访问 VPN 隧道 568
范例 4. 通过 SSL VPN Web 入口页面访问 584
范例 5. 通过 SSL VPN 隧道访问 593
范例 6. NAT 穿越 （IPSec VPN) 596
范例 7. HA 自动同步 （SSL VPN) 603
范例 8. IPSec VPN 隧道组 617
11.4 配置参数说明. 622
11.4.1 IPSec VPN 相关参数 622
11.4.2 SSL VPN 相关参数 628
11.4.3 IP 地址池相关参数. 632

12 高可用性 633
12.1 概述 633
12.1.1 标准 VRRP 和增强 VRRP 634
12.1.2 标准的 VRRP 配置 635
12.1.3 增强的 VRRP （VRDG/ 集群）配置 636
12.1.4 标准的 VRRP 运行原理 638
12.1.5 增强的 （VRDG/ 集群）运行原理 640
12.2 基本配置步骤. 642
12.2.1 VRRP 基本配置 642
12.2.2 增强的 （VRDG/ 集群） 644
12.3 范例 648
范例 1：增强 （VRDG/ 集群）基本配置 648
范例 2：主备选举 655
范例 3：负载分担 （主主模式） 660
范例 4：IP 探测 665
范例 5：集群同步 672
12.4 配置参数说明. 679
12.4.1 虚拟路由器 679

12.4.2 虚拟路由器探测组 680
12.4.3 集群 681

13 虚拟系统 683
13.1. 概述 683
13.1.1. 虚拟系统 （Vsys） 684
13.1.2. 虚拟网络 （Vnet） 685
13.2. 基本配置步骤 686
13.2.1. 创建三层接口 687
13.2.2. 创建虚拟系统 （资源限制 / 接口 / 管理 IP/UTM） 688
13.2.3. 创建虚拟系统管理员 689
13.2.4. 登录 / 切换虚拟系统 690
13.2.5. 管理虚拟系统 692
13.2.6. 创建虚拟网络 693
13.3. 场景 694
1. 透明模式 694
2. 路由模式 695
3. 混合模式 696
13.4. 范例 697
范例 1：基于三层共享接口的多 Vsys 应用 697
范例 2：基于 Trunk 接口的多 Vsys 应用 708
13.5. 配置参数说明 715
13.5.1. 虚拟系统 715
13.5.2. 虚拟网络 715
13.5.3. 虚拟系统中可配置的功能 716

14 监控 717
14.1 拓扑 718
14.2 流量统计 718
14.2.1 接口流量 719
14.2.2 应用排名 719
14.2.3 URL 排名 719
14.2.4 用户排名 719
14.2.5 IP 地址排名 719
14.3 虚拟系统 720
14.4 STP 721
14.5 路由 722
14.6 NAT 723
14.7 ARP 724
14.7.1 ARP 表 724

14.7.2 代理 ARP 表 724
14.8 CAM 725
14.9 DHCP IP 地址绑定状态 726
14.10 DHCPv6 客户端 727
14.11 DNS 缓存 728
14.12 高可用性 729
14.12.1 虚拟路由器 729
14.12.2 虚拟路由器探测组 730
14.12.3 集群 731
14.13 系统利用率 732
14.13.1 CPU 和内存利用率 732
14.13.2 磁盘利用率 732
14.13.3 进程 733
14.14 在线用户 734
14.14.1 WebAuth 用户 734
14.14.2 SSL VPN 用户 734
14.15 IPSec VPN 隧道 735
14.15.1 自动密钥隧道 735
14.15.2 手动密钥隧道 736
14.15.3 加速卡统计 736
14.15.4 软加密统计 737
14.15.5 隧道组 737
14.16 多播 738
14.16.1 DVMRP 邻居 738
14.16.2 IGMP Snooping 状态 738
14.17 报警 / 日志 739
14.17.1 系统日志 739
14.17.2 防病毒报警 740
14.17.3 反垃圾邮件报警 741
14.17.4 URL 过滤报警 742
14.17.5 IPS 报警 743
14.17.6 应用控制报警 744

15 报表 745
15.1 概述 746
15.1.1 记录的数据类别 746
15.1.2 报表内容及格式 746
15.1.3 定期生成报表 746
15.1.4 查看 / 下载 / 邮件发送报表结果 746
15.1.5 报表保留数目 746
15.2 基本配置步骤 747
15.2.1 配置常规设置 747
15.2.2 创建报表生成计划 748

15.2.3 管理报表结果 751
15.3 配置参数说明 752
15.3.1 SMTP 服务器参数. 752
15.3.2 报表计划参数 752
15.3.3 报表结果参数 753
15.3.4 全局内容参数 753
15.3.5 特定用户内容参数. 771

A MIB 库 773
n 公共 MIB 库 773
12.4. 私有 MIB 库 788

前言

本手册介绍东软集成安全网关（以下简称 NISG），由以下部分组成：

- 第 1 章，快速向导，介绍 NISG 初始化配置和验证，包括向导、WebUI 和 CLI 三种方式。
- 第 2 章，功能概述，介绍 NISG 各模块功能（第 3 章到第 15 章）。
- 第 3 章，系统配置，介绍与系统相关的配置。
- 第 4 章，网络配置，介绍 NISG 的接口、安全域、 STP、 DHCP、 DNS、 IPv6 功能。
- 第 5 章，路由，介绍路由和多播特性。
- 第 6 章，地址转换，介绍源地址转换（SNAT）、目的地址转换（ DNAT）和地址映射（MIP）。
- 第 7 章，服务质量，介绍 QoS 特性、配置和范例。
- 第 8 章，策略，介绍访问策略、会话策略、多播策略、 IP-MAC 绑定以及默认策略配置。
- 第 9 章，攻击防御，介绍针对网络攻击的探测和防御机制。
- 第 10 章，统一威胁管理，介绍出口控制、客户端保护和服务器保护。
- 第 11 章，虚拟专用网，介绍 IPSec VPN 和 SSL VPN（包括 SSL VPN Web 入口页面和 SSL VPN 隧道）。
- 第 12 章，高可用性，介绍标准 VRRP 和增强功能。
- 第 13 章，虚拟系统，介绍虚拟系统和虚拟网络。
- 第 14 章，监控，介绍信息监控功能。
- 第 15 章，报表，介绍生成报表的功能。
- 附录 A, MIB 库，介绍 NISG 支持的 MIB 对象的含义。

文档约定

表 1 图标约定

路由器	服务器	用户
交换机	数据库	用户
NISG	个人电脑	笔记本

相关手册

除了本手册，管理员还可获得产品附带的以下文档：

东软集成安全网关软件 V4.2 命令参考手册

1 快速向导

本章描述以下内容：

- 1.1 部署模式
- 1.2 使用向导进行初始化配置
- 1.3 使用 WebUI 进行初始化配置
- 1.4 使用 CLI 进行初始化配置

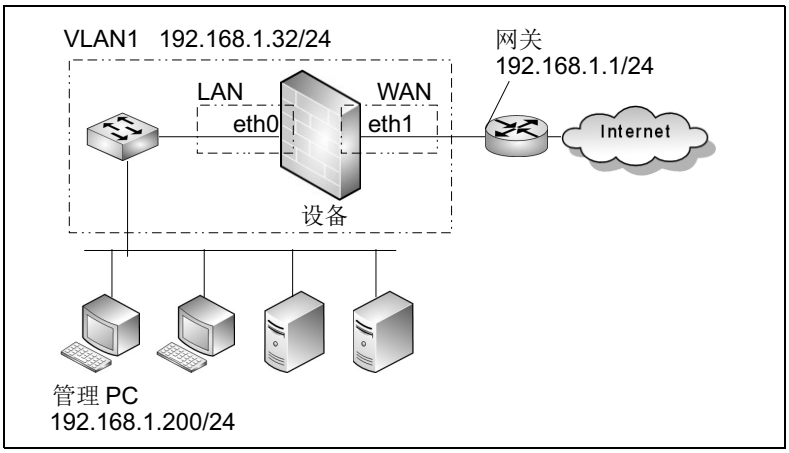
1.1 部署模式

NISG 提供如下两种部署模式，所有后续配置步骤均基于这两种模式。

- 1.1.1. 透明模式
- 1.1.2. 路由模式

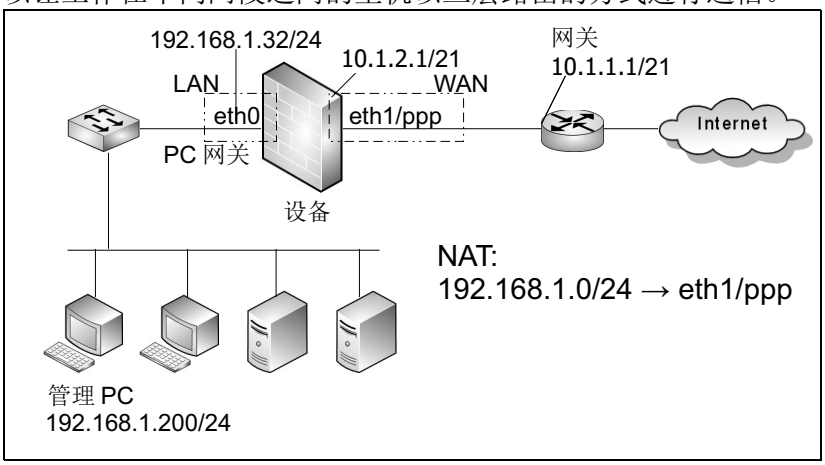
1.1.1. 透明模式

NISG 可部署在私有网络的现有网关后面，无缝集成到现有网络中。透明模式下， NISG 主要用于数据的二层转发。当客户需要在不改变网络拓扑的情况下提供安全保护时，可使用此工作模式。



1.1.2. 路由模式

NISG 可部署在公网和私网之间，作为局域网内主机的默认网关。路由模式下， NISG 可以让工作在不同网段之间的主机以三层路由的方式进行通信。



1.2 使用向导进行初始化配置

NISG 提供一个 WebUI 向导用于完成初始化。通过该向导，您可以完成以下配置：

- 1.2.1 登录
- 1.2.2 设置系统语言 / 主机名 / 系统时间
- 1.2.3 配置透明模式 （二层）
- 1.2.4 配置路由模式 （三层）

之后，可以通过 WebUI 完成以下配置：

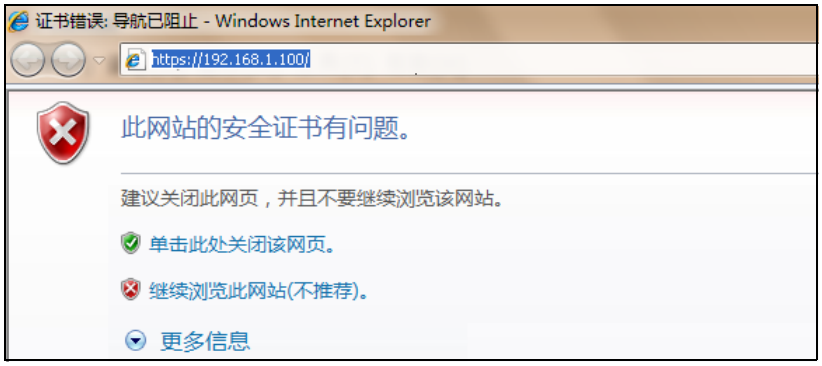
- 1.2.5 重置密码
- 1.2.6 导入 License

1.2.1 登录

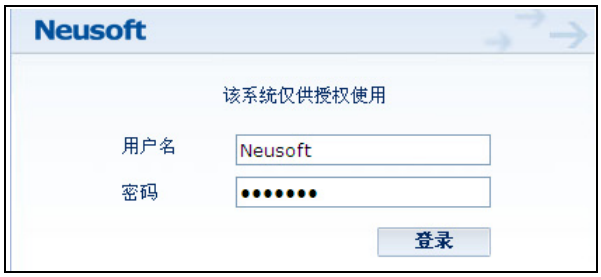
初始化向导仅在以下情况下弹出：

- 首次登录时
- 重置系统后

1. 启动 NISG 设备。
2. 打开终端浏览器，输入 https://192.168.1.100，确保该地址在用户网络环境中可达。
   NISG 支持如下版本的浏览器：
   - Microsoft Internet Explorer （7.0 或更高版本）
   - Mozilla Firefox （10.0 或更高版本）
   - Google Chrome （9.0 或更高版本）
   - Opera （11.x 或更高版本）
   - Safari （5.0 或更高版本）
3. 出现一个证书错误提示页面。点击 “ 继续访问该页面 （不推荐） ” 选择信任 NISG 证书。



4. 出现登录页面（可以在下一个页面修改显示语言）。在文本框中输入缺省用户名 Neusoft 和缺省密码 Neusoft，点击登录按钮。



提示：如果连续输入密码错误达到 5 次，账号将被锁定 20 分钟。

1.2.2 设置系统语言 / 主机名 / 系统时间

5. 登录后系统弹出**欢迎**页面。如果需要，在下拉框中选择相应的语言，点击**后一页**（右面的按钮）。

6. 配置主机名和系统时间，点击**后一页**。

7. 出现**模式**页面，选择一种部署模式。

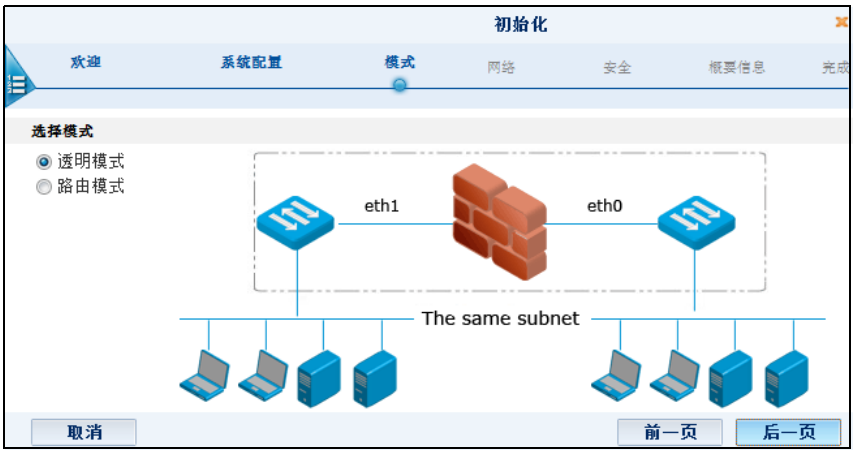
- 1.2.3 配置透明模式（二层）
- 1.2.4 配置路由模式（三层）

1.2.3 配置透明模式（二层）

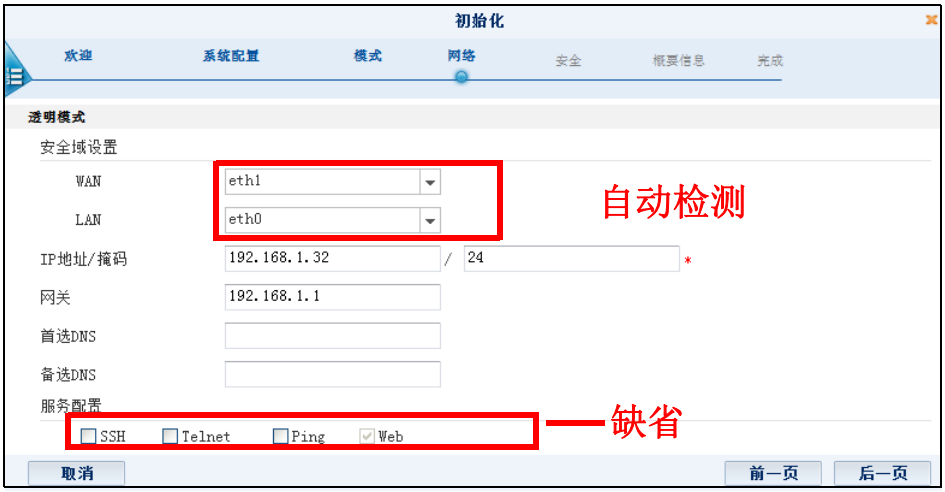
- 1.2.3.1 网络和安全设置
- 1.2.3.2 通过 WebUI 确认初始化配置

1.2.3.1 网络和安全设置

1. 选择**透明模式**，点击**后一页**。

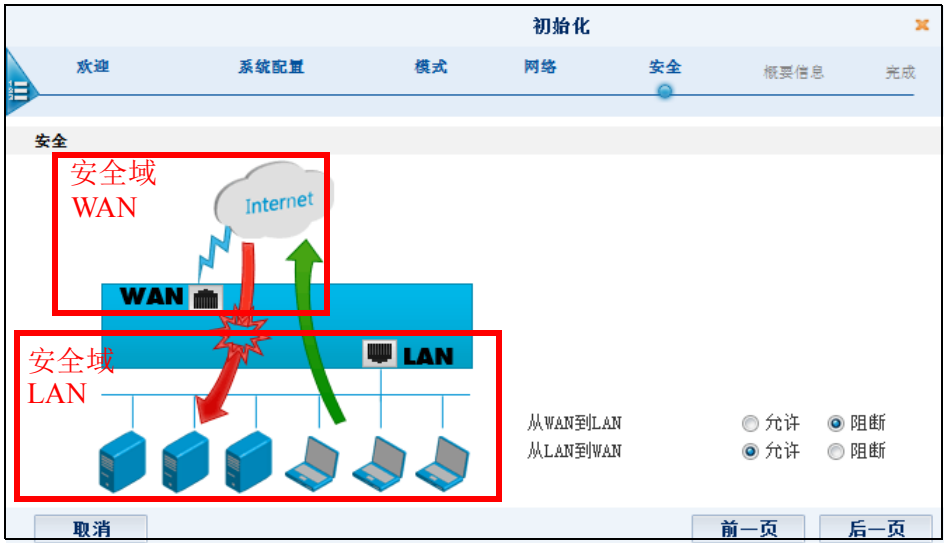


2. 配置网络设置：



- 安全域设置。缺省安全域包括：
  - LAN：二层模式，缺省包含系统检测到的第一个二层以太网接口 （即设备上编号最小的以太网接口）。
  - WAN：二层模式，缺省包含系统检测到的第二个二层以太网接口。
- IP 地址和掩码设置。
  - 缺省 VLAN 接口 vlan1 的 IP 地址默认为 192.168.1.100/24。
  - vlan1 默认包含所有以太网接口。
- NISG 网关地址。缺省为 192.168.1.1。
- DNS 服务器地址。用于解析 NISG 到 Internet 的 DNS 请求域名。
- 服务配置。启用 / 禁用用于管理 NISG 的相关服务。在初始化向导中，管理员只能为 LAN 配置访问服务。

3. 设置访问安全控制动作，点击**后一页**。



4. 检查配置信息，点击**结束**按钮。

5. 点击**关闭**退出初始化向导。

6. 系统自动跳转到登录页面。地址栏中的管理 IP 自动变为修改后的管理 IP。

1.2.3.2 通过 WebUI 确认初始化配置

要确认初始化配置是否生效，请执行以下操作：

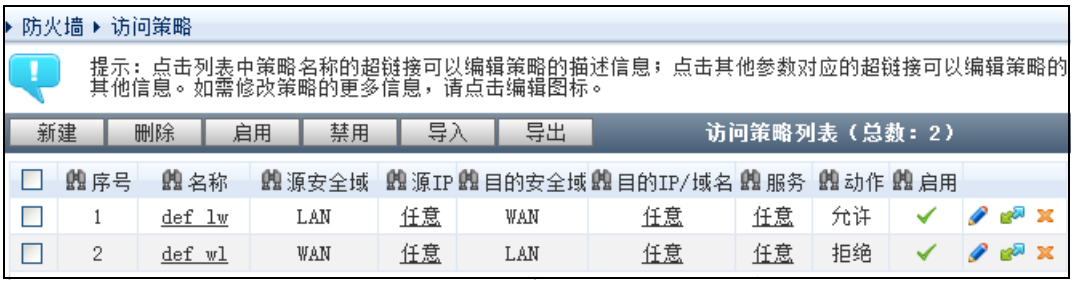
1. 输入缺省用户名和密码进行登录。
2. 查看主页上方的主机名和系统时间，可以看到新的主机名和系统时间已生效。

3. 选择**网络 > 接口**查看接口配置。可以看到新建 VLAN 接口 vlan1 包含 eth0 和 eth1，eth0 已经变为二层以太网接口。

4. 选择**网络 > 安全域**查看安全域配置 。可以看到新建二层安全域 LAN 和 WAN，LAN 包含 eth0， WAN 包含 eth1。安全域被缺省访问策略引用。

5. 选择**网络 > 路由 > 缺省路由**查看默认网关是否已经修改。下面是缺省配置。

6. 选择**防火墙 > 访问策略** 。可以看到系统已经添加两条缺省访问策略，允许 LAN 到 WAN 的访问，同时拒绝 WAN 到 LAN 的访问。



7. 选择**系统 > 服务配置 > 访问设置**查看服务是否已被启用或禁用。用户应根据实际情况配置所需的服务。

8. 通过测试网络连通性验证初始化配置是否生效：

   - 在管理 PC 上 Ping 一个 Internet 网站。按照初始配置，结果应该能 Ping 通，因为 LAN 到 WAN 的访问是被允许的。

```
C:\>ping www.wikipedia.com

Pinging wikipedia-lb.eqiad.wikimedia.org [208.80.154.225] with 32 bytes of data:

Reply from 208.80.154.225: bytes=32 time=375ms TTL=46
Reply from 208.80.154.225: bytes=32 time=381ms TTL=46
Reply from 208.80.154.225: bytes=32 time=381ms TTL=46
Reply from 208.80.154.225: bytes=32 time=344ms TTL=46

Ping statistics for 208.80.154.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 344ms, Maximum = 381ms, Average = 370ms
```

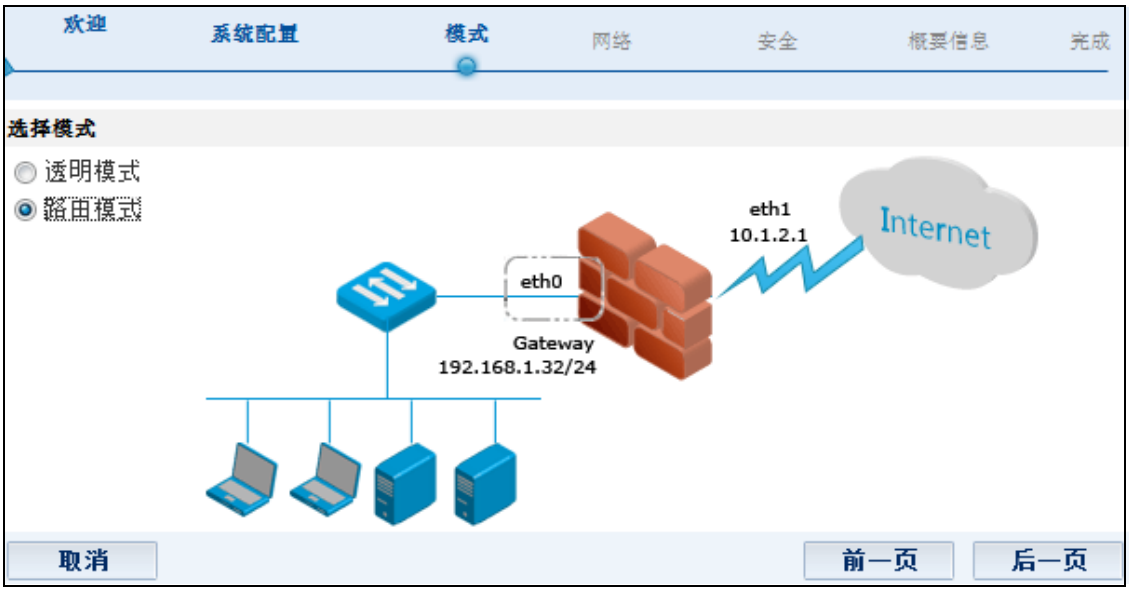
   - 在 WAN 内的一个客户端上 Ping 管理 PC。按照初始配置，结果应该是失败，因为 WAN 到 LAN 的访问是被拒绝的。

```
C:\>ping 192.168.1.200

Pinging 192.168.1.200 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.200:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

1.2.4 配置路由模式 （三层）

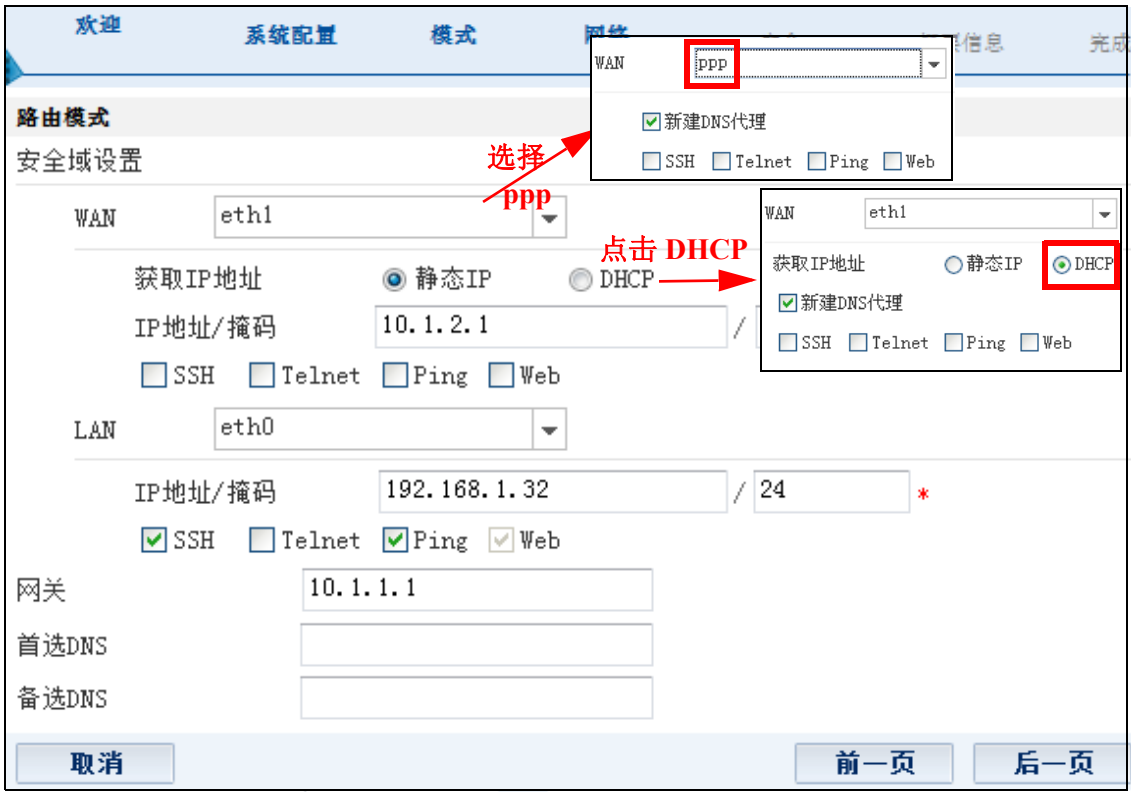
- 1.2.4.1 网络设置
  - 1.2.4.1.1 （网络）以太网设置
  - 1.2.4.1.2 （网络） PPPoE 设置
- 1.2.4.2 网络 NAT 设置
- 1.2.4.3 安全设置
- 1.2.4.4 确认和保存设置 （概要信息）
- 1.2.4.5 通过 WebUI 确认初始化配置

1. 选择**路由模式**， 点击**后一页**。



1.2.4.1 网络设置

2. 配置安全域、网关、 DNS 服务器地址和访问设置，点击**后一页**。



路由模式下的缺省网络配置：

LAN	缺省安全域，三层模式。缺省包含系统检测到的第一个三层以太网接口 （即设备上编号最小的以太网接口），并且该接口使用静态 IP 地址。
WAN	缺省安全域，三层模式。缺省包含系统检测到的第二个三层以太网接口，并且该接口使用静态 IP 地址。

3. 选择使用以太网接口或 PPPoE 接口访问 Internet：

- 1.2.4.1.1 （网络）以太网设置
- 1.2.4.1.2 （网络） PPPoE 设置 （PPPoE 主要用于小型网络）

1.2.4.1.1 （网络）以太网设置

要通过以太网接口访问 Internet，请执行以下操作：

1. 在 **WAN** 下拉框中选取 **eth1**。
   a. 设置 eth1 获取 IP 地址的方式，包括**静态 IP** 和 **DHCP**。
      如使用静态 IP，需手动设置接口的 IP 地址与掩码长度。
   b. 开启或关闭对安全域 WAN 的 SSH、 Telent、 Ping 和 Web 访问。
2. 在 **LAN** 下拉框中选取 **eth0**。
   a. 设置 eth0 接口的 IP 地址与掩码长度。
   b. 开启或关闭对安全域 LAN 的 SSH、 Telent、 Ping 访问， Web 访问方式默认开启。
   c. 设置 NISG 的下一跳网关地址及 DNS 服务器地址。
3. 点击**后一页**。跳转到 NAT 配置页。

1.2.4.1.2 （网络） PPPoE 设置

要通过 PPPoE 接口访问 ISP 网络，请执行以下操作：

1. 在 **WAN** 下拉框中选取 **ppp**。
2. 开启或关闭 ppp 接口的 DNS 代理功能，本页其余配置同以太网配置。点击**后一页**。
3. 在如下页面上配置 PPPoE 接口：

d. 配置 PPPoE 拨号的用户名和密码，用于 PPPoE 拨号连接。

- **用户名**：拨号用户的名称，长度范围为 0-127 字节。由数字、字母和下列特殊字符组成：`~!@#$%^&*()_+-=[]{}\|;:”<>,./?，且必须以数字或字母开头。
- **密码**：拨号用户的密码，由 0 ～ 127 字节的 UTF-8 字符组成（空格除外）。

如果用户名和密码为空，表示 PPPoE 连接不需要认证。

e. 设置连接方式：

- **自动**（缺省）：自动检查 ISP 连接的通断情况。如连接断开，将自动重连。
- **按需拨号**：仅当有数据访问请求时开始拨号。

f. 设置 PPPoE 拨号连接的重拨次数、重拨间隔和空闲时间。

- **重播次数**：拨号连接最大尝试次数。取值范围是 0 ～ 999，0 表示没有重拨次数限制，默认值 0。
- **重拨间隔**：拨号连接的时间间隔。取值范围是 5 ～ 600 秒，默认值 60 秒。
- **空闲时间**：拨号的空闲时间，即在所设置的时间内没有数据传输时，将断开拨号连接。取值范围是 0 ～ 120 分钟， 0 表示不断开连接，默认值 0。该属性仅在按需拨号方式时生效。

g. 设置 PPPoE 接口的 IP 地址。

该属性仅在 IPv4 模式下生效。地址格式为 [1-223].[0-225].[0-225].[0-225]，不允许输入 127.0.0.0-127.255.255.255 和 192.168.255.254。如不设置，则将从 ISP 获取的 IP 地址作为本端 IP 地址。

h. 设置 AC 名称与服务名称。

- **AC 名称**：该名称通常是 ADSL Modem 的商标、型号或序列号。
- **服务名称**：该名称通常是 ISP 的名称或 ISP 提供的服务名称。

AC 名称和服务名称由 ISP 负责提供，一般不需要配置。名称为 0-127 字节的 UTF-8 字符 （空格和问号除外）。

i. 在**以太网接口**下拉框中选取 **eth1**。

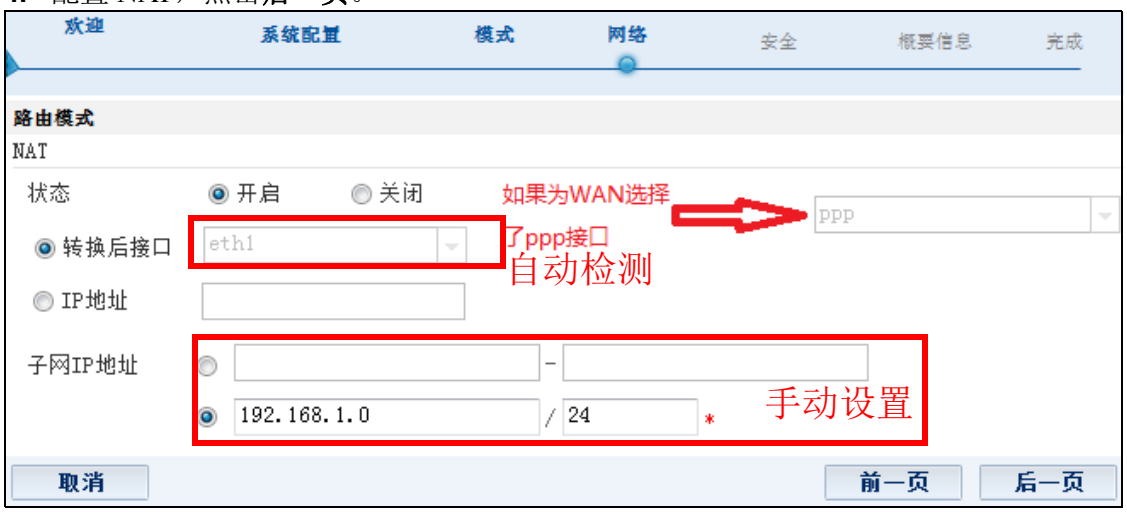
此接口必须是二层以太网接口或二层冗余接口。 PPPoE 接口默认绑定编号最小的以太网接口 （已经被 LAN 包含的以太网接口除外）。

j. 勾选最后两个复选框，从ISP获取的默认网关和DNS将作为系统默认网关和DNS。

- **覆盖默认网关**：进行 PPPoE 拨号后，默认网关将指向 PPPoE 接口。系统默认为禁用。
- **覆盖 DNS**：NISG（DNS 主机）上配置的 DNS 服务器信息将被从 ISP 获得的 DNS 信息所覆盖。该属性仅在 IPv4 模式下生效。系统默认为禁用。

1.2.4.2 网络 NAT 设置

4. 配置 NAT，点击**后一页**。



a. 开启 NAT，为内网提供安全保护。这里的 NAT 只转换到 Internet 的请求的源 IP。

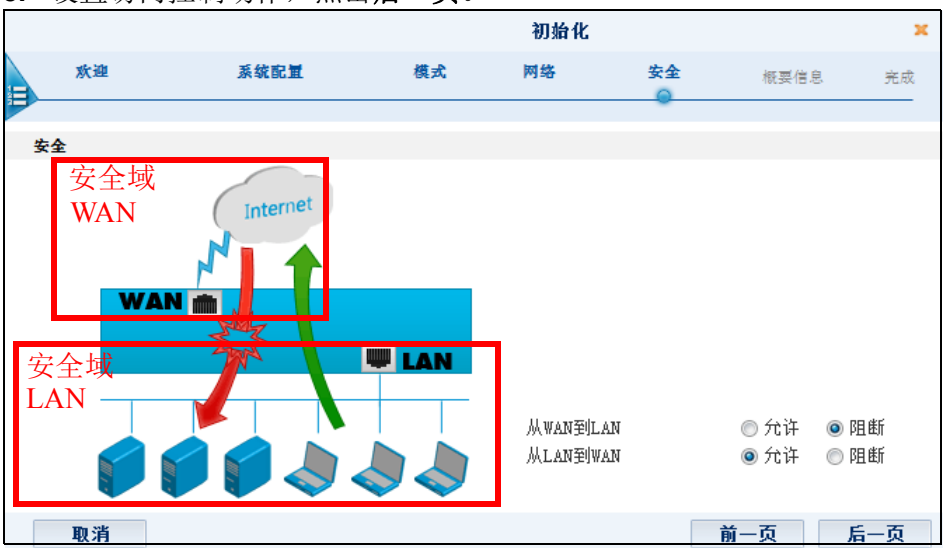
b. 选择转换方式：

- 点击**转换后接口**，系统自动选择管理员为 WAN 分配的接口（ethX 或 ppp）。数据包的源 IP 地址将被转换成指定接口的 IP 地址。
- 点击 **IP 地址**，输入转换后 IP 地址。数据包的源 IP 地址将被转换成指定 IP 地址。

c. 配置转换前子网 IP 地址。管理员可以选择配置转换 IP 地址段或子网 IP 地址。

1.2.4.3 安全设置

5. 设置访问控制动作，点击**后一页**。



1.2.4.4 确认和保存设置 （概要信息）

6. 确认配置信息，点击**结束**按钮。

7. 点击**关闭**退出初始化向导。

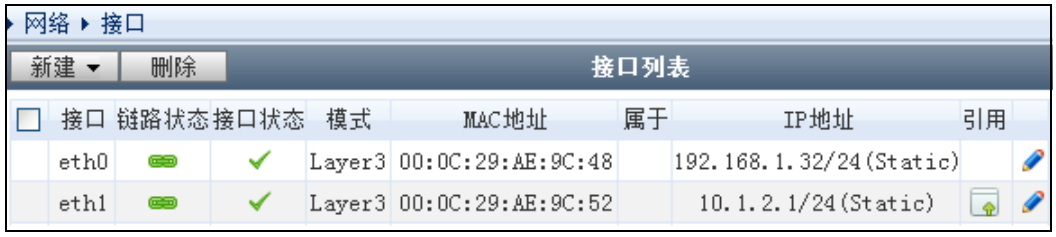
8. 系统自动跳转到登录页面。地址栏中的管理 IP 自动变为修改后的管理 IP。

1.2.4.5 通过 WebUI 确认初始化配置

要确认初始化配置是否生效，请执行以下操作：

1. 输入缺省用户名和密码进行登录。
2. 查看主页上方的主机名和系统时间，可以看到新的主机名和系统时间已生效。

3. 选择**网络 > 接口**查看接口配置。
   - 如果为 WAN 选择了 eth1：



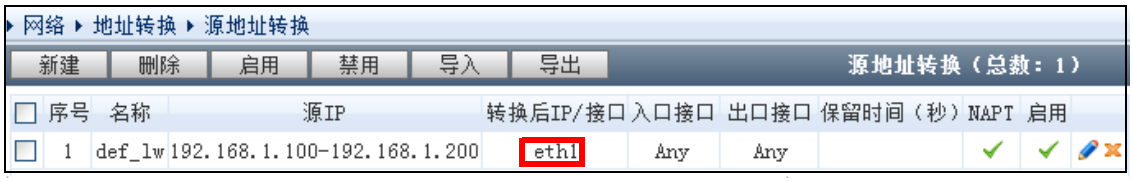
   - 如果为 WAN 选择了 **ppp**：

4. 选择**网络 > 安全域**查看新建的三层安全域 LAN 和 WAN 。
   - 如果为 WAN 选择了 eth1：

   - 如果为 WAN 选择了 **ppp**：

5. 选择**网络 > NAT > SNAT**，查看系统是否已按初始化配置创建了一条 SNAT 规则。

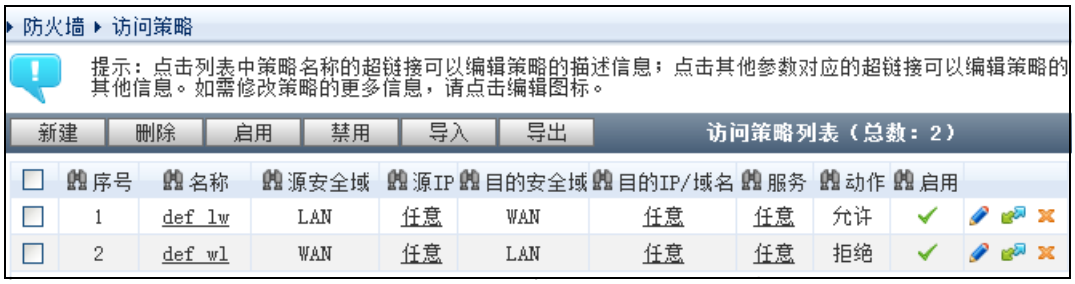
   - 如果为 WAN 选择了 eth1：



   - 如果为 WAN 选择了 **ppp**：

6. 选择**网络 > 路由 > 缺省路由**，查看缺省路由是否已按初始化配置修改。

7. 选择**防火墙 > 访问策略**，查看系统是否已创建了两条访问策略，允许 LAN 到 WAN 的访问，同时拒绝 WAN 到 LAN 的访问。



8. 选择**系统 > 服务配置 > 访问设置**，查看相关服务是否已经启用或禁用。用户应根据实际情况配置所需的服务。

9. 通过测试网络连通性验证初始化配置是否生效，步骤同透明模式。

1.2.5 重置密码

步骤同 WebUI。请参见 1.3.3 重置密码。

1.2.6 导入 License

步骤同 WebUI。请参见 1.3.7 导入 License。

1.3 使用 WebUI 进行初始化配置

- 1.3.1 登录
- 1.3.2 WebUI 概述
- 1.3.4 设置系统语言 / 主机名 / 系统时间
- 1.3.3 重置密码

选择配置以下任意一种工作模式：

- 1.3.5 配置透明模式
- 1.3.6 配置路由模式

要配置功能，需要导入有效的 License：

- 1.3.7 导入 License

1.3.1 登录

1. 通过 WebUI 向导登录，步骤同 1.2.1 登录。
2. 在**欢迎**页面选择**简体中文**，点击**跳过**，弹出如下 WebUI 页面：

1.3.2 WebUI 概述

WebUI 操作按钮如下表所示。

表 2 WebUI 操作按钮

按钮	描述	按钮	描述
	配置锁 （同一时间只能有一个管理用户拥有配置锁）		切换虚拟系统
	保存		编辑系统日期时间

表 2 WebUI 操作按钮 (*续*)

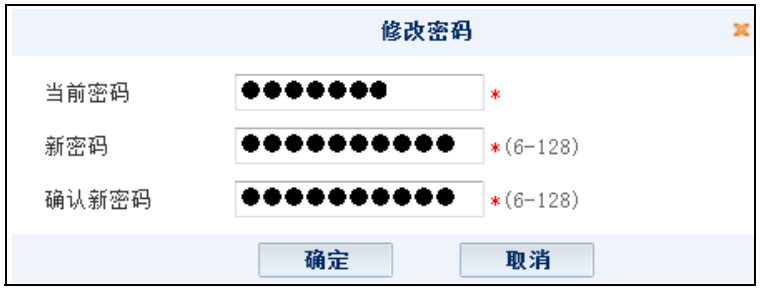
按钮	描述	按钮	描述
	在线帮助		被引用 （查看引用某条目的策略或防护配置）
	退出 （系统）		移动策略以改变其优先级
	刷新		克隆
	关闭 （或删除）		（条目）启用状态
	编辑		（条目）禁用状态
	删除		过滤条件被启用 （过滤条件用于设置要显示的参数项）
	恢复 （系统设置）		过滤条件被禁用
	查看		添加条目到列表框
	下载		从列表框删除条目
	导出		向上移动列表中的条目
	修改密码		向下移动列表中的条目

1.3.3 重置密码

要修改缺省登录密码，请执行以下操作：

1. 选择**系统 > 认证**。

2. 点击 修改密码。



3. 点击**确定**。新密码在下次登录时生效。

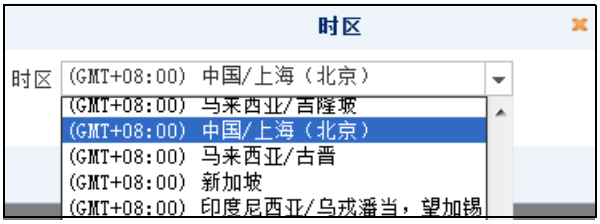
1.3.4 设置系统语言 / 主机名 / 系统时间

1. 选择**系统 > 概述**。

2. 点击**主机名**对应的按钮，修改主机名。

3. 点击**确定**。
4. 点击**语言**对应的按钮。

5. 选择一种语言，点击**确定**。
6. 点击**时区**和**当前时间**对应的按钮。



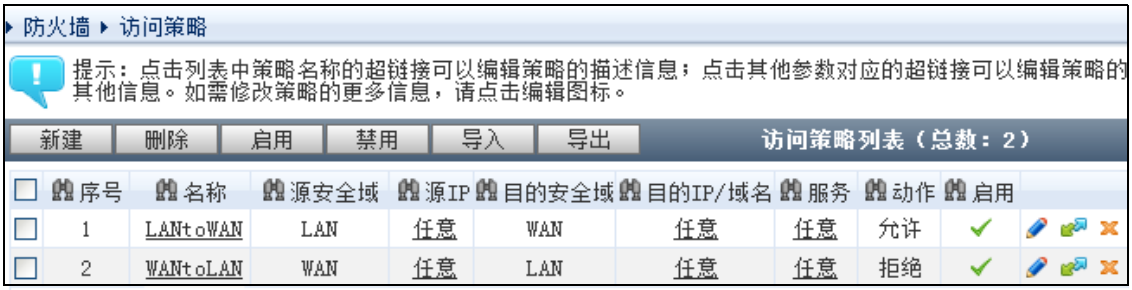
7. 编辑系统时间，点击**确定**。点击。

1.3.5 配置透明模式

1. 选择**网络 > 接口**。设置接口如下：

2. 选择**网络 > 安全域**，创建二层安全域 LAN 和 WAN。添加 eth0 到 LAN，添加 eth1 到 WAN。

3. 选择**防火墙 > 访问策略**，创建如下访问策略：



4. 点击 。

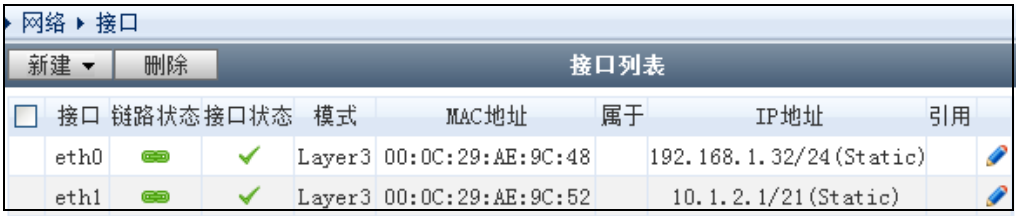
5. 验证以上初始化配置，步骤同 1.2.3.2 通过 WebUI 确认初始化配置。

1.3.6 配置路由模式

- 1.3.6.1 以太网连接
- 1.3.6.2 PPPoE 连接

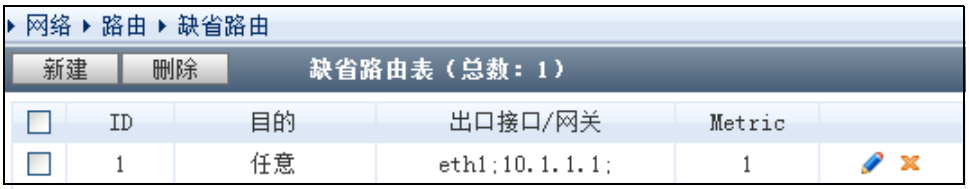
1.3.6.1 以太网连接

1. 选择**网络 > 接口**。设置接口如下：

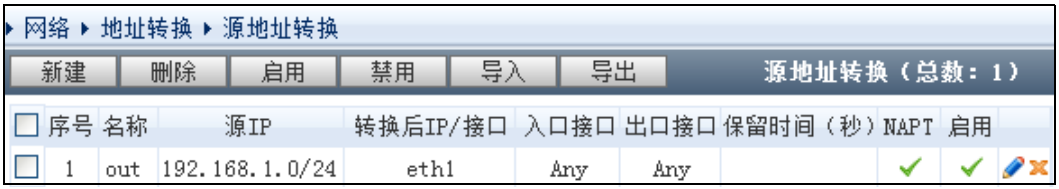


2. 创建三层安全域 LAN 和 WAN。添加 eth0 到 LAN，添加 eth1 到 WAN。

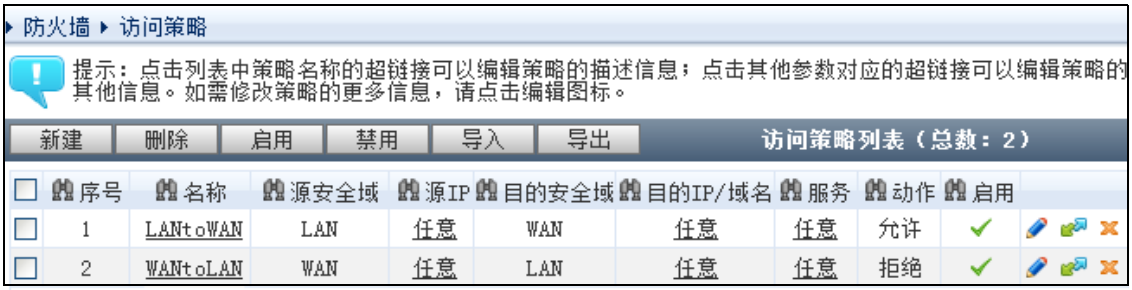
3. 修改缺省网关为 10.1.1.1。



4. 创建 SNAT 规则，将 192.168.1.0/24 转换成 eth1 的 IP 地址：



5. 创建访问策略，允许 LAN 到 WAN 的访问，拒绝 WAN 到 LAN 的访问。



6. 点击 。

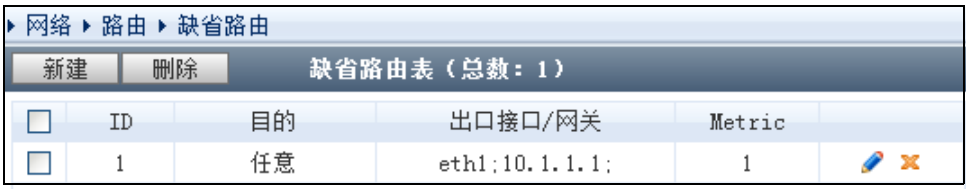
7. 验证以上初始化配置，步骤同 1.2.4.5 通过 WebUI 确认初始化配置。

1.3.6.2 PPPoE 连接

1. 选择**网络 > 接口**。设置接口如下：

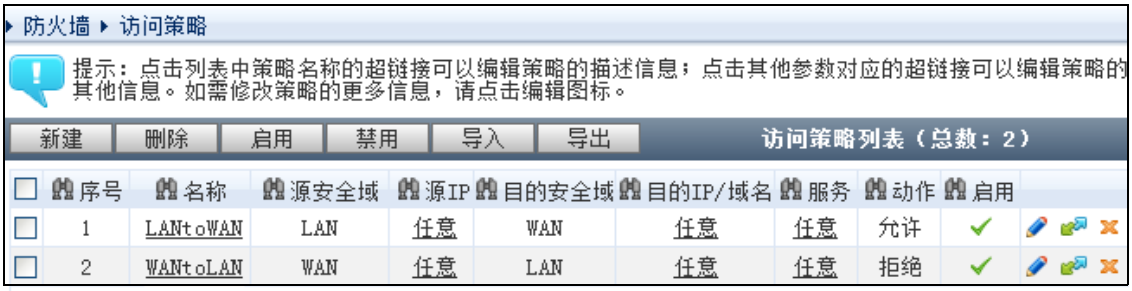
2. 创建三层安全域 LAN 和 WAN，添加 eth0 到 LAN，添加 ppp0 到 WAN。

3. 修改缺省网关为 10.1.1.1。



4. 创建 SNAT 规则，将 192.168.1.0/24 转换为 ppp0 的 IP 地址。

5. 创建访问策略，允许 LAN 到 WAN 的访问，拒绝 WAN 到 LAN 的访问。



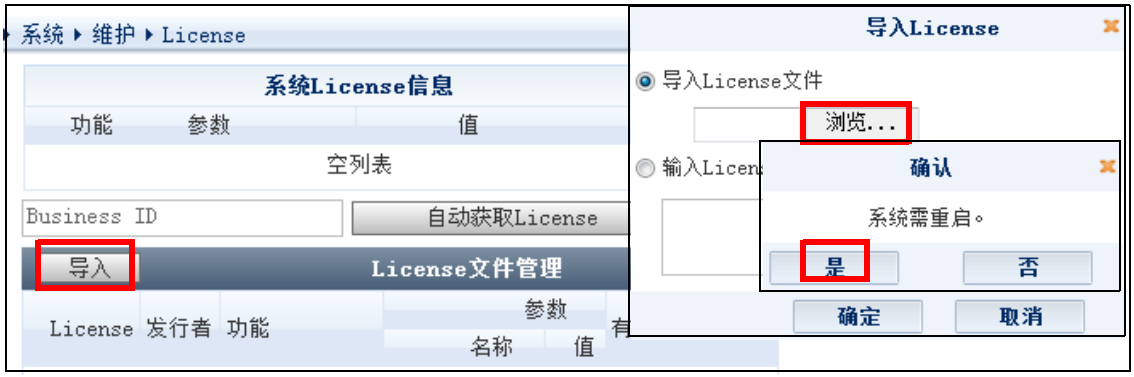
6. 点击 。

7. 验证以上初始化配置，步骤同 1.2.4.5 通过 WebUI 确认初始化配置。

1.3.7 导入 License

在进行以下步骤之前，请确认您已将有效 License 文件存放到本地 PC。

1. 选择**系统 > 维护 >License**。点击**导入**，上载 License 文件。系统提示重启，点击**是**。



提示：您也可以点击**自动获取 License** 按钮在线激活 License，但前提是您的 NISG 设备与 License 服务器之间是互通的。

2. 系统重启后自动跳转到登录页面，您可以登录后通过 WebUI 继续配置 NISG。

1.4 使用 CLI 进行初始化配置

- 1.4.1 CLI 基本信息
- 1.4.2 设置系统语言 / 主机名 / 系统时间
- 1.4.3 重置密码
- 1.4.4 配置透明模式
- 1.4.5 配置路由模式
- 1.4.6 导入 License
- 1.4.7 使用 SSH 登录
- 1.4.8 使用 Telnet 登录

1.4.1 CLI 基本信息

用户初次登录 NISG，可以通过 Console 控制台或 SSH 连接运行 CLI。下例表明如何使用 CLI 为以太网接口配置 IP 地址：

```
NetEye@root> configure mode override
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] ip address 192.168.1.32 255.255.255.0
NetEye@root-system-vlan1] end
NetEye@root> save config
NetEye@root> _
```

首次登录 CLI 会出现如下提示符：

NetEye@root>

在此提示符下可输入以下命令：

- **show 命令**：用于查看系统配置信息，如 **show system info**、 **show interface brief**、 **show service** 和 **show route**。
- 简单操作命令，如 **clear**、 **halt**、 **debug** 和 **save config**。
- **configure mode override**（如上面的范例所示）：如果输入此命令，其他管理员将不能继续配置 NISG，除非他们重新抢占配置锁，不过他们已经提交的修改不会丢失。执行此命令后，系统提示如下提示符：**NetEye@root-system]**。您可以在此命令符下输入下表中的命令进入相应的配置模式。

命令	配置项	提示符
vlan *vlan_id*	VLAN 接口	NetEye@root-system-vlan1]
interface ethernet *interface_id*	以太网接口	NetEye@root-system-if-eth1]
channel *channel_id*	以太网通道接口	NetEye@root-system-if-ch1]
tunnel *tunnel_id*	VPN 隧道接口	NetEye@root-system-tunnel1]
rint *rint_id*	冗余接口	NetEye@root-system-rint1]
veth *veth_id*	虚拟接口	NetEye@root-system-veth1]
loopback *lo_id*	回环接口	NetEye@root-system-lo1]
pppoe *pppoe_id*	PPPoE 接口	NetEye@root-system-pppoe1]
cluster	集群	NetEye@root-system-cluster]
virtual router *vrid*	虚拟路由器	NetEye@root-system-vr1]
detection group *group_id*	虚拟路由器探测组	NetEye@root-system-dg1]
policy route *policy_name*	基于策略的路由	NetEye@root-system-routepolicy-test]
vpn	VPN	NetEye@root-system-vpn]

命令	配置项	提示符
sslvpn	SSL VPN	NetEye@root-system-sslvpn]
vsys *vsys _id*	虚拟系统	NetEye@root-system-vsys1]
vnet *vnet_id*	虚拟网络	NetEye@root-system-vnet1]

输入以上任意一种命令，您可以对相应的配置项进行配置，如接口、集群 / 虚拟路由器、 VPN、 Vsys 等。在上面的例子中，你可以用 **ip address** 为接口配置 IP 地址。

CLI 支持：

- 在关键字或参数后输入 "**?**"，系统会提示该关键字或参数的帮助信息。
- 在关键字或参数后面加空格，然后再输入 "**?**"，系统会提示下一个关键字或参数。
- 可以通过按 Tab 键，补齐当前输入的关键字。如果有多个可选关键字，按 Tab 键则显示所有关键字。
- 支持缩写。例如，可以将命令 **configure mode** 缩写为 **con mo**。

1.4.2 设置系统语言 / 主机名 / 系统时间

1. 使用 **show system info** 命令查看系统信息：

```
Username:Neusoft
Password:
NetEye@root> show system info

Product Name:            Neusoft NISG
Model:                   VA
Software Name:           Neusoft NetEye Integrated Security Gateway
Build:                   BUILD900100
Release Time:            2014-06-05 19:18:12
Software Version:        4.2
Installation type:       disk-less
Serial Number:           f86eab44f3724f88927d7AEB3C1FF1FB
Current Time:            2014-01-22 00:30:37
System Uptime:           0 days 23 hours 21 mins
Memory:                  2048 MB
Basic MAC1:              7A:EB:3C:1F:F1:FB
Basic MAC2:              2E:B0:48:7F:5B:E2
```

2. 设置系统基本配置信息：

```
NetEye@root> configure mode override
NetEye@root-system] language Chinese
NetEye@root-system] hostname FW1
FW1@root-system] time 2014-03-20 14:04:00
FW1@root-system] end
FW1@root> save config
FW1@root>
```

1.4.3 重置密码

通过以下命令重置缺省登录密码：

1. 输入 **configure mode override** 命令，按 Enter 键。
2. 执行 **password simple** 命令。
3. 输入旧密码。
4. 输入新密码。
5. 重复新密码。

```
FW1@root> configure mode override
FW1@root-system] password simple
Old password(6-128):
Password(6-128):
Repeat Password(6-128):
FW1@root-system] _
```

1.4.4 配置透明模式

1. 配置 NISG 工作在透明模式：

```
FW1@root-system] interface ethernet 0
FW1@root-system-if-eth0] working-type layer2-interface
FW1@root-system-if-eth0] exit
FW1@root-system] vlan 1
FW1@root-system-vlan1] hold ethernet 0
FW1@root-system-vlan1] hold ethernet 1
FW1@root-system-vlan1] ip address 192.168.1.32 255.255.255.0
FW1@root-system-vlan1] exit
FW1@root-system] zone LAN
FW1@root-system] zone WAN
FW1@root-system] zone LAN based-layer2 vlan 1 eth0
FW1@root-system] zone WAN based-layer2 vlan 1 eth1
FW1@root-system] policy access LANtoWAN LAN any WAN any any any permit enable
FW1@root-system] policy access WANtoLAN WAN any LAN any any any deny enable
FW1@root-system] end
FW1@root> save config
FW1@root>
```

2. 查看接口配置信息：

```
FW1@root>
FW1@root> show interface brief
Name       Active     IP Address                      MAC               Held In
terfaces      MTU  Vsys
eth0       on         192.168.1.32/24(Static)         00:01:69:01:7F:30

              1500 root


Name       Active     Status     Mode           Vlan List

eth0       on         up         Layer3

eth1       on         up         Layer3

eth2       on         down       Layer2 Access
```

3. 查看安全域信息：

```
FW1@root> show zone
Name               Refcount  Policy                                  Descriptio
n
LAN                2         Access Policies
WAN                2         Access Policies
FW1@root> _
```

4. 查看访问策略：

```
FW1@root> show policy access
Number Name                From      To        Source ip       Destination ip
Source users Services      Action State  Tunnel
1      LANtoWAN             LAN       WAN       Any Ip          Any Ip
any user     any           permit enable
2      WANtoLAN             WAN       LAN       Any Ip          Any Ip
any user     any           deny   enable
FW1@root> _
```

5. 查看路由 （网关）：

```
FW1@root> show route

Routing table:
Type   Destination        Interface Gateway         Metric Weight Lb  IP-Track
C      192.168.1.0/24     vlan1                     0              No

Static default                        192.168.1.1     1              No


connected          1
Total              2


Routing IPv6 table:
Type   Destination                                  Interface Gateway       Met
ric Weight Lb  IP-Track

connected          0
Total              0

FW1@root> _
```

6. 查看服务设置：

```
FW1@root> show service
Telnet service:
  Allow Access: No
  Access:
Ssh service:
  Allow Access: Yes
  Access:
    allow any           0.0.0.0-255.255.255.255
Web service:
  Allow Access: Yes
  Access:
    allow any           0.0.0.0-255.255.255.255
Ping service:
  Allow Access: Yes
  Access:
    allow any           0.0.0.0-255.255.255.255
FW1@root>
```

7. 验证以上配置是否生效，步骤同 1.2.3.2 通过 WebUI 确认初始化配置。

1.4.5 配置路由模式

- 1.4.5.1 以太网连接
- 1.4.5.2 PPPoE 连接

1.4.5.1 以太网连接

1. 设置 NISG 工作在路由模式并通过以太网接口访问 Internet：

```
FW1@root-system] interface ethernet 1
FW1@root-system-if-eth1] working-type layer3-interface
FW1@root-system-if-eth1] ip address 10.2.1.100 255.255.255.0
FW1@root-system-if-eth1] exit
FW1@root-system] zone LAN
FW1@root-system] zone WAN
FW1@root-system] zone LAN based-layer3 eth0
FW1@root-system] zone WAN based-layer3 eth1
FW1@root-system] route default gateway 10.2.1.1 interface eth1
FW1@root-system] policy access LANtoWAN LAN any WAN any any any permit enable
FW1@root-system] policy access WANtoLAN WAN any LAN any any any deny enable
FW1@root-system] policy snat out netmask 192.168.1.0 255.255.255.0 interface eth1

 napt enable
FW1@root-system] end
FW1@root> save config
FW1@root>
```

2. 查看接口信息：

```
FW1@root> show interface brief
Name       Active     IP Address                      MAC               Held In
terfaces      MTU  Vsys
eth0       on         192.168.1.32/24(Static)         00:0C:29:85:BE:06
           1500 root
eth1       on         10.1.2.1/21(Static)             00:0C:29:85:BE:10
           1500 root

Name       Active     Status      Mode       Vlan List

eth0       on         up          Layer3

eth1       on         up          Layer3
```

3. 查看安全域信息：

```
FW1@root> show zone
Name              Refcount  Policy                                  Descriptio
n
LAN               2         Access Policies
WAN               2         Access Policies
FW1@root> _
```

4. 查看路由（网关）：

```
FW1@root> show route

Routing table:
Type   Destination        Interface Gateway         Metric Weight Lb  IP-Track
C      10.1.0.0/21        eth1                      0             No

C      192.168.1.0/24     eth0                      0             No

Static default                          192.168.1.1  1             No

Static default            eth1          10.1.1.1     1             No


connected          2
Total              4
```

5. 查看访问策略：

```
FW1@root> show policy access
Number Name                 From      To        Source ip       Destination ip
Source users Services      Action State  Tunnel
1      LANtoWAN             LAN       WAN       Any Ip          Any Ip
any user     any           permit enable
2      WANtoLAN             WAN       LAN       Any Ip          Any Ip
any user     any           deny   enable
FW1@root> _
```

6. 查看 SNAT 规则：

```
FW1@root> show policy snat

Num   Policy-Name          In-Interface Out-Interface Before-Trans      After-T
rans          Napt  State
1     out                  Any          Any           192.168.1.0/24    eth1
              True  Enable

FW1@root> _
```

7. 查看服务设置：

```
FW1@root> show service
Telnet service:
  Allow Access: No
  Access:
Ssh service:
  Allow Access: Yes
  Access:
    allow any          0.0.0.0-255.255.255.255
Web service:
  Allow Access: Yes
  Access:
    allow any          0.0.0.0-255.255.255.255
Ping service:
  Allow Access: Yes
  Access:
    allow any          0.0.0.0-255.255.255.255
```

8. 验证以上配置是否生效，步骤同 1.2.4.5 通过 WebUI 确认初始化配置。

1.4.5.2 PPPoE 连接

1. 设置 NISG 工作在路由模式并通过 PPPoE 接口访问 Internet：

```
FW1@root-system] pppoe 0
FW1@root-system-pppoe0] hold ethernet 1
FW1@root-system-pppoe0] username test password neteye
FW1@root-system-pppoe0] active on
FW1@root-system-pppoe0] exit
FW1@root-system] zone LAN
FW1@root-system] zone WAN
FW1@root-system] zone LAN based-layer3 eth0
FW1@root-system] zone WAN based-layer3 ppp0
FW1@root-system] route default gateway 10.1.2.1 interface ppp0
FW1@root-system] policy access LANtoWAN LAN any WAN any any any permit enable
FW1@root-system] policy access WANtoLAN WAN any LAN any any any deny enable
FW1@root-system] policy snat out netmask 192.168.1.0 255.255.255.0 interface ppp0

 napt enable
FW1@root-system] end
FW1@root> save config
```

2. 查看接口信息：

```
FW1@root> show interface brief
Name       Active     IP Address                    MAC               Held In
terfaces      MTU  Vsys
eth0       on         192.168.1.32/24(Static)       00:0C:29:3E:50:37
              1500 root


Name       Active     IP Address                    MAC               Held In
terfaces      MTU  Vsys
ppp0       on         10.1.2.1                      -                 eth1
              1454 root


Name       Active     Status     Mode            Vlan List

eth0       on         up         Layer3

eth1       on         up         Layer2 Access
```

3. 查看安全域信息：

```
FW1@root> show zone
Name              Refcount  Policy                              Descriptio
n
LAN               2         Access Policies
WAN               2         Access Policies
FW1@root> _
```

4. 查看路由 （网关）：

```
FW1@root> show route

Routing table:
Type   Destination        Interface Gateway         Metric Weight Lb  IP-Track
C       10.1.2.1/32       ppp0                      0             No

C      192.168.1.0/24     eth0                      0             No

Static default                        192.168.1.1    1             No


connected          2
Total              3
```

5. 查看访问策略：

```
FW1@root> show policy access
Number Name                 From      To        Source ip       Destination ip
Source users Services      Action State  Tunnel
1      LANtoWAN             LAN       WAN       Any Ip          Any Ip
any user     any           permit enable
2      WANtoLAN             WAN       LAN       Any Ip          Any Ip
any user     any           deny   enable
FW1@root> _
```

6. 查看 SNAT 规则：

```
FW1@root> show policy snat

Num   Policy-Name         In-Interface Out-Interface Before-Trans        After-T
rans         Napt  State
1     out                 Any          Any           192.168.1.0/24      ppp0
             True  Enable

FW1@root> _
```

7. 查看服务设置：

```
FW1@root> show service
Telnet service:
  Allow Access: No
  Access:
Ssh service:
  Allow Access: Yes
  Access:
    allow any           0.0.0.0-255.255.255.255
Web service:
  Allow Access: Yes
  Access:
    allow any           0.0.0.0-255.255.255.255
Ping service:
  Allow Access: Yes
  Access:
    allow any           0.0.0.0-255.255.255.255
FW1@root>
```

8. 验证以上配置是否生效，步骤同 1.2.4.5 通过 WebUI 确认初始化配置。

1.4.6 导入 License

1. 从 TFTP 服务器上载 License 文件。
2. 使用 **license import** 命令导入 License，根据提示输入 **y** 重启系统：

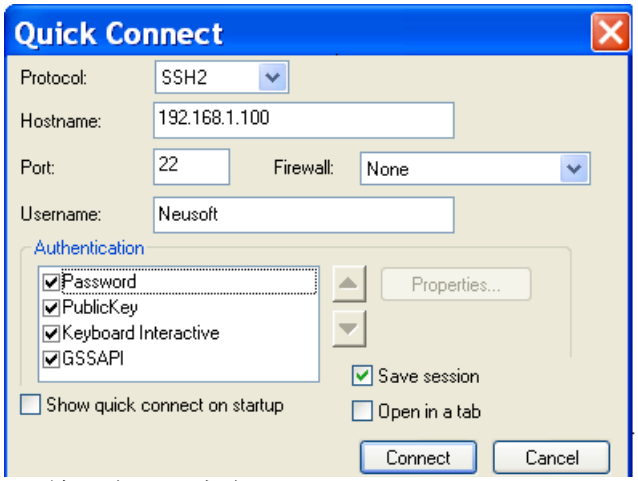
```
FW1@root-system] license import from tftp 192.168.1.200 FW1.dat

License upload succeeded. System needs to reboot.
Continue? (y/n)y
```

如果重启系统前不保存配置，所有配置将在重启系统后丢失。

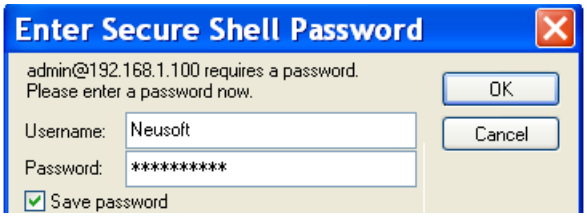
3. 重启后重新登录，并继续通过 CLI Console 配置 NISG。

1.4.7 使用 SSH 登录

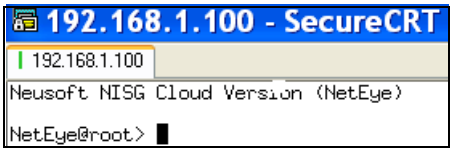
1. 打开 SecureCRT，点击 **Quick Connect**。在 **Hostname** 文本框中输入 NISG 的管理 IP 地址，在 **Username** 文本框中输入缺省用户名。点击 **Connect**。



2. 输入密码，点击 **OK**。



3. 登录后配置 NISG，配置方式同使用 CLI Console。



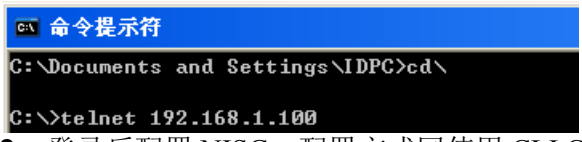
1.4.8 使用 Telnet 登录

Telnet 服务默认是关闭的。

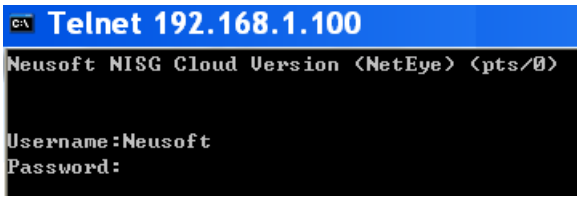
1. 使用 Telnet 连接之前，需要先通过 CLI Console 启用 Telnet 服务：

```
NetEye@root> configure mode override
NetEye@root-system1 service telnet on
NetEye@root-system1 service telnet allow zone any 0.0.0.0 255.255.255.255
```

2. 通过 Telnet 命令远程登录 NISG：



3. 登录后配置 NISG，配置方式同使用 CLI Console。



2 功能概述

本节概要介绍 NISG 的功能特性：

系统 / 网络基本配置

- 2.1. 系统配置：设置系统时间、本地访问控制、 License、用户和认证、证书、系统升级、备份和恢复、系统诊断、技术支持、集中管理、日志以及报警设置等系统基本信息。
- 2.2. 网络配置：配置接口、 ARP/CAM、 STP、安全域、 DNS、 DHCP 以及 IPv6（DHCPv6 和邻居发现）等功能。

路由 / 安全配置

- 2.3. 数据包处理流程：给出了数据包的处理流程图，简要描述了路由、地址转换、防火墙策略、攻击防御和 UTM 是如何处理数据包的。
- 2.4. 路由：关于数据包转发的路由和多播特性，包括静态路由、基于策略的路由、多播路由、 DVMRP、 IGMP Snooping 等。
- 2.5. 地址转换 （NAT）：包括源地址转换 （SNAT）、目的地址转换 （DNAT）和地址映射 （MIP）。
- 2.6. 服务质量 （QoS）：为指定网络提供更优服务 （流量控制）。
- 2.7. 防火墙策略：控制流量转发，包括访问策略、缺省策略设置、多播策略、会话策略以及 IP-MAC 绑定。
- 2.8. 攻击防御：防御常见的网络攻击。
- 2.9. 统一威胁管理 （UTM）：提供高级安全防护功能。
  - 出口控制：2.9.1. 应用控制， 2.9.2.HTTP 控制， 2.9.3.DNS 控制
  - 2.9.4. 客户端防护
  - 2.9.5. 服务器防护

虚拟专用网，高可用性，虚拟系统 / 虚拟网络

- 2.10. 虚拟专用网 （VPN）：包括 IPSec VPN、 SSL VPN (Web 入口页面 / 隧道）。
- 2.11. 高可用性 （HA）：通过虚拟路由器、虚拟路由器探测组和集群提供设备冗余和备份。
- 2.12. 虚拟系统 / 网络（Vsys/Vnet）：将根系统划分为多个虚拟系统，每个虚拟系统允许配置独立的管理员、策略和其他功能，大大降低了管理和硬件成本。虚拟网络使得虚拟系统之间可以通讯。

监控，日志和报表

- 2.13. 监控 / 日志：监控系统运行信息、提供日志查询。
- 2.14. 报表：基于 WebUI 的报表功能简单易用。可通过设定报表计划生成有关以下信息的报表：系统、流量、 Web 安全、 Mail 安全、防病毒、攻击、应用以及用户的统计信息。

2.1. 系统配置

下表给出了系统配置相关的 WebUI 菜单路径、简短描述以及到相关手册章节的链接。

表 1 系统配置步骤

	WebUI 菜单路径	描述信息	手册章节
系统基本信息			
1.	主页或 **系统 > 概述 > 系统信息**	查看系统概要信息参数。	3.1 WebUI 主页和 3.2 系统概述
2.	**系统 >** **服务配置 > 标题信息**	设置系统标题信息。	3.3 标题信息
3.	**系统 >** **资产信息 >** **资产汇总 , 版权信息**	查看系统资产和版权信息。	3.4 资产汇总和 3.5 版权信息
4.	**系统 >** **维护 > 日期时间**	设置系统日期、时间。	3.6 系统时间
License 和系统升级			
5.	**系统 >** **维护 > License**	License 概要信息，支持自动和手动激活。	3.7 License
6.	**系统 >** **系统升级 >** **安装升级包 , 管理安装升级包 ,** **管理增强升级包**	手动或自动加载升级包，包括安装包和增量升级包。	3.8 系统升级， 3.9 安装升级包管理和 3.10 增强升级包管理
访问设置			
7.	**系统 >** **服务配置 >** **访问设置 ,SNMP 配置**	设置对 Telnet、SSH、Web、Ping 和 root 用户的访问控制。配置 SNMP。	3.11 访问服务和 3.12 SNMP
授权和认证			
8.	**系统 >** **认证 >** **管理用户 , 网络用户**	管理用户的登录方式包括 Telnet、 SSH 和 Web。网络用户的类型包括 WebAuth、IPSec VPN 和 SSL VPN。	3.13 管理用户和 3.14 网络用户
9.	**系统 >** **认证配置 , 认证服务器 ,WebAuth 配置**	网络用户认证。	3.15 用户认证和 3.16 WebAuth 配置
系统维护			
10.	**系统 >** **维护 > 备份 / 恢复**	备份整机或根系统配置到备份文件，从备份文件恢复系统配置。	3.17 备份恢复
11.	**系统 >** **维护 > 技术支持**	生成系统诊断文件。	3.18 技术支持
12.	**系统 >** **维护 > 集中管理**	配置是否允许被集中管理系统管理。	3.19 集中管理
13.	**系统 >** **日志配置 >** **报警配置 , 日志维护**	配置本地日志、 Syslog、 SNMP 和 Email 报警策略，下载日志文件。	3.21 报警配置和 3.22 日志维护
供系统全局使用的配置			
14.	**系统 >** **证书 > 本地证书 ,CA 证书**	导入和管理 CA 和本地证书，用于用户认证和 VPN 隧道协商。	3.23 证书
15.	**系统 >** **对象 >IP 地址 , 服务**	为策略和规则添加 IP 和服务对象。	3.24 对象

2.2. 网络配置

下表给出了网络配置相关的 WebUI 菜单路径、简短描述以及到相关手册章节的链接。

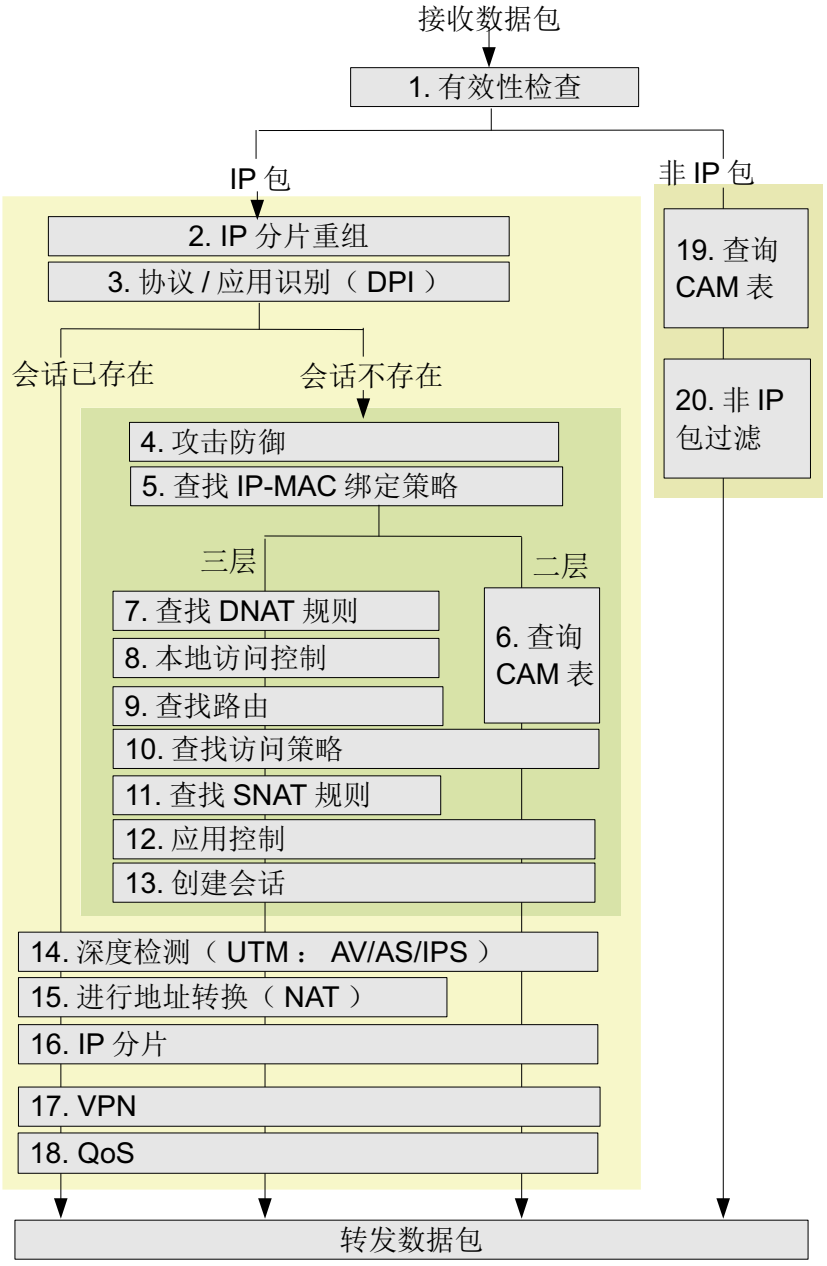
表 2 网络配置步骤

	WebUI 菜单路径	描述信息	手册章节
接口			
1.	**网络 > 接口**	允许流量流入、流出安全设备的接口。	4.1 接口概述， 4.2 以太网接口到 4.9 隧道接口
ARP 和 CAM			
2.	（无）	通过命令行配置 ARP 和 CAM 表。	4.10 ARP 和 4.11 CAM
安全域			
3.	**网络 > 安全域**	安全域是接口的集合，每个安全域连接到独立的网段。将接口绑定在一起使得 NISG 可以对一个逻辑网络进行统一的安全控制。	4.12 安全域
DNS 和 DHCP			
4.	**网络 > DNS > 主机 DNS 代理 静态缓存**	配置 NISG 作为 DNS 主机或代理工作时使用的 DNS 服务器，为 NISG 配置 DNS 静态缓存。支持 DNSv6。	4.13 DNS 主机、 4.14 DNS 代理和 4.15 DNS 缓存
5.	**网络 > DHCP > DHCP 服务器 DHCP 作用域**	设置 NISG 的 DHCP 工作模式，包括 DHCP 服务器、中继代理和客户端。工作模式为 DHCP 服务器时需要设置 DHCP 作用域。	4.16 DHCP 服务器和 4.17 DHCP 作用域
6.	**网络 > IPv6 > DHCPv6**	包括有状态 DHCPv6 （为主机分配 IPv6 前缀）和无状态 DHCPv6 （为主机分配域名和服务器地址）。	4.18 DHCPv6
STP 和邻居发现			
7.	**网络 > STP**	生成树协议 （STP）在提供路径冗余的同时可以避免二层网络环路。	4.19 STP
8.	**网络 > IPv6 > 邻居发现配置**	邻居发现 （ND）协议用于发现相同链路上的相邻节点 （主机或路由器）。	4.20 邻居发现

2.3. 数据包处理流程

数据包在 NISG 中的处理流程如下图所示。图中标注的编号在下一页会有更加详细的解释。

图 1 数据包处理流程



下表给出了上图中各个步骤的描述信息。# 表示图中标识的编号，“ 参考章节 ” 指出了可以查找更详细信息的手册章节。

表 3 数据包处理流程

#	IP	会话	2/3 层	NISG 处理数据包的功能	本章节	其他章节
1.				**有效性检查**。在数据包进入接口后， NISG 对数据包的合法性进行检查，即对数据包信息中的常规性错误进行检查，如：IP 地址全零、 MAC 地址全零等。（无需用户配置）	---	---
2.	IP			**IP 分片重组**。接收完数据包所有分片后， NISG 会对数据包进行重组。	---	---
3.	IP			**协议 / 应用识别 （DPI）**。 NISG 首先识别数据包使用的协议或应用，然后发送相关引擎进行检查。	---	---
4.	IP	No		运行**攻击防御**。检查 DoS、 Reconnaissance、 ICMP 等攻击，进行 IP 选项校验和 TCP 逃避控制。	2.8. 攻击防御	9.3. 基本配置步骤
5.	IP	No		匹配 **IP-MAC 地址绑定**策略，防止 IP 欺骗或地址伪装。	2.8. 攻击防御	9.3. 基本配置步骤
6.	IP	No	2	根据数据包的目的 IP 地址**查询 CAM 表**，将数据包通过对应的出口接口转发给目的 IP。然后跳转到步骤 9、11、 12、 13、 15、 16、 17。	2.2. 网络配置	4.11 CAM
7.	IP	No	3	查找目的地址转换 （**DNAT**）规则。	2.5. 地址转换 （NAT）	6.2.2 创建 DNAT 规则
8.	IP	No	3	进行**本地访问控制** （如访问设置、网关设置等）。	2.1. 系统配置	3.11 访问服务
9.	IP	No	3	**查询路由表**，查找到达目的地址的路由。	2.4. 路由	5.2. 基本配置步骤
10.	IP	No		**查找访问策略**，进行 IP 包过滤检测。	2.7. 防火墙策略	8.2.2 创建访问策略
11.	IP	No	3	查找源地址转换 （**SNAT**）规则。	2.5. 地址转换 （NAT）	6.2.1 创建 SNAT 规则
12.	IP	No		对应用层数据包进行**应用控制**。	2.9. 统一威胁管理 （UTM）	10.2. 基本配置步骤
13.	IP	No		**创建会话**。保存会话信息到会话表，转发会话请求。	---	---
14.	IP			进行**深度内容检测**，如 UTM 防病毒 （AV）、反垃圾邮件 （AS）、攻击签名检测 （IPS）等。	2.9. 统一威胁管理 （UTM）	10.2. 基本配置步骤
15.	IP		3	进行地址转换 （**NAT**）。	2.5. 地址转换 （NAT）	6.1 地址转换概述
16.	IP			进行 **IP 分片**。	---	---
17.	IP			**VPN**，封装数据包并引入 VPN 隧道。	2.10. 虚拟专用网 （VPN）	11.2 基本配置
18.	IP			**QoS**，对数据流量进行带宽控制。	2.6. 服务质量 （QoS）	7.2. 基本配置步骤
19.	Non-IP			根据数据包的目的 IP 地址**查询 CAM 表**，将数据包通过对应的出口接口转发给目的 IP。	2.2. 网络配置	4.11 CAM
20.	Non-IP			匹配**非 IP 包过滤**策略 （默认启用、动作为允许，无需用户配置）。	---	---

2.4. 路由

下面介绍了路由和交换的基本概念：

- 2.4.1. 三层单播路由 （缺省路由和策略路由）
- 2.4.2. 三层多播 （多播和 DVMRP）
- 2.4.3. 二层多播 （IGMP Snooping）

2.4.1. 三层单播路由 （缺省路由和策略路由）

三层单播路由基于以下内容转发数据包：

- （入口）匹配策略 （指定了数据包源相关参数）
- （出口）匹配策略中的匹配路由 （指定了数据包目的相关参数）

下表对 （1）策略和 （2）路由进行了总结。

1. 策略表格中包含了多条非默认策略和一条默认策略。

   （1a）非默认策略定义了单播数据包的源：

   - 接口 （1 个或所有）
   - IP 地址
   - TOS
   - 服务

   （1b）默认策略中定义参数均为任意。（当数据包未匹配到任何非默认策略的路由时匹配该条默认策略。）

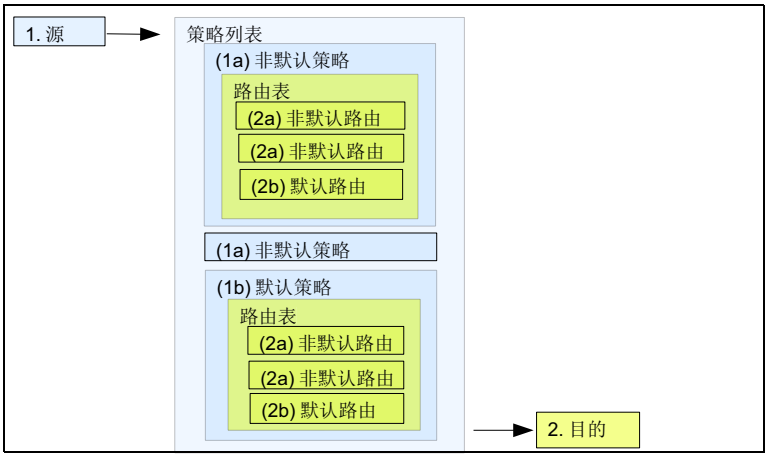
2. 策略路由表包含了多条非默认路由条目和一条默认路由条目。（每条策略都对应一个路由表）

   （2a）非默认路由定义了：

   - 单播数据包的目的 IP 地址。
   - 出口接口 （和网关）。如果启动了负载均衡，则定义多个出口接口 / 网关以及权重和探测相关参数。

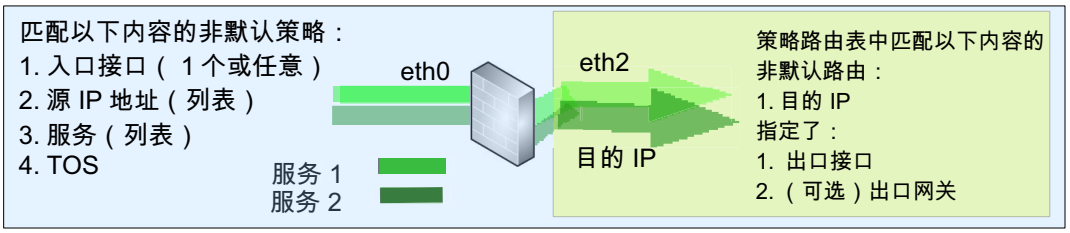
   （2b）默认路由定义了：

   - 出口接口 （和网关）。如果启动了负载均衡，则定义多个出口接口 / 网关以及权重和探测相关参数。

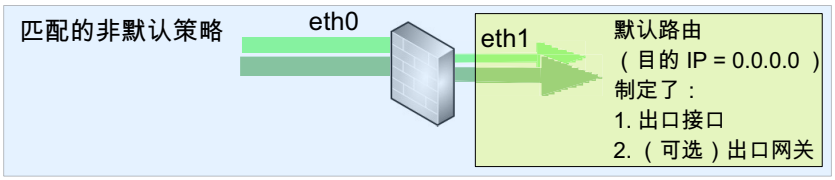


下面列出了策略和路由的几种组合：

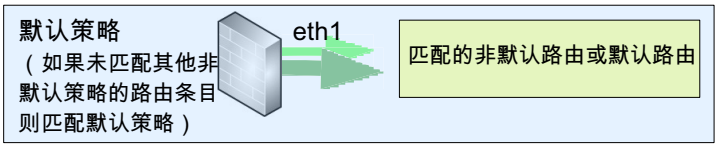
- （1a）非默认策略 + （2a）非默认路由：



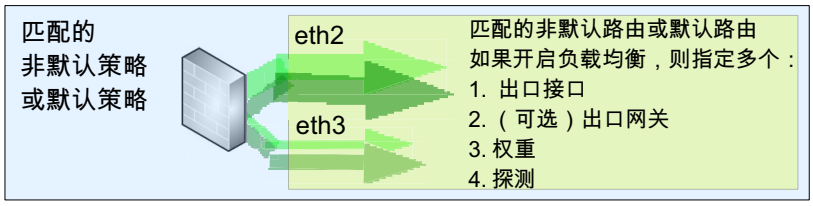
- （1a）非默认策略 + （2b）默认路由：



- （1a）默认策略 + （2a）默认路由 / （2b）默认路由：



- 启用负载均衡：



下表列出了单播路由相关的 WebUI 菜单路径、简短描述以及到相关手册章节的链接。

表 4 单播路由配置步骤

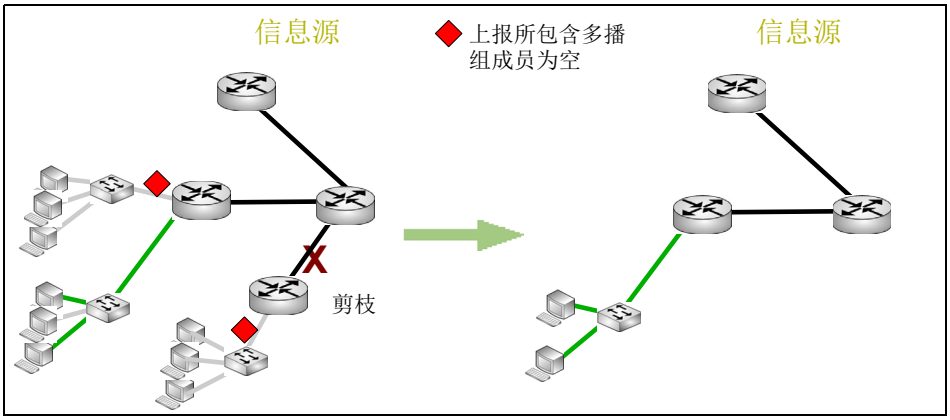
	WebUI 菜单路径	描述信息	手册章节
1.	网络 > 路由 策略路由	**三层单播策略**。根据匹配到入口接口、源 IP、服务和 TOS 的优先级最高的策略决定匹配哪个出口路由表。	5.2.1 单播
2.	网络 > 路由 缺省路由	**三层单播路由**。策略指定路由表中的匹配路由条目决定了数据包的出口接口（和网关）。	5.2.1 单播

2.4.2. 三层多播 （多播和 DVMRP）

三层多播路由分为动态和静态两种：

- **三层动态多播 （DVMRP）**：基于 DVMRP 动态生成一个路由表，包含多播组中每个接口所对应的矢量距离。 Metric 值决定了接口的相对 “ 开销 ”，用于决定数据包从哪个接口转发。阈值决定了数据包要被转发所需要的生存时间 （TTL），数据包的 TTL 必须大于这个值才能被转发。

  缓存和剪枝生存时间避免转发不必要的多播包。当接收不到成员报告时，多播组节点将被剪枝 （从多播组中去除）。



- **三层静态多播**：根据以下参数决定转发接口：

  1.源 IP 地址

  2.多播组 IP 地址

  3.入口接口

  转发接口必须开启 DVMRP。转发数据包还需要设置 TTL 值，实际功能同 DVMRP 中的阈值。

下表列出了三层多播相关的 WebUI 菜单路径、简短描述以及到相关手册章节的链接。

表 5 三层多播配置步骤

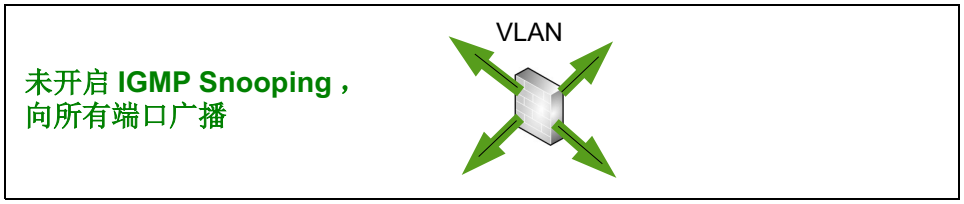
	WebUI 菜单路径	描述信息	手册章节
1.	**网络 > 多播 DVMRP**	**三层动态多播路由**。基于 DVMRP 为多播组成员接口动态生成路由表，路由表中包含到各个接口的距离信息。	5.2.2.1 三层动态多播
2.	**网络 > 路由 多播路由**	**三层静态多播路由**。基于源 IP 地址、多播组 IP 地址和入口接口决定转发接口。	5.2.2.2 三层静态多播

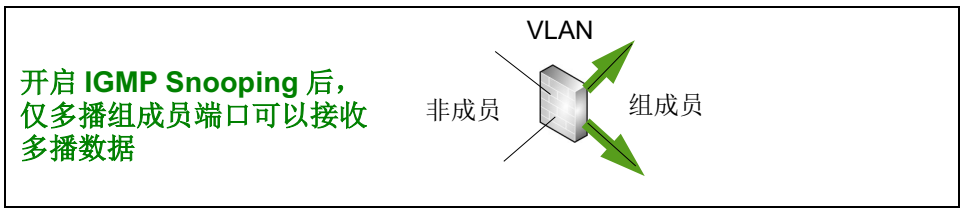
2.4.3. 二层多播 （IGMP Snooping）

二层多播包括动态和静态两种：

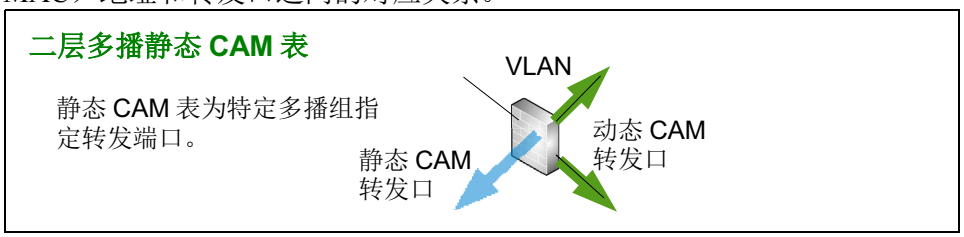
二层动态多播：主机通过 IGMP 协议可动态加入或离开多播组。 NISG 支持 IGMPv1 和 IGMPv2。

默认情况下，组播数据被广播给 VLAN 中的所有端口。在 NISG 上为 VLAN 接口开启 IGMP Snooping 后， NISG 动态生成一个映射多播组 MAC 地址和端口关系的 CAM 表，然后根据 CAM 表将收到的组播数据发送给指定的接收者。





二层静态多播：管理员也可手动创建 CAM 表 （即静态 CAM 表），指定多播组 IP （和 MAC）地址和转发口之间的对应关系。



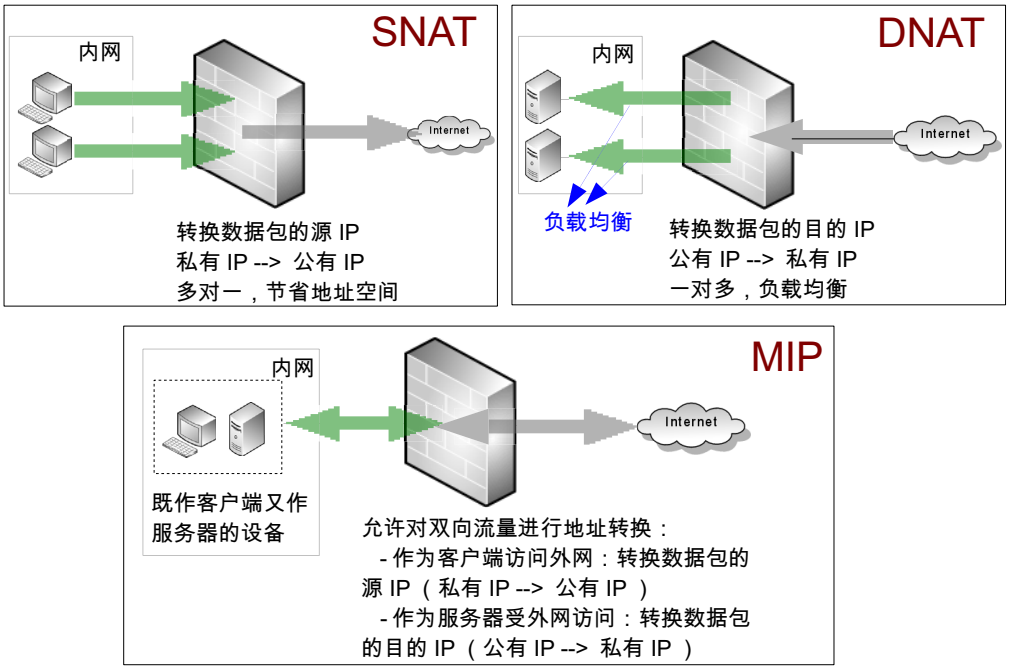
下表列出了二层多播相关的 WebUI 菜单路径、简短描述以及到相关手册章节的链接。

表 6 二层多播配置步骤

	WebUI 菜单路径	描述信息	手册章节
1.	网络 > 多播 IGMP Snooping	**二层动态多播**。通过 IGMP Snooping 学习路由和主机 MAC 地址信息，形成 MAC 地址与端口的映射关系表，即动态 CAM 表。	5.2.3.1 二层动态多播
2.	网络 > 路由 IGMP Snooping	**二层静态多播**。手动创建 CAM 表，指定多播组 IP 地址与转发口之间的对应关系。	5.2.3.2 二层静态多播

2.5. 地址转换 （NAT）

下图演示了 SNAT、 DNAT 和 MIP 的概念：



下表列出了地址转换的类别。

表 7 地址转换类别

	NAT 类别	优先级	转换类型
1.	SNAT	2	一对一；多对一；多对多
2.	DNAT	2	一对一；一对多
3.	MIP	1	一对一

下表给出了地址转换相关的 WebUI 菜单路径、简短描述以及到相关手册章节的链接。

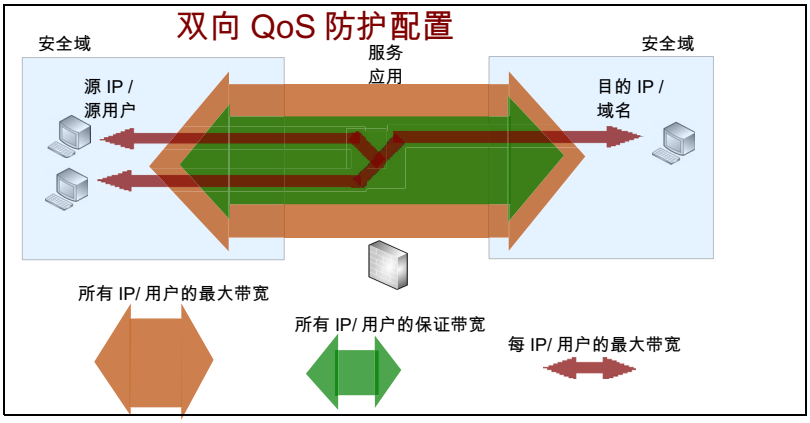
表 8 地址转换配置步骤

	WebUI 菜单路径	描述信息	手册章节
1.	**网络 > 地址转换 > 源地址转换**	源地址转换 （SNAT）。	6.2.1 创建 SNAT 规则
2.	**网络 > 地址转换 > 目的地址转换**	目的地址转换 （DNAT）。	6.2.2 创建 DNAT 规则
3.	**网络 > 地址转换 > 地址映射**	地址映射 （MIP），基本上是 SNAT 和 DNAT 的综合使用。	6.2.3 创建 MIP 规则

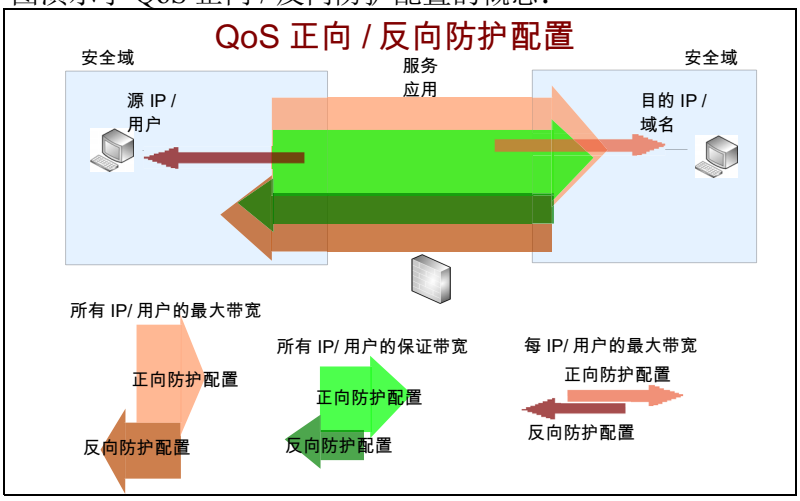
2.6. 服务质量 （QoS）

下图演示了 QoS 的概念。 QoS 策略指定：

- 源安全域 IP/ 用户和目的安全域 IP/ 域名之间传输的应用、服务的最大 / 保证带宽（源和目的安全域可以为 Any）。
- 每用户 /IP 的最大带宽。



下图演示了 QoS 正向 / 反向防护配置的概念：



下表给出了 QoS 相关的 WebUI 菜单路径、简短描述以及到相关手册章节的链接。

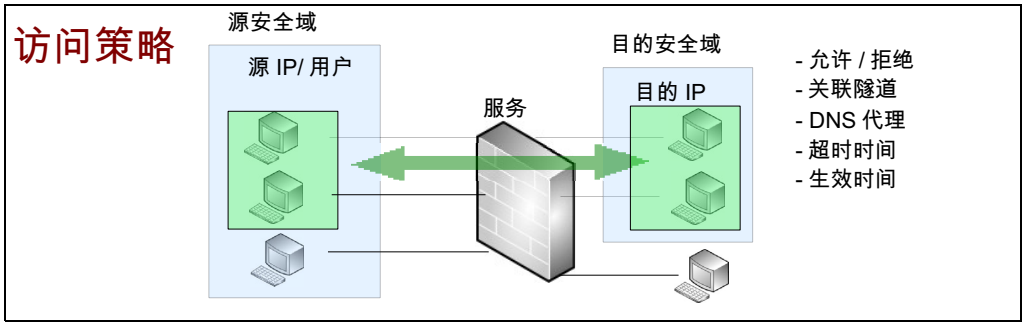
表 9 QoS 配置步骤

	WebUI 菜单路径	描述信息	手册章节
1.	**UTM > QoS > QoS 防护配置**	创建全局 QoS 防护配置，用于决定流量的优先级、最大带宽、保证带宽和 DSCP 值。	7.2.1 创建普通 QoS 防护配置
2.	**UTM > QoS > 每 IP/ 用户 QoS 防护配置**	创建每 IP/ 用户 QoS 防护配置，用于决定每 IP、用户流量的最大带宽。	7.2.2 创建每 IP/ 用户 QoS 防护配置
3.	**UTM > QoS > QoS 策略**	创建 QoS 策略，用于决定哪些流量要进行带宽控制。	7.2.3 创建 QoS 策略

2.7. 防火墙策略

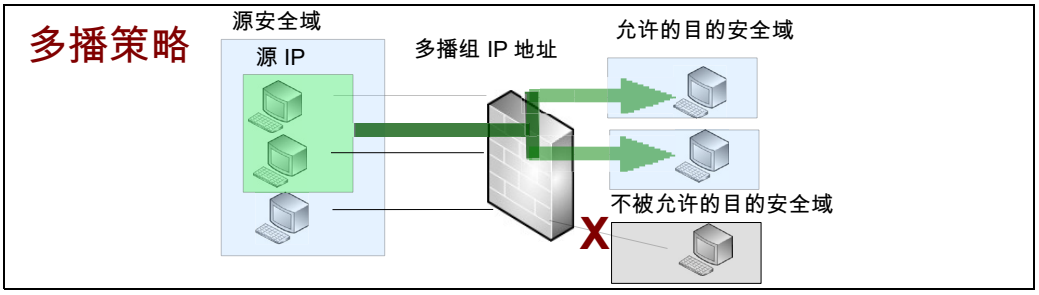
下图演示了防火墙 （非多播包）访问策略的概念：

- 允许 / 拒绝指定源安全域 IP/ 用户和目的安全域 IP 之间传输的数据包（安全域可以为 Any），并匹配以下可选配置项：
  - 隧道：指定的用于传输数据包的 VPN 隧道。
  - DNS 透明代理：启用 / 禁用。关于透明代理的信息，请参见 4.14DNS 代理。
  - 使用特定超时时间：如果到达设定的超时时间，相应的会话就会被删除。
  - 时间表：决定策略何时生效。



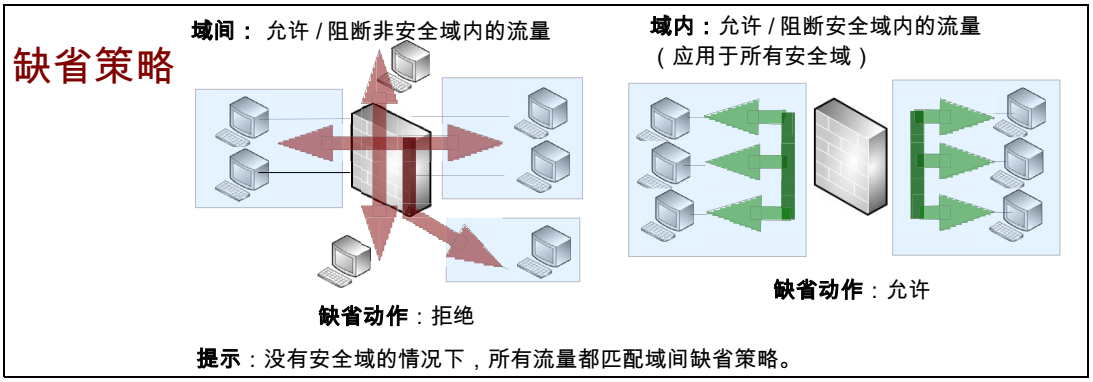
下图演示了防火墙多播策略的概念：

- 通过指定允许和阻断的目的安全域允许/拒绝从源安全域IP/用户到多播组IP的数据包（源安全域可以为 Any）。



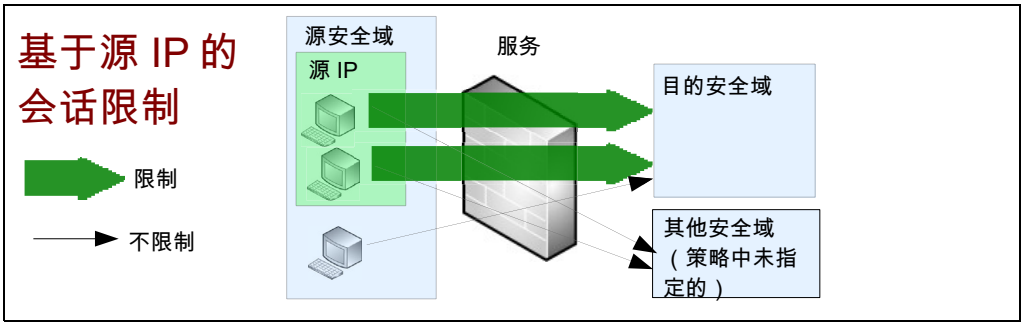
下图演示了防火墙缺省策略的概念：

- 域内策略：允许 / 阻断安全域内数据包传输 （应用于所有安全域）。
- 域间策略：允许 / 阻断非安全域内的数据包传输。

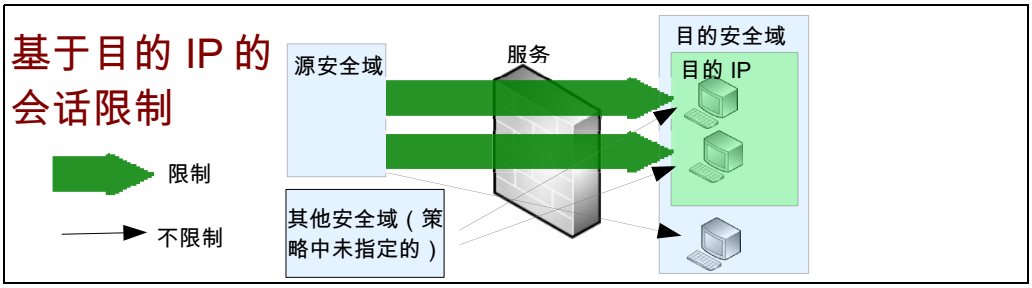


下面三个图演示了会话限制策略的概念。针对每种会话限制策略类型，超过限制的会话都将被丢弃 / 报警 （在策略启用的前提下）。

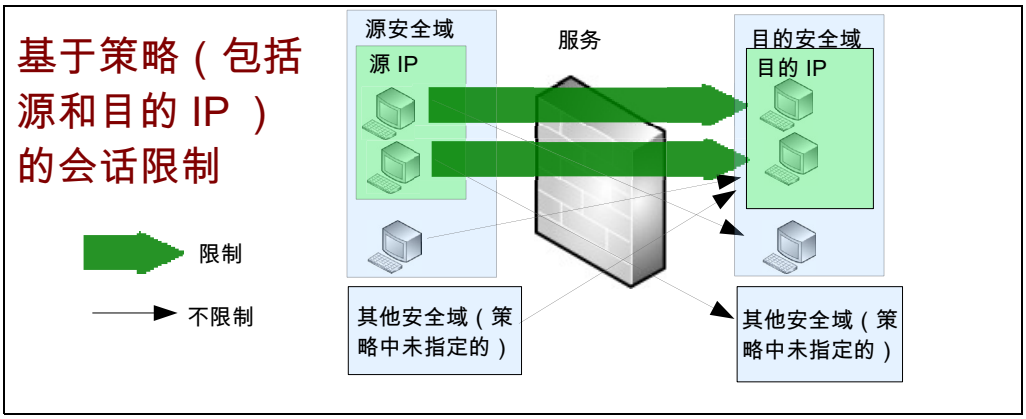
1. 基于源 IP 的会话限制策略：根据源安全域、源 IP、目的安全域和服务匹配会话。



2. 基于目的 IP 的会话限制策略：根据源安全域、目的安全域、目的 IP 和服务匹配会话。



3. 基于策略 （包括源和目的 IP）的会话限制策略：根据源安全域、源 IP、目的安全域、目的 IP 和服务匹配会话。



下表给出了防火墙策略的概要信息，包括优先级、数据包源和目的以及对应的动作等。

表 10 策略类别

	防火墙策略类别	优先级	匹配数据包源	匹配数据包目的	动作
1.	缺省策略设置 / 域间	2	（无）	（无）	允许 / 拒绝
	缺省策略设置 / 域内	2	安全域	安全域	允许 / 拒绝
2.	缺省策略设置 / 缺省会话超时设置	2	（无）	（无）	（超时）
3.	访问策略	1	安全域 IP 用户 服务	安全域 IP/ 域名 服务	允许 / 拒绝 隧道 DNS 代理 超时
4.	多播策略		安全域 （或 any） IP	多播组 IP 安全域	允许
5.	会话策略 / 基于以下参数的会话限制： 1. 策略 2. 源 IP 3. 目的 IP	1	安全域 （或 any） IP	安全域 （或 any） IP 服务	丢弃 报警 丢弃 + 报警

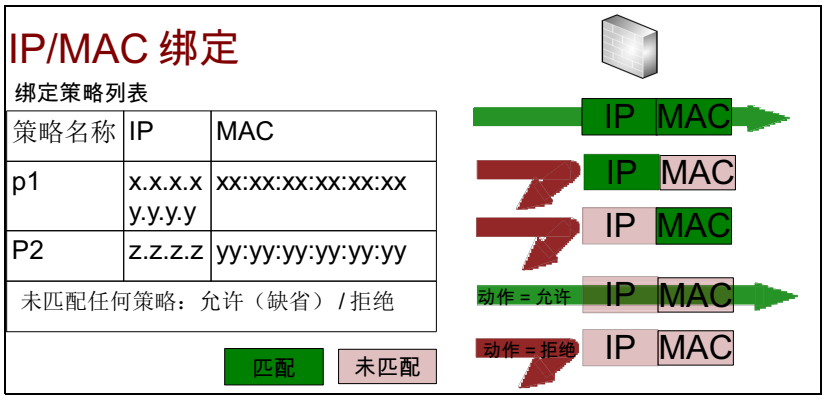
下表给出了防火墙策略相关的 WebUI 菜单路径、简短描述以及到相关手册章节的链接。

表 11 策略配置步骤

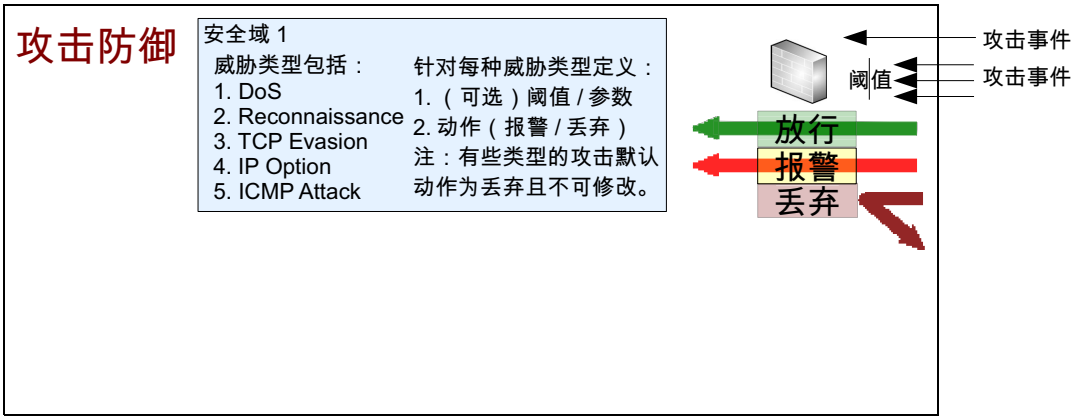
	WebUI 菜单路径	描述信息	手册章节
1.	**防火墙 > 访问策略**	安全域到安全域。	8.2.2 创建访问策略
2.	**防火墙 > 缺省策略设置**	所有安全域。	8.2.3 配置缺省访问策略
3.	**防火墙 > 多播策略**	多播安全域。	8.2.4 创建多播策略
4.	**防火墙 > 会话策略**	安全域到安全域的会话限制。	8.2.5 创建会话策略

2.8. 攻击防御

下图描述了 IP-MAC 绑定的概念：



下图描述了攻击防御的概念：



下表给出了攻击防御相关的 WebUI 菜单路径、简短描述以及到相关手册章节的链接。

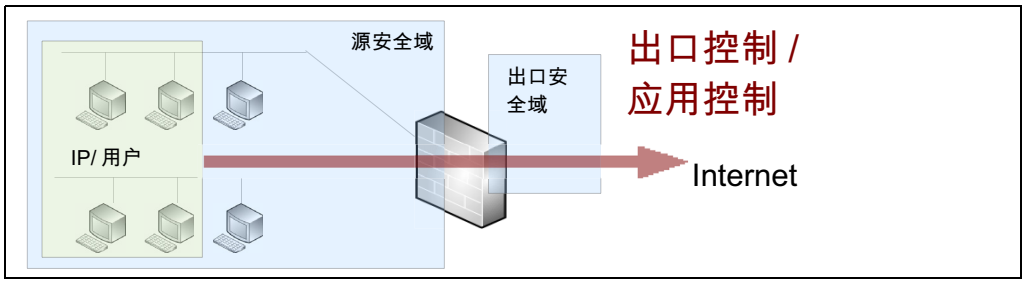
表 12 攻击防御配置步骤

	WebUI 菜单路径	描述信息	手册章节
1.	**防火墙 > IP-MAC 绑定**	绑定 IP 地址或 IP 地址段到 MAC 地址。	8.2.1 配置 IP-MAC 绑定
2.	**防火墙 > 攻击防御**	对于常见网络攻击的安全域级别的检测和防御机制。	第 9 章 , 攻击防御

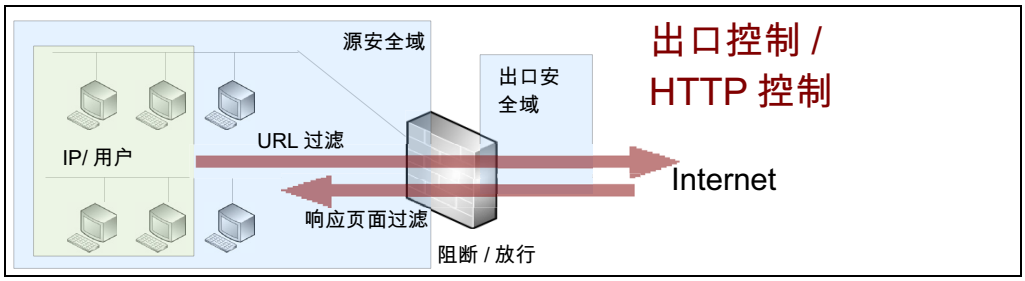
2.9. 统一威胁管理 （UTM）

NISG 提供扩展的统一威胁管理功能：

- 出口控制，包括：
  - 2.9.1. 应用控制：控制来自源安全域中指定 IP/ 用户、到出口安全域的应用流量。

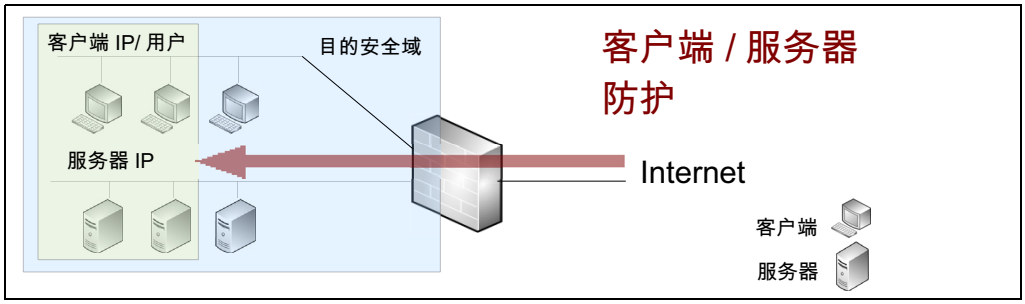


  - 2.9.2.HTTP 控制：控制来自源安全域中指定 IP/ 用户、到出口安全域的 URL 请求，并过滤其 HTTP 应答。



  - 2.9.3.DNS 控制。

- 2.9.4. 客户端防护和 2.9.5. 服务器防护：控制到目的安全域中指定客户端或服务器的流量。

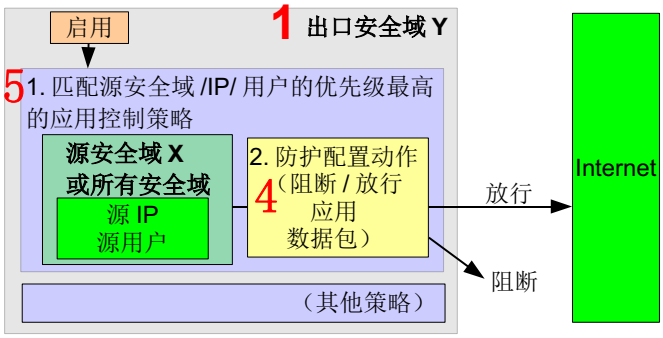


2.9.1. 应用控制

2.9.1.1. 数据包处理流程

UTM 出口控制中应用数据包处理步骤 （黑色编号）如下图所示 （红色编号为下表中的配置步骤）：

1. 根据源安全域 /IP/ 用户决定优先级最高的一条匹配策略。
2. 执行应用控制防护配置 （策略中指定的防护配置）动作。



2.9.1.2. 配置步骤

下表给出了应用控制相关的 WebUI 菜单路径 （按照配置顺序）、简短描述以及到相关手册章节的链接。

表 13 应用控制配置步骤

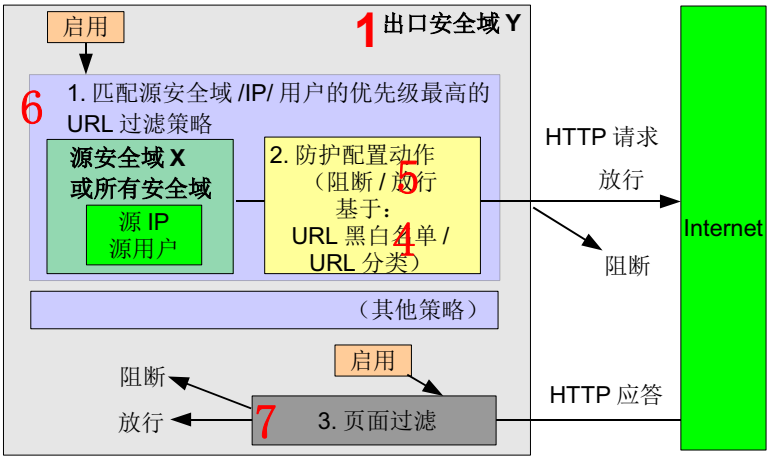
	WebUI 菜单路径	描述信息	手册章节
1.	**网络 > 安全域**	创建安全域。	10.2.1.1. 创建安全域 / 访问策略 / 缺省路由 /NAT 规则
2.	**UTM > 出口控制 > 应用控制 > 更新**	更新应用知识库。	10.2.1.2.1. 更新应用知识库（2a）
3.	**UTM > 出口控制 > 应用控制 > 应用知识库 , 自定义应用**	自定义应用匹配条件。	10.2.1.2.2. 添加自定义应用（2b）
4.	**UTM > 出口控制 > 应用控制 > 防护配置**	根据需要创建防护配置。每个防护配置指定了要控制的应用、针对每种应用的动作以及未指定应用的缺省动作。	10.2.1.2.3. 创建应用控制防护配置 （2c）
5.	**UTM > 出口控制 > 策略 > 应用控制**	针对每个出口安全域： ■ 根据需要创建应用控制策略。 ■ 开启应用控制功能。	10.2.1.2.4. 创建应用控制策略（2d）

2.9.2. HTTP 控制

2.9.2.1. 数据包处理流程

UTM 出口控制中 HTTP 数据包处理步骤 （黑色编号）如下图所示 （红色编号为下表的配置步骤）：

1. 根据源安全域 /IP/ 用户决定优先级最高的一条匹配策略。
2. 执行 （策略中指定的） URL 过滤防护配置动作。
3. 执行页面过滤。



2.9.2.2. 配置步骤

下表给出了 URL 过滤和 HTTP 响应页面过滤相关的 WebUI 菜单路径 （按照配置顺序）、简短描述以及到相关手册章节的链接。

表 14 URL 过滤和页面过滤配置步骤

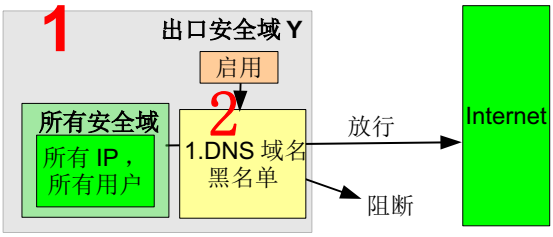
	WebUI 菜单路径	描述信息	手册章节
1.	**网络 > 安全域**	创建安全域。	10.2.1.1. 创建安全域 / 访问策略 / 缺省路由 /NAT 规则
2.	**UTM > 出口控制 > URL 过滤 > 更新**	更新 URL 过滤规则。	10.2.1.3.1. 更新 URL 分类库 （3a）
3.	**UTM > 出口控制 > URL 过滤 > 常规设置**	设置 URL 过滤引擎失效时 NISG 的处理动作。	10.2.1.3.2. 配置 URL 过滤常规设置 （3b）
4.	**UTM > 出口控制 > URL 过滤 > 黑白名单**	配置 URL 黑白名单	10.2.1.3.3. 创建 URL 过滤防护配置：黑白名单 （3c）
5.	**UTM > 出口控制 > URL 过滤 > 防护配置**	URL 过滤防护配置指定了要过滤的 URL 分类、针对分类执行的动作，以及对未知分类的缺省处理动作。	10.2.1.3.4. 创建 URL 过滤动作防护配置 （3d）
6.	**UTM > 出口控制 > 策略 > URL 过滤**	针对每个出口安全域： ■ 创建 URL 过滤策略。 ■ 开启 URL 过滤功能。	10.2.1.3.5. 创建 URL 过滤策略 （3e）
7.	**UTM > 出口控制 > 页面过滤**	配置全局页面过滤功能。不过需要为每个出口安全域单独开启该功能。	10.2.1.4. 配置 （HTTP 应答）页面过滤

2.9.3. DNS 控制

2.9.3.1. 数据包处理流程

UTM 出口控制中 DNS 数据包处理步骤 （黑色编号）如下图所示 （红色编号为下表的配置步骤）：

1. 阻断匹配 DNS 域名黑名单的 DNS 请求。



2.9.3.2. 配置步骤

下表给出了 DNS 域名黑名单相关的 WebUI 菜单路径 （按照配置顺序）、简短描述以及到相关手册章节的链接。

表 15 DNS 域名黑名单配置步骤

	WebUI 菜单路径	描述信息	手册章节
1.	**网络 > 安全域**	创建安全域。	10.2.1.1. 创建安全域 / 访问策略 / 缺省路由 /NAT 规则
2.	**UTM > 出口控制 > DNS 域名黑名单**和 **UTM > 出口控制 > 策略 > DNS 域名黑名单**	配置全局 DNS 域名黑名单功能。不过需要为每个出口安全域单独开启该功能。	10.2.1.5. 配置 DNS 域名黑名单

2.9.4. 客户端防护

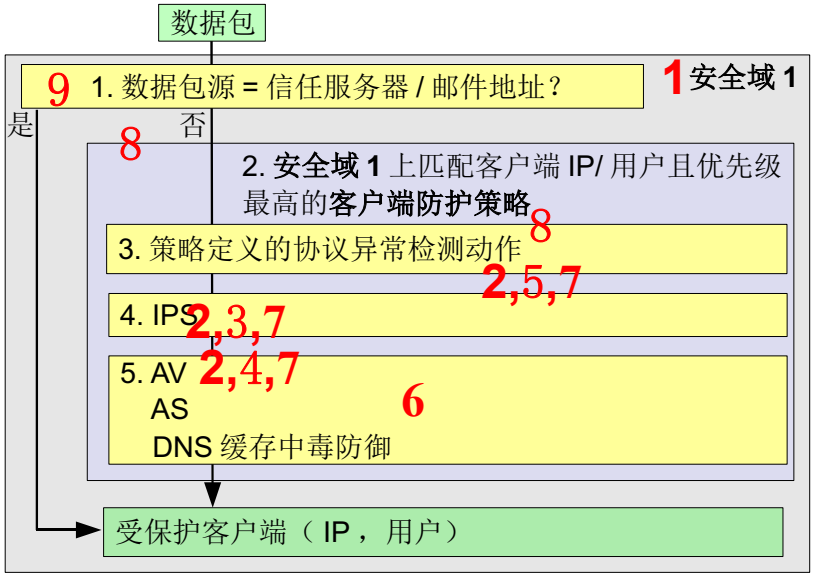
本节介绍客户端防护功能，包括：

- 2.9.4.1. 数据包处理流程
- 2.9.4.2. 配置步骤

2.9.4.1. 数据包处理流程

UTM 客户端保护中数据包处理步骤 （黑色编号）如下图所示 （红色编号对应下一页表格中的配置步骤编号）：

1. 如果来自 （针对安全域定义的信任列表中）信任服务器或邮件地址：放行。
2. 根据数据包中客户端 IP 地址或用户确定安全域上优先级最高的匹配策略。
3. 进行协议异常检测 （策略中定义）。
4. 进行 IPS 检测 （全局配置，包括协议限制和攻击签名检测）。
5. 进行防病毒扫描（全局配置）和 / 或反垃圾邮件检测（全局配置）。如果是 DNS 协议包，进行 DNS 缓存中毒防御检查 （全局配置）。



2.9.4.2. 配置步骤

下表给出了客户端防护相关的配置步骤 （上图中标注的）、 WebUI 菜单路径 （按照配置顺序）、简短描述以及到相关手册章节的链接。

表 16 客户端防护配置步骤

	WebUI 菜单路径	描述信息	手册章节
1.	**网络 > 安全域**	创建客户端保护安全域。	10.2.2.1. 创建安全域 / 访问策略 / 缺省路由 /NAT 规则
2.	**UTM > 防病毒 , 反垃圾邮件 ,IPS > 更新**	更新防病毒、反垃圾邮件、 IPS 攻击签名规则。	10.2.2.2. 更新 AV/AS/IPS 规则
3.	**UTM > 防病毒 > 常规设置 , 信任 URL, 信任 Web 服务器 , 信任客户端**	配置防病毒全局动作，包括扫描设置、滴流功能和信任列表。	10.2.2.3. 配置 AV 全局动作 （信任列表 / 病毒检测动作 / 启发式扫描 / 扫描限制）
4.	**UTM > 反垃圾邮件 > 常规设置 , 允许 / 阻断列表 , 关键字列表**	配置反垃圾邮件全局动作，包括扫描设置、阻断 / 允许列表、关键字列表。	10.2.2.4. 配置 AS 全局动作 （允许 / 阻断列表，关键字列表，扫描设置）
5.	**UTM > IPS > 协议限制**	设置全局 SMTP/POP3/IMAP/ DNS 协议限制。	10.2.2.5. 配置 IPS SMTP/POP3/ IMAP/DNS 协议限制 （客户端）
6.	**UTM > 客户端防护 > DNS 缓存中毒防御**	配置全局 DNS 缓存中毒防御功能，为指定安全域启用该功能。	10.2.2.6. 配置 DNS 缓存中毒防御全局动作
7.	**UTM > 防病毒 , 反垃圾邮件 ,IPS > 防护配置**	配置全局防病毒、反垃圾邮件和 IPS 防护配置。	10.2.2.7. 创建 AV/AS/IPS 防护配置
8.	**UTM > 客户端防护 > 策略**	为指定安全域配置客户端保护策略，指定： 1. 受保护的客户端 2. AV/AS/IPS 防护配置 3. 其他检测动作	10.2.2.8. 创建客户端防护策略
9.	**UTM > 客户端防护 > 信任服务器列表 , 信任邮件地址列表**	为指定安全域创建信任服务器和邮件地址列表。	10.2.2.9. 创建信任服务器 / 邮件列表

2.9.5. 服务器防护

- 2.9.5.1. 数据包处理流程
- 2.9.5.2. 配置步骤

2.9.5.1. 数据包处理流程

UTM 客户端保护中数据包处理步骤 （黑色编号）如下图所示 （红色编号为下一页的配置步骤编号）：

1. 如果来自 （基于安全域定义的信任列表）信任客户端或邮件地址：放行
2. 根据服务器 IP 地址确定安域上优先级最高的匹配策略。
3. 执行协议异常检测 （策略中定义）。
4. 进行 IPS 检测 （全局配置，包括协议限制和攻击签名检测）。
5. 根据协议不同，选择进行：
   - （全局配置的）防病毒扫描、反垃圾邮件检测、 Web 或邮件防护检查，或
   - （策略中定义的） Telnet 命令过滤和 DNS 外部请求限制。

2.9.5.2. 配置步骤

下表给出了服务器防护相关的配置步骤 （上图中标注的）、 WebUI 菜单路径 （按照配置顺序）、简短描述以及到相关手册章节的链接。

表 17 服务器防护配置步骤

	WebUI 菜单路径	描述信息	手册章节
1.	**网络 > 安全域**	创建服务器保护安全域。	10.2.3.1. 创建安全域 / 访问策略 / 缺省路由 /NAT 规则 ,
2.	**UTM > 防病毒 , 反垃圾邮件 ,IPS > 更新**	更新防病毒、反垃圾邮件、 IPS 攻击签名规则。	10.2.3.2. 更新 AV/AS/IPS 规则
3.	**UTM > 防病毒 > 常规设置 , 信任 URL, 信任 Web 服务器 , 信任客户端**	配置防病毒全局动作，包括扫描设置、滴流功能和信任列表。	10.2.3.3. 配置 AV 全局动作（信任列表 / 病毒检测动作 / 启发式扫描 / 扫描限制）
4.	**UTM > 反垃圾邮件 > 常规设置 , 允许 / 阻断列表 , 关键字列表**	配置防病毒全局动作，包括扫描设置、阻断 / 允许列表、关键字列表。	10.2.3.4. 配置 AS 全局动作（允许 / 阻断列表，关键字列表，扫描失败动作）
5.	**UTM > IPS > 协议限制**	设置全局 HTTP/SMTP/POP3/ IMAP/DNS 协议限制。	10.2.3.5. 配置 IPS 协议限制（HTTP/SMTP/POP3/IMAP/ DNS 服务器）
6.	**UTM > 服务器防护 > Web 防护 , 邮件防护**	为所有安全域配置 Web 和邮件防护。	10.2.3.6. 配置 web/ 邮件防护全局动作
7.	**UTM > 防病毒 , 反垃圾邮件 ,IPS > 防护配置**	配置全局防病毒、反垃圾邮件和 IPS 防护配置。	10.2.3.7. 创建 AV/AS/IPS 动作防护配置
8.	**UTM > 服务器防护 > 策略**	为指定安全域配置服务器防护策略，指定： • 受保护服务器 • AV/AS/IPS 防护配置 • 其他检测动作。	10.2.3.8. 创建服务器防护策略
9.	**UTM > 服务器防护 > 信任客户端列表 信任邮件地址列表**	为指定安全域创建信任客户端和邮件地址列表。	10.2.3.9. 创建信任客户端 / 邮件列表

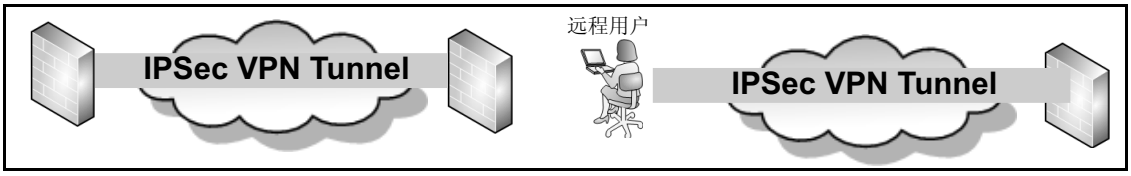
2.10. 虚拟专用网 （VPN）

NISG 提供高性能的 VPN 功能，包括：

- 2.10.1.IPSec VPN
- 2.10.2.SSL VPN Web 入口页面
- 2.10.3.SSL VPN 隧道

2.10.1. IPSec VPN

下图给出了 IPSec VPN 网段到网段和远程访问两种基本应用场景。



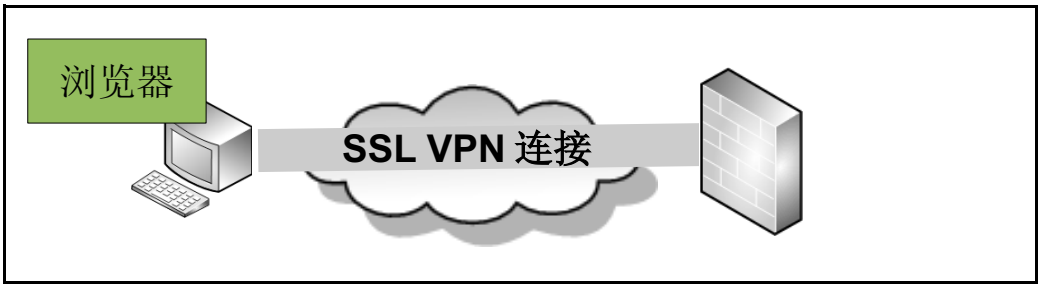
下表给出了 IPSec VPN 相关的 WebUI 菜单路径 （按照配置顺序）、简短描述以及到相关手册章节基本配置步骤的链接。

表 18 IPSec VPN 配置步骤

	WebUI 菜单路径	描述信息	手册章节
1.		配置接口、缺省路由和访问策略。	3.1 配置接口 IP 地址和缺省访问策略
2.	**系统 > 证书 > 本地证书，CA 证书**	设置预共享密钥或者导入证书。	3.4.1 使用预共享密钥认证 / 3.4.2 使用证书认证
3.	**系统 > 认证 > 网络用户 （Auto IKE)**	创建 IPSec VPN 用户或用户组 （远程拨号自动迷药隧道）	3.3 创建 IPSec VPN 用户
4.	**VPN > IPSec VPN > 自动 / 手册隧道**	创建自动或手动隧道。	1.2 创建手动密钥隧道 (联动创建隧道接口） / 2.2 创建自动密钥隧道（联动创建隧道接口）
5.	**网络 > 路由 > 缺省路由** 或 **防火墙 > 访问策略**	创建缺省路由或访问策略并指定引用隧道。	1.3 引用隧道
6.		配置对端 （仅针对拨号访问）。	3.2 Windows 客户端配置

2.10.2. SSL VPN Web 入口页面

下图给出了 SSL VPN web 入口页面的基本应用场景。



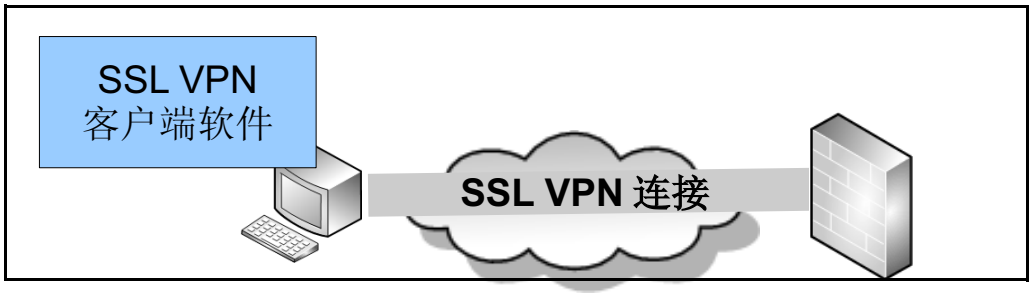
下表给出了 SSL VPN Web Portal 相关的 WebUI 菜单路径 （按照配置顺序）、简短描述以及到相关手册章节的链接。

表 19 SSL VPN Web 入口页面配置步骤

	WebUI 菜单路径	描述信息	手册章节
1.		配置接口 IP	4.1 配置接口 IP 地址
2.	系统 > 认证 > 网络用户 VPN > SSL VPN > 用户组	创建 SSL VPN 用户和用户组。	4.2 创建 IP 地址池， SSL VPN 用户， SSL VPN 用户组
3.	系统 > 证书 > 本地 / CA 证书	导入 CA/ 本地证书	4.3 导入 CA/ 本地证书
4.	VPN > SSL VPN Web 入口页面 > 应用 / 页面模板	应用包括 HTTP 和 HTTPs。 入口页面模板包括内容、布局和风格。	4.4 创建 SSL VPN 应用， SSL VPN 页面模板
5.	VPN > SSL VPN Web 入口页面 > 页面服务	启用 HTTPS 服务，在指定 IP 地址和端口为用户组提供服务。	4.5 创建 SSL VPN 页面服务

2.10.3. SSL VPN 隧道

下图给出了 SSL VPN 隧道的基本应用场景。



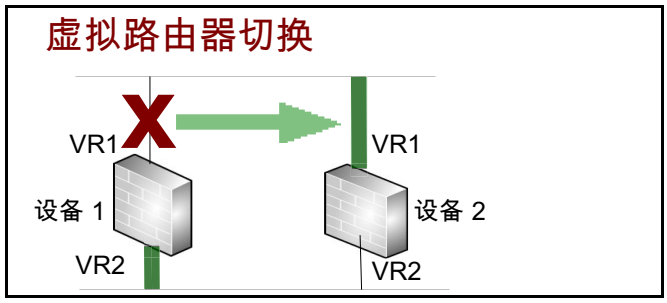
下表给出了 SSL VPN 隧道相关的 WebUI 菜单路径 （按照配置顺序）、简短描述以及到相关手册章节基本配置步骤的链接。

表 20 SSL VPN 隧道配置步骤

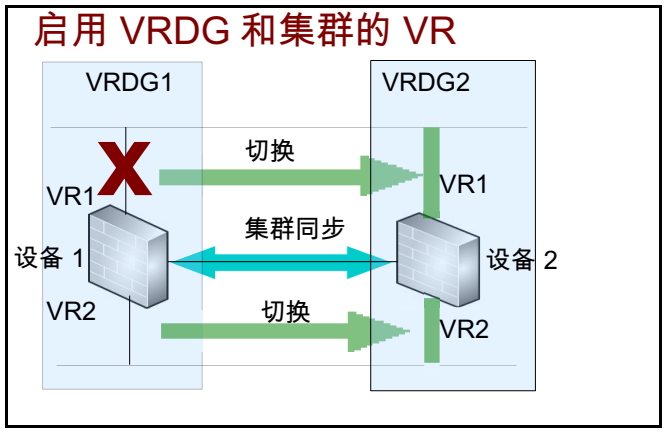
	WebUI 菜单路径	描述信息	手册章节
1.		配置接口 IP	5.1 配置接口 IP 地址
2.	**系统 > 认证 > 网络用户** **VPN > SSL VPN > 用户组**	创建 SSL VPN 用户和用户组。	5.3 创建 IP 地址池 /VPN 用户 /VPN 用户组
3.	**VPN > SSL VPN 隧道 > 隧道**	在服务器和客户端之间创建 SSL VPN 隧道。	5.4 创建 SSL VPN 隧道
4.		安装 SSL VPN 客户端软件。	5.2 安装 SSL VPN 客户端软件 / 添加 SSL VPN 连接

2.11. 高可用性 （HA）

下图演示了 HA 虚拟路由器故障切换的概念。设备 1 上的虚拟路由器 VR1 发生故障，切换到设备 2，设备 2 的 VR1 将接替设备 1 上 VR1 的工作。由于未开启探测组功能，两台设备上 VR2 之间不发生切换。



下图演示了 HA 虚拟路由器故障切换以及虚拟路由器探测组和集群的概念。设备 1 上 VR1 发生故障，探测组同时调整 VR1 和 VR2 的优先级，所以两台设备上的 VR1 之间和 VR2 之间同时发生切换，使得整个设备发生切换。设备 1 和设备 2 之间进行了配置同步，使得两台设备之间能够完成无缝切换。



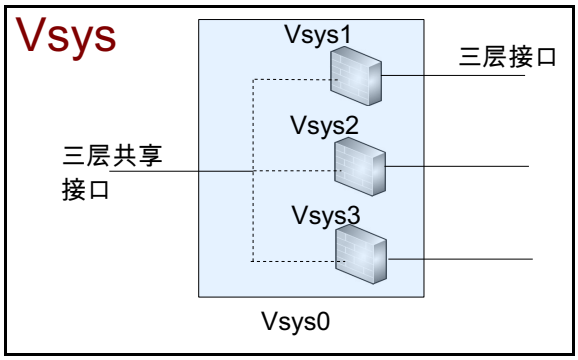
下表给出了 （高可用性）虚拟路由器相关的 WebUI 菜单路径 （按照配置顺序）、简短描述以及到相关手册章节基本配置步骤的链接。

表 21 高可用性配置步骤

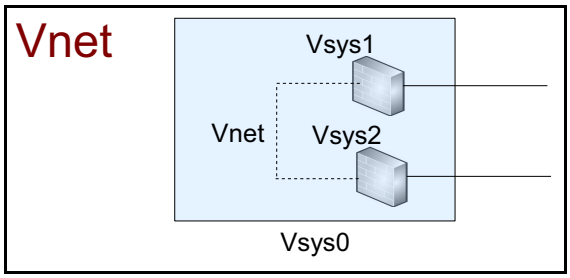
	WebUI 菜单路径	描述信息	手册章节
1.	**系统 > 高可用性 > 虚拟路由器**	使用 VRRP 协议达到备份和冗余的目的。一个虚拟路由器可以代表一组路由器作为默认网关工作。如果一个路由器被选举为主设备，则其他路由器则作为备设备工作。	12.2.1.1 Device1：配置 VR
2.	**系统 > 高可用性 > 虚拟路由器探测组**	增强的 VRRP 功能。一个探测组将多个虚拟路由器绑定在一起，以达到整体切换的目的。	12.2.2.2 Device1：配置 VRDG
3.	**系统 > 高可用性 > 集群**	一个集群由配置相同的设备组成。任何成员设备的配置修改都将被同步到组内其他成员设备上。 NISG 支持配置信息、运行信息和系统时间同步。	12.2.2.3 Device1：配置集群

2.12. 虚拟系统 / 网络 （Vsys/Vnet）

下图演示了虚拟系统的概念。设备上默认存在根系统 Vsys 0，管理员可以创建虚拟系统，每个虚拟系统有自己的资源限制、接口、管理 IP、 UTM 设置以及用户和管理员设置。



下图演示了虚拟网络的概念：



下表给出了虚拟系统相关的 WebUI 菜单路径 （按照配置顺序）、简短描述以及到相关手册章节基本配置步骤的链接。

表 22 虚拟系统配置步骤

	WebUI 菜单路径	描述信息	手册章节
1.	**网络 > 接口**	创建三层接口，如 VLAN 和 Channel 接口，用于划分到 Vsys 中。	13.2.1. 创建三层接口
2.	**系统 > 虚拟系统 > 虚拟系统**	创建虚拟系统，指定最大资源限制、包含的三层接口、管理接口 /IP、 UTM 功能。	13.2.2. 创建虚拟系统（资源限制 / 接口 / 管理 IP/UTM）
3.	**系统 > 认证 > 管理用户**	创建 Vsys 管理员。	13.2.3. 创建虚拟系统管理员
4.	在浏览器中输入 https://+vsys_management_IP 登录虚拟系统。	登录并管理 Vsys。每个 Vsys 都有自己的管理员和策略等配置。	13.2.4. 登录 / 切换虚拟系统和 13.2.5. 管理虚拟系统
5.	**系统 > 虚拟系统 > 虚拟网络**	创建虚拟网络连接虚拟系统。需要将虚拟接口提前划分指定的虚拟系统。	13.2.6. 创建虚拟网络

2.13. 监控 / 日志

下表给出了监控和日志相关的 WebUI 菜单路径。

表 23 监控 / 日志查看路径

	WebUI 菜单路径	描述信息	手册章节
1.	**监控 > 拓扑 / 流量统计数据 / 虚拟系统 /STP/ 路由 / 地址转换 /ARP/ CAM/DHCP IP 地址绑定状态 /DHCPv6 客户端 /DNS 缓存 / 高可用性 / 系统利用率 / 在线用户 /IPSec VPN 隧道 / 多播 / 报警 / 日志**	所有功能的实时监控信息。	第 14 章 , 监控

2.14. 报表

下表给出了报表相关的 WebUI 菜单路径 （按照配置顺序）、简短描述以及到相关手册章节基本配置步骤的链接。

表 24 报表配置路径

	WebUI 菜单路径	描述信息	手册章节
1.	**监控 > 报表 > 常规设置**	所有报表的全局设置。	15.2.1 配置常规设置
2.	**监控 > 报表 > 计划**	创建报表模板。	15.2.2 创建报表生成计划
3.	**监控 > 报表 > 结果**	查看生成的报表。	15.2.3 管理报表结果

3 系统配置

本章介绍 NISG 提供的如下管理功能：

- 系统基本信息
  - 3.1 WebUI 主页
  - 3.2 系统概述
  - 3.3 标题信息
  - 3.4 资产汇总
  - 3.5 版权信息
  - 3.6 系统时间
- License 与升级
  - 3.7 License
  - 3.8 系统升级
  - 3.9 安装升级包管理
  - 3.10 增强升级包管理
- 访问设置
  - 3.11 访问服务
  - 3.12 SNMP
- 用户与认证
  - 3.13 管理用户
  - 3.14 网络用户
  - 3.15 用户认证
  - 3.16 WebAuth 配置
- 系统维护
  - 3.17 备份恢复
  - 3.18 技术支持
  - 3.19 集中管理
  - 3.20 诊断工具
- 报警和日志
  - 3.21 报警配置
  - 3.22 日志维护
- 系统全局应用
  - 3.23 证书
  - 3.24 对象

3.1 WebUI 主页

NISG WebUI 主页展示系统相关信息，包括资源信息、接口状态、日志、防病毒报警、在线用户等。

点击**主页**选项卡查看详细信息。管理员可以根据需要查看具体页面。可以点击 手动刷新页面，点击 关闭当前信息窗口，或点击 编辑刷新频率、刷新方式、显示的信息条数、显示格式等。当鼠标指针变为 时，可以将该栏目拖到任何位置，改变页面布局。点击**更多**进入相应配置页面进行更多配置。

表 25 主页信息

参数	说明
系统信息	显示系统信息，包括型号、软件名称、软件版本、释放时间、序列号、内存和系统运行时间。
资源使用情况	显示系统资源使用情况，包括 CPU、内存、日志存储空间、会话、策略、 VPN 和 NAT 资源。
接口状态	显示接口状态。已启用处于连通状态的接口显示为绿色，被禁用的接口显示为灰色。
系统日志	显示生成的不同安全级别的日志信息。 Emergency 和 Alert 以红色标示， Critical 和 Error 黄色标示， Warning 和 Notice 绿色标示， Informational 和 Debugging 蓝色标示。
防病毒报警	显示经过防病毒扫描后，被 NISG 记录的隔离文件信息。
反垃圾邮件报警	显示经过反垃圾邮件扫描后，被 NISG 记录的隔离文件信息。
URL 排名	显示 URL 排名相关信息。
用户排名	显示用户排名相关信息。
IP 地址排名	显示 IP 地址排名相关信息。
应用排名	显示应用排名相关信息。
WebAuth 用户	显示在线 WebAuth 用户相关信息，包括用户、 IP 地址、在线时间、实时流量、总流量及空闲时间。
SSL VPN 用户	显示在线 SSL VPN 用户相关信息，包括用户、登录类型、 IP 地址、在线时间、接收和发送字节数及空闲时间。

3.2 系统概述

系统概述页面显示系统信息、访问设置及系统重启关闭等相关内容。

- 3.2.1 基本配置步骤
- 3.2.2 配置参数说明

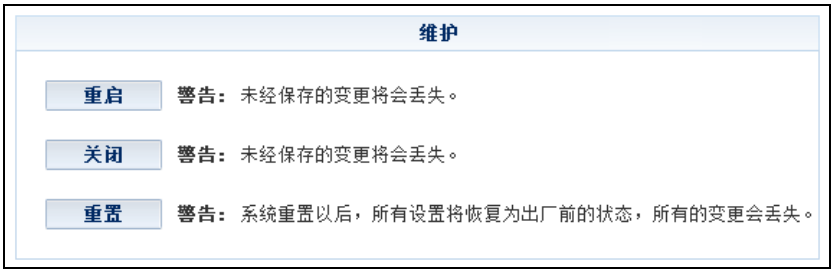
3.2.1 基本配置步骤

选择**系统** > **概述**。

1. 点击系统信息参数对应的 编辑系统信息。

2. 点击**访问设置**区域的 进入**系统 > 服务配置 > 访问设置**页面配置访问服务。关于访问服务的更多信息，请参见 3.11 访问服务。

3. 在**维护**区域重启、关闭或重置系统。



配置注意事项

- 只有根管理员和根系统管理员可以重启和关闭系统。只有根系统管理员可以重置系统。
- 当系统重启、关闭或者重置时，未经保存的配置信息将会丢失。系统重置后，之前的日志会清除。请在执行该操作前，确认重要配置信息已经保存，避免信息丢失。

表 26 系统信息命令

show system info	查看系统信息。
hostname *name*	修改主机名。
language {**Chinese** | **English**}	设置系统语言。
timezone *timezone_id*	设置系统时区。
time *date time*	手动设置系统时间。
license import from	上载 License 文件。

表 27 重启和关闭命令

reboot	重启系统。
halt	关闭系统。
reset	重置系统。

3.2.2 配置参数说明

表 28 系统信息参数

参数	说明
主机名	系统主机名。长度 1-24 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #。不能以 “-” 开头。默认主机名为 NetEye。
语言	当前系统语言，包括简体中文和英语。默认语言为英文。
时区	当前系统所在时区。默认时区为 GMT+8:00 中国 上海 /（北京）。
当前时间	当前系统时间。
License	当前系统的 License 信息。
SNMP	SNMP 服务状态。
上次更新时间	上次系统更新时间。

3.3 标题信息

- 3.3.1 概述
- 3.3.2 基本配置步骤

3.3.1 概述

标题信息是在以 CLI 方式登录 NISG 时， NISG 所显示的标识信息。标题信息的长度范围是 1-64 字节。

3.3.2 基本配置步骤

选择**系统** > **服务配置** > **标题信息**。设置 Console 或 Telnet/SSH 登录标题信息。

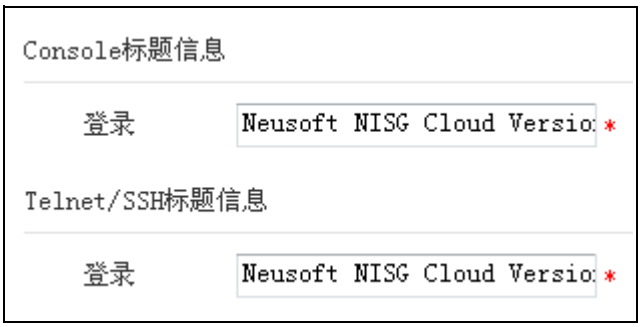


表 29 标题信息命令

banner {**console** | **vty**} *string*	设置 NISG 的标题信息。

3.4 资产汇总

资产汇总对 NISG 硬件和操作系统信息进行了概括总结。

选择**系统** > **资产信息** > **资产汇总**。查看硬件和操作系统信息。

硬件信息	
平台	VA
机箱序列号	000C29D13E9E
CPU制造商	GenuineIntel
CPU型号	Intel(R) Core(TM) i7-3770 CPU @ 3.40GHz
CPU频率	3.39GHz
内存	2048 MB
磁盘0容量	4096 MB
磁盘0型号	Virtual disk
磁盘1容量	0 MB
磁盘1型号	Not installed
主板型号	VMware Virtual Platform
主板修订版	None
BIOS制造商	Phoenix Technologies LTD
BIOS版本	6.00
BIOS日期	06/22/2012

系统信息	
产品型号	VA
内部版本	4.2-BUILD900100

表 30 资产信息命令

show assetinfo	查看资产信息。

3.5 版权信息

选择**系统** > **资产信息** > **版权信息**。查看 NISG 遵循的源组织协议和版权信息。

3.6 系统时间

- 3.6.1 概述
- 3.6.2 基本配置步骤
- 3.6.3 配置参数说明

3.6.1 概述

管理员可以通过以下操作设置系统时间：

- 手动校时

  NISG 系统时间范围为 1970 年 1 月 1 日 0 时 0 分 0 秒至 2037 年 12 月 31 日 23 时 59 分 59 秒。

- NTP 校时

  NISG 支持 NTP 校时，实现系统立即校时或自动周期性校时。自动校时默认为禁用。在启用 NTP 校时前，要先设置 NTP 服务器地址。 NISG 支持一个主服务器和两个备份服务器。进行 NTP 校时时， NISG 最先向主 NTP 服务器发出校时请求。

  NISG 支持 NTP 同步认证功能，默认为禁用。启用此功能前，要与 NTP 服务器管理员确定与每个 NTP 服务器对应的唯一的密钥 ID 和预共享密钥。

- 时区设置

  管理员可以查看和设置 NISG 系统时区。在所设置的时区内，还可以启用或关闭夏令时功能。

3.6.2 基本配置步骤

选择**系统** > **维护** > **日期时间**。

1. 手动校时。点击**当前时间**所对应的 ，在弹出的**当前时间**窗口手动设置系统时间。

2. NTP 校时。启用立即同步或自动周期性同步，设置 NTP 服务器、同步周期及最大时间误差。启用同步认证。

3. 设置时区，启用或禁用夏令时。

配置注意事项

- 要设置系统时间，需要以根系统管理员身份登录。
- 配置完时区后，需要保存当前配置并重新启动系统，以保证时区配置生效。

表 31 系统时间命令

time *date time*	手动同步系统时间。
ntp auto-syn {enable | disable}	启用或禁用 NTP 周期性校时。
ntp synchronize	启用或禁用 NTP 立即校时。
ntp authentication {enable | disable}	启用或禁用 NTP 认证。
ntp server {server1 | server2 | server3} {*ipv4* | *domain_name*} [**key_id** *id_num* **key** *password*]	添加 NTP 服务器。
unset ntp server {server1 | server2 | server3}	删除 NTP 服务器。
ntp auto-syn adjust *max_adjustment*	设置最大时间误差。
timezone *timezone_id*	设置系统时区。
timezone dst {on default | off}	启用或禁用夏令时。

3.6.3 配置参数说明

表 32 手动校时配置信息

参数	说明
日期	输入格式为 YYYY-MM-DD。
时间	输入格式为 HH:MM:SS。 • 小时的取值范围是 0~23。 • 分的取值范围是 0~59。 • 秒的取值范围是 0~59。

表 33 NTP 校时配置信息

参数	说明
NTP 校时	启用 NTP 校时，需要设置主备服务器 IP 地址或域名： • IP 地址的范围为 [1-223].[0-255].[0-255].[0-255]。 • 域名长度为 2 ～ 255 字节。
认证	当开启同步认证时，需要设置主备服务器密钥 ID 和预共享密钥： • 密钥 ID：取值范围为 1-65535。 • 预共享密钥：字符串，长度为 1-32 字节。 密钥 ID 和预共享密钥必须成对出现。
更新系统时钟	NTP 自动校时周期，可以选择每月、每周、每天。系统默认每周一 23:00 自动校时。
最大时间误差	系统当前时间与 NTP 服务器时间的最大允许差值。最大时间误差取值范围为 0-3600 秒，默认为 0 秒。 • 仅当系统时钟与 NTP 服务器时间的差值小于最大时间误差时， NISG 才会按照 NTP 服务器的时间校时。 • 当最大时间误差值为 0 时，只要系统时钟与 NTP 服务器时间存在差值， NISG 就会按照 NTP 服务器时间调整系统时间。

表 34 时区配置信息

参数	说明
时区	当前系统所设置的时区。默认时区为 GMT+8:00 中国 上海 /（北京）。
启用夏令时	启用或禁用夏令时。默认为禁用。

3.7 License

- 3.7.1 概述
- 3.7.2 基本配置步骤
- 3.7.3 配置参数说明

3.7.1 概述

申请 License，需要获取 NISG 的序列号和型号信息 （显示于**主页** > **系统信息**）。

1. 激活 （首次安装）：
   a. 选择**主页 > 系统信息**。
   b. 点击**序列号**对应的**激活**按钮。
      - 在**输入 License** 文本框中，手动输入 License 字符串。
      - 点击**自动获取 License**，输入创建客户订单时自动生成的 Business ID。
2. License 维护。选择**系统** > **维护** > **License**：
   - 输入 Business ID，点击**自动获取 License**，连接 License 服务器。认证成功后，License 服务器会自动返回设备 License，并自动上载 License。
   - 点击**导入**，导入 License 文件或手动输入 License 字符串。

当 NISG 上存在可用 License 时，新上载的 License 将覆盖原有 License。要成功上载其他功能的 License，必须先上载 FW 功能的 License。 NISG 最多可以上载 20 个 License。如果不同的 License 限制了同一功能，该功能的参数以后上载的 License 为准。

3.7.2 基本配置步骤

选择**系统** > **维护** > **License**。

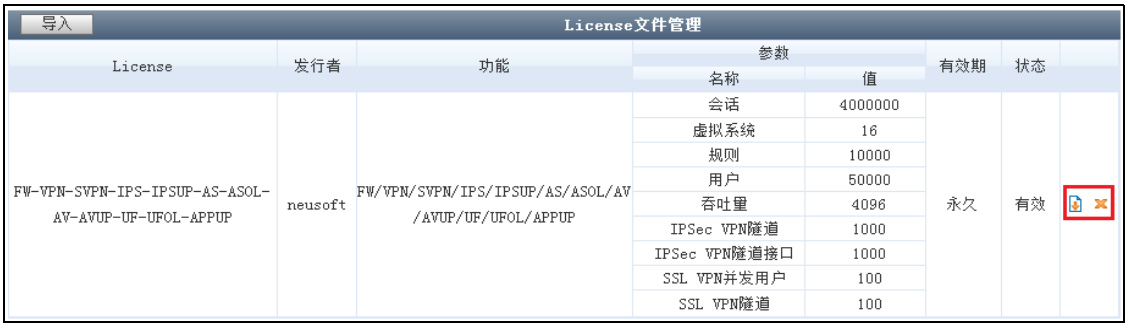
1. 查看 License 信息。

功能	参数	值	有效期
防火墙	虚拟系统	2	永久
	用户	50000	永久
	规则	10000	永久
	会话	1000000	永久
IPSec VPN	IPSec VPN隧道接口	1000	永久
	IPSec VPN隧道	1000	永久
SSL VPN	SSL VPN隧道	50	永久
	SSL VPN并发用户	50	永久
	ET	20140516	永久
IPS			永久
防病毒			永久
反垃圾邮件			永久
URL过滤			永久
IPS更新			2019-03-21
防病毒更新			2019-03-21
反垃圾更新			2019-03-21
URL过滤更新			2019-03-21
应用更新			2019-03-21

2. 输入 Business ID，并点击**自动获取 License**。 Business ID 是客户订单的唯一标识，在创建客户订单时自动生成。

3. 上载 License 文件。

4. 删除或下载 License。



配置注意事项

- 要下载License到本地或指定的TFTP/SFTP服务器对License进行备份，请以根管理员或根系统管理员身份登录。
- 通过 CLI 上载 License 时， License 文件名不能包含空格。
- 某些License上载后需要重新启动系统才能生效，如带有FW和VPN功能的License。

表 35 License 命令

show license	查看 License 信息。
license import from {**x**/**zmodem** | **tftp** *ip_tftp file_name* | **sftp** *ip_sftp* **username** *user_name* **password** *password file_name*}	上载 License 文件。
license word import *string*	上载 License 字符串。
unset license word *trait_name*	删除 License 文件。
license download to {**x**/**zmodem** *trait_name* | **tftp** *ip_tftp trait_name* | **sftp** *ip_sftp* **username** *user_name* **password** *password file_name*}	下载 License 文件。
license automatic activate	自动激活 License。

3.7.3 配置参数说明

表 36 无 License 时的操作权限

模块	权限
系统	• 查看资产及版权信息 • 查看和设置系统信息、系统时间、 Licenses、管理用户及访问服务 • 修改根管理员和根系统管理员密码 • 使用 ping、 ping6 和 traceroute • 重启、重置和关闭系统
网络	• 查看邻居发现和 DHCPv6 配置 • 查看和配置接口、 STP、安全域、 DNS 主机、 DNS 代理、 DHCP 服务器、 DHCP 作用域、缺省路由、多播路由、源 / 目的地址转换、地址映射、 DVMRP 和 IGMP Snooping
防火墙	• 查看和配置访问策略、多播策略和缺省策略
监控	• 查看拓扑、接口流量、 STP、路由、地址转换、 DVMRP 邻居和 IGMP Snooping 状态等监控信息

表 37 NISG License 的控制对象

功能	详细信息
防火墙	虚拟系统、用户、策略、会话的最大数目及有效期。
IPSec VPN	IPSec VPN 隧道及隧道接口的最大数目及有效期。
SSL VPN	SSL VPN 隧道及 SSL VPN 并发用户的最大数目及有效期。
UTM 相关	IPS、防病毒、反垃圾邮件、应用控制及 URL 过滤功能及 IPS、防病毒、反垃圾邮件、应用控制及 URL 过滤功能规则更新。

3.8 系统升级

- 3.8.1 概述
- 3.8.2 基本配置步骤
- 3.8.3 配置参数说明

3.8.1 概述

系统升级通过安装升级包和增强升级包实现。安装升级包仅用于手动升级，增强升级包用于手动和自动升级。

- 手动升级

  管理员通过 WebUI 或者 CLI 将获取的升级包手动上载到系统，完成升级。

- 自动升级

  NISG 支持立即升级和自动周期性升级。启用自动周期性升级，管理员需要设置升级模式和升级周期。

- 升级历史

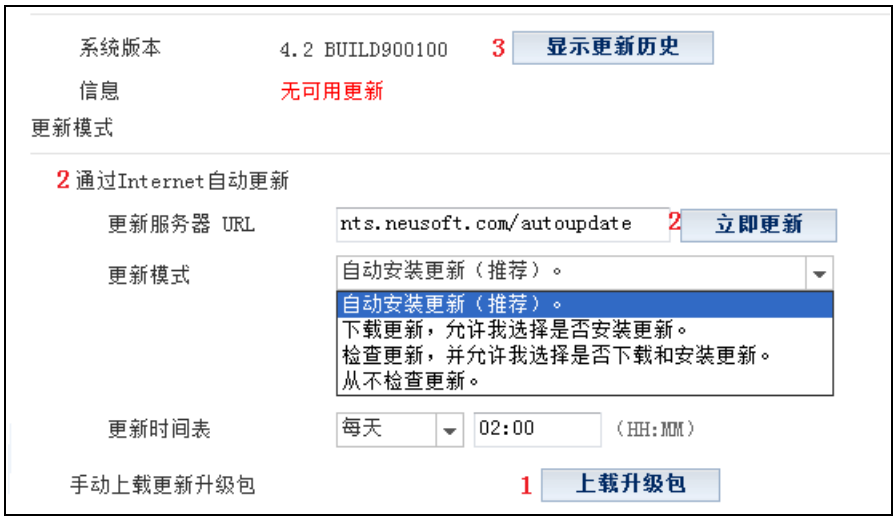
  NISG 最多支持 50 条升级记录。

3.8.2 基本配置步骤

选择**系统** > **系统升级** > **安装升级包**。

1. 手动升级：
   - 通过 WebUI 将本地升级包通过 HTTPS 上载。
   - 通过 CLI 将本地升级包通过 X/Zmodem 或者 SFTP/TFTP 上载。
2. 自动升级：
   - 点击**立即更新**立即升级系统。
   - 设置升级服务器地址、升级模式及升级周期进行自动周期性升级。

3. 查看或导出升级记录。



配置注意事项

- 当系统无法连接升级服务器时，自动升级模式下会重试 3 次，立即升级模式下只重试 1 次。如果仍然无法连接，那么系统将等待至下一次升级周期开始。
- 当更新多个增强升级包时，系统将一次完成所有的升级操作。有些增强升级包安装后重启才能生效，此时 NISG 会提示用户重启系统。请在执行该操作前，确认已保存了重要的配置信息，以防配置丢失。

表 38 系统升级命令

show package upgrade config	查看系统升级配置。
package upgrade immediately	立即进行系统升级。
package upgrade from {**x/zmodem** | **tftp** *ip_tftp file_name* | **sftp** *ip_sftp* **username** *user_name* **password** *password file_name* | **internal** *file_name*}	安装系统升级包。
package upgrade server {*server_name* | *server_ip*}	设置系统升级服务器。
package upgrade mode {**install update-schedule** {**daily** *time* | **weekly** *weekday* | **monthly** *date*} | {**download** | **check**} **check-schedule** {**daily** *time* | **weekly** *weekday* | **monthly** *date*} | **never**}	设置系统升级模式。
show package upgrade config	查看系统升级配置。

3.8.3 配置参数说明

表 39 系统升级配置信息

参数	说明
更新信息	• 系统版本：当前升级包的版本信息。 • 信息：可用升级包信息。
更新模式	可以选择通过 Internet 自动更新或手动上载升级包更新。选择自动更新，需设置： • 更新服务器 URL：默认的升级服务器地址为 nts.neusoft.com/autoupdate。 • 更新模式：NISG 支持四种自动更新模式： - 下载更新，允许我选择是否安装更新。 - 自动安装更新 （推荐）。 - 检查更新，并允许我选择是否下载和安装更新。 - 从不检查更新。默认的升级模式为从不检查更新。 • 检查时间表：自动安装升级包的周期。周期可以设置为每天、每周或者每月中的某一固定时刻。系统默认升级时间为每天 02:00 开始自动升级。

3.9 安装升级包管理

选择**系统** > **系统升级** > **管理安装升级包**。

1. 切换安装升级包。
2. 删除安装升级包。

配置注意事项

- 只有根系统管理员可以切换或删除安装升级包。
- 安装升级包后，系统将重启，请在系统重新启动之前，确认已保存了重要的配置信息，以防配置丢失。
- NISG 同时只启用一个安装升级包。正在使用的安装升级包不能被删除。

表 40 安装升级包命令

system switch *file_name*	切换系统版本。
delete system *file_name*	删除非启用状态的安装升级包。

3.10 增强升级包管理

选择**系统** > **系统升级** > **管理增强升级包**。

1. 启用或禁用增强升级包。
2. 删除增强升级包。

配置注意事项

- 只有根管理员和根系统管理员能够查看增强升级包信息。
- 根系统管理员可以启用、禁用以及删除增强升级包。
- 手动升级中，每次只允许上载一个增强升级包。自动升级中，升级服务器可以一次上载多个增强升级包。
- 启用或删除增强升级包之后，系统可能会提示重新启动。请在执行该操作前，确认已保存了重要的配置信息。
- 通过禁用增强升级包，管理员可以将 NISG 系统回退到升级之前的版本。最多可保留一个增强升级包，支持回退一次。

表 41 增强升级包命令

patch {enable | disable}	启用或禁用增强升级包。
delete patch *file_name*	删除增强升级包。

3.11 访问服务

NISG 为远程主机提供多种服务，包括支持远程主机以 Telnet、 SSH、 Web 方式访问 NISG，使用 Ping 服务测试远程主机和 NISG 之间的连通性，以及支持根管理员远程访问 NISG。

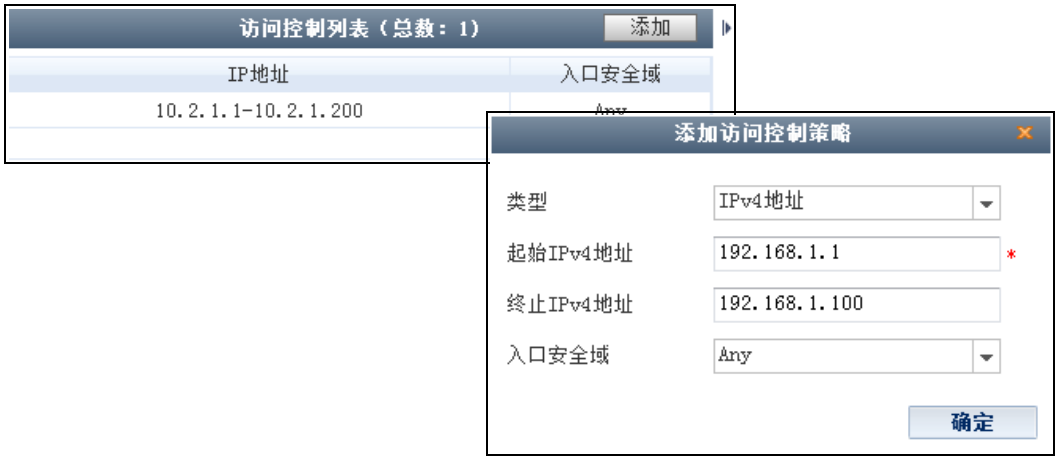
- 3.11.1 基本配置步骤
- 3.11.2 配置参数说明

3.11.1 基本配置步骤

选择**系统** > **服务配置** > **访问设置**。

1. 启用访问服务并设置服务端口号。

2. 创建访问控制策略。



3. 允许或拒绝根管理员远程登录。

表 42 访问服务命令

show service [**telnet** | **web** | **ping** | **ssh**]	查看访问服务信息。
show root-net-login	查看根管理员远程访问控制。
service {**telnet** | **web** | **ping** | **ssh**} {**on** | **off**}	启用或禁用 Telnet、 Web、 Ping 或 SSH 访问服务。
service {**telnet** | **ssh** | **web**} **port** *num*	设置服务端口号。
service {**telnet** | **web** | **ping** | **ssh**} **allow** {**mgt-interface** | **zone** {*zone_name* | **any**} } *start_ip* [*end_ip*]	添加访问控制策略。
unset service {**telnet** | **web** | **ping** | **ssh**} [**allow** {**mgt-interface** | **zone** {*zone_name* | **any**}} *start_ip* [*end_ip*]]	删除访问控制策略。
service root-net-login {**enable** | **disable**}	允许或阻断根管理员远程登录。

3.11.2 配置参数说明

表 43 访问服务配置信息

参数	说明
服务状态	访问服务的状态。 Telnet 缺省为关闭， SSH、 Web 和 Ping 缺省为开启。
端口号	Telnet、 SSH 和 Web 端口范围均为 1-65535，缺省端口号分别为 23、 22 和 443。
访问控制列表	包含访问控制策略。每个访问控制列表最多支持 32 条策略。每条策略限定了 IP 地址范围和入口安全域。 IP 地址范围和入口安全域范围内的主机可以通过访问服务访问 NISG。 • Web、 SSH 和 Ping 服务默认的 IP 地址范围是 0.0.0.0-255.255.255.255，默认的入口安全域为 Any。 • 如果访问控制列表为空，即使服务为启用状态， NISG 仍拒绝任何主机以任意服务访问 NISG。
root 用户访问控制	允许或阻断根管理员远程访问 NISG，缺省为允许。

3.12 SNMP

- 3.12.1 概述
- 3.12.2 基本配置步骤
- 3.12.3 配置参数说明

3.12.1 概述

NISG 支持 SNMP，可以作为被管设备接受管理站的访问，允许管理站查询 NISG 的状态信息。

- 支持的 SNMP 版本

  NISG 支持 SNMPv1、 v2 和 v3。

- SNMP 用户

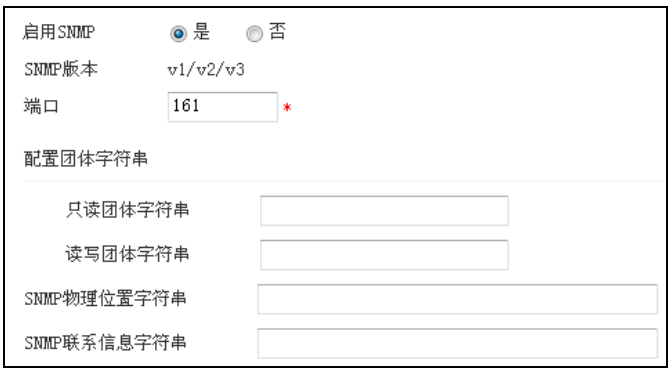
  在 SNMPv3 中，管理站和被管设备之间通过 SNMP 用户进行认证。 NISG 作为被管设备接受管理站的访问时，会根据 NISG 上保存的 SNMP 用户信息对管理站进行认证。

  SNMP 用户信息与系统用户信息是分别保存的，尽管 SNMP 用户可以和系统用户重名。

3.12.2 基本配置步骤

选择**系统** > **服务配置** > **SNMP 配置**。

1. 查看 SNMP 配置信息；启用或禁用 SNMP；设置端口号和团体、物理位置及联系信息字符串。



2. 配置 SNMP 用户。

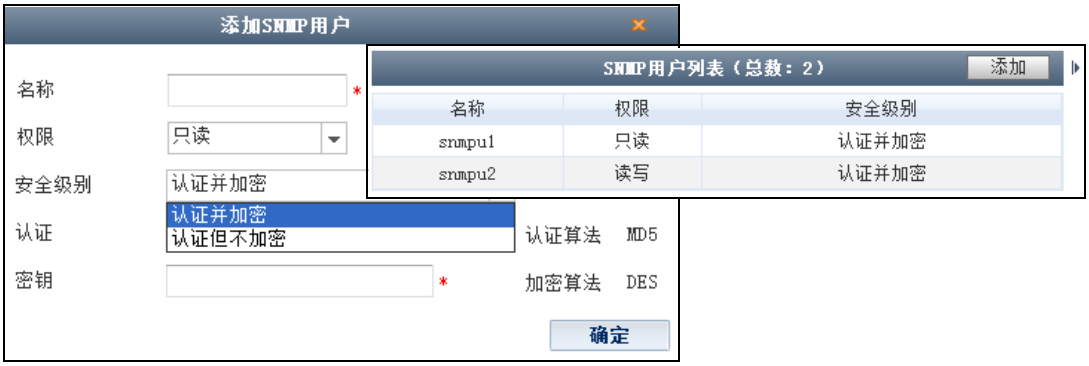


表 44 SNMP 命令

show snmp {daemon | port | community {read-only | read-write} | location | contact}	查看 SNMP 配置信息。
snmp daemon {on | off }	启用或禁用 SNMP。
snmp port *port_num*	设置 SNMP 服务端口号。
snmp community *string* **{read-only | read-write}**	添加指定权限的团体字符串。
snmp {location | contact} *string*	添加物理位置或联系信息字符串。
unset snmp {community {read-only | read-write} | location | contact}	删除团体、物理位置或联系信息字符串。
show snmp usm user [*user_name*]	查看 SNMP 用户信息。
snmp usm user *user_name* **seclvl authNoPriv authpro MD5 authpassphrase** *auth_password* **{read-only | read-write}**	添加安全级别为认证但不加密的 SNMP 用户。
snmp usm user *user_name* **seclvl authPriv authpro MD5 authpassphrase** *auth_password* **privpro DES privpassphrase** *privacy_password* **{read-only | read-write}**	添加安全级别为认证并加密的 SNMP 用户。
unset snmp usm user [*user_name*]	删除 SNMP 用户。

3.12.3 配置参数说明

表 45 SNMP 配置信息

参数	说明
启用 SNMP	启用或禁用 SNMP 功能。缺省为禁用。
SNMP 版本	NISG 支持 SNMPv1、 SNMPv2 和 SNMPv3。
端口	端口范围为 1~65535。默认端口为 161。
团体字符串	管理站和被管对象之间进行身份识别的字符串。 团体字符串包括两种类型：只读和读写。由字母、数字、 @、下划线、连字符或句点构成，长度为 0-128 字节。
SNMP 物理位置字符串	描述 NISG 设备物理位置的信息。 由字母、数字、 @、下划线、连字符或句点构成，长度为 0-128 字节。
SNMP 联系信息字符串	管理员的联系信息。 由字母、数字、 @、下划线、连字符或句点构成，长度为 0-128 字节。

表 46 SNMPv3 用户配置信息

参数	说明
名称	SNMP 用户的名称。长度 1-63 字节，UTF-8 字符。不能包含空格和以下字符：* ? , " ' \ < > & #。 NISG 最多支持 5 个 SNMP 用户。
权限	SNMP 用户的权限： • 只读：只可以查询 NISG 的状态信息。 • 读写：既可以查询 NISG 的状态信息，又可以修改 NISG 的部分配置信息。可修改的配置信息包括团体字符串、物理位置字符串和联系信息字符串。
安全级别	SNMP 数据包在网络上传输的安全级别，包括认证并加密和认证但不加密。缺省为认证并加密。
认证	用于确认身份的字符串。长度 8-128 字节， ASCII 字符。不能包含空格和以下字符：? " ' < > &。
认证算法	认证所使用的算法。 NISG 将 MD5 作为认证算法。
密钥	用于信息加密的字符串。长度 8-128 字节， ASCII 字符。不能包含空格和以下字符：? " ' < > &。
加密算法	加密使用的算法。 NISG 将 DES 作为加密算法。

3.13 管理用户

- 3.13.1 概述
- 3.13.2 基本配置步骤
- 3.13.3 配置参数说明

3.13.1 概述

- 3.13.1.1 管理用户
- 3.13.1.2 配置锁

3.13.1.1 管理用户

NISG 的管理角色包括：

- 根管理员

  从属于根系统，不能被删除。其缺省用户名和初始口令分别为 “root” 和 “Neusoft”。

- 根系统管理员

  由根管理员创建和管理。具有读写权限，可以查看和设置整个 NISG 的配置信息。缺省根系统管理员名称为 “Neusoft”，初始密码为 “Neusoft”。

- 根系统审计员

  由根系统管理员创建和管理。具有只读权限，只可以修改其自身的信息和查看 NISG 的配置信息，不可以设置 NISG。

- Vsys 管理员

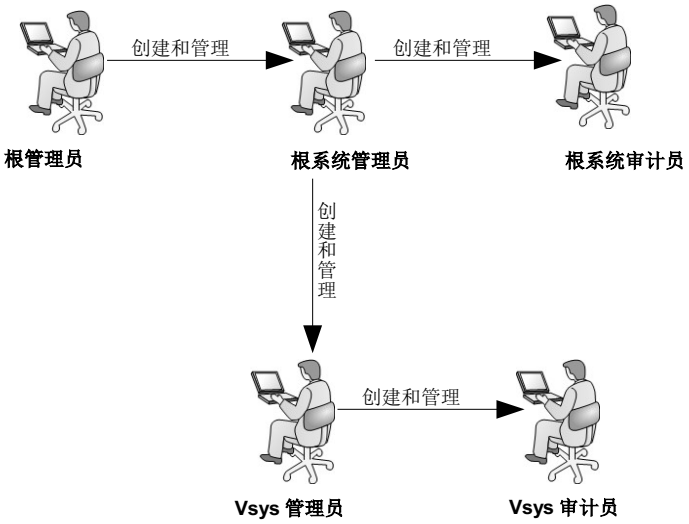
  由根系统管理员创建、管理和分配 Vsys 资源。具有读 / 写权限，可以查看和同时设置管理一个或者多个虚拟设备信息。

- Vsys 审计员

  由 Vsys 管理员设置、管理和分配 Vsys 资源。具有只读权限，只能查看 NISG 的配置信息，不能设置 NISG。

管理角色之间的关系如图 2 所示：

图 2 管理角色关系



3.13.1.2 配置锁

为了防止配置冲突，NISG 采用了配置锁机制。同一时间只允许一个管理用户对 NISG 进行配置操作。

- WebUI 中的配置锁

  以 WebUI 方式管理 NISG 时，如果想要修改 NISG 的配置信息，在登录成功后，需选择覆盖配置锁。如果没有选择覆盖配置锁，那么在 WebUI 界面的右上方可以看到，可以点击该图标获得配置锁。之前已获得配置锁的管理员将立即失去配置锁，只能进行查看操作。

  点击退出登录，即可自动释放配置锁。如果获得了配置锁但未退出登录而直接关闭浏览器，那么配置锁会一直有效直到会话超时或者配置锁被覆盖。所以修改配置完成后，退出登录时，建议释放配置锁，以使其他用户能够及时申请到配置锁。

  以 WebUI 方式管理 NISG 时，获得配置锁后如果 30 分钟内无任何操作， NISG 将自动断开本次连接，同时释放配置锁。

- CLI 中的配置锁

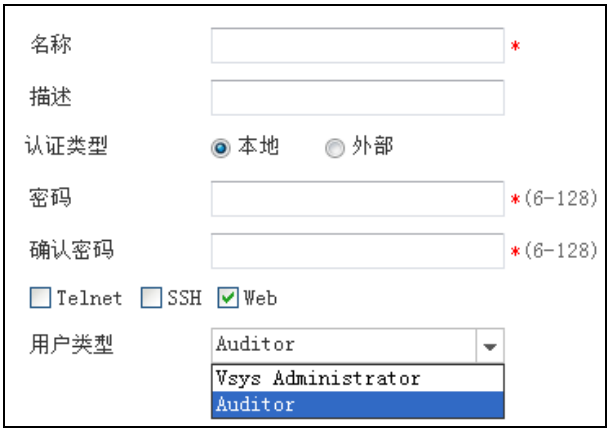
  以 CLI 方式管理 NISG 时，管理员登录后，如果配置锁未被其他管理员占用，则可以通过 CLI 命令 “**configure mode**” 进入全局配置模式，进行配置操作。如果配置锁正在被其他管理用户占用，可以通过 CLI 命令 “**configure mode override**” 覆盖其他管理员的配置锁。管理员退出全局配置模式时，可以通过 CLI 命令 “**exit**”，释放配置锁。

3.13.2 基本配置步骤

选择**系统** > **认证** > **管理用户**。

1. 查看或删除管理用户，修改管理用户密码。

2. 创建或编辑管理用户。



配置注意事项

- 管理用户名称须唯一。
- 根系统管理员默认从属于根系统。根系统管理员可以分配给多个虚拟系统，获得相应 Vsys 管理员的权限。

表 47 管理用户命令

show user administrator	查看管理用户信息。
password	修改管理用户口令。
user administrator	创建管理用户。
unset user administrator	删除管理用户。

3.13.3 配置参数说明

表 48 管理角色配置权限

管理角色	配置权限
根管理员	• 设置管理用户 - 创建、删除和编辑根系统管理员 - 修改根管理员和根系统管理员口令 • 设置 NISG - 上载、下载和删除 License - 重启和关闭 NISG - 为管理用户设置本地认证 - 切换语言 • 查看系统配置信息
根系统管理员	• 设置管理用户 - 创建、删除和编辑根系统审计员和 Vsys 管理员 - 修改根系统审计员和 Vsys 管理员口令 - 指定根系统管理员为 Vsys 管理员 • 设置 NISG - 切换 Vsys - 设置系统维护、网络配置、服务配置、对象、用户与认证、高可用性、路由、地址转换、策略、虚拟专用网、攻击防御、统一威胁管理及虚拟系统 • 查看系统配置信息
根系统审计员	• 修改根系统审计员的口令 • 查看系统配置信息
Vsys 管理员	• 设置管理用户 - 创建、删除和修改当前 Vsys 的审计员 - 修改 Vsys 审计员和 Vsys 管理员的口令 • 设置虚拟系统 - 切换到其他 Vsys - 设置当前 Vsys • 查看当前虚拟系统配置信息
Vsys 审计员	• 修改 Vsys 审计员的口令 • 查看当前虚拟系统配置信息

表 49 管理用户配置信息

参数	说明
名称	管理用户名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：* ? , " ' \ < > & #。
描述	管理用户的描述信息。长度 0-255 字节， UTF-8 字符。不能包含以下字符：? " ' \ < > &。
认证类型	管理用户认证类型，包括本地认证和远程认证。默认选择本地认证。
密码	根系统管理员或 Vsys 管理员登录 NISG 的密码。长度范围为 6-128 个字符。
登录类型	管理用户登录方式，包括 Telnet、 SSH 和 Web。 Web 为缺省类型。
虚拟系统列表	Vsys 管理员或 Vsys 审计员所属的 Vsys。一个 Vsys 管理员可属于多个 Vsys。一个 Vsys 审计员只能属于一个 Vsys。

3.14 网络用户

- 3.14.1 概述
- 3.14.2 基本配置步骤
- 3.14.3 配置参数说明

3.14.1 概述

网络用户指通过 NISG 认证和授权后可访问网络资源的用户。 NISG 网络用户包括：

- WebAuth 用户

  管理员需要为 NISG 上集成的 WebAuth 服务器指定 IP 地址和端口以供 WebAuth 用户登录。WebAuth 用户需要预先知道认证服务器的访问方式和合法的用户名和口令，才可以进行网络访问。 WebAuth 用户可以通过主动或被动认证登录。关于 WebAuth 认证的详细信息，请参见 3.16 WebAuth 配置。

- IPSec VPN 用户

  IPSec VPN 用户包括 Xauth 用户和 L2TP 用户，可以通过外部认证服务器认证或本地认证。 NISG 将 IPSec VPN 用户定义为远程拨号用户来进行管理。 IPSec VPN 用户要接入 VPN 前，必须接受 NISG 对其进行的身份认证。认证通过后，方可接入 VPN。

- SSL VPN 用户

  SSL VPN 用户指通过 SSL VPN 服务接入访问的用户。 SSL VPN 用户可以划入 SSL VPN 用户组成为组内成员。 SSL VPN 用户可通过本地数据库或外部认证服务器进行认证。

NISG 允许网络用户进行多点登录。网络用户可以通过单点或多点登录到 NISG。

NISG 对网络用户的在线时间和流量进行记录，通过 RADIUS 服务器对用户产生的流量进行计费。如果一个网络用户在规定的超时时间内没有流量， NISG 则会认为其下线。超时时间可以针对用户单独配置。如果不配置，则超时时间取网络用户所在虚拟系统默认配置的时间。

对未在本地配置的网络用户， NISG 提供默认配置。管理员可以通过点击超链接设置未在本地配置的用户的默认配置，包括用户超时时间及用户类型等信息。

3.14.2 基本配置步骤

选择**系统** > **认证** > **网络用户**。

1. 查看、删除、启用或禁用网络用户，修改用户密码。

2. 创建或编辑网络用户。

3. 设置未在本地配置的网络用户的默认配置。

表 50 网络用户命令

show user authuser	查看网络用户信息。
user authuser enable,disable	启用或禁用网络用户。
user authuser password	修改网络用户密码。
user authuser	创建网络用户。
unset user authuser	删除网络用户。

3.14.3 配置参数说明

表 51 网络用户配置信息

参数	说明
名称	网络用户名称。长度 1-63 字节，UTF-8 字符。不能包含空格和以下字符：* ? , " ' \ < > & #。
认证类型	网络用户的认证类型，包括本地认证和外部认证。默认为本地认证。
用户类型	网络用户的类型，包括 WebAuth、 IPSec VPN 和 SSL VPN。缺省类型为 WebAuth。
超时时间	网络用户的超时时间，范围是 0-3600 秒，缺省为 300 秒。如果配置为 0 秒，则不限制该网络用户的超时时间，只要用户不主动下线，则永远不会下线 （管理员强制其下线除外）。
引用	引用该用户的访问策略列表。
启用	启用或禁用网络用户。只有启用后，网络用户才能通过 NISG 访问网络资源。
密码	网络用户的认证密码。长度 1-127 个字节。
分配的 IP	为 IPSec VPN 和 SSL VPN 用户分配地址，包括用户 IP 地址、主备 DNS 服务器地址及主备 WINS 服务器地址。用户地址可以是静态 IP 或从 IP 地址池获得。
IPSec VPN 配置	IPSec VPN 用户配置： • 用户类型：包括 Xauth 和 L2TP。 • ID 类型：包括 IPV4_ADDR、 FQDN、 USER_FQDN、 DER_ASN1_DN 和 KEY_ID。

3.15 用户认证

- 3.15.1 概述
- 3.15.2 基本配置步骤
- 3.15.3 配置参数说明

3.15.1 概述

- 3.15.1.1 本地 / 外部认证
- 3.15.1.2 外部认证服务器

3.15.1.1 本地 / 外部认证

在 NISG 中，管理用户及网络用户的认证方式分为两种，可以通过本地数据库或外部认证服务器进行认证。

- 本地数据库认证

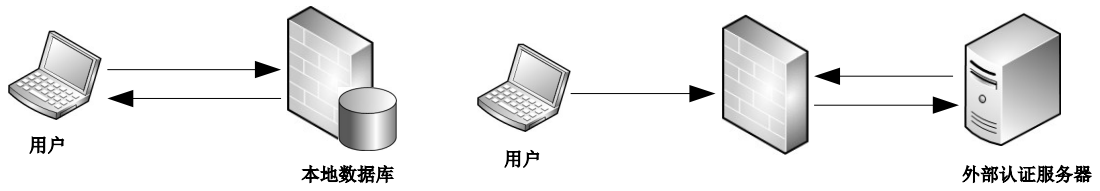
  本地认证中，用户认证信息保存在 NISG 本地数据库中。用户登录时需要向 NISG 提供用户名和密码。 NISG 将用户信息与本地数据库中保存的用户信息进行匹配，如果一致，则认证成功。

- 外部服务器认证

  外部认证中，用户认证信息保存在管理员配置的外部认证服务器中。 NISG 收到用户的登录请求后，会向配置的外部认证服务器发出验证请求。服务器将用户提供的信息与存储的信息进行匹配。如果一致，则认证成功。

本地认证的优先级高于外部认证。本地创建的管理用户，即使认证方式设为外部， NISG 仍然首先查找本地数据库进行本地认证，本地无身份信息后查找外部认证服务器。本地认证和外部认证如图 3 所示。

图 3 本地 / 外部认证



3.15.1.2 外部认证服务器

NISG 支持以下四种外部认证服务器：

- RADIUS 服务器

  NISG 还可以通过 RADIUS 服务器实现实现对网络用户的计费功能。

- LDAP 服务器
- Active Directory 服务器
- eDirectory 服务器

  LDAP、 Active Directory 及 eDirectory 服务器认证过程基于 LDAPv3。

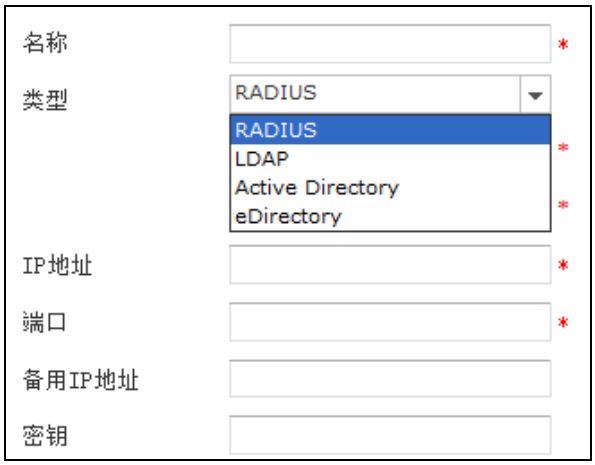
NISG 支持备用服务器。当 NISG 与主服务器无法建立连接或者主服务器在默认超时时间（30 秒）内无应答时，启用备用服务器。主备服务器端口必须一致。

3.15.2 基本配置步骤

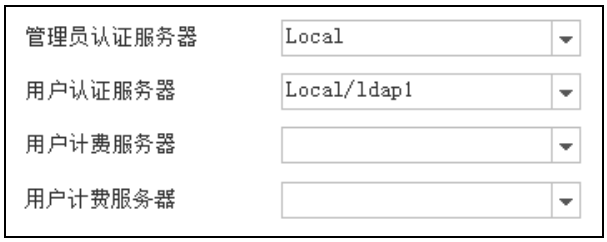
选择**系统** > **认证** > **认证服务器**。

1. 查看或删除认证服务器。

2. 添加或编辑认证服务器。



3. 选择**系统 > 认证 > 认证配置**。为管理用户和网络用户设置认证服务器。



配置注意事项

- 外部认证服务器名称须唯一。
- NISG 最多支持四个外部认证服务器。
- 正在被使用的服务器不可被直接删除。如果要删除，请先指定其他外部认证服务器。
- 修改认证服务器的配置参数，不影响已经完成认证的连接，只对更改之后发起的认证生效。
- 根管理员仅可以设置管理用户的认证方式，且只能将认证方式设置为本地。

表 52 认证配置命令

server authentication type administrator | authuser	指定管理用户或网络用户的认证服务器。
server account	指定网络用户的计费服务器。
unset server account	删除计费服务器。
show server authentication	查看认证服务器。
show server account	查看计费服务器。

表 53 认证服务器命令

radius | ldap | active-directory | edirectory server	添加 RADIUS、 LDAP、 Active Directory 或 eDirectory 服务器。
unset radius | ldap | active-directory | edirectory server	删除 RADIUS、 LDAP、 Active Directory 或 eDirectory 服务器。
show radius | ldap | active-directory | edirectory server	查看 RADIUS、 LDAP、 Active Directory 或 eDirectory 服务器。

3.15.3 配置参数说明

表 54 认证服务器和计费服务器配置信息

参数	说明
管理员认证服务器	为管理用户指定认证服务器，可以是本地或者指定的外部服务器。缺省为本地认证。
用户认证服务器	为网络用户指定认证服务器，可以是本地或者指定的外部服务器。缺省为本地认证。
用户计费服务器	为网络用户指定计费服务器， RADIUS 服务器有计费功能。缺省为空，即不进行计费。

表 55 认证服务器配置信息

参数	说明
名称	认证服务器名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & #。
IP 地址 / 域名	认证服务器的 IPv4 地址或域名。 NISG 将向此 IP 地址或域名发送认证请求。域名长度为 2-255 字节。
端口	认证服务器端口号。 NISG 将向此端口发送认证请求。端口的取值范围为 1-65535。 • RADIUS：缺省的认证和计费端口号分别为 1812 和 1813。 • LDAP/Active Directory/eDirectory：当安全连接类型为 None 或者 STARTTLS 时，缺省端口号为 389 ；当安全连接的类型为 SSL / TLS 时，缺省端口号为 636。
备用 IP 地址 / 域名	认证服务器的备用 IPv4 地址或域名。域名长度为 2-255 字节。
安全连接	如果传输需要使用 SSL 加密，则需启用安全连接。安全连接类型包括 SSL/TLS 和 STARTTLS。
证书	启用安全连接后服务器使用的 CA 证书。
公共名标识符	用来识别在 LDAP 服务器中输入的个体的标识符。由除空格和问号外的任意 UTF-8 字符组成。取值范围为 0-80 字节。
识别名称	认证服务器在使用公共名标识符搜索具体条目前使用的路径。由除空格和问号外的任意 UTF-8 字符组成。取值范围为 0-511 字节。
管理员识别名称	具有管理员权限的用户 DN，用来与认证服务器绑定以获取查询权限。由除空格和问号外的任意 UTF-8 字符组成。取值范围为 0-511 字节。
密钥	• RADIUS：服务器与 NISG 协商的共享密钥，用来验证 RADIUS 数据包的合法性。只有在密钥一致的情况下，彼此才能接收对方发来的数据包，并作出响应。长度范围为 0-64 字节。 • LDAP/Active Directory/eDirectory：具有管理员权限的用户密码。长度范围为 0-127 字节。
状态	认证服务器当前的使用状态。如果正在被使用，其状态显示为 In Use。

3.16 WebAuth 配置

WebAuth 认证对用户通过 NISG 的网络访问进行有效的控制。本节包括：

- 3.16.1 概述
- 3.16.2 基本配置步骤
- 3.16.3 配置参数说明
- 3.16.4 范例：用户认证

3.16.1 概述

WebAuth 认证可以在以下三层接口上开启：

- 以太网接口
- Channel 接口
- 冗余接口
- PPPoE 接口
- VLAN 接口

管理员可以设置 WebAuth 端口号，缺省为 4325。

实现 WebAuth 认证需满足以下条件：

1. WebAuth 认证已启用，用户通过认证接口访问网络。
2. 用户数据包匹配自动重定向策略。
3. 用户为未认证用户。

WebAuth 认证成功后，用户可以实现网络访问。

3.16.2 基本配置步骤

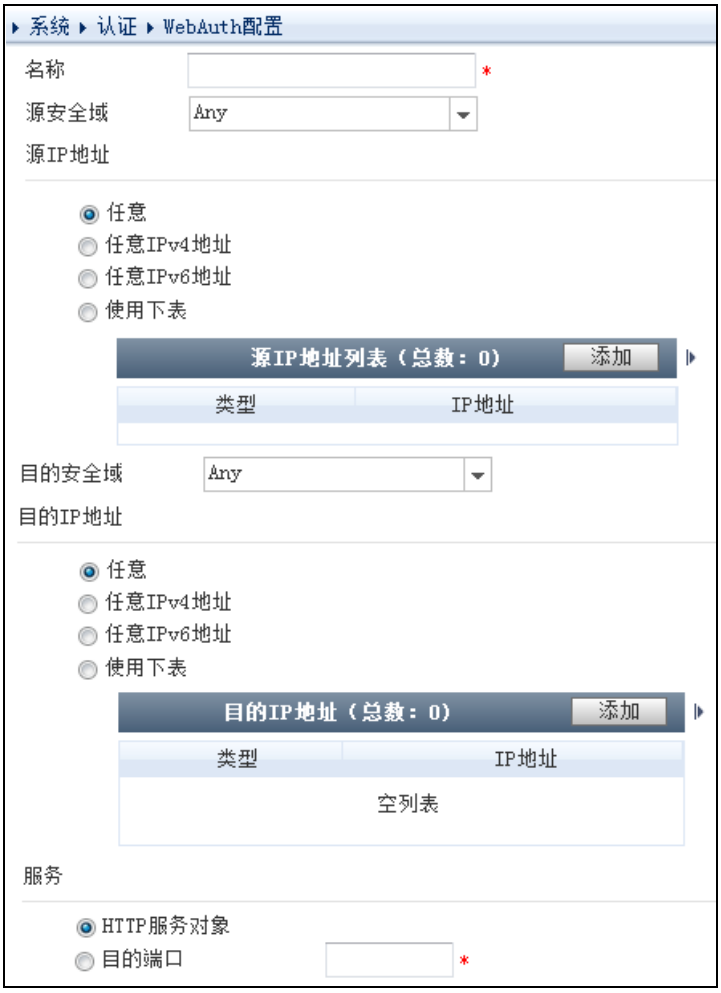
选择**系统** > **认证** > **WebAuth 配置**。

1. 三层接口上开启 WebAuth 认证。

2. 设置 WebAuth 认证成功或失败的标题信息和端口号。

3. 查看或删除 WebAuth 自动重定向策略。

4. 创建或编辑 WebAuth 自动重定向策略。



配置注意事项

- 每个虚拟系统最多支持 64 条自动重定向策略。
- 每条策略中最多可以添加 4096 个源 IP 地址条目和 4096 个目的 IP 地址条目。

表 56 WebAuth 认证命令

webauth banner	设置 WebAuth 标题信息。
webauth auth-port	设置 WebAuth 端口号。
webauth on,off	启用或禁用 WebAuth 认证。
webauth policy	创建 WebAuth 自动重定向策略。
unset webauth policy	删除 WebAuth 自动重定向策略。

3.16.3 配置参数说明

表 57 WebAuth 自动重定向策略配置信息

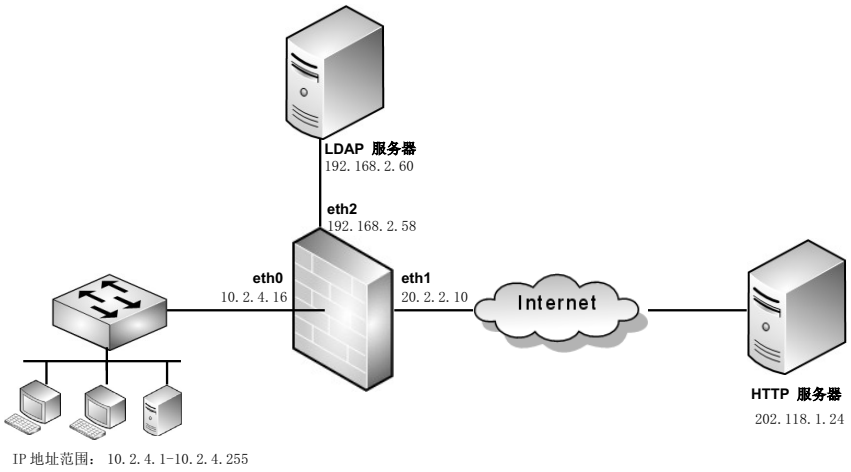
参数	说明
名称	WebAuth 自动重定向策略的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #。每条策略都有独特的名称，在创建后不能修改。
源安全域	发出数据包的安全域。
目的安全域	接收数据包的安全域。
源 IP 地址	发出数据包的 IPv4 或 v6 地址。
目的 IP 地址	接收数据包的 IPv4 或 v6 地址。
服务	进行被动认证连接的端口号，可以是 HTTP 服务对象 （目的端口为 80）或目的端口 （端口范围 1-65535）。

表 58 WebAuth 认证配置信息

参数	说明
WebAuth 标题信息	用户经过 WebAuth 服务器验证身份后返回的提示信息。长度 1-220 字节， UTF-8 字符。不能包含空格和以下字符：？" ' \ < > &。
WebAuth 端口号配置	连接 WebAuth 服务器的端口号。端口号取值范围为 1-65535，缺省为 4325。
接口	启用 WebAuth 功能的接口。此接口可以是除环回接口和隧道接口外的其他所有三层接口。
WebAuth	启用或禁用 WebAuth 功能。

3.16.4 范例：用户认证

本范例中，网络用户 “testuser” 要通过 NISG 访问 IP 地址为 202.118.1.24 的 HTTP 服务器。设置 LDAP 服务器、 WebAuth 认证控制用户访问。



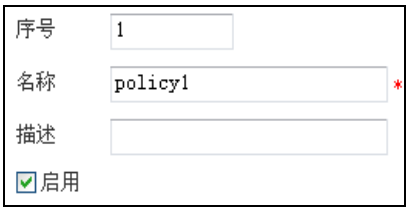
配置步骤如下：

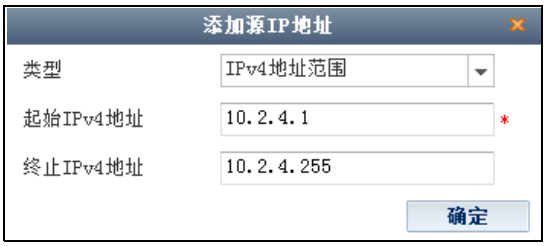
- 3.16.4.1 配置 LDAP 服务器
- 3.16.4.2 NISG 上设置 LDAP 服务器
- 3.16.4.3 设置网络用户认证服务器
- 3.16.4.4 开启 WebAuth 认证
- 3.16.4.5 设定用户 WebAuth 角色
- 3.16.4.6 创建 WebAuth 自动重定向策略

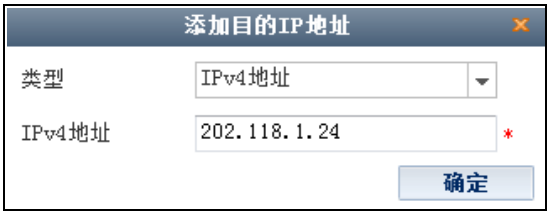
用户认证通过以下方式：

- 3.16.4.7 被动认证
- 3.16.4.8 主动认证

在执行以上列出配置前，需先设置访问策略允许该用户访问。







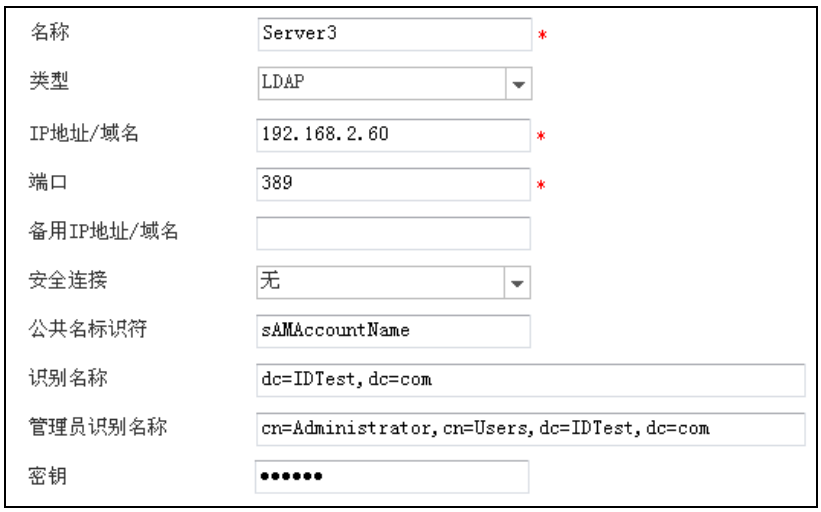
3.16.4.1 配置 LDAP 服务器

1. Windows Server 2003 上安装 Active Directory 服务。
2. 将用户的认证信息存储至新建的 LDAP 服务器。用户名：testuser; 密码：test.12

3.16.4.2 NISG 上设置 LDAP 服务器

提示
服务器配置信息需与以上创建的 LDAP 服务器配置一致。

1. 选择**系统** > **认证** > **认证服务器**。
2. 点击**新建**设置 LDAP 服务器。输入以下服务器信息：
   公共名标示符：sAMAccountName; 识别名称：dc=IDTest,dc=com
   管理员识别名称：cn=Administrator,cn=Users,dc=IDTest,dc=com
   密钥：123456 （LDAP 服务器管理员密码）



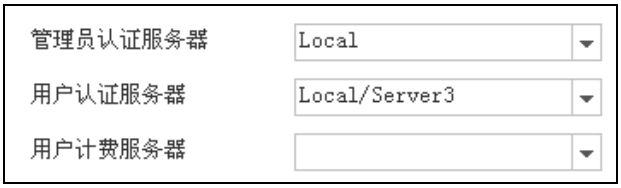
3. 点击**确定**。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] ldap server Server3 ip/domain 192.168.2.60 port
389 Secure_Connection none
NetEye@root-system] ldap server Server3 Admin_DN
cn=Administrator,cn=Users,dc=IDTest,dc=com
NetEye@root-system] ldap server Server3 Common_Name_Identifier
sAMAccountName
NetEye@root-system] ldap server Server3 Distinguished_Name
dc=IDTest,dc=com
NetEye@root-system] end
NetEye@root> save config
```

3.16.4.3 设置网络用户认证服务器

1. 选择**系统** > **认证** > **认证配置**。
2. 指定网络用户认证服务器为 “Server3”。



3. 点击**确定**。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] server authentication type authuser Server3
NetEye@root-system] end
NetEye@root> save config
```

3.16.4.4 开启 WebAuth 认证

1. 选择**系统** > **认证** > **WebAuth 配置**。在 eth0 上启用 WebAuth 功能。

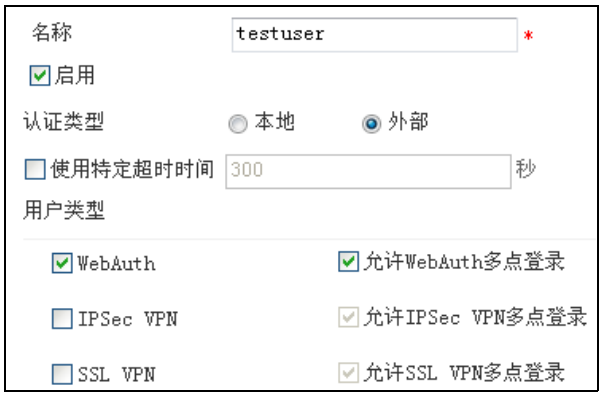
2. 点击**确定**。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] webauth ethernet eth0 on
NetEye@root-system] end
NetEye@root> save config
```

3.16.4.5 设定用户 WebAuth 角色

1. 选择**系统 > 认证 > 网络用户**，进入**网络用户**页面。
2. 点击**新建**创建 WebAuth 用户。用户名：testuser；认证类型：外部。勾选 **WebAuth**。



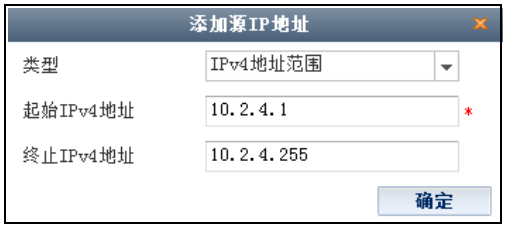
3. 点击**确定**。

CLI

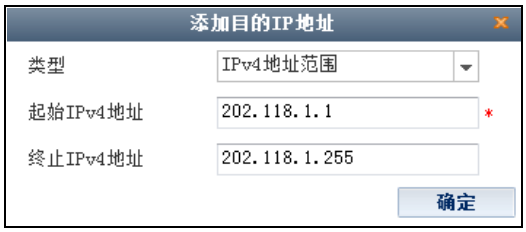
```
NetEye@root> configure mode override
NetEye@root-system] user authuser testuser authtype external enable
NetEye@root-system] user authuser testuser auth
NetEye@root-system] user authuser testuser auth multipoint enable
NetEye@root-system] end
NetEye@root> save config
```

3.16.4.6 创建 WebAuth 自动重定向策略

1. 点击**对未标识会话进行被动 WebAuth 认证**。点击**新建**，创建 WebAuth 自动重定向策略 “policy2”。
2. 在**源 IP 地址列表**区域，设置源 IP 地址范围为 10.2.4.1-10.2.4.255。



3. 在**目的 IP 地址**区域，设置目的 IP 地址范围为 202.118.1.1-202.118.1.255。



4. 点击，使以上配置生效。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] webauth policy policy2 any 10.2.4.1-10.2.4.255 any
202.118.1.1-202.118.1.255 service http
NetEye@root-system] end
NetEye@root> save config
```

3.16.4.7 被动认证

上述配置后，用户输入 http://202.118.1.24, 页面跳转至 WebAuth 认证登录页面 （https://10.2.4.16:4325）。输入用户名和密码后， NISG 显示登录成功的信息。之后用户可以输入 http://202.118.1.24 进行访问。

3.16.4.8 主动认证

用户也可以直接输入认证接口 IP 地址 https://10.2.4.16:4325。在认证页面输入用户名和密码。当跳转到登录成功的页面后，即可访问 http://202.118.1.24。

3.17 备份恢复

- 3.17.1 概述
- 3.17.2 基本配置步骤

3.17.1 概述

NISG 支持对除系统日志、诊断文件和 License 文件之外的系统配置文件进行备份。

- 备份系统配置

  管理员应定期对 NISG 系统配置进行备份。

- 管理备份文件

  管理员可以查看、删除和下载系统备份文件，也可以将备份文件复制到本地存储介质上（仅在 CLI 下）。一个 Vsys 的备份文件不能被复制到另一 Vsys 中。

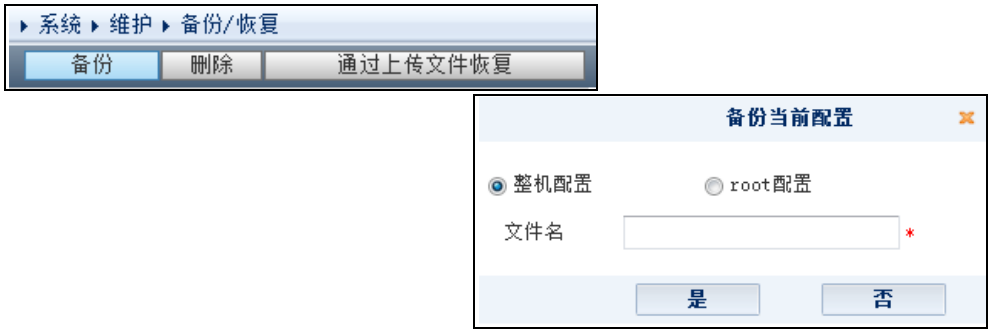
- 恢复系统配置

  管理员可以通过保存在本地或远程主机上的备份文件进行系统恢复。远程恢复时，远程主机上的备份文件会被临时上载到本地。系统恢复结束后，该备份文件将被自动删除。

3.17.2 基本配置步骤

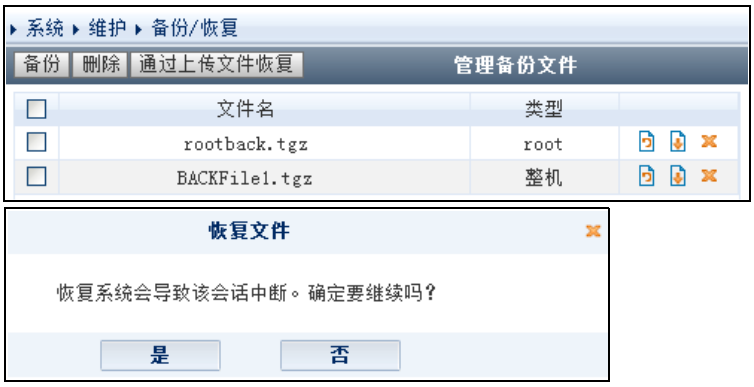
选择**系统** > **维护** > **备份 / 恢复**。

1. 备份整机或 root 配置。



2. 下载或删除备份文件。

3. 通过本地备份文件恢复系统配置。



4. 通过上传文件恢复系统配置。

配置注意事项

- 备份文件名由字母、数字和下划线组成，并且不能以下划线开头。文件名的长度范围是 1-128 字节。备份文件名称不能重复。
- 根系统最多支持 5 个整机配置备份文件和 5 个根系统配置备份文件，每虚拟系统最多支持 5 个备份文件。
- 只有根系统管理员和 Vsys 管理员才能备份系统。根系统管理员可以备份根系统和整机的配置信息，而 Vsys 管理员只能备份其所登录管理的 Vsys 的配置信息。

表 59 备份恢复命令

backup	备份系统配置。
copy backup	下载系统备份文件。
delete backup	删除备份文件。
restore from internal	用本地保存备份文件恢复系统。
restore from	通过上载备份文件恢复系统。

3.18 技术支持

- 3.18.1 概述
- 3.18.2 基本配置步骤

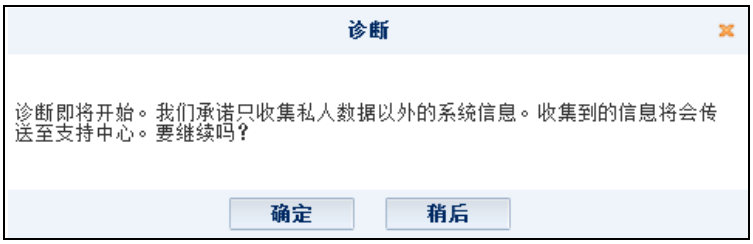
3.18.1 概述

管理员可以通过一键式操作，方便地将诊断文件发送给 NISG 的技术支持中心，尽快地解决问题。诊断信息的内容包括配置文件信息、系统状态信息、事件日志信息等。诊断文件保存在 NISG 上，可以查看、删除或下载。当生成新的诊断文件时，旧文件会被覆盖。

3.18.2 基本配置步骤

选择**系统** > **维护** > **技术支持**，进入**技术支持**页面。

1. 开启诊断功能。



2. 查看、删除或下载生成的诊断文件。

3.19 集中管理

- 3.19.1 概述
- 3.19.2 基本配置步骤

3.19.1 概述

集中管理系统提供对网络安全产品的集中管理，对被管理设备提供报警、监控、日志和报表等功能。NISG 支持集中管理服务器的管理，但一台 NISG 设备同时只能接受一台服务器的管理。

NISG 上不上载任何 License 时也能够接受集中管理服务器的管理。

NISG 上开启允许集中管理后，会对向其发出管理请求的集中管理服务器进行认证，通过认证的服务器才能对 NISG 进行管理。集中管理服务器进行管理后，可以配置系统，但需要临时抢占配置锁。配置完成后，会自动释放配置锁。

3.19.2 基本配置步骤

选择**系统** > **维护** > **集中管理**，进入**集中管理**页面，开启集中管理服务器管理功能。

3.20 诊断工具

NISG 提供以下诊断工具：

- 3.20.1 Ping：测试 NISG 与远程主机之间的连通性。
- 3.20.2 Traceroute：探测数据包在传输过程中所经过的路径。
- 3.20.3 Debug：监听数据包和会话信息。

3.20.1 Ping

表 60 Ping 命令

ping {*host_name* | *ipv4_address*} [*num*] **ping6** {*host_name* | *ipv6_address* [**interface** *interface_name*]} [*num*]	检查 NISG 与目的 IP 之间是否连通。

3.20.2 Traceroute

Traceroute 工具用于探测数据包到目的主机所经过的路径，可以帮助管理员了解网络连接状态。

Traceroute 学习路由的过程如下：

1. 发送一个 TTL 值为 1 的数据包给目的主机。当这个数据包到达第一个路由器的时候，路由器会将它的 TTL 值减 1。此时，由于该数据包的 TTL 值变为 0，路由器将丢弃该数据包，并向 NISG 回应一个表示超时的 ICMP 数据包。这样， NISG 就获得了数据包到达第一个路由器的时间和第一个路由器的 IP 地址。
2. 再发一个TTL值为2的数据包。同理，NISG将得到数据包到达第二个路由器的时间和第二个路由器的 IP 地址。
3. 依此下去，直到数据包到达目的主机， NISG 便获得了数据包到目的主机所经过的完整路径。

在 Traceroute 运行过程中，路径中的每个路由器会被探测三次。输出格式如下所示：

序号 IP 地址或域名 探测时间 1 探测时间 2 探测时间 3

- **序号**：路由器在整个路径中的序号，表示当前路由器是数据包经过的第几个路由器。
- **IP 地址**：数据包到达的当前路由器 （或服务器）的 IPv4 地址或者域名。
- **探测时间 1、2、3**：对当前路由器进行第一、二、三次探测时，数据包到达路由器并返回的时间。单位为毫秒。

表 61 Traceroute 命令

traceroute {*ipv4_address* | *domain name*}	探测到达路由器或服务器的路径。

3.20.3 Debug

管理员可使用 NISG 提供的 Debug 工具对数据包包进行监听和跟踪。

- 3.20.3.1 通用 Debug
- 3.20.3.2 VPN Debug
- 3.20.3.3 PPPoE Debug

3.20.3.1 通用 Debug

下表给出通用 Debug 的相关命令：

- 基本命令：如 **show debug**、 **debug clear** 等。
- **debug dump hook**：通过此命令设置监听对象。
- **debug match**：通过此命令设置匹配条件监听指定数据包。
- **debug dump**：通过此命令设置诊断信息的输出条件。

表 62 Debug 命令

show debug	查看 Debug 配置信息。
debug start *time* [*file_name*]	设置监听数据包时长 （3-14400 秒）。
debug stop	停止监听数据包。
debug file remove [*file_name*]	删除 Debug 文件。
debug file download	下载 Debug 文件。
debug clear	停止 Dump 并重置监听匹配条件。
debug dump hook all	监听所有数据包。
debug dump hook dnat	监听执行过 DNAT 的数据包。
debug dump hook error	监听传输中出错的数据包。
debug dump hook input	监听接收的数据包。
debug dump hook input_error	监听接收的数据包和出错的数据包。
debug dump hook input_output	监听接收和成功发送的数据包。
debug dump hook output	监听成功发送的数据包。
debug dump hook output_error	监听发送的数据包和出错的数据包。
debug dump hook policy	监听匹配策略的数据包。
debug dump hook route	监听匹配路由的数据包。
debug dump hook snat	监听执行过 SNAT 的数据包。
debug match bidir	设置是否进行双向监听。
debug match input	设置入口接口，包括任意接口、以太网通道、以太网接口、本地接口、PPPoE 接口、冗余接口及 VLAN 接口。
debug match ip	设置源和目的 IP 地址。此地址可以为 IPv4 或 IPv6 地址。
debug match mac	设置源和目的 MAC 地址。
debug match output	设置出口接口，包括任意接口、以太网通道、以太网接口、本地接口、PPPoE 接口、冗余接口及 VLAN 接口。
debug match port	设置源和目的端口。

表 62 Debug 命令 (续)

debug match protocol	设置协议类型，包括指定协议号、任意协议、ARP、ICMP、ICMPv6、TCP 及 UDP。
debug match tunnel	设置 VPN 隧道。
debug dump bytes	设置单个数据包内容的最大输出字节数。
debug dump session	设置是否输出会话信息。
debug dump complex	设置是否输出数据包包头的详细标记信息。

3.20.3.2 VPN Debug

VPN Debug 功能默认是关闭的，管理员可以打开 VPN Debug，对指定或所有自动密钥隧道进行调试。

输出的调试信息包含以下数据：

- 协商结果和协商状态
- 当前信息所属隧道
- 协商包的每个字段的信息

表 63 VPN Debug 命令

show debug vpn [**all-tty**]	查看当前或所有终端的 VPN Debug 配置信息。
unset debug vpn [**all-tty**]	取消输出当前或所有终端的 VPN Debug 信息。
debug vpn ipsec *timeout*	输出 IPSec Debug 信息
debug vpn isakmp {**error** | **basic** | **detail**}	输出不同级别的 ISAKMP Debug 信息。
unset debug vpn isakmp [**tunnel** *tunnel_name*]	取消输出 ISAKMP Debug 信息。
debug vpn l2tp	输出所有隧道的 L2TP Debug 信息。
unset debug vpn l2tp	取消输出隧道的 L2TP Debug 信息。
debug sslvpn {**on** | **off**}	输出或取消输出 SSL VPN Debug 信息。

3.20.3.3 PPPoE Debug

管理员可以通过相关命令设置和查看 PPPoE Debug 的相关信息。

表 64 PPPoE Debug 命令

show debug pppoe [all-tty]	查看 PPPoE Debug 配置信息。
debug pppoe	输出 PPPoE Debug 信息。
unset debug pppoe [**all-tty**]	取消输出 PPPoE Debug 信息。
show debug pppoev6 [**all-tty**]	查看 PPPoEv6 Debug 配置信息。
debug pppoev6	输出 PPPoEv6 Debug 信息。
unset debug pppoev6 [**all-tty**]	取消输出 PPPoEv6 Debug 信息。

3.21 报警配置

- 3.21.1 概述
- 3.21.2 基本配置步骤
- 3.21.3 配置参数说明

3.21.1 概述

当有事件发生时， NISG 会检查报警策略，如果匹配了报警策略，那么 NISG 将根据管理员设置以简体中文或英语生成日志，并将日志发送到对应的服务器。

NISG 支持如下报警策略：

- 本地日志报警策略

  NISG 缺省提供了名称为 “internal” 的本地日志类型的报警策略。该策略不可以被删除。

- Syslog 报警策略

  NISG 将系统日志信息发送到远程 Syslog 服务器。

- 邮件报警策略

  NISG 可以采用电子邮件方式将报警信息通过邮件服务器发送给指定的邮件地址。

- SNMP Trap 报警策略

  NISG 可以利用 SNMP Trap 方式，将系统日志发送给 SNMP 客户端。也支持向多个 SNMP Trap 服务器发送日志信息。 SNMP Trap 中有两个协议版本， v1 和 v2c。

- 终端输出报警策略

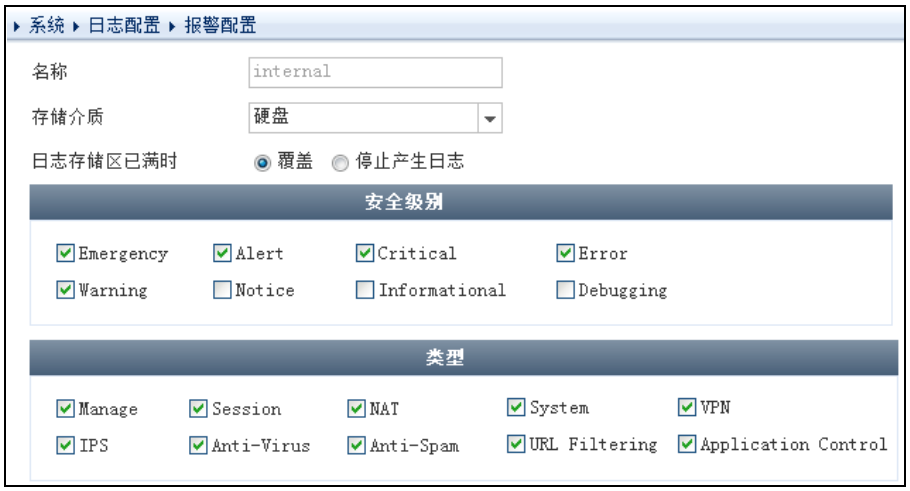
提示：Syslog 报警策略、电子邮件报警策略和 SNMP Trap 报警策略， NISG 每种策略最多支持 15 条。

3.21.2 基本配置步骤

选择**系统** > **日志配置** > **报警配置**。

1. 查看或删除报警策略。

2. 编辑本地日志报警策略。



提示

如果系统日志存储介质不是硬盘，则无法编辑本地日志报警策略。

3. 创建或编辑：

- Syslog 报警策略

- SNMP trap 报警策略

- 邮件报警策略

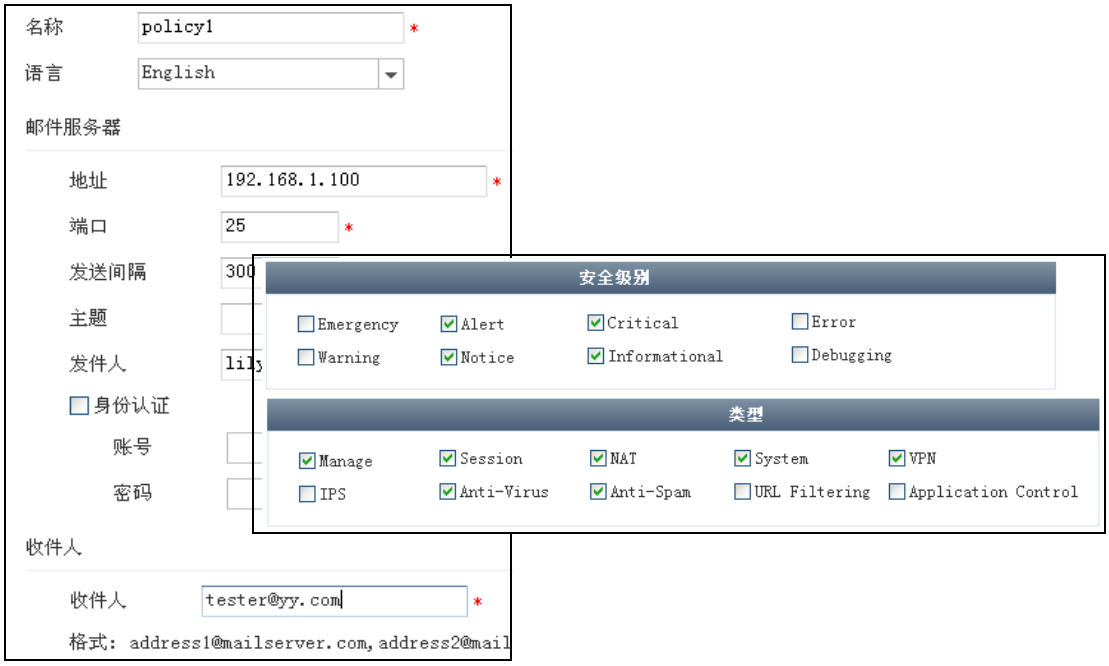


表 65 报警策略命令

show alert-config	查看报警策略。
alert-config local-syslog | syslog | snmp-trap | mail	编辑本地日志报警策略或创建 Syslog、 SNMP Trap 或邮件报警策略。
unset alert-config syslog | snmp-trap | mail	删除 Syslog、 SNMP Trap 或邮件报警策略。

3.21.3 配置参数说明

表 66 本地日志报警策略配置信息

参数	说明
名称	本地日志报警策略名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #。
存储介质	系统日志的存储介质，不允许切换存储介质。
日志存储区已满时	设置日志存储策略，覆盖或停止产生日志。
安全级别	系统日志输出事件的安全级别，包括 Emergency、 Alert、 Critical、 Error、 Warning、 Notice、 Informational 和 Debugging。
类型	系统日志的来源类型，包括 Manage、 Session、 NAT、 System、 VPN、 IPS、 Anti-Virus、 Anti-Spam、 URL Filtering 和 Application Control。

表 67 Syslog 报警策略配置信息

参数	说明
名称	Syslog 报警策略名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #。
Syslog 服务器	设置 Syslog 服务器 IP 地址和端口： • IP 地址：取值范围为 [0-223].[0-255].[0-255].[0-255]。 • 端口：取值范围为 1-65535，默认为 514。
输出方式	日志输出到 Syslog 服务器的方式： • 完整输出：将整条系统日志完整地输出，包括事件头和事件内容。输出格式： <pri> 月份 + 日期 + 时间 + 主机名：虚拟系统名 + 事件库版本 - 语言标识 - 模块 ID - 事件 ID + 日志等级 + 模块类型 + 用户名 + rep= 重复次数 | 消息体 • 精简输出：将系统日志部分地输出。输出格式： <pri> 月份 + 日期 时间 + 主机名：虚拟系统名 + 事件库版本 - 语言标识 - 模块 ID - 事件 ID + 日志等级 + 模块类型 缺省为完整输出。
语言	日志输出语言，简体中文或英语。
安全级别	系统日志输出事件的安全级别。
类型	系统日志的来源类型。

表 68 邮件报警策略配置信息

参数	说明
名称	邮件报警策略名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #。
语言	日志输出语言，简体中文或英语。

表 68 邮件报警策略配置信息 (*续*)

参数	说明
邮件服务器	设置接收邮件的邮件服务器： • 地址：IP 地址或域名。 IP 地址的范围为 [0-255].[0-255].[0-255].[0-255]。域名长度范围为 2-255 字节。 • 端口：1-65535。缺省端口号为 25。 • 发送间隔：取值范围为 1-2678400 秒。 • 主题：0-64 字节， UTF-8 字符。不能包含空格和以下字符：? ' \ 。NISG 以邮件形式发送系统日志时，会在邮件主题前添加产品序列号。 • 发件人：NISG 用于发送邮件的邮件地址。 • 身份认证：邮件服务器对邮件发送者进行身份验证。当启用身份验证时必须设置账号及密码。密码长度为 1-255 字节。
收件人	接收报警信息的邮件地址，最多添加 10 个邮件地址。多个地址以逗号分隔。
安全级别	系统日志输出事件的安全级别。
类型	系统日志的来源类型。

表 69 SNMP Trap 报警策略配置信息

参数	说明
名称	SNMP Trap 报警策略名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & #。
SNMP Trap 地址	设置 SNMP Trap 地址： • IP 地址：接收 SNMP Trap 格式日志的 SNMP 服务器 IP 地址。范围为 [0-223].[0-255].[0-255].[0-255]。 • 版本：SNMP 服务器接收 SNMP 的版本号， v1 和 v2c。
语言	日志输出语言，简体中文或英语。
安全级别	系统日志输出事件的安全级别。
类型	系统日志的来源类型。

3.22 日志维护

- 3.22.1 概述
- 3.22.2 基本配置步骤
- 3.22.3 配置参数说明

3.22.1 概述

当有事件发生时， NISG 会根据报警策略生成日志。系统日志存储在硬盘中，本地不保存日志， CF 卡不存储日志。管理员不可以切换日志存储介质。当日志文件大小超过存储空间时， NISG 会覆盖产生时间最早的日志文件或停止产生新日志。

不同报警策略类型的日志输出格式如表 70 所示：

表 70 报警策略的日志输出格式

策略类型	日志输出格式
本地日志	输出格式： **<pri> 年 - 月 - 日 时 : 分 : 秒 主机名 :Vsys 名称 事件库版本 - 语言标识 - 模块 ID- 事件 ID 日志等级 模块类型 用户名 rep= 重复次数 | 消息体** 示例：<165>2013-03-18 14:52:01 NetEye:root 03-01-275-0000 Notice Manage N/A rep=1| 管理用户 root 通过 Web 登录成功， IP 为 10.2.1.119。
Syslog	Syslog 报警策略包含两种系统日志输出格式： • **完整输出**：将整条系统日志完整地输出： **<pri> 年 - 月 - 日 时 : 分 : 秒 主机名 :Vsys 名称 事件库版本 - 语言标识 - 模块 ID- 事件 ID 日志等级 模块类型 用户名 rep= 重复次数 | 消息体** 示例：<165>2013-03-18 14:52:01 NetEye:root 03-01-275-0000 Notice Manage N/A rep=1| 管理用户 root 通过 Web 端登录成功， IP 为 10.2.1.119。 • **精简输出**：将整条系统日志部分地输出（不包含日志的重复次数和消息体部分）： **<pri> 年 - 月 - 日 时 : 分 : 秒 主机名 :Vsys 名称 事件库版本 - 语言标识 - 模块 ID- 事件 ID 日志等级 模块类型** 示例：<165>2013-03-18 14:52:01 NetEye:root 03-01-275-0000 Notice Manage
邮件	输出格式： **<pri> 年 - 月 - 日 时 : 分 : 秒 主机名 :Vsys 名称 事件库版本 - 语言标识 - 模块 ID- 事件 ID 日志等级 模块类型 用户名 rep= 重复次数 | 消息体** 示例：<165>2013-03-18 14:52:01 NetEye:root 03-01-275-0000 Notice Manage N/A rep=1| 管理用户 root 通过 Web 登录成功， IP 为 10.2.1.119。 报警邮件的邮件名格式： [syslog] + MAC + 用户自定义主题 示例：当 MAC 地址为 000C29FB8FF0 的 NISG 设备发送一封自定义主题为 test 的系统日志报警邮件时，邮件主题为： [syslog]000C29FB8FF0test
SNMP Trap	输出格式： **<pri> 年 - 月 - 日 时 : 分 : 秒 主机名 :Vsys 名称 事件库版本 - 语言标识 - 模块 ID- 事件 ID 日志等级 模块类型 用户名 rep= 重复次数 | 消息体** 示例：<165>2013-03-18 14:52:01 NetEye:root 03-01-275-0000 Notice Manage N/A rep=1| 管理用户 root 通过 Web 登录成功， IP 为 10.2.1.119。

3.22.2 基本配置步骤

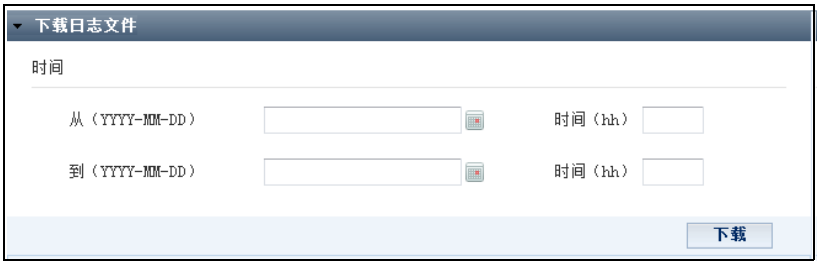
选择**系统** > **日志配置** > **报警配置**。点击缺省的本地日志报警策略 “internal” 所对应的 进入编辑页面设置日志存储策略。

提示

如果日志存储介质不是硬盘，则无法编辑本地日志报警策略，无法设置日志存储策略。

选择**系统** > **日志配置** > **日志维护**。

1. 下载日志文件。



2. 删除所有日志或指定时间段内日志。

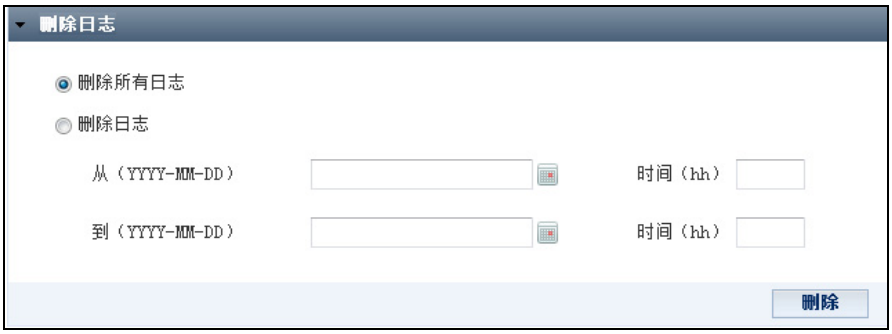


表 71 系统日志命令

logging policy	设置系统日志存储策略。
delete log all,time	删除系统日志。

3.22.3 配置参数说明

表 72 系统日志参数信息

参数	说明
优先级	日志信息的优先级。
日期时间	系统日志产生的时间。 显示格式为：**YYYY-MM-DD hh:mm:ss** 示例： 2013-03-18 02:34:45
Vsys 和主机名	产生系统日志的 NISG 的主机名及 Vsys。 显示格式为：**主机名 :Vsys 名称** 示例： 如主机名是 henry， Vsys 是根系统 (root)，即为：henry:root。
基本信息	系统日志的基本信息，包括事件库版本、语言标识、模块 ID、事件 ID。 显示格式为： **事件库版本 - 语言标识 - 模块 ID- 事件 ID** • 事件库 （主）版本为两字节整数，当前事件库主版本号为 03。 • 语言标识为两字节整数， 01 代表简体中文， 02 代表英文。 • 模块 ID 为两字节整数。 • 事件 ID 为四字节整数。
级别	系统日志的安全级别： • Emergency：代表内存不足或者电源、 CPU 等硬件异常情况。该级别 ID 为 0。 • Alert：代表根据当前的情形需要立即做出响应的事件。如，攻击防御部分收到攻击包或 IP 分片中收到了类似的攻击包。该级别 ID 为 1。 • Critical：代表影响设备功能的条件信息，如拔插网线、启用 / 禁用网卡。该级别 ID 为 2。 • Error：代表所有添加、删除、修改动作失败的信息，包重组失败信息以及所有的匹配策略失败的错误信息。该级别 ID 为 3。 • Warning：代表可能影响系统功能的条件信息。如，连接邮件服务器失败或者认证失败、超时。该级别 ID 为 4。 • Notice：代表对普通事件的通告。如，由管理员进行添加、删除和修改操作的成功信息。该级别 ID 为 5。 • Informational：代表系统操作的通用信息。该级别 ID 为 6。 • Debugging：代表与调试相关的信息。该级别 ID 为 7。
类型	产生系统日志的模块类型，包括 Manage （管理）、 System （系统）、 Session （会话）、 NAT （地址转换）、 VPN （虚拟专用网）、 IPS （入侵防御系统）、 Anti-Virus （防病毒）、 Anti-Spam （反垃圾邮件）、 URL Filtering （URL 过滤）和 Application Control （应用控制）。
用户	触发系统日志产生的用户名称 （包括管理用户、网络用户、系统自身）。 • Manage 类型的事件大多数由管理员操作触发，所以用户名为当前管理员名称。 • 由于系统处理的会话和转发数据产生的日志需要关联到该数据的源用户，所以用户名即发起该会话或发送该数据的认证用户；如果该会话没有认证信息，用户名为 “N/A”。 • 由于系统自身运行而产生的日志 （包括按预定计划定时执行的任务触发的日志，如 DHCP 或 SAC 自动配置地址等），用户名为 “N/A"。 • 其他不可确认事件对应用户的，用户名均使用 “N/A”。
重复次数	系统日志的重复次数。 NISG 可以对一定时间内内容重复的系统日志进行合并，以标明重复次数的方式提醒管理员注意。
日志信息	系统日志的主体部分，具体介绍发生了什么。内容包括系统日志的主体描述和参数等。

3.23 证书

- 3.23.1 概述
- 3.23.2 基本配置步骤
- 3.23.3 范例：自动生成证书
- 3.23.4 本地证书参数
- 3.23.5 CA 证书参数

3.23.1 概述

数字证书是由证书权威机构 （CA）颁发并受其管理的一种特殊电子文档。数字证书可以用于 IKE 协商过程中的身份认证， NISG 支持这种认证方式，但不支持证书颁发功能。 NISG 需要 CA 的协助实现证书认证。

- 本地证书

  要申请本地证书，必须先创建证书请求。本地证书可以手动或自动两种方式获取。手动获取本地证书，保存生成的证书请求文件到本地，联系 CA，获取本地证书。NISG 也支持简单证书注册协议 （SCEP），通过与 SCEP 服务器进行交互，实现证书自动注册和自动更新。启用证书自动更新功能后， NISG 会在证书过期之前的指定时间内，向 CA 服务器发出证书自动更新请求。

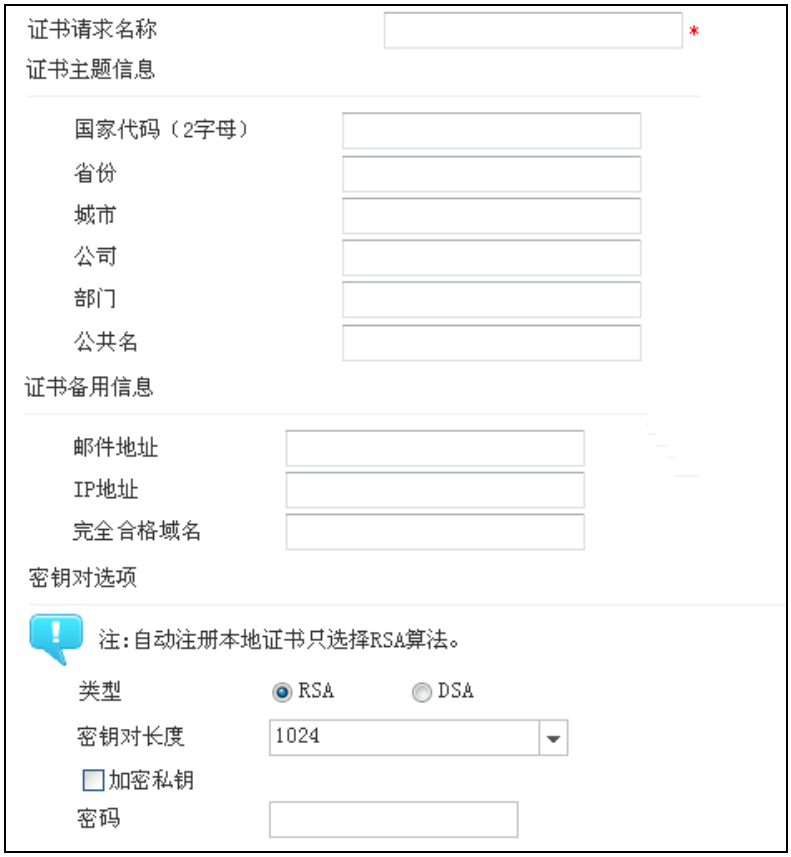
- CA 证书

  CA 证书用于验证 CA 所签发的证书。 NISG 支持以下两种验证证书有效性的方法：在线证书状态协议 (OCSP) 和证书吊销列表 (CRL)。缺省方法是使用 CRL。 CRL 列表中包含 CA 签发的所有无效或已过期的证书。 NISG 使用 OCSP 验证证书有效性时，作为 OCSP 客户端，向 OCSP 服务器发送验证请求，当 OCSP 服务器收到请求后，将确认证书的状态，并向 NISG 返回证书信息。

3.23.2 基本配置步骤

选择**系统** > **证书** > **本地证书**。

1. 生成证书请求文件。



2. 保存证书请求文件至本地手动申请或启用证书自动注册。

3. 查看、删除或上载本地证书。

选择**系统** > **证书** > **CA 证书**。

1. 查看、删除或上载 CA 证书。

2. 将证书导入或导出证书吊销列表。

配置注意事项

- 当首次向CA服务器申请注册证书时，系统提示确认CA证书的“指纹”。如果确认此“指纹”，则继续进行证书注册。
- 上载证书的顺序是CA证书、CRL和本地证书。因为CA证书和CRL用于检验本地证书是否由 CA 签发以及是否有效。
- 被 IPSec VPN 隧道引用的本地证书不可以被删除。

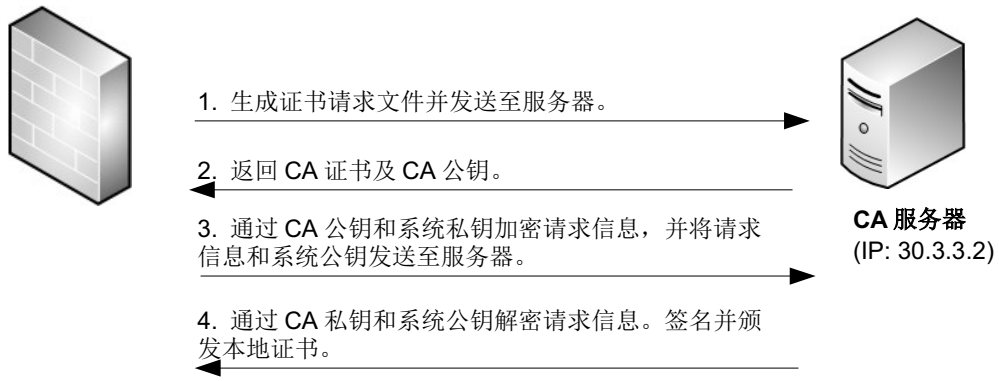
表 73 证书命令

generate certificate-request	生成本地证书请求。
enroll request ca	发送本地证书请求至 CA。
enroll request accept-ca-certificate	接受或拒绝 CA 证书指纹。
ca certificate checkmethod	设置本地证书检测方式。
delete certificate req	删除本地证书请求。
delete certificate ca, crl, local	删除 CA 证书、 CRL 或本地证书。
import certificate	上载 CA 证书或本地证书。
import certificate crl	上载 CRL。

3.23.3 范例：自动生成证书

本范例介绍 NISG 如何通过 CA 服务器自动生成证书。

图 4 证书注册



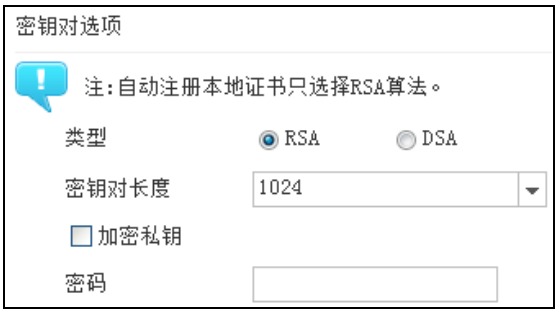
配置步骤如下：

- 3.23.3.1 创建证书请求
- 3.23.3.2 自动注册证书

3.23.3.1 创建证书请求

1. 选择**系统 > 证书 > 本地证书**。
2. 点击**新建证书请求**进入**本地证书**页面。输入证书请求名称和证书主题及备用信息。

3. 指定密钥对选项信息。



4. 点击**确定**。
5. 在本地证书列表中查看已生成的证书请求文件。

CLI

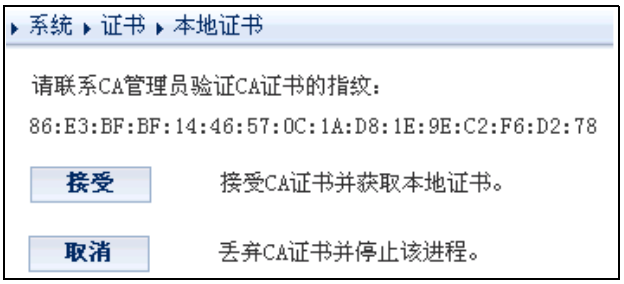
```
NetEye@root> configure mode override
NetEye@root-system] generate certificate-request test country CN state-or-province LN locality none organization none organizational-unit none common-name none ip-address none email-address none dns none rsa 1024
NetEye@root-system] end
NetEye@root> save config
```

3.23.3.2 自动注册证书

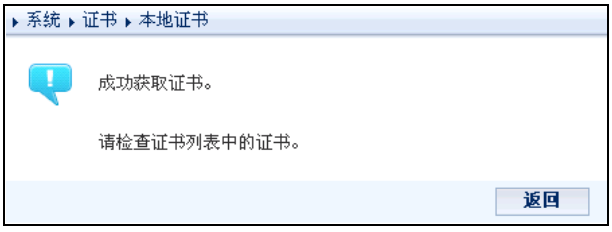
1. 点击新生成的证书请求文件所对应的 进入**本地证书**页面。
2. 勾选**自动注册 （SCEP）**。输入 CA 服务器名、地址、 CA 证书标识及挑战码信息。

> **提示**
> CA 服务器地址、挑战码及指纹信息从 CA 服务器获得。

3. 点击**确定**并验证 CA 证书指纹。如果指纹正确点击**接受**。



4. 证书已生成。点击**返回**在**本地证书列表**中查看生成的本地证书。



5. 在 **CA 证书列表**中查看生成的 CA 证书。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] enroll request test ca CC url http://30.3.3.2/certsrv/mscep/mscep.dll ident none challenge 8AE0AA7D70B3F623 polling disable
% Please contact the CA administrator to verify the finger print of CA certificate:
        86:E3:BF:BF:14:46:57:0C:1A:D8:1E:9E:C2:F6:D2:78
NetEye@root-system] enroll request test accept-ca-certificate accept
% You have successfully generated the certificate.
Please check the certificates in the certificate list.
NetEye@root-system] end
NetEye@root> save config
```

3.23.4 本地证书参数

表 74 本地证书请求配置信息

参数	说明
证书请求名称	长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #。
证书主题信息	证书主题信息包括： • 国家代码：由两个英文字母组成，代表 NISG 设备所在的国家。 • 省份：长度 0-127 字节， UTF-8 字符。不能包含空格和以下字符：` ？, " ' \ < > &。 • 城市：长度 0-127 字节， UTF-8 字符。不能包含空格和以下字符：` ？, " ' \ < > &。 • 公司：长度 0-64 字节， UTF-8 字符。不能包含空格和以下字符：` ？, " ' \ < > &。 • 部门：长度 0-64 字节， UTF-8 字符。不能包含空格和以下字符：` ？, " ' \ < > &。 • 公共名：长度 0-64 字节， UTF-8 字符。不能包含空格和以下字符：` ？, " ' \ < > &。
证书备用信息	证书备用信息包括： • 邮件地址：对证书负责的联系人的邮件地址。长度 5-64 字节。 • IP 地址：使用证书的安全设备的 IPv4 地址。最大长度 64 字节。 • 完全合格域名：使用证书的安全设备的完全合格域名。长度 2-64 字节。可以输入不带点 （.）的域名。 证书主题信息和证书备用信息部分至少需要设置一项。
密钥对选项	密钥对选项包括： • 类型：包括 RSA 和 DSA，自动注册证书只能选择 RSA 算法。 • 密钥对长度：密钥越长，越安全，但加密和解密速度越慢。密钥对长度可以为 768、 1024、 1536 和 2048, 缺省为 1024。 • 加密私钥：选择是否加密证书私钥。缺省为禁用。 • 密码：个人密钥，长度 0-127 字节。

表 75 证书自动注册和更新配置信息

参数	说明
自动注册 (SCEP)	启用或禁用自动注册证书，默认为禁用。
选择 CA 服务器	注册证书的 CA 服务器，可以选择 NISG 上已经存在的 CA 证书或手动输入 CA 服务器。 NISG 支持下列 CA 服务器：Baltimore、 Entrust、 Microsoft、 Netscape、 RSA Keon 和 Verisign。
CA 服务器地址	签发证书的 CA 服务器的 URL 地址。长度范围为 2-255 字节。
CA 证书标识	所生成的 CA 证书的 ID，是证书在 NISG 上的唯一标识。最大长度为 255 字节。
挑战码	当 CA 采用预共享密钥方式认证证书请求者身份时，挑战码用于 CA 对证书请求者的身份验证。最大长度为 127 字节。
轮询	如果管理员启用轮询功能，在等待 CA 服务器认证证书注册请求过程中，作为请求的发送方，会不断地发送轮询消息，直到达到最大轮询次数或 CA 服务器返回状态标识为止。此功能默认为禁用。 • 轮询间隔：连续两次轮询的间隔时间。取值范围为 1-600 分。 • 轮询次数：最多可发送轮询消息的次数，取值范围为 1-1000。

表 76 本地证书配置信息

参数	说明
名称	本地证书名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & #。
发行者	发放、管理和撤消本地证书的机构。
主题	本地证书的主题信息。
有效期	本地证书的有效期。
状态	本地证书注册过程中的各个状态： • Valid：证书有效。 • Pending：证书注册处于轮询状态，一般发生在 CA 服务器采用手动认证的情况。 • Keypair：证书请求标识。 • Expired：证书已经过期。 • Not yet valid：证书尚未生效。

3.23.5 CA 证书参数

表 77 证书验证配置信息

参数	说明
检查方式	证书撤销检查方法，包括 CRL、 OCSP 或不指定。
严格检查	当使用 OCSP 验证证书状态时，如果 NISG 与 OCSP 服务器连接失败，或者 OCSP 服务器返回检查结果为 “ 未知 ” 时，在勾选严格检查复选框的情况下，证书无效；在不选严格检查复选框的情况下，证书合法。 当使用 CRL 方法验证证书状态时，如果 NISG 中不存在 CRL，在勾选严格检查复选框的情况下，证书无效；在不选严格检查复选框的情况下，证书合法。
OCSP URL	OCSP 服务器的 URL，例如：http://ocsp.test.com。根据需要，也可以在设置 OCSP 服务器的 URL 同时，设置端口号，例如：http://ocsp.test.com:8080。 NISG 支持以下 OCSP 服务器：Entrust、 microsoft、 RSA Keon 和 Verisign。

表 78 CA 证书配置信息

参数	说明
名称	CA 证书名称。不能为 any （不区分大小写）。
主题	CA 证书的主题信息。
有效期	CA 证书的有效期。
状态	CA 证书的状态： • Valid：在有效期内的本地证书。 • Expired：标识证书已经过期失效。 • Not yet valid：该证书还未生效。
CA 服务器	CA 服务器的配置。

3.24 对象

NISG 策略可以引用 IP 地址对象、 IP 地址对象组、服务对象及服务对象组。

- 3.24.1 IP 地址
- 3.24.2 服务

3.24.1 IP 地址

可以将一个或多个 IP 地址定义为一个对象。还可以将相同类型的 IP 地址对象划分到一个 IP 地址对象组中，以简化配置。

- 3.24.1.1 基本配置步骤
- 3.24.1.2 IP 地址对象参数
- 3.24.1.3 IP 地址对象组参数

3.24.1.1 基本配置步骤

1. 选择**系统** > **对象** > **IP 地址** > **IP 地址对象**。
2. 点击**新建**创建一个对象。点击**添加**编辑该对象包含的 IP 地址。

3. 选择**系统** > **对象** > **IP 地址** > **IP 地址对象组**。
4. 点击**新建**创建 IP 地址对象组。从**备选对象**中选择 IP 地址对象加入对象组。

配置注意事项

- 被策略引用的 IP 地址对象或对象组不能被删除。
- 最多可创建 1024 个 IP 地址对象，每个 IP 地址对象最多可包含 128 个 IP 地址条目。
- 最多可创建1024个IP地址对象组，每个IP地址对象组最多可包含128个IP地址对象。IP 地址对象组不能和其对象成员重名。

表 79 IP 地址对象 /IP 地址对象组命令

object ipaddr *object_name* **description** *string*	设置指定 IP 地址对象的备注信息。
object group *group_name* **type ipaddr** [**object** *object_list*]	添加 IP 地址对象组 , 或者向已存在的 IP 地址对象组中添加对象成员。
object group *group_name* **type ipaddr description** *string*	设置指定 IP 地址对象组的备注信息。
object ipaddr *object_name* [*ipv4_list* | *ipv6_list*]	添加 IP 地址对象或向已存在的 IP 地址对象中添加 IP 地址。
unset object ipaddr [*object_name*]	删除 IP 地址对象。
unset object group type ipaddr [*group_name*]	删除 IP 地址对象组。
unset object group type ipaddr *group_name* **object** *object_name*	删除 IP 地址对象组的指定成员。
unset object ipaddr *object_name* {*ipv4_list* | *ipv6_list*}	删除指定 IP 地址对象中的 IP 地址。

3.24.1.2 IP 地址对象参数

表 80 IP 地址对象参数

参数	说明
名称	IP 地址对象名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #
描述	IP 地址对象备注信息，长度 0-255 字节， UTF-8 字符。不能包含以下字符：？" ' \ < > &
类型	IP 类型，包括 IPv4 和 IPv6。
IP 地址	IP 地址对象包含的 IP 地址，可以为单个 IPv4 或 IPv6 地址、 IPv4 或 IPV6 地址范围、 IPv4 地址 / 掩码、 IPv6 地址 / 前缀。
引用	显示引用 IP 地址对象的策略。

3.24.1.3 IP 地址对象组参数

表 81 IP 地址对象组参数

参数	说明
组名称	IP 地址对象组名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #
描述	IP 地址对象组备注信息。长度 0-255 字节， UTF-8 字符。不能包含以下字符：？" ' \ < > &
包含对象	IP 地址对象组包含的 IP 地址对象。
引用	显示引用 IP 地址对象组的策略。

3.24.2 服务

可以将一个或多个服务定义为一个对象。还可以将多个服务对象划分到一个服务对象组中，以简化配置。

- 3.24.2.1 基本配置步骤
- 3.24.2.2 服务对象参数
- 3.24.2.3 服务对象组参数

3.24.2.1 基本配置步骤

1. 选择**系统** > **对象** > **服务** > **服务对象**。
2. 点击**新建**创建一个对象。点击**添加**编辑该对象包含的服务。

3. 选择**系统 > 对象 > 服务 > 服务对象组**。
4. 点击**新建**创建服务对象组。从**备选对象**中选择服务对象加入服务对象组。

配置注意事项

- 被策略引用的服务对象或对象组不能被删除。
- 最多可创建 1024 个服务对象，每个服务对象最多可包含 128 个服务条目。
- 最多可创建 1024 个服务对象组，每个服务对象组最多可包含 128 个服务对象。服务对象组不能和其对象成员重名。

表 82 服务对象 / 服务对象组命令

object service *object_name* **description** *string*	设置指定服务对象的备注信息。
object group *group_name* **type service** [**object** *object_list*]	添加服务对象组 , 或者向已存在的服务对象组中添加对象成员。
object group *group_name* **type service description** *string*	设置指定服务对象组的备注信息。
object service *object_name* [{**tcp | udp**} {*src_port* | *src_port_range*} {*dst_port* **|** *dst_port_range*} | **icmp** {*icmp_type* | *icmp_list* | **Any** } | **icmpv6** {*icmpv6_type* | *icmpv6_list* | **Any**} | **other** *protocol_num*]	添加服务对象或者向已存在的服务对象中添加服务列表。
unset object service [*object_name*]	删除服务对象。
unset object group type service [*group_name*]	删除服务对象组。
unset object group type service *group_name* **object** *object_name*	删除服务对象组的指定成员。
unset object service *object_name* {{**tcp | udp**} {*src_port* | *src_port_range*} {*dst_port* **|** *dst_port_range*} | **icmp** {*icmp_type* | *icmp_list* | **Any**} | **icmpv6** {*icmpv6_type* | *icmpv6_list* | **Any**} | **other** *protocol_num*}	删除指定服务对象中的服务。

3.24.2.2 服务对象参数

表 83 服务对象参数

参数	说明
名称	服务对象名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #
描述	服务对象备注信息。长度 0-255 字节， UTF-8 字符。不能包含以下字符：？" ' \ < > &
服务	网络协议类型和与之对应的 ICMP 协议类型、端口号或者协议号。网络协议类型包括 ICMP、ICMPv6、TCP、UDP 和 Other，其中 Other 是除了 ICMP、ICMPv6、TCP、UDP 之外的协议。
引用	显示引用服务对象的策略。

3.24.2.3 服务对象组参数

表 84 服务对象组参数

参数	说明
对象组名称	服务对象组名称。长度 1-63 字节，UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #
描述	服务对象组备注信息。长度 0-255 字节， UTF-8 字符。不能包含以下字符：？" ' \ < > &
包含对象	服务对象组包含的服务对象。
引用	显示引用服务对象组的策略。

4 网络配置

本章介绍网络配置的相关内容。

- 接口
  - 4.1 接口概述
  - 4.2 以太网接口
  - 4.3 以太网通道
  - 4.4 冗余接口
  - 4.5 虚拟接口
  - 4.6 VLAN 接口
  - 4.7 环回接口
  - 4.8 PPPoE 接口
  - 4.9 隧道接口
- ARP/CAM
  - 4.10 ARP
  - 4.11 CAM
- 4.12 安全域
- DNS
  - 4.13 DNS 主机
  - 4.14 DNS 代理
  - 4.15 DNS 缓存
- DHCP
  - 4.16 DHCP 服务器
  - 4.17 DHCP 作用域
  - 4.18 DHCPv6
- STP，邻居发现
  - 4.19 STP
  - 4.20 邻居发现

4.1 接口概述

- 4.1.1 工作模式
- 4.1.2 接口属性

4.1.1 工作模式

接口的工作模式分为二层和三层。其中，除了虚拟接口外，其他二层接口有以下两种工作模式：

- Access 模式（缺省模式）：工作在 Access 模式的接口是交换端口，负责二层数据交换，并通常作为接入端口，用来连接终端设备。处于 Access 模式下的接口只能被划分到一个 VLAN 中。
- Trunk 模式：通过将二层接口设置为 Trunk 模式的接口（即 Trunk 端口），可以实现多个 VLAN 在同一条链路上复用。
  - NISG 的 Trunk 端口采用 IEEE802.1Q 协议封装。
  - 管理员也可以配置某个 Trunk 端口的 Native VLAN，以接收非 802.1Q 格式的数据包。否则将丢弃未经 IEEE802.1Q 封装的数据包。

  Trunk 模式一般应用于内网接口数量较少的情形。关于 Trunk 接口的应用，请参见 范例 2：基于 Trunk 接口的多 Vsys 应用。

4.1.2 接口属性

接口具有一些通用属性，例如：接口名称、链路状态等。此外，二层接口和三层接口还分别具有一些特有的属性。

- 4.1.2.1 通用属性
- 4.1.2.1 二层特有属性
- 4.1.2.1 三层特有属性

4.1.2.1 通用属性

表 85 通用属性

配置信息	说明
接口	指接口的名称。每种类型的接口有相应的命名规范，管理员不可以修改。例如：以太网接口 eth1、以太网通道 ch1、 VLAN 接口 vlan1、隧道接口 tunnel1、冗余接口 rint2、虚拟接口 veth3、环回接口 lo2、 PPPoE 接口 ppp2。
链路状态	指接口的连接状态。该属性由系统自行维护。 • **绿色图标 （Up）**：表示已连接，且链路协商成功。 • **红色图标 （Down）**：表示已断开。 环回接口的链路状态永远是 Up。

表 85 通用属性 (*续*)

配置信息	说明
接口状态	指接口的活动状态。该属性通常由管理员控制 （隧道接口除外）。 • **绿色图标 （开）**：表示激活接口，使其处于活动状态。 • **红色图标 （关）**：表示禁用接口，使其处于非活动状态。 隧道接口的活动状态由对应的隧道状态决定。
模式	接口的工作模式，包括二层、三层和三层共享模式。 可以配置二层接口的高级设置，指定接口工作在二层 Access 模式或 Trunk 模式。 根系统管理员可以将以太网接口、以太网通道和冗余接口设置为三层共享模式。三层共享接口默认不属于任何 Vsys （包括根系统），一个三层共享接口可以被划分到多个 Vsys 中，供多个 Vsys 同时使用。三层共享接口一般应用于外网接口数量较少的情形。关于共享接口在 Vsys 中的应用，请参见 范例 1：基于三层共享接口的多 Vsys 应用。
MAC 地址	指接口的 MAC 地址。隧道接口、环回接口和 PPPoE 接口没有 MAC 地址。
引用	指引用相应接口的条目列表。引用中的接口不能被删除；要删除该接口，需要首先解除引用关系。
使用特定 MAC 地址	勾选该复选框，管理员可手动指定 MAC 地址。环回接口、隧道接口、虚拟接口和 PPPoE 接口不具有该属性。 该功能默认为禁用。
连接到虚拟网络	指虚拟接口连接的虚拟网络。仅有虚拟接口具有该属性。
描述	接口的描述信息。为 0 ～ 255 个字节的 UTF-8 字符，不包含：?'\"<>&。

4.1.2.1 二层特有属性

表 86 二层特有属性

配置信息	说明
属于	指二层接口所属的 VLAN 或以太网通道。
二层接口列表	将以太网接口划分到以太网通道中。 以太网接口应为二层 Access 模式，且未被划分到任何 VLAN 中。
二层高级设置	指二层接口的工作模式，分为 Access 模式（缺省模式）和 Trunk 模式。 • 当接口工作在 Access 模式下，可将该接口划分到某个 VLAN，或者不属于任何 VLAN。 • 当接口工作在 Trunk 模式下，可在 **VLAN 列表**中配置该 Trunk 所允许的 VLAN，并可配置它的 Native VLAN。

4.1.2.1 三层特有属性

表 87 三层特有属性

配置信息	说明
MTU	指最大传输单元（Maximum Transmission Unit）。三层接口的 MTU 只对出口接口的数据包起作用，即当数据包的长度大于三层接口的 MTU 时，在出口接口进行分片操作。 MTU 取值范围如下： • 在 IPv4 中，环回接口 MTU 取值范围为 68 ～ 65535 字节， PPPoE 接口的 MTU 取值范围为 68 ～ 1492 字节，其他三层接口的 MTU 取值范围为 68 ～ 1500 字节。 • 在 IPv6 中，环回接口 MTU 取值范围为 1280 ～ 65535 字节， PPPoE 接口的 MTU 取值范围为 1280 ～ 1492 字节，其他三层接口的 MTU 取值范围为 1280 ～ 1500 字节。 PPPoE 的 MTU 缺省为 1454 字节，其他三层接口的 MTU 缺省为 1500 字节。
二层接口列表	可以配置将二层 Access 模式的以太网接口、以太网通道、冗余接口以及虚拟接口划分到 VLAN 中或将二层以太网接口划分到以太网通道中。 VLAN 接口和以太网通道具有该属性。
IP 探测	用于探测 IP 地址。包括两种探测类型： • **IPv4 探测类型**：选项包括 None, Ping 和 ARP Ping。 • **IPv6 探测类型**：选项包括 None, Ping 和 NS Ping。 • **等待时间**：冗余接口恢复故障的时间。 仅有冗余接口具有该属性。
IPv4 地址配置	获取 IP 地址的方式包括静态 IP 和 DHCP。 • **静态 IP**：手动配置三层接口的静态 IP 地址。需要在 IP 地址列表中配置相关内容。 • **DHCP**：从 DHCP 服务器上获得动态分配的 IP 地址。管理员可以设置是否启用 DNS 代理。如果启用，系统将根据该接口通过 DHCP 方式获得的 DNS 自动添加代理。
IPv4 地址列表	该列表中包括主地址、 IPv4 地址和掩码长度，管理员可以添加最多 32 个 IPv4 地址。主地址表示该接口的主 IP 地址。

表 87 三层特有属性 (*续*)

配置信息	说明
IPv6 地址配置	包括配置链路本地地址以及 ULA 或全球单播地址。 • **链路本地地址**：包括自动生成 （缺省方式）和手动指定两种方式。 •当勾选**自动配置链路本地地址**时， NISG 根据链路本地地址前缀及接口的 MAC 地址，自动为该接口生成链路本地地址； •当取消勾选**自动配置链路本地地址**时，表示采用手动指定方式。 • **ULA 或全球单播地址**： •当勾选**无状态自动配置**时，表示采用无状态自动配置方式； •当取消勾选**无状态自动配置**时，表示采用手动配置方式 （缺省方式），需要在 **IP 地址列表**中配置相关内容。
IPv6 地址列表	该列表中的配置项包括 IPv6 地址、前缀长度、类型和状态，管理员最多可以向列表中手动添加 31 个 IPv6 全球单播地址。 • **类型**：表示手动配置 ULA 或全球单播地址的类型，包括手动和 EUI-64。 •当指定**手动**时，表示不使用 EUI-64 格式的接口标识； •当指定 **EUI-64** 时，表示使用 EUI-64 格式的接口标识。 • **状态**：表示 IPv6 地址的状态，包括临时地址 （TENTATIVE）、重复地址 （DUPLICATE）、首选地址 （PREFERRED）、不推荐地址 （DEPRECATED）以及无效地址 （INVALID）。

4.2 以太网接口

- 4.2.1 概述
- 4.2.2 基本配置步骤
- 4.2.3 范例：以太网接口

4.2.1 概述

缺省情况下， NISG 只有一个三层模式的以太网接口 eth0，其默认 IP 地址为 192.168.1.100/24，其他所有以太网接口都工作在二层 Access 模式。更多信息，请参见 4.1.1 工作模式。

- 管理接口

  管理员可以将三层以太网接口指定为专用管理口，以 （M）标识。该接口不能被划分到任何安全域。当专用管理口的工作模式或所属 Vsys 发生变化时，系统自动取消其管理功能，使其恢复为正常的数据转发接口。

  专用管理口可应用于：

  - Telnet、 SSH、 Web 和 Ping 访问设置；
  - SNMP、接口 WebAuth 认证、外部服务器认证和 NTP 校时；
  - 系统升级；
  - 发送 Syslog、电子邮件和 SNMP Trap 报警信息。
- 访问控制

  通过专用管理口访问 NISG 时，受访问控制策略的限制。请参见 3.11 访问服务。
- Vsys

  管理员可以将三层以太网接口划入到某个 Vsys 中。请参见第 13 章，虚拟系统。

4.2.2 基本配置步骤

- 4.2.2.1 二层接口
- 4.2.2.2 三层接口
- 4.2.2.3 三层共享接口

4.2.2.1 二层接口

1. 选择**网络** > **接口**。
2. 点击 ，设置接口为二层工作模式。

a. 将接口设置为 Access 模式，并将其划分到 VLAN 中。

b. 将接口设置为Trunk模式。从**VLAN列表**中选择的VLAN不能与Native VLAN相同。

3. 在**高级设置**区域，进行如下设置。“ 使用特定 MAC 地址 ” 功能对二层接口无效。

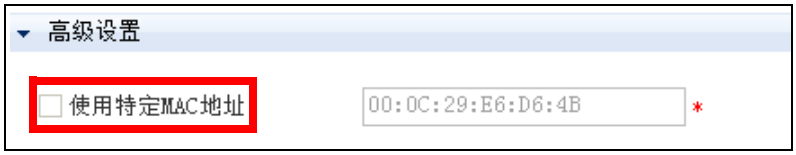


表 88 二层以太网接口命令

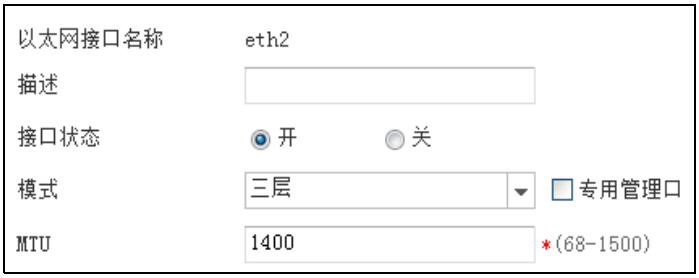
interface ethernet *interface_id*	进入指定的以太网接口配置模式。
working-type layer2-interface	设置接口为二层工作模式。
shutdown	禁用接口。
unset shutdown	启用接口。
port mode {access | trunk}	设置二层接口 （虚拟接口除外）的工作模式。

表 88 二层以太网接口命令 (*续*)

port access vlan *vlan_id*	将二层接口划分到指定 VLAN 中。
unset port access vlan	删除二层接口所隶属的 VLAN。
port trunk allowed vlan	设置指定 Trunk 端口所允许的 VLAN，即对允许的 VLAN 中的数据进行 802.1Q 封装。
unset port trunk allowed vlan	删除指定 Trunk 端口所允许的 VLAN。
port trunk native vlan *vlan_id*	设置指定 Trunk 端口所允许的 Native VLAN。即不对该 VLAN 中的数据进行 802.1Q 封装。
unset port trunk native	删除指定 Trunk 端口所允许的 Native VLAN。
hold ethernet *interface_id*	设置隶属于以太网通道的二层以太网接口。
unset hold ethernet *interface_id*	删除隶属于以太网通道的二层以太网接口。

4.2.2.2 三层接口

1. 选择**网络** > **接口**。
2. 点击 ，设置接口的工作模式、 MTU 值，并将其设置为管理接口。



3. 配置 IPv4 地址 （静态 IP）。**主**表示该地址作为主地址，优先被使用。

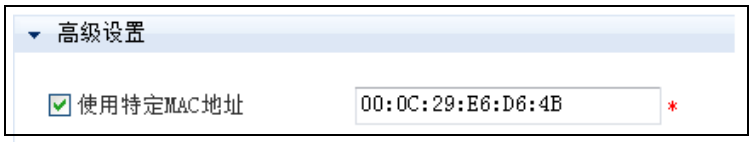
4. 配置 IPv4 地址 （DHCP）。

- 勾选**启用 DNS 代理**，为 DHCP 客户端接口自动添加 DNS 代理。
- 一个接口最多能够配置 32 个 IPv4 地址。

5. 配置 IPv6 地址。

- 缺省情况下，链路本地地址为自动生成。取消勾选**自动配置链路本地地址**，用户可指定链路本地地址。
- 勾选**无状态自动配置**，可以通过无状态地址自动配置的方式自动生成 IPv6 地址。
- 在 **IPv6 地址列表**中，可以手动配置 IPv6 地址。
- NISG 支持同时进行 IPv6 地址的自动配置和手动配置。
- 一个接口最多支持32个IPv6地址（包括1个链路本地地址和31个全球单播地址）。
- 链路本地地址和以无状态方式自动配置的地址不能用作主地址。

6. 在**高级设置**区域，勾选**使用特定 MAC 地址**，可以修改当前 MAC。



- 缺省情况下，系统提供一个特定的 MAC 地址。

表 89 三层以太网接口命令

working-type layer3-interface	设置接口为三层工作模式。
management-only	设置三层以太网接口为专用管理口。
unset management-only	取消设置三层以太网接口为专用管理口。
mtu {*mtu_value* | **default**}	设置三层或三层共享接口的 MTU。
ip address *ipv4 netmask* [**secondary**]	为指定的三层或三层共享接口添加 IPv4 地址。
unset ip address [*ipv4*]	删除指定三层或三层共享接口的 IPv4 地址。
dhcp client	在三层或三层共享接口上启用 DHCP 客户端。该接口会通过 DHCP 服务器自动获得动态 IP 地址。
unset dhcp client	删除 DHCP 客户端的设置。
dhcp update ip address	重新获得动态 IP 地址。
dhcp enable-dns-proxy	启用为 IPv4 工作模式的 DHCP 客户端接口自动添加 DNS 代理的功能。
unset dhcp enable-dns-proxy	禁用为工作在 IPv4 模式的 DHCP 客户端接口自动添加 DNS 代理功能。
ipv6 enable	启用指定三层或三层共享接口的 IPv6 功能。
unset ipv6 enable	禁用指定三层或三层共享接口的 IPv6 功能。
ipv6 address {*ipv6* | **auto**} **link-local**	为指定的三层或三层共享接口设置链路本地地址。
ipv6 address autoconfig	启用指定三层或三层共享接口的无状态地址自动配置功能。
unset ipv6 address autoconfig	禁用指定三层或三层共享接口的无状态地址自动配置功能。
ipv6 address {*ipv6* | *ipv6/prefix*} [**eui-64**]	为指定的三层或三层共享接口手动添加 ULA 地址和全球单播地址。
unset ipv6 address	删除指定三层或三层共享接口的 ULA 地址和全球单播地址。
default mac	获取以太网接口、以太网通道、 VLAN 或冗余接口的默认 MAC 地址。
mac address *mac_address*	修改以太网接口、以太网通道、 VLAN 或冗余接口的 MAC 地址。
show interface [**brief**]	显示所有接口信息。
show interface ethernet [*interface_id* | **brief**]	显示以太网接口信息。

4.2.2.3 三层共享接口

1. 选择**网络** > **接口**。
2. 点击以太网接口所对应的 ，进行如下配置。只有首先将三层共享接口划分到 Vsys 后，才可以为其添加地址。

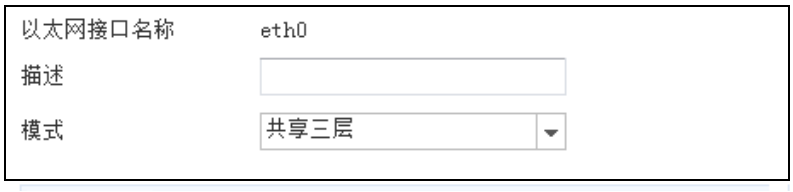


表 90 三层共享以太网接口命令

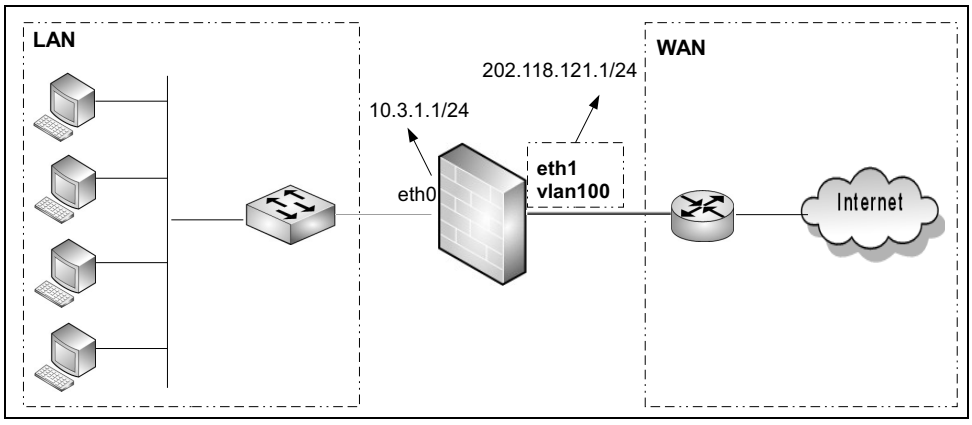
working-type layer3-shared-interface	设置接口为三层共享工作模式。

4.2.3 范例：以太网接口

本范例需完成如下设置：

- 设置 eth0 为三层接口，并设置 IP 地址为 10.3.1.1，掩码长度为 24。
- 创建vlan100，将二层接口eth1划分到vlan100内，并设置IP地址为202.118.121.1，掩码长度为 24。

图 5 接口配置

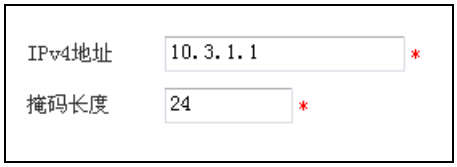


具体操作如下：

WebUI

1. 选择**网络** > **接口**。
2. 在**接口列表中**点击 eth0 所对应的 ，进行如下配置。

3. 在 **IP 地址列表**中点击**添加**。



4. 点击**确定**。

5. 点击**新建** >**VLAN**，进行如下配置：

6. 点击 ，进入到 vlan100 的编辑页面，进行如下配置：

7. 在 **IP 地址列表**中点击**添加 ,** 进行如下配置：

8. 点击**确定**。
9. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] interface ethernet 0
NetEye@root-system-if-eth0] working-type layer3-interface
NetEye@root-system-if-eth0] ip address 10.3.1.1 255.255.255.0
NetEye@root-system-if-eth0] exit
NetEye@root-system] vlan 100
NetEye@root-system-vlan100] hold ethernet 1
NetEye@root-system-vlan100] ip address 202.118.121.1 255.255.255.0
NetEye@root-system-vlan100] end
NetEye@root> save config
```

4.3 以太网通道

- 4.3.1 概述
- 4.3.2 基本配置步骤

4.3.1 概述

以太网通道 （即 Channel 接口）是把两个或多个以太网接口绑定在一起作为一个逻辑接口来用，以增加带宽，提高容错能力。 NISG 最多支持 8 个以太网通道。

- 以太网通道成员之间通过使用同一个 MAC 地址来扮演同一个接口的角色。
- 以太网通道的传输速率是通道中包含的所有以太网接口的传输速率的总和。
- 当以太网通道内的某个以太网接口出现故障时，数据包将由通道内的其他以太网接口转发。
- 管理员可以将三层以太网通道划分到某个 Vsys 中。

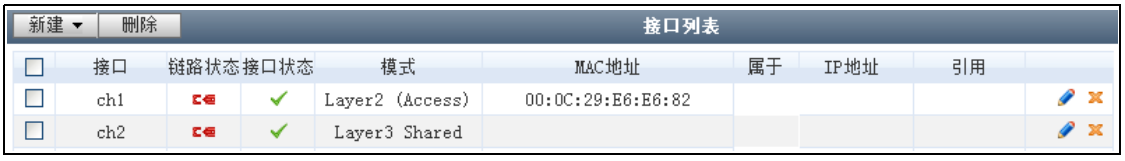
4.3.2 基本配置步骤

- 4.3.2.1 二层接口
- 4.3.2.2 三层接口
- 4.3.2.3 三层共享接口

4.3.2.1 二层接口

1. 选择**网络** > **接口**。
2. 点击**新建**。

3. 查看以太网通道。



4. 点击以太网通道所对应的 ，为其分配未使用的二层以太网接口。

5. 二层高级设置 （Access 和 Trunk 模式）和 MAC 地址设置与以太网接口相同。详见 4.2.2.1 二层接口的步骤 2-3。

表 91 二层以太网通道命令

channel *channel_id*	创建以太网通道或者进入指定的以太网通道配置模式。
unset channel *channel_id*	删除指定的以太网通道。
show interface channel [*channel_id* | **brief**]	显示以太网通道信息。
shutdown	禁用接口。
unset shutdown	启用接口。
hold ethernet *interface_id*	设置隶属于以太网通道的二层以太网接口。
unset hold ethernet *interface_id*	删除隶属于以太网通道的二层以太网接口。
working-type layer2-interface	设置接口为二层工作模式。

4.3.2.2 三层接口

1. 选择**网络** > **接口**。
2. 点击 ，配置 IPv4 地址（静态 IP 和 DHCP 方式）和 IPv6 地址。配置方式同以太网接口，详见 4.2.2.2 三层接口的步骤 3-5。
3. 在**高级设置**区域，如果不使用默认的 MAC 地址，可以指定一个 MAC 地址。

关于 IPv4 和 IPv6 的 CLI 配置，参见表 89 三层以太网接口命令。

4.3.2.3 三层共享接口

1. 选择**网络** > **接口**。
2. 点击以太网通道所对应的 ，为其分配未使用的二层以太网接口，并设置工作模式。

表 92 三层共享以太网通道命令

hold ethernet *interface_id*	设置隶属于以太网通道的二层以太网接口。
unset hold ethernet *interface_id*	删除隶属于以太网通道的二层以太网接口。
working-type layer3-shared-interface	设置接口为三层共享工作模式。

4.4 冗余接口

- 4.4.1 概述
- 4.4.2 基本配置步骤

4.4.1 概述

冗余接口 （即 Redundant 接口）是将两个以太网接口绑定在一起作为一个逻辑接口使用，起到冗余的作用，实现了接口级的高可靠性。 NISG 允许最多创建 4 个冗余接口。

- 一个以太网接口充当主接口，另外一个充当备用接口。
- 没有数据流量通过备用接口。
- 当主接口发生故障时，备用接口成为主接口并接管流量。故障切换自动进行。
- 当其中一个成员以太网接口被删除时，另外一个也会自动被删除。
- 管理员可以将三层模式的冗余接口划分到某个 Vsys 中。

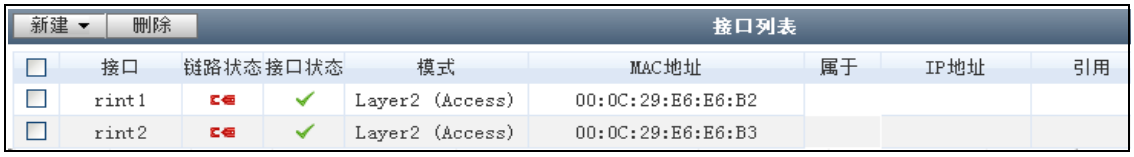
4.4.2 基本配置步骤

- 4.4.2.1 二层接口
- 4.4.2.2 三层接口
- 4.4.2.3 三层共享接口

4.4.2.1 二层接口

1. 选择**网络** > **接口**。
2. 点击**新建**。

3. 查看冗余接口。



4. 点击冗余接口所对应的 ，为其分配两个二层以太网接口（主和备用接口），并设置为二层工作模式。

必须同时选择两个以太网接口或者一个都不选。

5. 设置等待时间，即冗余接口从故障恢复所花费的时间。

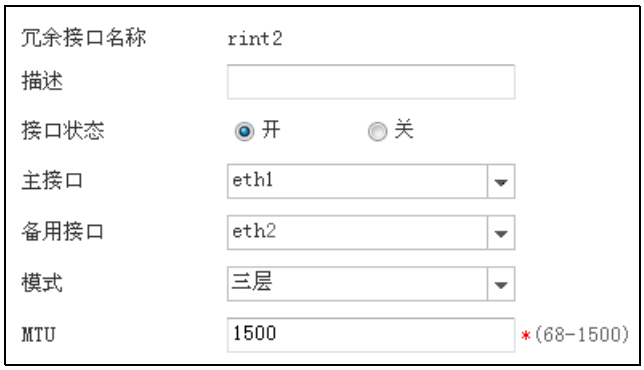
6. 二层高级设置（Access 和 Trunk 模式）和 MAC 地址设置与以太网接口相同。详见 4.2.2.1 二层接口的步骤 2-3。

表 93 二层冗余接口命令

rint *rint_id*	创建冗余接口或者进入指定的冗余接口配置模式。
unset rint *rint_id*	删除指定的冗余接口。
show interface rint [*rint_id* | **brief**]	显示冗余接口信息。
shutdown	禁用接口。
unset shutdown	启用接口。
hold ethernet primary *interface_id* **secondary** *interface_id*	设置冗余接口的主备以太网接口。
unset ethernet	删除冗余接口的主备接口。
switch	进行冗余接口的主备切换。
working-type layer2-interface	设置接口为二层工作模式。
wait-time *wait_time*	设置冗余接口的故障恢复等待时间。

4.4.2.2 三层接口

1. 选择**网络** > **接口**。
2. 点击冗余接口所对应的 ，为其分配主和备用接口，并设置工作模式及 MTU 值。 配



置 IPv4 地址 （静态 IP 和 DHCP 方式）和 IPv6 地址。配置方式同以太网接口，详见 4.2.2.2 三层接口的步骤 3-5。

3. 在**高级设置**区域，可以修改 MAC 地址，并进行探测配置。

在指定 IPv6 探测类型前，需要首先勾选**启用 IPv6**，启用冗余接口的 IPv6 功能。

表 94 三层冗余接口命令

hold ethernet primary *interface_id* **secondary** *interface_id*	设置冗余接口的主备以太网接口。
unset ethernet	删除冗余接口的主备接口。
working-type layer3-interface	设置接口为三层工作模式。
mtu {*mtu_value* | **default**}	设置三层或三层共享接口的 MTU。
default mac	获取以太网接口、以太网通道、 VLAN 或冗余接口的默认 MAC 地址。
mac address *mac_address*	修改以太网接口、以太网通道、 VLAN 或冗余接口的 MAC 地址。
monitor type	设置指定三层或三层共享冗余接口的 IPv4 探测方式。
unset monitor type	删除指定三层或三层共享冗余接口的 IPv4 探测方式。

表 94 三层冗余接口命令 (*续*)

monitor typev6	设置指定三层或三层共享冗余接口的 IPv6 探测方式。
unset monitor typev6	删除指定三层或三层共享冗余接口的 IPv6 探测方式。
wait-time *wait_time*	设置冗余接口的故障恢复等待时间。

关于 IPv4 和 IPv6 的 CLI 配置，参见表 89 三层以太网接口命令。

4.4.2.3 三层共享接口

1. 选择**网络** > **接口**。
2. 点击冗余接口所对应的 ，为其分配未使用的二层以太网接口，并设置工作模式。

表 95 三层共享冗余接口命令

hold ethernet primary *interface_id* **secondary** *interface_id*	设置冗余接口的主备以太网接口。
unset ethernet	删除冗余接口的主备接口。
working-type layer3-shared-interface	设置接口为三层共享工作模式。

4.5 虚拟接口

- 4.5.1 概述
- 4.5.2 基本配置步骤

4.5.1 概述

虚拟接口 （Virtual Interface）可以连接不同的虚拟网络，使 Vsys 之间不必依赖于以太网接口，而可以互相通信，更多信息，请参见 13.1.2. 虚拟网络 （Vnet）。 NISG 最多支持创建 1023 个虚拟接口。管理员可以将三层模式的虚拟接口划分到某个 Vsys 中。虚拟接口的使用方式和以太网接口类似，区别是：

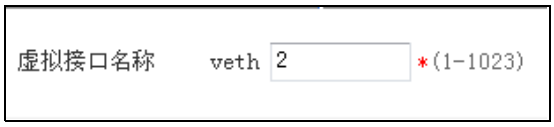
- 虚拟接口不能被划入以太网通道或冗余接口中；
- 不能作为 HA 接口；
- 也不能设置为 Trunk 模式。

4.5.2 基本配置步骤

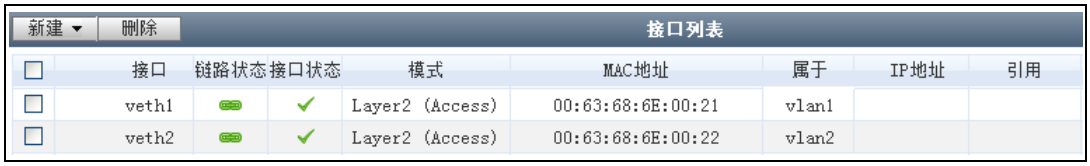
- 4.5.2.1 二层接口
- 4.5.2.2 三层接口

4.5.2.1 二层接口

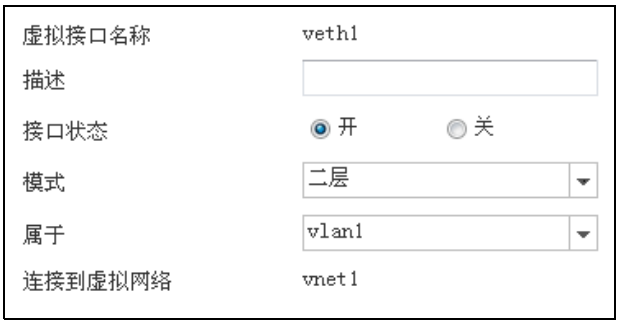
1. 选择**网络** > **接口**。
2. 点击**新建**。



3. 查看二层虚拟接口。



4. 点击虚拟接口所对应的 ，设置工作模式并指定其所属的 VLAN。



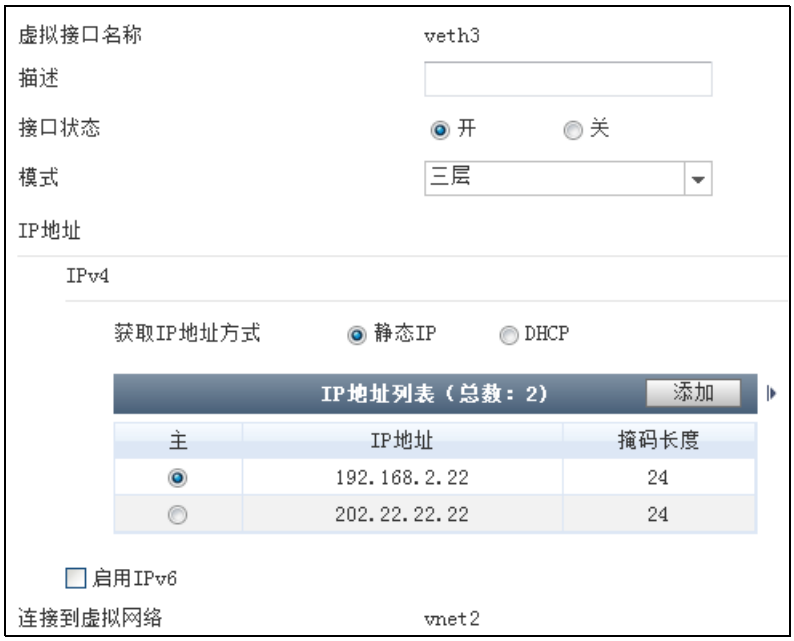
选择**系统 > 虚拟系统 > 虚拟网络**，将 veth1 划分到虚拟网络 vnet1 中，系统将自动显示上述结果。

表 96 二层虚拟接口命令

veth *veth_id*	创建虚拟接口或进入指定的虚拟接口配置模式。
unset veth *veth_id*	删除指定的虚拟接口。
show interface veth [*veth_id* | **brief**]	显示虚拟接口信息。
shutdown	禁用接口。
unset shutdown	启用接口。
working-type layer2-interface	设置接口为二层工作模式。
port access vlan *vlan_id*	将二层接口划分到 VLAN 中。
unset port access vlan	删除二层接口所隶属的 VLAN。

4.5.2.2 三层接口

1. 选择**网络** > **接口**。
2. 点击虚拟接口所对应的 ，进行如下配置。



- 虚拟接口不能工作在三层共享模式。
- 虚拟接口没有 MTU 值。
- 配置 IPv4 地址（静态 IP 和 DHCP 方式）和 IPv6 地址。配置方式同以太网接口，详见 4.2.2.2 三层接口的步骤 3-5。
- 关于 CLI 配置，参见表 89 三层以太网接口命令。

4.6 VLAN 接口

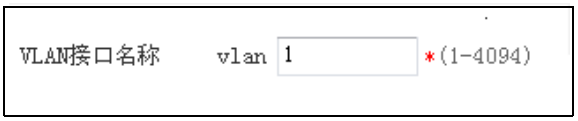
- 4.6.1 概述
- 4.6.2 基本配置步骤
- 4.6.3 范例：VLAN 接口

4.6.1 概述

VLAN （虚拟局域网）是将网络上的主机逻辑划分到一个广播域，而不在意这些主机的物理位置。 VLAN 接口实际就是一个包含二层接口的 VLAN。同一个 VLAN 内的成员通过二层交换模式直接通信，不同 VLAN 之间的成员则通过三层路由模式通信。在 NISG 中，管理员最多可以创建 4094 个 VLAN 接口。

4.6.2 基本配置步骤

1. 选择**网络** > **接口**。
2. 点击**新建**。



3. 查看 VLAN 接口。

4. 点击 VLAN 接口所对应的 ，为其分配未使用的二层接口。 VLAN 接口可以包含如下二层接口：以太网接口、以太网通道、冗余接口和虚拟接口。

5. 配置 IPv4 地址（静态 IP 和 DHCP 方式）和 IPv6 地址。配置方式同以太网接口，详见 4.2.2.2 三层接口的步骤 3-5。
6. 在**高级设置**区域，如果不使用默认的 MAC 地址，可以指定一个 MAC 地址。

表 97 VLAN 接口命令

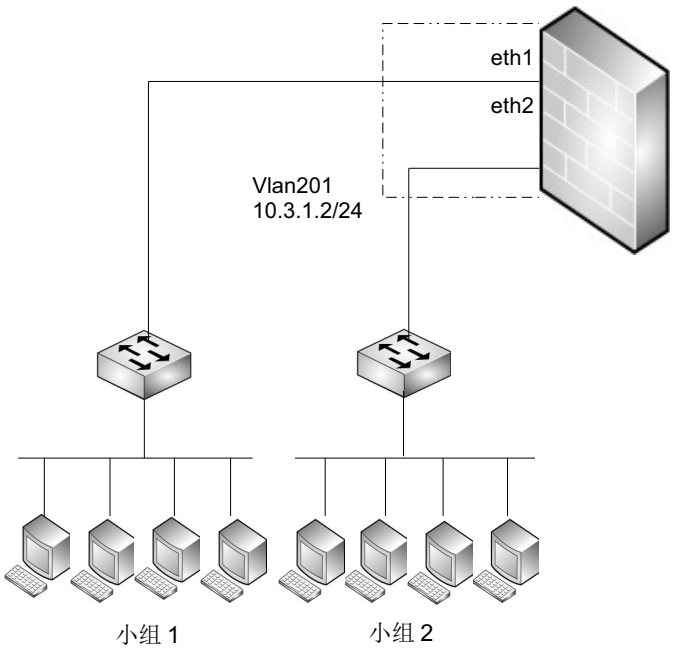
vlan *vlan_id*	创建 VLAN 或进入指定的 VLAN 配置模式。
unset vlan *vlan_id*	删除指定的 VLAN。
show interface vlan [*vlan_id* | **brief**]	显示 VLAN 信息。
shutdown	禁用接口。
unset shutdown	启用接口。
hold ethernet, channel, rint, veth	设置隶属于 VLAN 的二层接口。
unset hold ethernet, channel, rint, veth	删除隶属于 VLAN 的二层接口。
mtu {*mtu_value* | **default**}	设置三层或三层共享接口的 MTU。
default mac	获取以太网接口、以太网通道、 VLAN 或冗余接口的默认 MAC 地址。
mac address *mac_address*	修改以太网接口、以太网通道、 VLAN 或冗余接口的 MAC 地址。

关于 IPv4 和 IPv6 的 CLI 配置，参见表 89 三层以太网接口命令。

4.6.3 范例：VLAN 接口

部门 A 中有两个小组：小组 1 和小组 2。通过划分 VLAN 来实现同一部门之间以二层交换的方式通信。

图 6 VLAN 应用

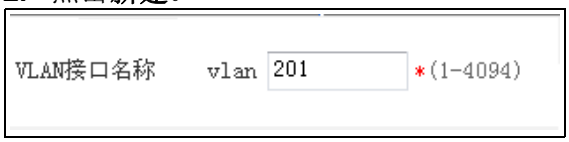


本范例需完成如下设置：

- 创建 vlan201。
- 将二层接口 eth1 和 eth2 划分到 vlan201 内。
- 为 vlan201 设置 IP 地址为 10.3.1.2，掩码长度为 24。

具体操作如下：

1. 选择**网络配置** > **接口**。
2. 点击**新建**。



3. 点击 vlan201 所对应的 ，进行如下配置：

4. 配置 IP 地址。

5. 点击**确定**。
6. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] vlan 201
NetEye@root-system-vlan201] hold ethernet 1,2
NetEye@root-system-vlan201] ip address 10.3.1.2 255.255.255.0
NetEye@root-system-vlan201] exit
NetEye@root-system-vlan201] end
NetEye@root> save config
```

4.7 环回接口

- 4.7.1 概述
- 4.7.2 基本配置步骤

4.7.1 概述

环回接口 （即 Loopback 接口）是三层逻辑接口。 NISG 最多支持 1023 个环回接口。

环回接口的链路状态永远处于已连接 （Up）状态，除非接口状态被禁用或所属的设备关闭。

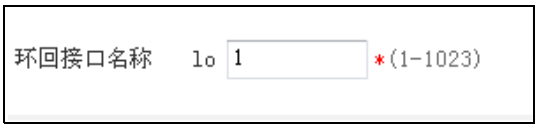
- 管理员可以利用环回接口的链路状态来探测设备状态。例如，网络管理站可以使用 SNMP 协议，获取 NISG 的状态信息和监控信息。更多信息，请参见 3.12 SNMP。
- 当环回接口正确配置了 IP 地址和相应的路由信息后，管理员可以通过此 IP 地址对 NISG 进行管理。
- 通过环回接口的数据访问受访问控制策略的限制。

在 Vsys 中应用时，环回接口：

- 可以由其所属 Vsys 的管理员自行创建和配置。
- 不同 Vsys 下的环回接口允许重名。
- 当 Vsys 被删除时，其包含的环回接口也将被删除。
- Vsys 内创建的环回接口不可以被划分到其他 Vsys 中。

4.7.2 基本配置步骤

1. 选择**网络** > **接口**。
2. 点击**新建**。



3. 查看环回接口。

4. 点击环回接口所对应的 ，进行如下配置。

- 一个环回接口只能配置一个 IPv4 地址和一个 IPv6 地址。
- IPv4 地址格式为：[1-223].[0-255].[0-255].[0-255]，不可以为 127.0.0.0~127.255.255.255 或者 192.168.255.254。
- 环回接口不支持 IPv6 地址自动配置 （链路本地地址除外）。

表 98 环回接口命令

loopback *lo_id*	创建环回接口或者进入指定的环回接口配置模式。
unset loopback *lo_id*	删除指定的环回接口。
show interface loopback [*lo_id* | **brief**]	显示环回接口信息。
shutdown	禁用接口。
unset shutdown	启用接口。
mtu {*mtu_value* | **default**}	设置三层或三层共享接口的 MTU。

关于 IPv4 和 IPv6 的 CLI 配置，参见表 89 三层以太网接口命令。

4.8 PPPoE 接口

- 4.8.1 概述
- 4.8.2 基本配置步骤
- 4.8.3 配置参数说明

4.8.1 概述

PPPoE 接口是三层逻辑接口。 NISG 最多允许创建 8 个 PPPoE 接口。

- 一个 PPPoE 接口必须绑定一个二层以太网接口或者二层冗余接口。
- 多个 PPPoE 接口可以对应同一个二层以太网接口或二层冗余接口。

NISG 可充当 PPPoE 客户端，通过 PPPoE 拨号功能，与 ISP 之间建立 PPP 连接。在这个过程中， PPPoE 接口可以获得本地 IP 地址、对端 IP 地址以及 DNS 服务器的 IP 地址。

NISG 支持两种 PPPoE 协议：PPPoEv4 和 PPPoEv6。前者基于 IPv4, 后者基于 IPv6。

- PPPoE 接口可作为 PPPoEv6 的客户端，通过 DHCPv6-PD（前缀分配）功能获得前缀信息，形成 PPPoE 接口的 IPv6 地址。
- 同一个二层以太网接口或二层冗余接口可以同时用于 PPPoEv4 接口和 PPPoEv6 接口。关于 PPPoE 接口的配置信息，请参见表 100 PPPoE 接口属性。

4.8.2 基本配置步骤

1. 选择**网络** > **接口**。
2. 点击**新建**。

3. 查看 PPPoE 接口。

4. 点击 PPPoE 接口所对应的 ，进行如下配置。

PPPoE 接口的 IPv6 地址只能通过 DHCPv6 获取。

表 99 PPPoE 接口命令

pppoe *pppoe_id*	创建 PPPoE 接口或者进入指定的 PPPoE 接口配置模式。
unset pppoe *pppoe_id*	删除指定的 PPPoE 接口。
show interface pppoe [*pppoe_id* | **brief**]	显示 PPPoE 接口信息。
active {**on** | **off**}	启用或禁用 PPPoE 接口。
mtu {*mtu_value* | **default**}	设置三层或三层共享接口的 MTU。
mode {**ipv4** | **ipv6**}	设置指定 PPPoE 接口的工作模式。
username *user_name* **password** *passwd*	配置拨号用户。
unset user	删除拨号用户。

表 99 PPPoE 接口命令 (*续*)

connection-type	配置拨号方式
connection-type ondemand idle	配置拨号闲置时间，在这个时间内如果没有数据传输，会自动断开拨号连接。
ip address *ipv4 netmask* [**secondary**]	为指定的三层或三层共享接口添加 IPv4 地址。
unset ip address [*ipv4*]	删除指定三层或三层共享接口的 IPv4 地址。
interface-id *if_id*	为指定的 PPPoE 接口配置接口标识。
unset interface-id	删除指定 PPPoE 接口的接口标识。
acname *ac_name*	设置 AC 名称。
unset acname	删除 AC 名称。
servicename *service_name*	设置服务名称。
unset servicename	删除服务名称。
hold {**ethernet** *interface_id* | **rint** *rint_id*}	设置隶属于 PPPoE 接口的二层以太网接口或二层冗余接口。
unset hold	删除隶属于 PPPoE 接口的二层接口。
overwrite-default-gateway	启用指定 PPPoE 接口的覆盖系统默认网关功能。
unset overwrite-default-gateway	禁用指定 PPPoE 接口的覆盖系统默认网关功能。
overwrite-dns	启用 IPv4 模式 PPPoE 接口的覆盖系统 DNS 功能。
unset overwrite-dns	禁用 IPv4 模式 PPPoE 接口的覆盖系统 DNS 功能。
enable-dns-proxy	启用为 IPv4 工作模式的 PPPoE 接口自动添加 DNS 代理的功能。
unset enable-dns-proxy	禁用为 IPv4 工作模式的 PPPoE 接口自动添加 DNS 代理的功能。
dhcp-prefix-delegate	启用指定 PPPoE 接口的自动触发 DHCPv6 客户端请求功能。
unset dhcp-prefix-delegate	禁用指定 PPPoE 接口的自动触发 DHCPv6 客户端请求功能。

4.8.3 配置参数说明

表 100 PPPoE 接口属性

配置信息	说明
接口状态	PPPoE 接口状态。 • **开**：表示该接口已连接。 • **关**：表示该接口已断开 （默认状态）。
MTU	最大传输单元。 • 在 IPv4 中， 68 ～ 1492 字节。 • 在 IPv6 中， 1280 ～ 1492 字节。 默认 MTU 值为 1454 字节。
模式	PPPoE 接口的工作模式，包括 IPv4 （默认模式）和 IPv6。
用户名	拨号用户的名称，长度范围为 0-127 字节。由数字、字母和下列特殊字符组成：`~!@#$%^&*()_+-=[]{}|;:"<>,./?，且必须以数字或字母开头。

表 100 PPPoE 接口属性 (*续*)

配置信息	说明
密码	拨号用户的密码，由 0 ～ 127 字节的 UTF-8 字符组成 （空格除外）。
连接方式	拨号类型。包括： • **自动拨号** （默认方式）：自动连接到 ISP。当连接断开时， NISG 将自动重连。 • **按需拨号**：根据访问需求进行拨号。
重拨次数	拨号连接最大尝试次数。 取值范围是 0 ～ 999， 0 表示没有重拨次数限制，默认值 0。
重拨间隔	拨号连接的时间间隔。 取值范围是 5 ～ 600 秒，默认值 60 秒。
空闲时间	拨号的空闲时间，即在所设置的时间内没有数据传输时，将断开拨号连接。 取值范围是 0 ～ 120 分钟， 0 表示不断开连接，默认值 0。 该属性仅在按需拨号方式时生效。
IP 地址	在 PPPoE 接口上配置的 IPv4 地址，用于 PPPoE 通信。地址格式为 [1-223].[0-225].[0-225].[0-225]，不允许输入 127.0.0.0-127.255.255.255 和 192.168.255.254。 该属性仅在 IPv4 模式下生效。
接口 ID	64 位的手动配置的接口标识。当接口标识无法通过自动 PPPoE 协商获得时，需要用户进行手动配置。 该属性仅在 IPv6 模式下生效。
AC 名称	该名称通常是 ADSL Modem 的商标、型号或序列号，由 ISP 负责提供，一般不需配置。 名称为 0-127 字节的 UTF-8 字符 （空格和问号除外）。
服务名称	该名称通常是 ISP 的名称或 ISP 提供的服务名称，由 ISP 负责提供，一般不需要配置。 名称为 0-127 字节的 UTF-8 字符 （空格和问号除外）。
以太网接口	该接口用于 PPPoE 通信时接收或发送数据包。 此接口必须是二层以太网接口或二层冗余接口。
覆盖默认网关	进行 PPPoE 拨号后，默认网关将指向 PPPoE 接口。 系统默认为禁用。
覆盖 DNS	NISG 中的 DNS 主机上配置的 DNS 服务器信息将被从 ISP 获得的 DNS 信息所覆盖。该属性仅在 IPv4 模式下生效。 系统默认为禁用。
启用 DNS 代理	系统将根据该接口通过 PPPoE 拨号方式获得的 DNS 自动添加 DNS 代理。该属性仅在 IPv4 模式下生效。 系统默认为禁用。
DHCP 前缀分配	充当 DHCPv6 客户端的 PPPoE 接口将在 PPPoE 协商成功后自动向 DHCPv6 服务器请求分配前缀和其他配置参数。该属性仅在 IPv6 模式下生效。 系统默认为禁用。

4.9 隧道接口

- 4.9.1 概述
- 4.9.2 基本配置步骤
- 4.9.3 配置参数说明

4.9.1 概述

隧道接口 （即 Tunnel 接口）是三层逻辑接口，用于建立 VPN 通信。 NISG 不允许管理员手动创建隧道接口。

- 管理员在创建基于路由的 IPSec VPN 隧道和 SSL VPN 隧道时，将联动创建一个隧道接口。
- 隧道被删除时，其联动创建的的隧道接口也将被相应删除。
- 管理员不能直接删除隧道接口。
- 隧道接口不支持 IPv6 配置。
- 对于联动创建的隧道接口，配置了静态 IP 地址后，系统将自动添加以该隧道接口为出口的直连路由，能够将信息流引入到对应的 IPSec 或 SSL VPN 隧道。

管理员可以为隧道接口配置静态 IP 地址，请参见表 102 隧道接口属性。隧道接口也可以借用其他三层或三层共享接口的 IP 地址作为自己的地址，既能完成隧道接口的路由交换，又能节省 IP 地址资源。更多信息，请分别参见第 5 章，路由和第 11 章，虚拟专用网。

4.9.2 基本配置步骤

1. 选择**网络** > **接口**。
2. 点击隧道接口所对应的 。
3. 配置 IPv4 地址 （静态 IP）。

隧道接口不支持 IPv6 地址配置。

4. 通过从其他接口借用 IP，配置 IPv4 地址：

- 一个隧道接口一次只能借用一个 IP 地址。
- 当要借用的接口具有两个以上的 IP 地址时，隧道接口将借用主 IP 地址。更多信息，请参见表 102 隧道接口属性。

表 101 隧道接口命令

tunnel *tunnel_id*	进入指定的 VPN 隧道接口配置模式。
mtu {*mtu_value* | **default**}	设置三层或三层共享接口的 MTU。
unnumbered *l3_interface_name*	借用三层或三层共享接口 （PPPoE 接口除外） IP 地址。
unset unnumbered	删除借用其他三层或三层共享接口的 IP 地址。
show interface tunnel [*tunnel_id* | **brief**]	显示 VPN 隧道接口信息。

关于 IPv4 和 IPv6 的 CLI 配置，参见表 89 三层以太网接口命令。

4.9.3 配置参数说明

管理员可以查看和编辑 IPSec VPN 隧道和 SSL VPN 隧道所联动创建的隧道接口。

表 102 隧道接口属性

配置信息	说明
类型	隧道接口的类型，分为 IPSec VPN 和 SSL VPN 两种，管理员不能修改。
MTU	最大传输单元。 隧道接口的 MTU 取值范围为 68~1500，默认 MTU 值为 1500。
获取 IP 地址方式	获取 IP 地址的方式包括静态 IP 和借用 IP。 • **静态 IP**：手动配置三层接口的静态 IP 地址。需要在 **IP 地址列表**中配置。 • **借用 IP**：允许隧道接口借用其他三层接口的 IP 地址。隧道接口可以借用其他接口 （包括 VLAN 接口、环回接口、三层或三层共享以太网接口、三层或三层共享以太网通道、三层或三层共享冗余接口以及三层虚拟接口）的 IP 地址作为自己的地址，参与路由交换。
IP 地址列表	该列表中包括主地址、 IPv4 地址和掩码长度，管理员可以添加最多 32 个 IPv4 地址，主地址表示该接口使用的首选 IP 地址。
引用	联动创建的隧道接口被管理员所配置的路由所引用。 如果隧道接口正被管理员配置的路由所引用，其对应的隧道将无法被删除。

4.10 ARP

- 4.10.1 概述
- 4.10.2 基本配置步骤
- 4.10.3 配置参数说明

4.10.1 概述

地址解析协议 （Address Resolution Protocol， ARP）是一种将网络层 IP 地址解析为数据链路层 MAC 地址的协议。用来记录 IP 地址和 MAC 地址一一对应关系的表叫 ARP 表。

NISG 的 ARP 表是一个用来对数据包进行三层转发的缓存表，最多可存储 32768 条表项。 NISG 的 ARP 表包括以下三种类型的 ARP 表项：

- 静态 ARP 表项

在 NISG 中，管理员可以手动创建和删除静态 ARP 表项。创建时需要输入 IP 地址、MAC 地址及所属三层接口。

- 动态 ARP 表项

NISG 支持自动创建动态 ARP 表项。 NISG 收到据包时，会根据数据包的目的 IP 地址，在 ARP 表中查询对应的 MAC 地址，如果没有匹配到 ARP 表项，则创建动态 ARP 表项，并以广播的形式向所有主机发送 ARP 请求，符合条件的目的主机告知自己的 MAC 地址。此时， NISG 会更新相应的 ARP 表项。如果没有收到应答，则删除该表项。

- 代理 ARP 表项

在 NISG 中，管理员可以创建和删除代理 ARP 表项。如果设置了对某 IP 地址的代理 ARP，则 NISG 会用该代理 ARP 表项中三层接口的 MAC 地址应答该 IP 地址的 ARP 请求。当虚拟专用网 （VPN）的两端子网处于同一网段的情况下，需要手动添加代理 ARP 表项，实现两端子网的通信；在三层接口上不设置 IP 地址时，也可以通过手动添加代理 ARP 表项实现路由功能。

4.10.2 基本配置步骤

表 103 ARP 命令

show arp [**vlan** *vlan_id* | **ethernet** *interface_id* | **channel** *channel_id* | **rint** *rint_id* | **veth** *veth_id* | *ipv4*]	查看当前系统的 ARP 表项。
show arp static	查看静态 ARP 表项。
show arp dynamic	查看动态 ARP 表项。
show arp timeout	查看动态 ARP 表项的超时时间。
show arp proxy	查看代理 ARP 表项。
arp {**vlan** *vlan_id* | **ethernet** *interface_id* | **channel** *channel_id* | **rint** *rint_id* | **veth** *veth_id*} *ipv4 mac_address*	创建静态 ARP 表项。
arp proxy {**vlan** *vlan_id* | **ethernet** *interface_id* | **channel** *channel_id* | **rint** *rint_id* | **veth** *veth_id*} *ipv4 mac_address*	创建代理 ARP 表项。
unset arp *ipv4*	删除指定 IPv4 地址的 ARP 表项。
unset arp static [**vlan** *vlan_id* | **ethernet** *interface_id* | **channel** *channel_id* | **rint** *rint_id* | **veth** *veth_id*]	删除静态 ARP 表项。

表 103 ARP 命令 (*续*)

unset arp dynamic [**vlan** *vlan_id* **| ethernet** *interface_id* **| channel** *channel_id* **| rint** *rint_id* **| veth** *veth_id*]	删除动态 ARP 表项。
unset arp proxy [**vlan** *vlan_id* **| ethernet** *interface_id* **| channel** *channel_id* **| rint** *rint_id* **| veth** *veth_id*]	删除代理 ARP 表项。
arp {**vlan** *vlan_id* **| ethernet** *interface_id* **| channel** *channel_id* **| rint** *rint_id* **| veth** *veth_id*} **timeout** {*timeout_value* **| default**}	编辑动态 ARP 表项的超时时间。

4.10.3 配置参数说明

管理员可以通过 WebUI 监控 ARP 表，或者通过 CLI 进行与 ARP 表相关的配置。更多信息，请参见 14.7 ARP。

表 104 ARP 表属性

配置信息	说明
IP 地址	即目的主机 IP 地址。该 IP 地址不能是环回地址、多播地址、指向子网的广播地址或受限制的广播地址。 添加静态 / 代理 ARP 条目时， IP 地址不可以是不可以是 0.0.0.0 和 255.255.255.255，也不可以是接口自身的 IP 地址。
MAC 地址	即与 IP 地址相对应的 MAC 地址。该 MAC 地址不能是广播或多播 MAC 地址。
类型	即 ARP 表项类型。 • 静态：表示静态 ARP 表项。 • 动态：表示动态 ARP 表项。 • 代理：表示代理 ARP 表项。
状态	即 ARP 表项的状态。包括四种： • **INCOMPLETE**：已发送 ARP 请求但还没有应答时的状态。 • **REACHABLE**：可用状态。 • **STALE**：可用，但生存时间过长，应再次查询学习。 • **FAILED**：不可用状态，该状态不可见。
生存时间	即动态 ARP 表项存活时间。
接口	即所属的三层接口。包括以太网接口、以太网通道、 VLAN 接口、虚拟接口、冗余接口和三层共享接口。

4.11 CAM

- 4.11.1 概述
- 4.11.2 基本配置步骤
- 4.11.3 配置参数说明

4.11.1 概述

内容可寻址存储器 （Content Addressable Memory，CAM）是一种系统内存结构，可以优化地址查询速度。 CAM 表是用于二层交换的地址表，提供 MAC 地址和二层接口的映射关系。当 NISG 接收到一个数据帧时，根据该数据帧的目的 MAC 地址查询 CAM 表，如果在该表中找到与 MAC 地址对应的 CAM 表项，则根据查询的结果从对应接口转发该数据帧；如果找不到对应的 CAM 表项，则在所属 VLAN 内广播。

NISG 的 CAM 表支持以下类型的表项， NISG 的 CAM 表最多可存储 16384 条表项。

- 本地 CAM 表项

本地 CAM 表项即 NISG 自身三层接口的 MAC 地址所对应的 CAM 表项，随三层接口创建和删除。

- 静态 CAM 表项

管理员手动创建和删除的 CAM 表项。创建时需要输入指定 VLAN、 MAC 地址和接口，该表项永不超时，只能手动删除。

- 动态 CAM 表项

NISG 支持动态 CAM 表项的动态学习。管理员可以设置动态 CAM 表项超时时间。当表项达到超时时间，将被删除。

- 多播 CAM 表项

在 VLAN 内发送多播数据包时使用该类型。

4.11.2 基本配置步骤

表 105 CAM 命令

show cam-table [vlan *vlan_id* | *mac_address*]	查看 CAM 表项。
show cam-table timeout	查看动态 CAM 表项的超时时间。
cam-table vlan *vlan_id* {**channel** *channel_id* | **ethernet** *interface_id* **| rint** *rint_id* **| veth** *veth_id*} *mac_address*	创建 CAM 表项。
unset cam-table *mac_address*	删除指定 MAC 地址的 CAM 表条目。
unset cam-table static vlan *vlan_id* [*mac_address*]	删除静态 CAM 表项。
unset cam-table dynamic [**vlan** *vlan_id*]	删除动态 CAM 表项。
cam-table timeout [**vlan** *vlan_id*] {*timeout_value* | **default**}	编辑动态 CAM 表的超时时间。

4.11.3 配置参数说明

管理员可以通过 WebUI 监控 CAM 表，或者通过 CLI 进行与 CAM 表相关的配置。更多信息，请参见 14.8 CAM。

表 106 CAM 表属性

配置信息	说明
目的地址	即数据包发往的 MAC 地址。该地址不能为 00:00:00:00:00:00 或 FF:FF:FF:FF:FF:FF.。
地址类型	即 CAM 表项类型。 • Local：表示本地 CAM 表项。 • Static：表示静态 CAM 表项。 • Dynamic：表示动态 CAM 表项。 • Multicast：表示多播 CAM 表项。
三层接口信息	即表项所属 VLAN。
目的端口	当表项为动态或静态类型时，对应的二层接口；当表项为多播类型时，是一个二层接口表，表示多播数据包应从这些二层接口转发出去。
超时时间	即动态 CAM 表的超时时间，取值范围为 10 ～ 30000 秒，缺省为 300 秒。

4.12 安全域

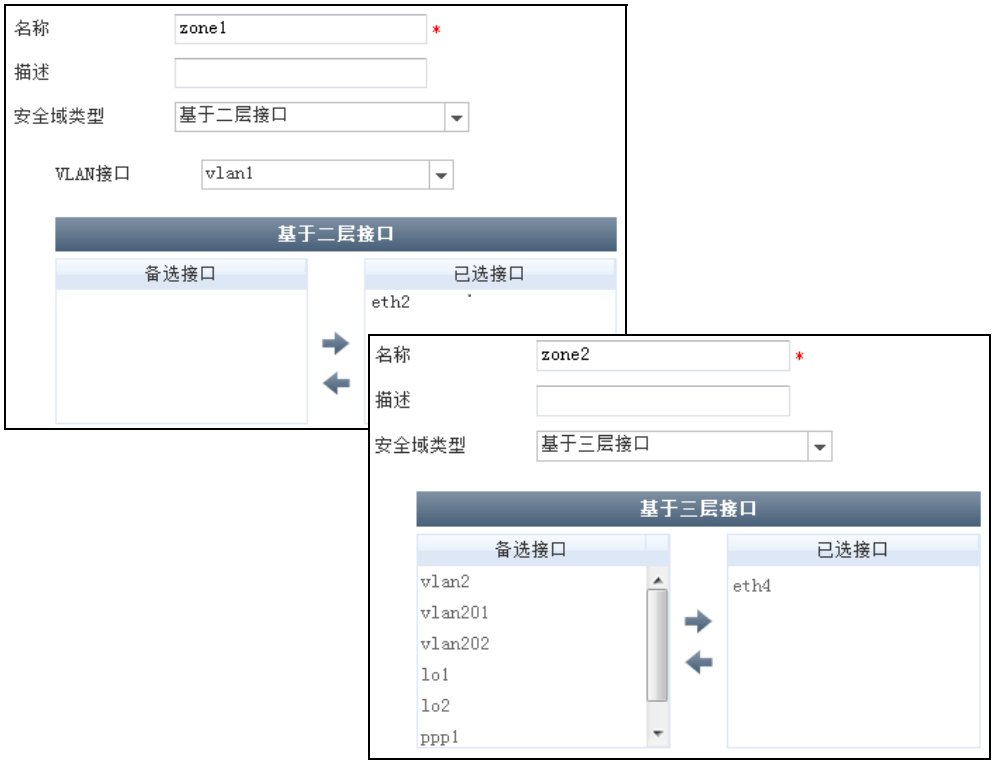
- 4.12.1 概述
- 4.12.2 基本配置步骤
- 4.12.3 范例：安全域应用
- 4.12.4 配置参数说明

4.12.1 概述

安全域是接口的集合，将这些接口所连接的若干个网络捆绑成一个区域，以便进行统一的安全管理。不同安全域之间只有通过配置访问策略才能相互访问。 NISG 系统默认不存在任何安全域， NISG 最多允许创建 30 个安全域。

4.12.2 基本配置步骤

1. 选择**网络** > **安全域**。
2. 点击**新建**，进行如下配置。



- 三层 （三层共享）接口和二层接口不能划分到同一个安全域中。
- 配置基于二层接口的安全域，需要为其指定一个 VLAN，并在 VLAN 中选择至少一个二层接口，将其划分给安全域。

- 若 VLAN 中所有二层接口被清空，该安全域仍为基于二层接口的安全域。
- 若包含这些二层接口的 VLAN 被删除，则原基于二层接口的安全域将自动变成基于三层接口的安全域。

3. 查看安全域。

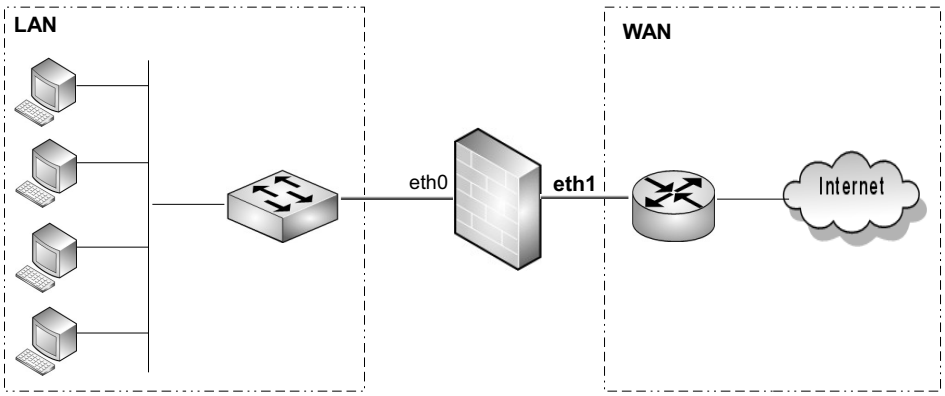
表 107 安全域命令

zone *zone_name*	创建安全域。
unset zone [*zone_name*]	删除安全域。
zone based-layer2	配置基于二层接口的安全域。
unset zone based-layer2	删除安全域中的二层接口。
zone based-layer3	配置基于三层或三层共享接口的安全域。
unset zone based-layer3	删除安全域中的三层或三层共享接口。
zone description	设置安全域的描述信息。
show zone [*zone_name*]	显示安全域的信息。

4.12.3 范例：安全域应用

某公司通过 NISG 与互联网进行通信，如下图所示。

图 7 安全域应用



本范例需完成如下设置：

- 创建一个安全域 LAN，将三层接口 eth0 划分到 LAN 中。
- 创建一个安全域 WAN，将三层接口 eth1 划分到 WAN 中。
- 设置安全域间缺省策略的动作为允许。

具体操作如下：

WebUI

1. 选择**网络** > **安全域**。
2. 点击**新建**，进入安全域的创建页面，进行如下配置：

3. 点击**确定**。

4. 点击**新建**，进入安全域的创建页面，进行如下配置：

5. 点击**确定**。
6. 选择**防火墙** > **缺省策略设置**。
7. 在**配置域间缺省策略**区域，进行如下配置：

8. 点击**确定**。
9. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] zone LAN
NetEye@root-system] zone LAN based-layer3 eth0
NetEye@root-system] zone WAN
NetEye@root-system] zone WAN based-layer3 eth1
NetEye@root-system] policy default inter-zone access permit
NetEye@root-system] exit
NetEye@root> save config
```

4.12.4 配置参数说明

表 108 安全域属性

配置信息	说明
名称	安全域的名称， 1~63 字节的 UTF-8 字符，不包含：?,'\"<>&# 和空格 名称不允许为 Any 和 mgt-interface。
类型	安全域类型。分为基于二层接口和基于三层接口 （缺省类型）。
接口	安全域包含的接口，一个接口只能划分到一个安全域中。
引用	引用安全域的策略列表。 被策略引用的安全域不能被删除。如需删除它们，应首先解除相应的引用关系。
描述	安全域的描述信息。 0 ～ 255 个字节的 UTF-8 字符，不包含：?'\"<>&。

4.13 DNS 主机

- 4.13.1 概述
- 4.13.2 基本配置步骤
- 4.13.3 配置参数说明

4.13.1 概述

NISG 可作为 DNS 客户端从 DNS 服务器请求域名解析。管理员最多能够设置三个 IPv4 DNS 服务器和两个 IPv6 DNS 服务器 IP 地址，提供域名解析服务 , 如解析 NISG 系统升级服务器、 UTM 规则升级服务器、 LDAP 服务器等域名。

4.13.2 基本配置步骤

1. 选择**网络 >DNS> 主机**。
2. 进行如下配置。

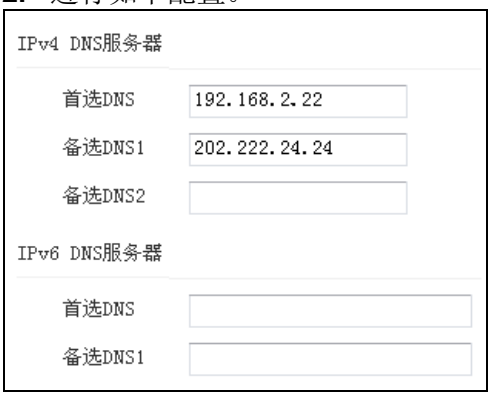


表 109 DNS 主机命令

dns host	配置 NISG 域名服务器。
unset dns host	删除域名服务器配置。
show dns host	显示 DNS 服务器配置。

4.13.3 配置参数说明

表 110 DNS 主机属性

配置信息	说明
IPv4 DNS 服务器	IPv4 DNS 服务器的 IP 地址，包括首选 DNS、备选 DNS1 以及备选 DNS2。可以输入的 IP 地址范围为：[1-223].[0-255].[0-255].[0-255]，不可以为 127.0.0.0~127.255.255.255 或者 192.168.255.254。
IPv6 DNS 服务器	IPv6 DNS 服务器的 IP 地址，包括首选 DNS 和备选 DNS1。不可为 IPv6 DNS 服务器配置下列 IP 地址：环回地址 （::1）、多播地址 （FF00/8~FFFF/8）、未指定地址（::）、 ::FFFF:0:0/96。

4.14 DNS 代理

- 4.14.1 概述
- 4.14.2 基本配置步骤
- 4.14.3 配置参数说明

4.14.1 概述

NISG 的 DNS 代理具有以下优点：

- DNS 代理具有分隔 DNS 查询请求的功能。
- DNS 代理允许通过隧道接口发送 DNS 请求。
- 通过在 NISG 上的本地缓存，提升 DNS 查询的速度。

DNS 代理分为非透明代理和透明代理服务， NISG 默认不开启这两种服务。

- 非透明代理

如果把 DNS 客户端的 DNS 服务器指向 NISG，那么对于 DNS 客户端来说， NISG 就相当于 DNS 服务器。

当管理员配置 DNS 代理服务器或者添加本地静态缓存时， NISG 即开启非透明代理服务。更多信息，请参阅 4.14.3 配置参数说明和 4.15.3 配置参数说明。

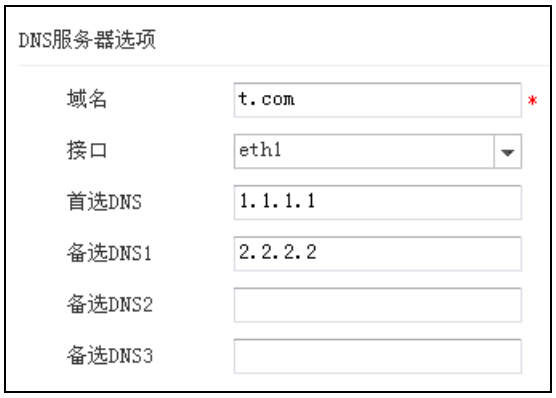
- 透明代理

当 DNS 客户端将网关指向 NISG， DNS 服务器指向真正的 DNS 服务器的 IP 地址时，DNS 代理对用户完全透明。

当管理员配置访问策略，并在策略中启用 DNS 代理时， NISG 即开启透明代理服务。更多信息，请参阅 8.1.2 访问策略。

4.14.2 基本配置步骤

1. 选择**网络 >DNS>DNS 代理**。
2. 进行如下配置。



- NISG 最多支持 2048 个 DNS 代理条目。
- 管理员可以在一个 DNS 代理条目中同时配置 IPv4 和 IPv6 DNS 服务器的 IP 地址。
- 可为 DNS 服务器配置的的 IPv4 地址范围为：[1-223].[0-255].[0-255].[0-255]，不允许输入 127.0.0.0~127.255.255.255 或者 192.168.255.254。不可为 DNS 服务器配置下列 IPv6 地址：环回地址 （::1）、多播地址 （FF00/8~FFFF/8）、未指定地址 （::）、::FFFF:0:0/96。

3. 查看 DNS 代理条目。

表 111 DNS 代理命令

dns server-select	添加 DNS 代理。
unset dns server-select	删除 DNS 代理。
show dns server-select	显示 DNS 代理配置信息。

4.14.3 配置参数说明

表 112 DNS 代理配置信息

配置信息	说明
域名	需要使用 DNS 代理的域名。 可以输入合法的域名或输入 *（表示匹配所有的域名）。
接口	即转发域名解析请求的三层接口。缺省情况下接口设置为 Any，环回接口除外。
首选 DNS	即首选 DNS 服务器的 IPv4 或 IPv6 地址。
备选 DNS1	即第一备选 DNS 服务器的 IPv4 或 IPv6 地址。
备选 DNS2	即第二备选 DNS 服务器的 IPv4 或 IPv6 地址。
备选 DNS3	即第三备选 DNS 服务器的 IPv4 或 IPv6 地址。

4.15 DNS 缓存

- 4.15.1 概述
- 4.15.2 基本配置步骤
- 4.15.3 配置参数说明

4.15.1 概述

当用户通过 NISG 使用 DNS 查询时：

1. 首先在静态缓存中查找记录。
2. 如果没有查询到相应的信息，则继续查找动态缓存。
3. 如果仍然没有查询到相应的信息，则通过代理功能向其他 DNS 服务器转发请求包，直到查找成功并把此次查询结果记录在动态缓存中。

NISG 支持两种缓存类型：

- 动态缓存

  动态缓存会动态记录 IP 地址、相应的域名和生存时间。动态缓存表最多保存 1024 条条目。

- 静态缓存

  配置静态缓存时，需要设置 IP 地址、相应的域名和入口接口信息。静态缓存表最多保存 2048 条条目。

4.15.2 基本配置步骤

1. 选择**网络 >DNS> 静态缓存**。
2. 进行如下配置。

- 要使 DNS 静态缓存功能生效，需要在 **DNS 静态缓存**区域点击**启用**，启用该功能。

- 管理员可以通过 **unset dns cache dynamic** [*domain_name*] 命令删除 DNS 动态缓存。

3. 查看静态缓存条目。

表 113 DNS 缓存命令

dns cache	添加静态 DNS 缓存。
dns cache-state {on | off}	启用或禁用 DNS 静态缓存。
unset dns cache dynamic	删除动态 DNS 缓存。
unset dns cache static	删除静态 DNS 缓存。
show dns cache	显示 DNS 缓存信息。
show dns cache-state	显示 DNS 静态缓存状态。

4.15.3 配置参数说明

表 114 DNS 静态缓存配置信息

配置信息	说明
域名	即静态缓存条目中的域名。
IP 地址	即静态缓存条目中与域名相对应的 IP 地址。可以在一个 DNS 静态缓存条目中同时配置 IPv4 和 IPv6 地址。 IPv4 地址格式为：[1-223].[0-255].[0-255].[0-255]，不能输入 127.0.0.0~127.255.255.255 或者 192.168.255.254。 一个域名可以同时对应最多 32 个 IP 地址。
接口	即收到域名解析请求的三层接口，环回接口除外。

4.16 DHCP 服务器

- 4.16.1 概述
- 4.16.2 基本配置步骤
- 4.16.3 DHCP 范例
- 4.16.4 配置参数说明

4.16.1 概述

动态主机配置协议 （Dynamic Host Configuration Protocol， DHCP）用于动态地分配 IP 地址。 NISG 可以同时充当 DHCP 客户端、服务器和中继代理。

NISG 支持三种 DHCP 角色，一个接口上只能配置一种 DHCP 角色。

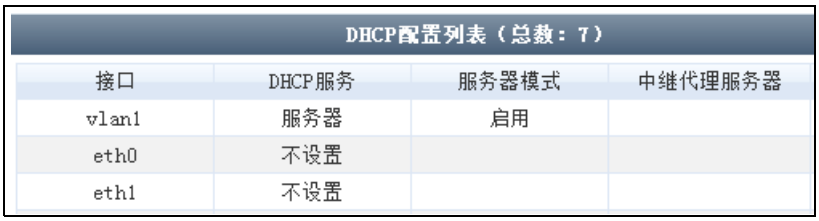
- **DHCP 服务器:** 为任意安全域的任意接口上的主机（充当 DHCP 客户端）动态分配 IP 地址。
- **DHCP 中继代理:** 接收来自 DHCP 服务器的 DHCP 信息，然后将这些信息转发给任意安全域的任意接口上的主机。
- **DHCP 客户端:** 接收动态分配的 IP 地址。相关配置需要在 “ 接口 ” 部分进行，请参见 4.2.2.2 三层接口的步骤 4。

4.16.2 基本配置步骤

1. 选择**网络 >DHCP>DHCP 服务器**。
2. 进行如下配置。只有配置了合法 IP 地址的接口才能够进行 DHCP 服务器与 DHCP 中继代理的配置。

- 在**DHCP 服务器**页面中，管理员可以通过点击**DHCP IP 地址绑定状态**进入监控页面，查看 DHCP IP 地址绑定状态信息。
- 配置 DHCP 中继代理时，如果勾选**将客户端网关 IP 地址指向中继接口**，则 NISG 将把转发的 DHCP 应答报文中的网关字段强制修改为该 DHCP 中继接口的 IP 地址 （如果 DHCP 应答报文中没有网关字段，那么强制添加）。

3. 查看 DHCP 配置条目。



DHCP配置列表（总数：7）

接口	DHCP服务	服务器模式	中继代理服务器
vlan1	服务器	启用	
eth0	不设置		
eth1	不设置		

表 115 DHCP 服务器命令

dhcp interface none	取消指定接口的 DHCP 角色。
dhcp interface relay	设置指定接口为 DHCP 中继代理。
unset dhcp interface relay	取消指定接口的 DHCP 中继代理角色。
dhcp interface relay change-gateway	设置接口的 DHCP 中继代理是否更新网关。
dhcp interface server {auto | enable | disable}	设置指定接口的 DHCP 服务器模式。
unset dhcp interface all	删除所有接口的 DHCP 配置。
show dhcp interface [*interface_name*]	显示 DHCP 接口的配置信息。
show dhcp server ip-binding	显示 DHCP 服务器的 IP 地址绑定状态。

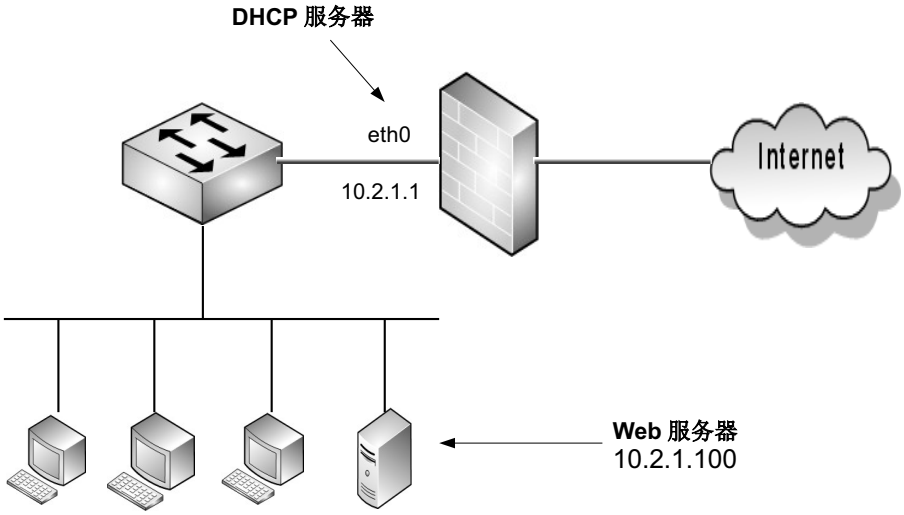
4.16.3 DHCP 范例

- 范例 1：配置 DHCP 服务器
- 范例 2：配置 DHCP 中继代理

范例 1：配置 DHCP 服务器

NISG 的接口 eth0 配置为 DHCP 服务器，为内网的 DHCP 客户端动态分配子网 10.2.1.0/24 中的 IP 地址以及其他网络配置参数。其中，内网中有一台 MAC 地址为 44:37:E6:27:C5:D5 的 Web 服务器需要固定获取 10.2.1.100 的 IP 地址。

图 8 配置 DHCP 服务器



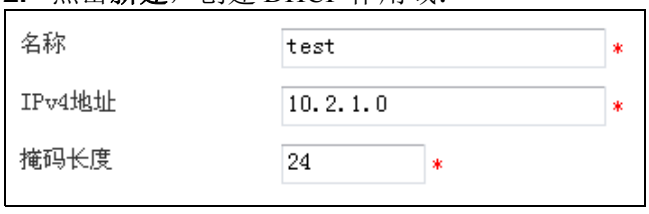
本范例需完成如下设置：

- 创建一个 DHCP 服务器作用域：test，网段为 10.2.1.0/24。
- 设置 eth0 接口为 DHCP 服务器。
- 设置保留 IP 地址 10.2.1.100。

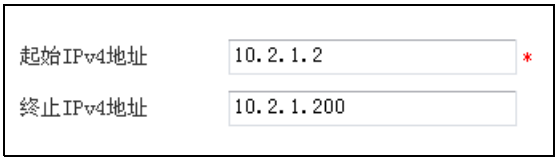
具体操作如下：

WebUI

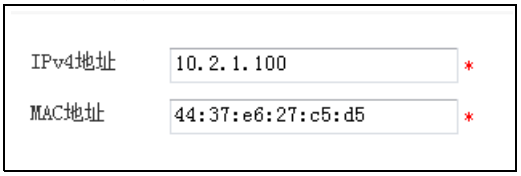
1. 选择**网络 >DHCP>DHCP 作用域**。
2. 点击**新建**，创建 DHCP 作用域：



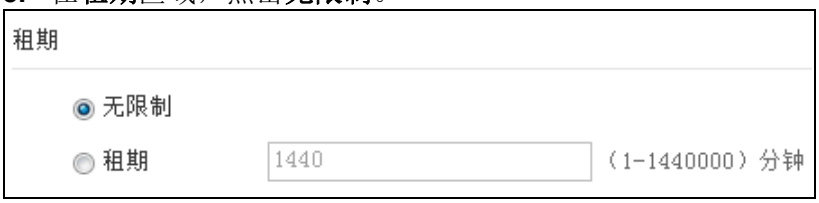
3. 点击 **IP 地址池列表**中的**添加**，进行如下设置：



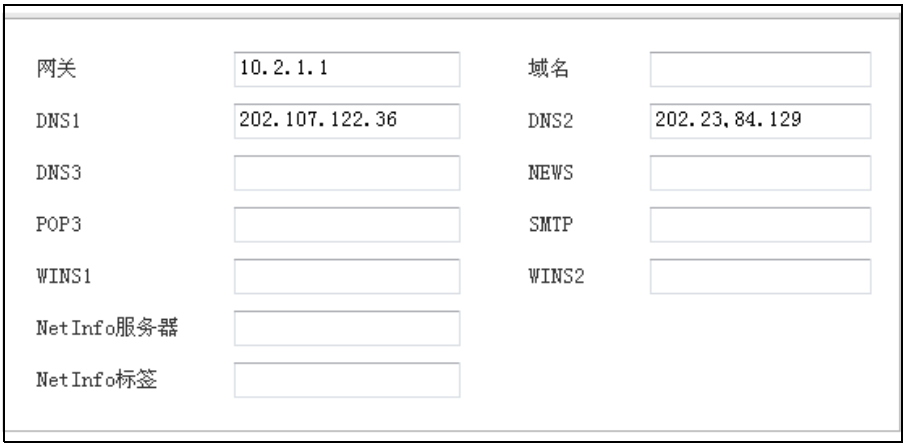
4. 点击**保留地址列表**中的**添加**，进行如下设置：



5. 在**租期**区域，点击**无限制**。



6. 点击**高级设置**区域，进行如下设置：



7. 点击**确定**。
8. 选择**网络 >DHCP>DHCP 服务器**。
9. 在 **DHCP 配置列表**中点击 eth0 所所对应的 ，进入 eth0 的编辑页面。
10. 在**服务器**区域，将服务器模式设置为**自动**。

11. 点击**确定**。
12. 点击 。

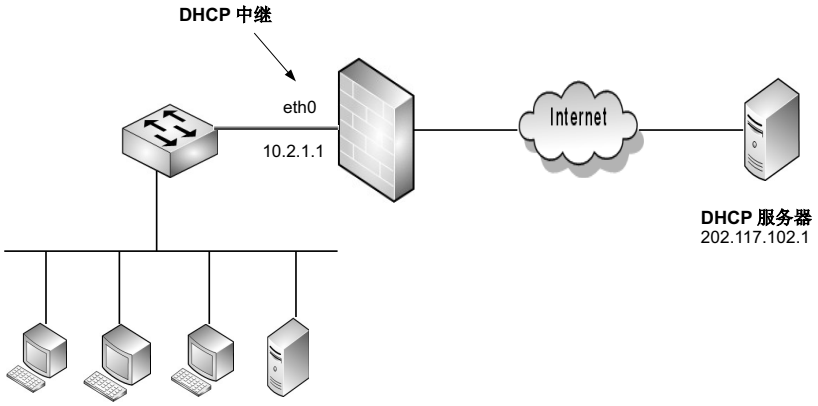
CLI

```
NetEye@root> configure mode
NetEye@root-system] dhcp subnet test 10.2.1.0 24
NetEye@root-system] dhcp subnet test dynamic 10.2.1.2-10.2.1.200
NetEye@root-system] dhcp subnet test reserve 10.2.1.100
44:37:E6:27:C5:D5
NetEye@root-system] dhcp subnet test lease unlimited
NetEye@root-system] dhcp subnet test gateway 10.2.1.1
NetEye@root-system] dhcp subnet test dns 202.107.122.36
NetEye@root-system] dhcp subnet test dns2 202.23.84.129
NetEye@root-system] dhcp interface eth0 server auto
NetEye@root-system] exit
NetEye@root> save config
```

范例 2：配置 DHCP 中继代理

NISG 的接口 eth0 配置为 DHCP 中继代理，为内网的 DHCP 客户端转发 DHCP 服务器 202.117.102.1 的 DHCP 数据报文。

图 9 配置 DHCP 中继代理



本范例需完成如下设置：

- 设置 eth0 接口为 DHCP 中继代理，设置中继代理服务器为 202.117.102.1。
- 强制将内网 DHCP 客户端的网关地址修改为 eth0 接口的 IP 地址。

具体操作如下：

WebUI

1. 选择**网络 >DHCP>DHCP 服务器**。
2. 在 **DHCP 配置列表**中点击 eth0 所对应的 ，进入 eth0 的编辑页面，进行如下配置：

3. 点击**确定**。
4. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] dhcp interface eth0 relay 202.117.102.1 primary
NetEye@root-system] dhcp interface eth0 relay change-gateway enable
NetEye@root-system] exit
NetEye@root> save config
```

4.16.4 配置参数说明

表 116 DHCP 服务配置信息

属性	说明
接口	配置 DHCP 服务的接口。可以是三层或三层共享以太网接口、三层或三层共享以太网通道、三层或三层共享冗余接口、 VLAN 接口或虚拟接口。
DHCP 服务	即 NISG 提供的 DHCP 服务。 DHCP 的服务类型包括： • **不设置**：表示三层接口没有启用任何 DHCP 功能。 • **中继**：表示三层接口处于 DHCP 中继代理的功能状态。 • **服务器**：表示三层接口处于 DHCP 服务器的功能状态。 • **客户端**：表示三层接口处于 DHCP 客户端的功能状态。
服务器模式	即 NISG 中指定的三层接口作为 DHCP 服务器状态时的工作模式，包括： • **自动**：自动模式。 NISG 自动检测网络上是否存在外部服务器。如果存在，NISG 上的 DHCP 服务器将停止工作，否则为网络中的 DHCP 客户端分配动态 IP 地址。 • **启用**：启用模式。 NISG 上的 DHCP 服务器始终开启并工作， NISG 不检测网络上是否存在外部服务器。 • **禁用**：禁用模式。 NISG 上的 DHCP 服务器始终关闭，但是仍然保留已分配地址等信息。
中继代理服务器	即 NISG 中指定的三层接口作为 DHCP 中继代理时，设置的代理服务器 IPv4 地址。地址格式为：[1-223].[0-255].[0-255].[0-255]，不能输入 127.0.0.0~127.255.255.255 或者 192.168.255.254。

4.17 DHCP 作用域

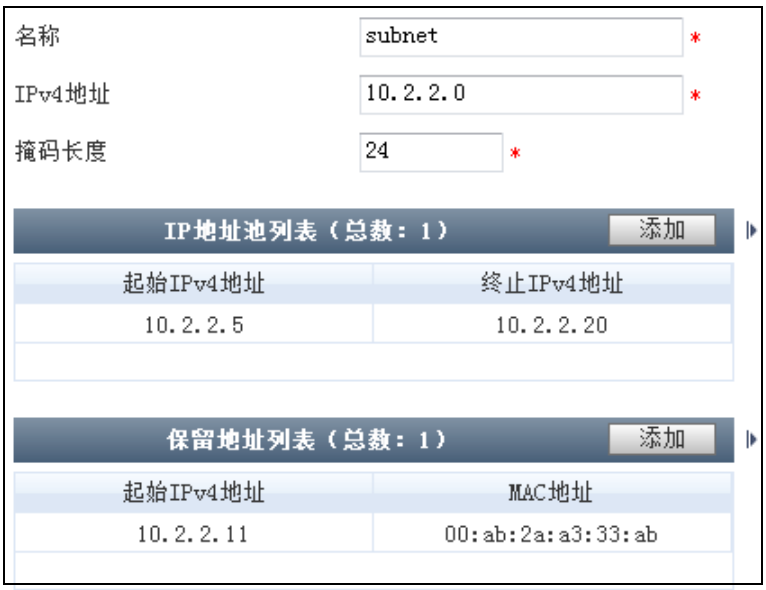
- 4.17.1 概述
- 4.17.2 基本配置步骤
- 4.17.3 配置参数说明

4.17.1 概述

作用域的功能是当 NISG 的某个三层接口作为 DHCP 服务器，为 DHCP 客户端分配 IP 地址时提供地址池。 NISG 支持 256 个作用域。

4.17.2 基本配置步骤

1. 选择**网络 >DHCP>DHCP 作用域**。
2. 配置用于 DHCP 分配的 IP 地址范围和保留 IP 地址。



3. 配置租期和高级设置。

表 117 DHCP 作用域命令

dhcp subnet	添加 DHCP 作用域。
unset dhcp subnet	删除 DHCP 作用域。
dhcp subnet domain	设置指定作用域的域名。
unset dhcp subnet domain	删除指定作用域的域名。
dhcp subnet dynamic	为指定的作用域添加地址池。
unset dhcp subnet dynamic	删除指定作用域的地址池。
dhcp subnet reserve	设置指定作用域的保留地址。
unset dhcp subnet reserve	删除指定作用域的特定保留地址。
dhcp subnet gateway, wins, dns, smtp, pop3, news, nis	设置指定作用域的特定服务的 IP 地址。
unset dhcp subnet gateway, wins, dns, smtp, pop3, news, nis	删除指定作用域的特定服务的 IP 地址。
dhcp subnet nistag	设置指定作用域的网络信息服务器的标签。
unset dhcp subnet nistag	删除指定作用域的网络信息服务器的标签。
dhcp subnet lease	设置指定作用域的租期。
show dhcp server subnet	显示 DHCP 作用域的配置信息。

4.17.3 配置参数说明

表 118 作用域配置信息

配置信息	说明
名称	作用域的名称。 1~63 字节的 UTF-8 字符，不包含：?,'\"<>&# 和空格。
网络地址	为作用域配置的子网及掩码长度。地址类型为 IPv4 地址，格式为 [1-223].[0-225].[0-225].[0-225]，不能输入 127.0.0.0~127.255.255.255。
IP 地址池	即动态地址池范围。可以通过配置起始地址和终止地址来为 NISG 配置作用域地址池，也可以通过在起始地址处直接配置一个 IP 地址。起始地址不能大于终止地址。配置的 IP 地址必须都在其所属的作用域内。 IP 地址池列表中，最多支持 256 个 IP 地址。
保留 IP 地址	为 DHCP 客户端绑定保留的 IP 地址，通过 DHCP 服务器将配置的 IP 地址发给指定的客户端。保留地址列表中，最多支持 256 个保留地址。
租期	即在作用域内分配的 IP 地址租期时间。租期时间范围为 1 ～ 1440000 分钟，缺省为 1440 分钟，也可以不限制租期时间。如果在 NISG 运行期间修改了租期时间，那么对于正在使用的租期将采用原有配置，直到相应客户端发送 DHCPREQUEST 报文请求更新租期后， NISG 自动更新租期时间。
高级设置	为 DHCP 客户端分配的其他网络配置参数，包括网关、域名、 DNS 服务器、 NEWS 服务器、 POP3 服务器、 SMTP 服务器、 WINS 服务器、 NetInfo 服务器以及 NetInfo 标签。 网关及上述服务器的 IP 地址格式为 [1-223].[0-255].[0-255].[0-255]，不能输入 127.0.0.0~127.255.255.255 或者 192.168.255.254。 NetInfo 标签名字为 0~255 字节的 UTF-8 字符，不包含：?'\"<>&。

4.18 DHCPv6

- 4.18.1 概述
- 4.18.2 基本配置步骤
- 4.18.3 DHCPv6 范例
- 4.18.4 配置参数说明

4.18.1 概述

DHCPv6 （IPv6 动态主机配置协议）用于 IPv6 寻址，为主机分配 IPv6 地址、 IPv6 前缀及其他网络配置参数。

- 有状态 DHCPv6 配置：指通过 DHCPv6 服务器分配 IPv6 地址和前缀。由于 DHCPv6 服务器保留已分配的地址和前缀信息，所以该过程称为有状态配置。
- 无状态 DHCPv6 配置：指设备通过无状态地址自动配置获取 IPv6 地址之后，再利用 DHCPv6 服务器获取除了地址以外的其他网络配置参数 （如 DNS 服务器、域名等）。在无状态 DHCPv6 配置过程中， DHCPv6 服务器不需要保存客户端的状态信息，因此称为无状态 DHCPv6 配置。

NISG 当前可以：

- 作为客户端，支持对 DHCPv6 前缀和其他网络配置参数的分配请求，暂不支持 DHCPv6 地址分配请求。
- 作为无状态 DHCPv6 服务器，为客户端分配 DNS 服务器地址、SNTP (Simple Network Time Protocol) 服务器地址和域名等网络配置参数。

下列接口可以作为 DHCPv6 客户端和无状态服务器：

表 119 DHCPv6 接口

DHCPv6 客户端	无状态 DHCPv6 服务器
三层或三层共享以太网接口	三层或三层共享以太网接口
三层或三层共享以太网通道	三层或三层共享以太网通道
三层或三层共享冗余接口	三层或三层共享冗余接口
三层虚拟接口	三层虚拟接口
VLAN 接口	VLAN 接口
PPPoE 接口	

4.18.2 基本配置步骤

在为三层或三层共享接口配置 DHCPv6 之前，需要首先选择**网络** > **接口**，启用该接口的 IPv6 功能。

1. 选择**网络** >**IPv6**>**DHCPv6**。
2. 进行如下配置。

- 一个 DHCPv6 客户端接口可以被多个无状态 DHCPv6 服务器引用。
- 引用中的客户端接口无法被删除。

表 120 DHCPv6 命令

dhcpv6 type {client | none | server}	设置指定三层或三层共享接口的 DHCPv6 工作模式。
dhcpv6 ip	为指定的 DHCPv6 客户端接口配置 SLA 以及接口标识。
unset dhcpv6 ip	删除指定 DHCPv6 客户端接口的 SLA 以及接口标识。
dhcpv6 prefix-assignment	为指定的 DHCPv6 客户端接口配置前缀推送接口以及前缀推送接口的 SLA 和接口标识。
unset dhcpv6 prefix-assignment	删除指定 DHCPv6 客户端接口的前缀推送接口以及前缀推送接口的 SLA 和接口标识。
dhcpv6 overwrite-dns	为指定的 DHCPv6 客户端接口启用 DNS 覆盖功能。
unset dhcpv6 overwrite-dns	为指定的 DHCPv6 客户端接口禁用 DNS 覆盖功能。
dhcpv6 enable-dns-proxy	启用为 DHCPv6 客户端接口自动添加 DNS 代理的功能。
unset dhcpv6 enable-dns-proxy	禁用为 DHCPv6 客户端接口自动添加 DNS 代理的功能。
dhcpv6 client send-request	向 DHCPv6 服务器发送 DHCPv6 客户端请求。
show dhcpv6-client	显示 DHCPv6 客户端接口从 DHCPv6 服务器获取的配置信息。
show dhcpv6-client-config	显示 DHCPv6 客户端接口的配置信息。
dhcpv6 server-type {auto interface | manual}	通过手动方式或自动从 DHCPv6 客户端接口更新的方式配置无状态 DHCPv6 服务器信息。
dhcpv6 server {dns | dns2}	设置无状态 DHCPv6 服务器的 DNS 服务器信息。
unset dhcpv6 server {dns | dns2}	删除无状态 DHCPv6 服务器的 DNS 服务器配置信息。
dhcpv6 server domain_search_list	向无状态 DHCPv6 服务器的 Domain Search List （域名搜索列表）添加域名信息。
unset dhcpv6 server domain_search_list	删除无状态 DHCPv6 服务器的域名搜索列表中的指定域名信息。
dhcpv6 server {sntp | sntp2}	设置无状态 DHCPv6 服务器的 SNTP 服务器信息。
unset dhcpv6 server {sntp | sntp2}	删除无状态 DHCPv6 服务器的 SNTP 服务器信息。
show dhcpv6-server-config	显示无状态 DHCPv6 服务器接口的配置信息。

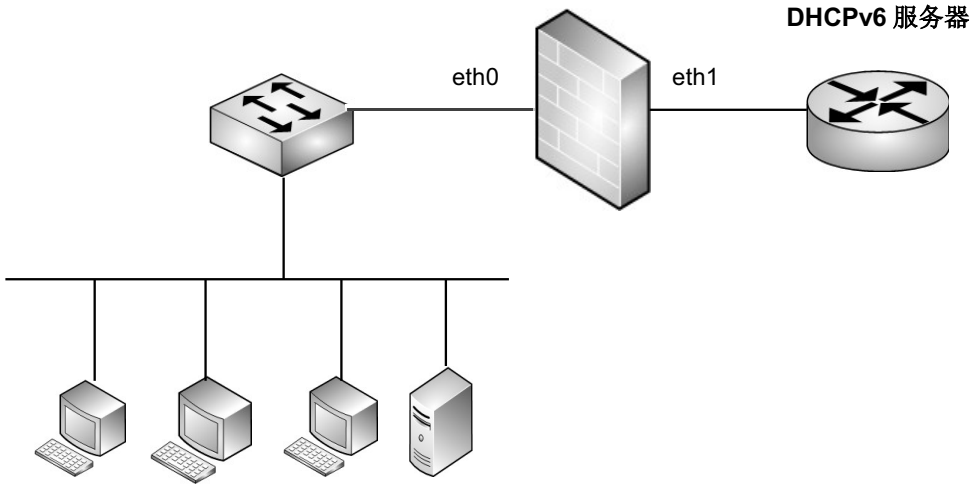
4.18.3 DHCPv6 范例

- 范例 1：配置 DHCPv6 客户端
- 范例 2：配置无状态 DHCPv6 服务器

范例 1：配置 DHCPv6 客户端

NISG 的 eth1 接口为 DHCPv6 客户端，连接 DHCPv6 服务器。 eth0 接口连接内网，使用 RA 将前缀信息告知内网主机，内网主机通过无状态地址自动配置获取 IPv6 地址。

图 10 配置 DHCPv6 客户端



本范例需完成如下设置：

- 编辑接口 eth0 和 eth1，启用它们的 IPv6 配置，启用无状态自动配置。
- 设置 eth1 接口为 DHCPv6 客户端。在 **IPv6 地址列表**中，配置 SLA 为 23ed，接口 ID 为 EUI-64。
- 在**前缀地址列表**中，配置 eth0 接口的 SLA 为 32af，接口 ID 为 EUI-64。
- 将从DHCPv6服务器获取的DNS服务器地址替换掉NISG的DNS主机中设置的DNS服务器地址。

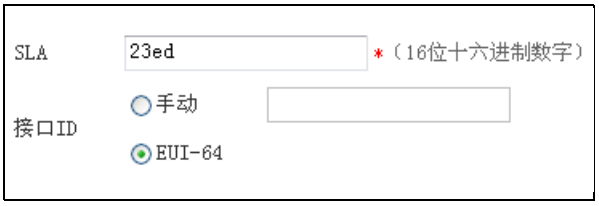
具体操作如下：

WebUI

1. 选择**网络** > **接口**。
2. 在**接口列表**中点击 eth0 和 eth1 所对应的 ，进入到相应接口的编辑页面，进行如下配置：

3. 点击**确定**。
4. 选择**网络** >**IPv6**>**DHCPv6**。
5. 在 **DHCPv6 接口列表**中点击 eth1 所对应的 ，进入到 eth1 的编辑页面，进行如下配置：
   a. 在**类型**下拉框中选取**客户端**。

   b. 在 **IPv6 地址列表**中点击**添加**，进行如下配置：



   c. 在**前缀分配列表**中点击**添加**，进行如下配置：
   d. 勾选**覆盖 DNS**。
6. 点击**确定**。
7. 在 **DHCPv6 接口列表**中点击 eth1 所对应的 ，进入到 eth1 的编辑页面，点击**发送 DHCP 请求**。
8. 点击 。

CLI

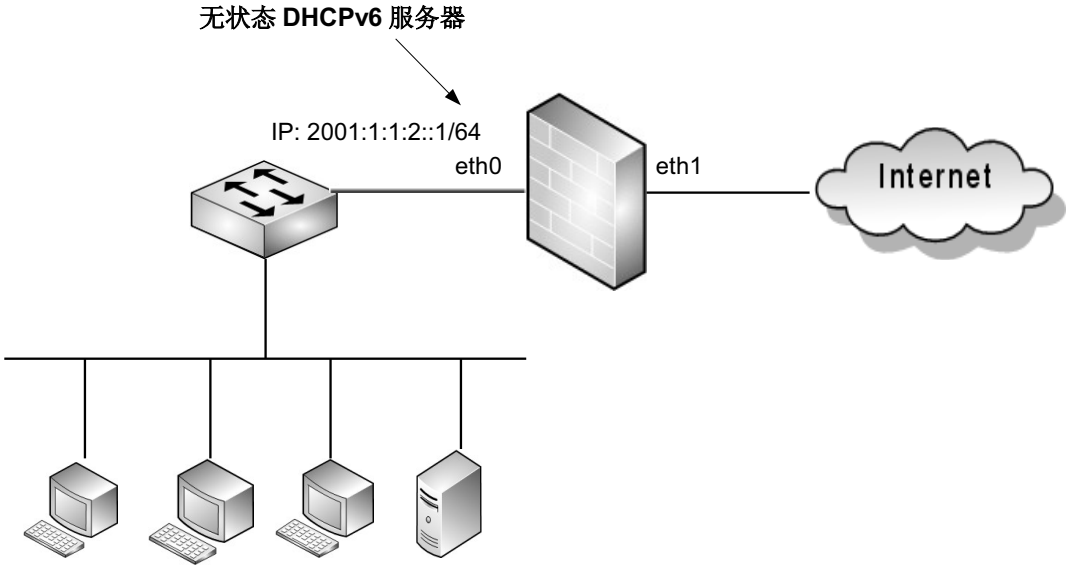
```
NetEye@root> configure mode
NetEye@root-system] interface ethernet 0
```

```
NetEye@root-system-if-eth0] ipv6 enable
NetEye@root-system-if-eth0] ipv6 address autoconfig
NetEye@root-system-if-eth0] exit
NetEye@root-system] interface ethernet 1
NetEye@root-system-if-eth1] ipv6 enable
NetEye@root-system-if-eth1] ipv6 address autoconfig
NetEye@root-system-if-eth1] dhcpv6 type client
NetEye@root-system-if-eth1] dhcpv6 ip SLA 23ed eui-64
NetEye@root-system-if-eth1] dhcpv6 prefix-assignment interface
ethernet 0 SLA 32af eui-64
NetEye@root-system-if-eth1] dhcpv6 overwrite-dns
NetEye@root-system-if-eth1] dhcpv6 client send-request
NetEye@root-system-if-eth1] end
NetEye@root> save config
```

范例 2：配置无状态 DHCPv6 服务器

NISG 的 eth0 接口连接内网，并充当无状态 DHCPv6 服务器，其 IPv6 地址为 2001:1:1:2::1/64。

图 11 配置无状态 DHCPv6 服务器



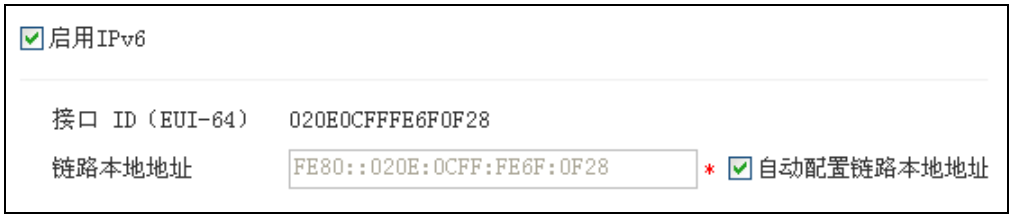
本范例需完成如下设置：

- 编辑接口 eth0，启用 IPv6 功能，并手动配置 IPv6 地址。
- 设置 eth0 接口为无状态 DHCPv6 服务器，并配置要分配给内网主机的无状态 DHCPv6 配置信息，如 DNS、 SNTP 和 Domain Search List。

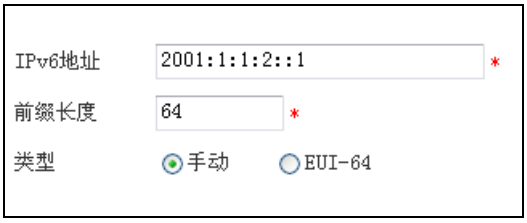
具体操作如下：

WebUI

1. 选择**网络** > **接口**。
2. 在**接口列表**中点击 eth0 所对应的 ，进入到相应接口的编辑页面，进行如下配置：
   a. 勾选**启用 IPv6**。



b. 在 **IP 地址列表**中，点击**添加**，添加 IPv6 地址。



3. 点击**确定**。
4. 选择**网络 >IPv6>DHCPv6**。
5. 在 **DHCPv6 接口列表**中点击 eth0 所对应的 ，进入到 eth0 的编辑页面，进行如下配置：

   a. 在**类型**下拉框中选取**服务器**。

   b. 在**服务器信息**区域，选择**手动**，进行如下配置：

6. 点击**确定**。
7. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] interface ethernet 0
NetEye@root-system-if-eth0] ipv6 enable
NetEye@root-system-if-eth0] ipv6 address 2001:1:1:2::1/64
NetEye@root-system-if-eth0] dhcpv6 type server
NetEye@root-system-if-eth0] dhcpv6 server dns 2000::1
NetEye@root-system-if-eth0] dhcpv6 server dns2 2000::2
NetEye@root-system-if-eth0] dhcpv6 server domain_name_list test.com
NetEye@root-system-if-eth0] dhcpv6 server sntp 2ffe::1
NetEye@root-system-if-eth0] dhcpv6 server sntp2 2ffe::2
NetEye@root-system-if-eth0] end
NetEye@root> save config
```

4.18.4 配置参数说明

表 121 DHCPv6 客户端属性

配置信息	说明
接口	DHCPv6 客户端接口。可以是三层或三层共享以太网接口、三层或三层共享以太网通道、三层或三层共享冗余接口、三层虚拟接口、 VLAN 接口以及 PPPoE 接口。
DUID	DHCPv6 设备的唯一标识符 （包括 DHCPv6 客户端、中继和服务器），用于 DHCPv6 设备之间的相互验证。该值是系统自动生成的。
类型	接口的 DHCPv6 工作模式，包括以下三种： • **不使用探测**：表示不使用 DHCPv6 探测功能。 • **客户端**：表示 DHCPv6 客户端模式。 • **服务器**：表示无状态 DHCPv6 服务器模式。
发送 DHCP 请求	点击该按钮，作为 DHCPv6 客户端的接口会先后发送 DHCP-PD 和 DHCP-inform 请求。
IPv6 地址列表	通过配置该列表，可以为工作模式为 DHCPv6 客户端的接口配置 IPv6 地址，配置项包括 SLA 以及接口 ID。 • **SLA**：表示对 DHCPv6 获得前缀的子网划分功能，取值范围为 0000 ～ FFFF。SLA 与 DHCPv6 获得的前缀进行右对齐计算出 64 位前缀。 • **接口 ID**：包括手动和 EUI-64。当指定手动时，表示不使用 EUI-64 格式的接口标识；当指定 EUI-64 时，表示使用 EUI-64 格式的接口标识。 SLA 和接口 ID 结合 DHCP-PD 请求获得的前缀，共同组成一个前缀长度为 64 的 IPv6 地址。管理员最多可以添加 8 个条目。
前缀分配列表	通过配置该列表，可以为指定的三层接口所在的子网推送含有 64 位前缀的 RA 通告，同时为该接口配置基于推送前缀的 IPv6 地址。 配置项包括接口、 SLA 以及接口 ID。这里的接口指请求客户端之外的三层接口 （不包括环回接口、隧道接口和 PPPoE 接口）， SLA 和接口 ID 属性与 **IPv6 地址列表**中的属性相同。 对于每个接口，管理员最多可以添加 8 个条目。

表 121 DHCPv6 客户端属性 (*续*)

配置信息	说明
覆盖 DNS	NISG 发送 DHCP 请求时，会用获取到的 DNS 覆盖 NISG 中原有的 DNS 服务器信息。缺省情况下，该功能是关闭的。
启用 DNS 代理	系统将根据通过 DHCPv6 客户端接口获得的 DNS 自动添加 DNS 代理。缺省情况下，该功能是关闭的。

表 122 无状态 DHCPv6 服务器属性

配置信息	说明
接口	无状态 DHCPv6 服务器接口，可以是三层或三层共享以太网接口、三层或三层共享以太网通道、三层或三层共享冗余接口、三层虚拟接口以及 VLAN 接口。
DUID	DHCPv6 设备的唯一标识符 （包括 DHCPv6 客户端、中继和服务器），用于 DHCPv6 设备之间的相互验证。该值是系统自动生成的。
类型	接口的 DHCPv6 工作模式，包括以下三种： • **不使用探测**：表示不使用 DHCPv6 探测功能。 • **客户端**：表示 DHCPv6 客户端模式。 • **服务器**：表示无状态 DHCPv6 服务器模式。
服务器信息	包括两种配置无状态 DHCPv6 服务器信息的方式。 • **从 DHCPv6 客户端接口更新**：表示通过指定 DHCPv6 客户端接口更新无状态 DHCPv6 信息。即服务器从指定 DHCPv6 客户端获取无状态信息作为自身的配置，并将这些配置信息分配给请求客户端。当指定 DHCPv6 客户端的无状态信息发生变化时，服务器需要同步更新自身的配置。 • **手动**：手动配置服务器无状态信息。当有客户端发起请求时，服务器将无状态 DHCPv6 信息分配给客户端。 **•DNS**：DNS 服务器的 IPv6 地址，包括 DNS1 和 DNS2。不可以是环回地址 （::1）、多播地址 （FF00/8~FFFF/8）、未指定地址 （::）和 ::FFFF:0:0/96。 **•域名搜索列表**：由最多 8 个域名组成。 **•SNTP 服务器**：SNTP 服务器的 IPv6 地址，包括 SNTP 服务器 1 和服务器 2。不可以是环回地址 （::1）、多播地址 （FF00/8~FFFF/8）、未指定地址 （::）和 ::FFFF:0:0/96。

4.19 STP

- 4.19.1 概述
- 4.19.2 基本配置步骤
- 4.19.3 范例：STP 应用
- 4.19.4 配置参数说明

4.19.1 概述

生成树协议 （Spanning Tree Protocol， STP）有狭义和广义两层含义。狭义 STP 指 IEEE802.1D 中定义的标准 STP 协议，广义 STP 包括 IEEE802.1D 定义的 STP 协议和各种在其基础上衍生改进的生成树协议，如 RSTP 和 MSTP 等。

4.19.1.1 STP

STP 是由 IEEE802.1D 标准定义的一个二层交换网络管理协议，其目的是可以在布满网桥 （通常是交换机）的网络中形成以根网桥为树根其他网桥伸展如叶的树状拓扑结构。其主要作用是将拓扑中某些网桥的某些端口置于阻塞状态，避免桥接或交换的网络拓扑中产生环路，同时保障链路冗余。当一条链路发生故障时，被阻塞的端口将被启用，起到备份链路的作用。

NISG 实现了每 VLAN 生成树 (Per-VLAN Spanning Tree) 特性，即能够在二层交换网络中的每个 VLAN 上独立设置启用 STP 或 RSTP 协议，每个 VLAN 单独维护一个生成树。不仅可以保证每个 VLAN 内没有环路，而且在某些情况下，能够有效实现二层网络的负载均衡。

STP 运行过程如下：

1. 确定根网桥
   根网桥是网桥 ID 最小的网桥。在一个二层网络中，只有一个根网桥。当网络拓扑稳定以后，只有根网桥能发送 BPDU （Bridge Protocol Data Unit，建立无环路树形拓朴结构所需的信息）报文，其他网桥只能对其进行接收和转发。
2. 确定根端口
   根端口是在非根网桥上存在的到达根网桥的路径开销最小的端口，一个非根桥设备上只有一个根端口。
3. 确定指定端口
   指定端口是一个网段的所有端口中到达根网桥的路径开销最小的端口，一个网段上只有一个指定端口。
4. 确定阻塞端口
   阻塞端口既不是根端口，也不是指定端口，只监听 BPDU 报文。

4.19.1.2 RSTP

快速生成树协议 （Rapid Spanning Tree Protocol， RSTP）由 IEEE802.1w 标准定义，是对 STP 协议的改进，并与 STP 协议完全兼容，主要实现了网络拓扑的快速收敛。启用 RSTP 协议的网桥会根据收到的 BPDU 版本号自动判断与之相连的网桥是支持 STP 协议还是支持 RSTP 协议。

缺省情况下， STP 协议的收敛时间为 50 秒，而 RSTP 协议的收敛时间最快可以达到 1 秒以内。

- 快速收敛。 RSTP 协议的快速收敛主要依赖于以下方面来实现：
  - 边缘端口 （Edge Port）

    边缘端口是与服务器等终端设备直接相连的端口。边缘端口无需参与生成树计算，可以省略侦听和学习的状态，无时延地直接进入转发状态。

  - 链路类型

    启用 RSTP 协议时，网桥 （交换机）根据端口的双工模式自动判断链路类型。如果端口工作在全双工模式下，则为点到点 （Point-to-Point Link）链路类型，端口可以快速地从阻塞状态进入转发状态，而无需等待转发延迟时间。

- 端口角色。除了拥有和 STP 相同作用的根端口和指定端口外，RSTP 协议新增下列端口角色，可以加快端口状态的转换：
  - **替换端口 (Alternate Port)—** 根端口的备份端口。
  - **备份端口 (Backup Port)—** 某个网段指定端口的备份端口。
- 端口状态。 RSTP 协议只有三种端口状态：丢弃、学习和转发。处于丢弃状态的端口实际上就是 STP 协议中禁用、阻塞和侦听三种状态的集合。
- 强制运行 RSTP。

  可以提高数据转发效率。如果管理员确定和 NISG 相连的设备都运行 RSTP 协议，那么可以在 NISG 上启用强制运行 RSTP 的功能；如果与之直连的设备只支持 STP 协议，在 NISG 上强制运行 RSTP，将会导致互相不兼容的问题。

4.19.2 基本配置步骤

1. 选择**网络 >STP**。
2. 进行如下配置。

- 需要在 VLAN 列表中双击一个 VLAN 条目进行编辑。
- 一个 VLAN 不可以同时配置成根网桥和备用根网桥。
- 当 VLAN 被删除时，其所有生成树配置将一同被删除；当接口从 VLAN 中移除时，相应的端口配置随之被移除，但不影响 VLAN 中其他端口的配置。
- 管理员通过 CLI 可以配置 STP 定时器 （Hello， Max-age 以及 Forward-delay）。
- NISG 最多支持在 64 个 VLAN 上开启 STP 或 RSTP 实例。

3. 点击**确定**。
4. 点击 。

表 123 STP 命令

show spanning-tree {brief | vlan *vlan_id*}	显示 STP 信息。
spanning-tree {enable per-vlan-stp | disable}	启用或禁用 NISG 设备的 STP 功能。
spanning-tree {enable {stp | rstp [protocol-migration]} | disable}	启用或禁用某个 VLAN 的 STP 功能。
spanning-tree default	重置 STP 配置信息，恢复默认配置。
spanning-tree root {primary | secondary}	将某个 VLAN 设置为根网桥或备用根网桥。
unset spanning-tree root {primary | secondary}	取消设置根网桥或备用根网桥。
spanning-tree bridge-priority	设置网桥优先级。
spanning-tree interface port-priority	设置指定接口的端口优先级。

表 123 STP 命令 (*续*)

spanning-tree interface path-cost	设置指定接口的端口路径开销。
spanning-tree interface edge-port	设置某个接口为边缘端口。
unset spanning-tree interface edge-port	取消设置某个接口为边缘端口。
spanning-tree forward-delay	设置转发延迟时间。
spanning-tree hello-time	设置 Hello 时间。
spanning-tree max-age	设置 BPDU 报文最大生存时间。

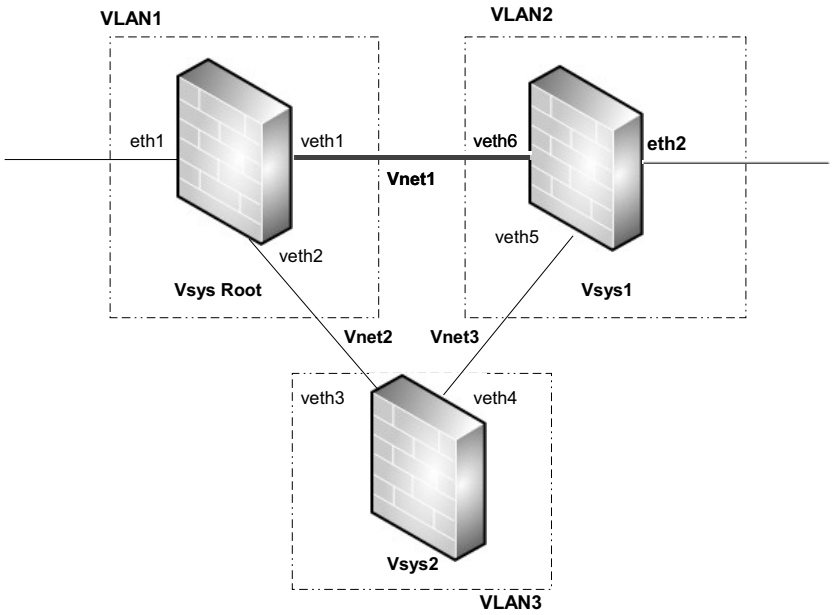
4.19.3 范例：STP 应用

本范例是 STP 功能的简单应用，用于检测在链路冗余的网络拓扑中运行 STP 协议，是否有端口被阻塞；当主链路发生故障时，被阻塞的端口是否启用，恢复链路畅通。

管理员需要在 NISG 上搭建如下网络拓扑环境：

- 创建 VLAN1、VLAN2 和 VLAN3，创建虚拟接口 veth1 ～ veth6，将 eth1、veth1 和 veth2 划入到 VLAN1 中，将 veth3 和 veth4 划入到 VLAN3 中，将 veth5、 veth6 和 eth2 划入到 VLAN2 中。
- 创建虚拟系统 Vsys1 和 Vsys2。将 VLAN2 划入到 Vsys1 中，将 VLAN3 划入到 Vsys2 中。
- 创建虚拟网络 Vnet1、Vnet2 和 Vnet3。将 veth1 和 veth6 划入到 Vnet1 中用于连接 Vsys Root 和 Vsys1 ； 将 veth2 和 veth3 划入到 Vnet2 中用于连接 Vsys Root 和 Vsys2 ； 将 veth4 和 veth5 划入到 Vnet3 中用于连接 Vsys1 和 Vsys2。
- 在 VLAN1、VLAN2 和 VLAN3 上分别开启 STP 功能，将 VLAN1 设置为根网桥。修改 veth5 的端口路径开销为 10， veth6 的端口路径开销为 20，其他虚拟接口采用默认的端口路径开销 200,000,000。

图 12 链路冗余拓扑



本范例包含如下 WebUI 和 CLI 配置：

- 1. 创建接口
- 2. 创建虚拟系统
- 3. 创建虚拟网络
- 4. 配置 STP
- 5. 查看结果

1. 创建接口

WebUI

1. 选择**网络** > **接口**。
2. 点击**新建**，选择 **VLAN**，创建 VLAN 接口 VLAN1。
3. 以同样的方式创建 VLAN2 和 VLAN3。
4. 点击**新建**，选择 **Virtual Interface**，创建虚拟接口 veth1。
5. 以同样的方式创建 veth2~veth6。
6. 在**接口列表**中点击 VLAN1 所对应的 ，进入到 VLAN1 的编辑页面。

7. 在**二层接口列表**区域内的**备选接口**列表中选择 eth1、veth1 和 veth2，点击➡，添加到右侧的**已选接口**列表中，即添加到 VLAN1 中。

8. 点击**确定**。
9. 以同样的方式将eth2、veth5和veth6划入到VLAN2中，将veth3和veth4划入到VLAN3中。
10. 点击💾。

CLI

```
NetEye@root> configure mode
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] vlan 2
NetEye@root-system-vlan2] vlan 3
NetEye@root-system-vlan3] veth 1
NetEye@root-system-veth1] veth 2
NetEye@root-system-veth2] veth 3
NetEye@root-system-veth3] veth 4
NetEye@root-system-veth4] veth 5
NetEye@root-system-veth5] veth 6
NetEye@root-system-veth6] exit
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] hold ethernet eth1
NetEye@root-system-vlan1] hold veth veth1,veth2
NetEye@root-system-vlan1] vlan 2
NetEye@root-system-vlan2] hold ethernet eth2
NetEye@root-system-vlan2] hold veth veth5,veth6
NetEye@root-system-vlan2] vlan 3
NetEye@root-system-vlan3] hold veth veth3,veth4
NetEye@root-system-vlan3] end
NetEye@root> save config
```

2. 创建虚拟系统

WebUI

1. 选择**系统 > 虚拟系统 > 虚拟系统**。
2. 点击**新建**，创建虚拟系统 Vsys1，并将 VLAN2 划入到 Vsys1 中。

3. 点击**新建**，创建虚拟系统 Vsys2，并将 VLAN3 划入到 Vsys2 中。

4. 点击**确定**。
5. 点击 。

CLI

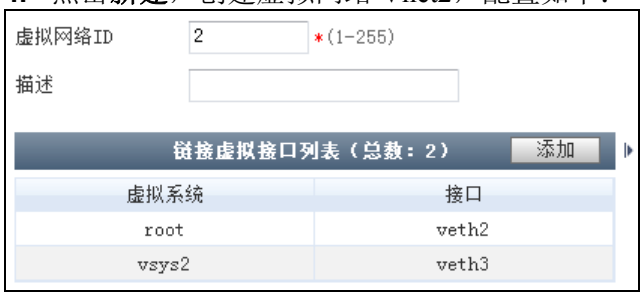
```
NetEye@root> configure mode
NetEye@root-system] vsys 1 resource-limit 20
NetEye@root-system-vsys1] hold vlan 2
NetEye@root-system-vsys1] exit
NetEye@root-system] vsys 2 resource-limit 20
NetEye@root-system-vsys2] hold vlan 3
NetEye@root-system-vsys2] end
NetEye@root> save config
```

3. 创建虚拟网络

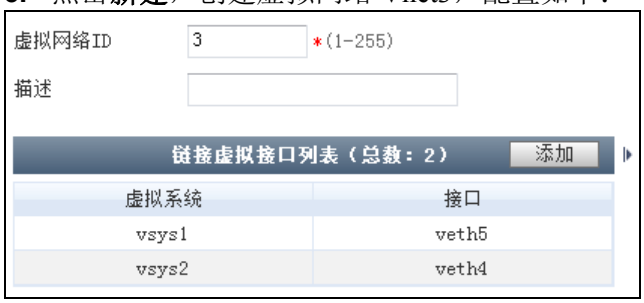
WebUI

1. 选择**系统 > 虚拟系统 > 虚拟网络**。
2. 点击**新建**，创建虚拟网络 Vnet1，配置如下：

3. 点击**确定**。
4. 点击**新建**，创建虚拟网络 Vnet2，配置如下：



5. 点击**确定**。
6. 点击**新建**，创建虚拟网络 Vnet3，配置如下：



7. 点击**确定**。
8. 点击 。

CLI

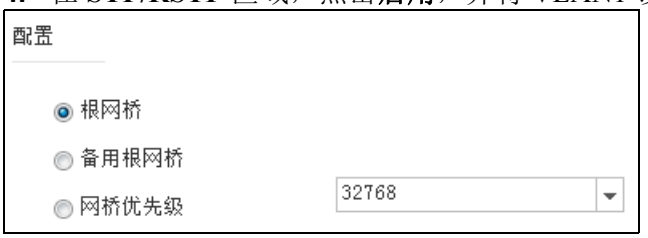
```
NetEye@root> configure mode
NetEye@root-system] vnet 1
NetEye@root-system-vnet1] hold veth 1
NetEye@root-system-vnet1] hold veth 6
NetEye@root-system-vnet1] vnet 2
NetEye@root-system-vnet2] hold veth 2
NetEye@root-system-vnet2] hold veth 3
NetEye@root-system-vnet2] vnet 3
NetEye@root-system-vnet3] hold veth 4
NetEye@root-system-vnet3] hold veth 5
NetEye@root-system-vnet3] end
NetEye@root> save config
```

4. 配置 STP

WebUI

1. 选择**网络** >**STP**。
2. 在 **STP** 区域，点击**启用**。
3. 在 **VLAN 列表**中双击 VLAN1，弹出**编辑 VLAN 配置**窗口。

4. 在 **STP/RSTP** 区域，点击**启用**，并将 VLAN1 设置为根网桥。



5. 点击**确定**。
6. 在 **VLAN 列表**中双击 VLAN2，弹出**编辑 VLAN 配置**窗口。
7. 在 **STP/RSTP** 区域，点击**启用**。
8. 在**端口配置列表**中，点击 veth5，在**端口路径开销**中输入 10； 点击 veth6，在**端口路径开销**中输入 20。

9. 点击**确定**。
10. 在 **VLAN 列表**中双击 VLAN3，弹出**编辑 VLAN 配置**窗口。
11. 在 **STP/RSTP** 区域，点击**启用**。
12. 点击**确定**两次。
13. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] spanning-tree enable per-vlan-stp
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] spanning-tree enable stp
NetEye@root-system-vlan1] spanning-tree root primary
NetEye@root-system-vlan1] vlan 2
NetEye@root-system-vlan2] spanning-tree enable stp
NetEye@root-system-vlan2] spanning-tree interface veth5 path-cost 10
NetEye@root-system-vlan2] spanning-tree interface veth6 path-cost 20
NetEye@root-system-vlan2] vlan 3
NetEye@root-system-vlan3] spanning-tree enable stp
NetEye@root-system-vlan3] end
NetEye@root> save config
```

5. 查看结果

完成上述配置，可以通过 WebUI 或 CLI 查看 STP 的实时信息。选择**监控 >STP** 进入 STP 页面，或在 CLI 下执行 **show spanning-tree vlan** 命令。由于 VLAN1 是根网桥，veth6 与 veth3 各自成为 VLAN2 和 VLAN3 的根端口； veth5 的路径开销 (20+10=30) 低于 veth4(200,000,000x2=400,000,000)，成为整个网段的指定端口； veth4 既不是根端口也不是指定端口，因此被阻塞，处于 Blocking 状态，其他接口处于 Forwarding 状态。

然后手动禁用 veth6 接口，查看被阻塞的 veth4 接口是否重新启用，网络是否恢复链路畅通。具体操作如下：

WebUI

1. 选择**网络** > **接口**。
2. 在**接口列表**中点击 veth6 所对应的 ，进入**编辑**页面，禁用 veth6 接口。

3. 点击**确定**。
4. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] veth 6
NetEye@root-system-veth6] shutdown
NetEye@root-system-veth6] end
NetEye@root> save config
```

完成上述配置，通过 WebUI 界面在 STP 页面上查看 STP 的实时信息，会发现 veth6 接口处于 Disable 状态，其他接口处于 Forwarding 状态。也可以通过 **show spanning-tree vlan** 命令可以在 CLI 界面下查看 STP 的实时信息。

4.19.4 配置参数说明

在 NISG 上， STP 功能只能在根系统下进行配置，在虚拟系统中可以查看 STP 配置。不支持 HA 同步。

表 124 STP 配置信息

配置信息	说明
STP	在 NISG 上启用或禁用生成树协议 (STP)。默认为禁用状态。当 STP 功能禁用时， NISG 支持对 STP 和 RSTP 的 BPDU 消息的透明传输，对 BPDU 不做任何处理直接转发。
协议	仅包含每 VLAN STP 一个选项。
VLAN 列表	包含以下两个选项： • **接口 —** 可以为该 VLAN 接口启用 STP/RSTP。 • **协议 —** 可以选择 STP、 RSTP 或强制运行 RSTP。 当 VLAN 中有新的二层接口加入时， NISG 会自动检测该接口，并为其分配一套默认参数配置，包括端口路径开销等。在该列表中双击某个 VLAN 条目，可进入**编辑 VLAN 配置**页面。
STP/RSTP	启用或禁用某个 VLAN 的 STP 或 RSTP，每个 VLAN 具有独立的 STP 配置。默认禁用。 当一个 VLAN 不包含任何二层接口时，能够开启 STP/RSTP，但不会进行生成树计算。
恢复默认设置	点击**重置**按钮，则当前 VLAN 恢复系统默认的 STP 配置。
类型	网桥使用的生成树协议类型，管理员可以进行如下选择： • **STP—** 网桥只支持 STP 协议， STP 为缺省设置。 • **RSTP—** 与网桥相连的设备使用 STP 协议时，网桥自动使用 STP 协议与之兼容。 • **强制运行 RSTP—** 网桥不会兼容二层网络中其他 STP 设备，而强制运行 RSTP 协议。
根网桥	设置该 VLAN 所代表的虚拟网桥为其所在二层交换网络的根网桥。 一个二层网络中只能有一个根网桥。如果同时有多个网桥被配置成根网桥，则比较每个网桥的 MAC 地址，最小者为根网桥。根网桥优先级为 0。
备用根网桥	设置该 VLAN 所代表的虚拟网桥为其所在二层交换网络的备用根网桥。备用根网桥主要起到对根网桥的备份作用，可以在二层网络中设置多个备用根网桥。备用根网桥优先级为 4,096。
网桥优先级	自定义设置 VLN 网桥的优先级。 根网桥 （缺省设置）、备用根网桥和网桥优先级的设置只能选取其中一种。网桥优先级取值范围为 0 ～ 61,440，且必须为 4,096 的倍数，默认优先级为 32,768。
端口优先级	设置 VLAN 中所包含各个端口的优先级。取值范围为 0 ～ 240，且必须为 16 的倍数，默认优先级为 128。
端口路径开销	设置一个 VLAN 中所包含的各个端口的路径开销。默认情况下，系统将根据端口链路速率自动判断路径开销。链路速率越高，路径开销值越小。 端口路径开销取值范围为 1 ～ 200,000,000。
边缘端口	设置工作在 Access 模式的二层以太网接口为边缘端口。边缘端口能够直接进入转发状态，加快收敛时间。 当管理员取消勾选**边缘端口**复选框或该边缘端口从网络中接收到 BPDU 消息时，该端口就会变成一个正常的生成树端口，参与生成树计算。

4.20 邻居发现

- 4.20.1 概述
- 4.20.2 基本配置步骤
- 4.20.3 ND 范例
- 4.20.4 配置参数说明

4.20.1 概述

邻居发现协议 （ND）被节点 （主机和路由器）用来发现同一链路上的邻居。

- ND 报文类型

表 125 ND 报文类型

ND 消息名称	ICMPv6 类型值	作用
路由器请求 （RS）	133	当接口启用时，主机向路由器发送 RS 消息，请求立即产生 RA 消息，而不必等到下次预计的时间。
路由器通告 （RA）	134	路由器通告其自身的存在，并携带各种链路参数与互联网参数，例如前缀、当前跳数限值等。 RA 消息可以由路由器周期性发出，也可以因响应 RS 消息而发出。
邻居请求 （NS）	135	节点发出 NS 消息，以探测邻居的链路层地址，或者验证邻居仍然是可达的。此外也用于进行重复地址检测。
邻居通告 （NA）	136	对 NS 消息的响应。节点也可以发送非请求的 NA 消息，以通告链路层地址的改变。
重定向 （Redirect）	137	路由器用该消息通知源主机可以到达目的地的更优第一跳。

- ND 的功能

ND 提供如下几种主要功能解决网络中邻居节点之间通讯和互动的问题：

- 路由器、前缀、参数发现
- 下一跳判定
- 地址解析与邻居不可达检测
- 无状态地址自动配置与重复地址检测
- 重定向

4.20.2 基本配置步骤

1. 选择**网络 >IPv6> 邻居发现配置**。
2. 进行如下配置。

在配置 ND 前，需要首先选择**网络 > 接口**，启用三层或三层共享接口的 IPv6 功能。

表 126 ND 命令

ipv6 nd dad detect	设置重复地址检测时发送邻居请求消息的次数。
ipv6 nd reachable-time	为指定的接口设置保持邻居可达状态的时间。
ipv6 nd retrans-timer	为指定的接口设置邻居请求消息的重传时间间隔。
ipv6 nd ra suppress	抑制指定的接口发送 RA 消息。
unset ipv6 nd ra suppress	允许指定接口发送 RA 消息。
ipv6 nd ra router-lifetime	设置 RA 消息中发布的路由器生存时间。
ipv6 nd ra interval	设置 RA 消息发布的时间间隔。
ipv6 nd ra hop-limit	设置 RA 消息中发布的跳数限制。
ipv6 nd ra managed-flag {on | off}	设置 RA 消息中的被管理地址配置标志位。
ipv6 nd ra other-flag {on | off}	设置设置 RA 消息中的其他配置标志位。
ipv6 nd ra retrans-timer {on | off}	设置 RA 消息中是否携带邻居请求消息的重传时间间隔。
ipv6 nd ra reachable-time {on | off}	设置 RA 消息中是否携带接口保持邻居可达状态的时间。
ipv6 nd ra link-address {on | off}	设置 RA 消息中是否携带接口的 MAC 地址。
ipv6 nd ra advlinkmtu {on | off}	设置 RA 消息中是否携带接口的 MTU。
ipv6 nd ra prefix	设置 RA 消息中的前缀信息及其相关的通告参数。
unset ipv6 nd ra prefix	删除 RA 消息中的前缀信息及其相关的通告参数。

4.20.3 ND 范例

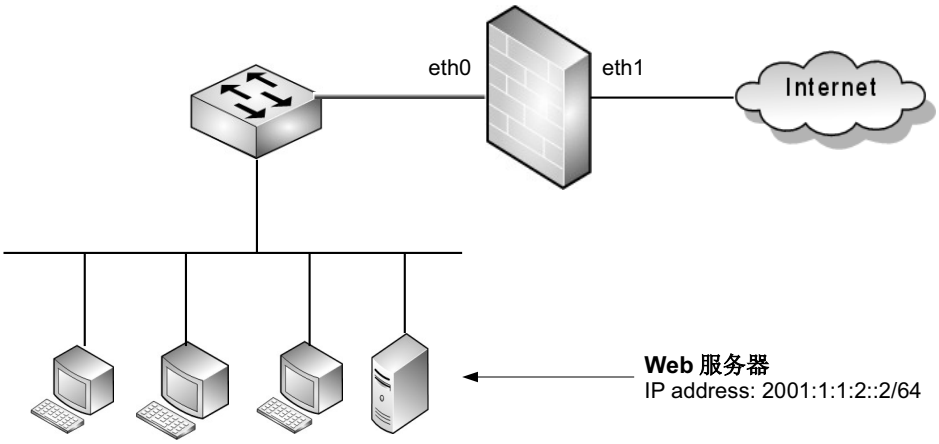
- 范例 1：重复地址检测
- 范例 2：路由器通告 （RA）配置

提示：在配置 ND 前，需要首先选择**网络 > 接口**，启用三层或三层共享接口的 IPv6 功能。

范例 1：重复地址检测

NISG 的 eth0 接口连接内网，内网中有一台 Web 服务器，其 IP 地址为 2001:1:1:2::2/64。

图 13 配置 ND



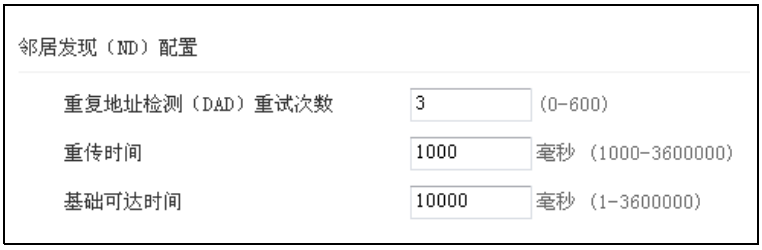
本范例需完成如下设置：

- FW 设备在 eth0 接口上执行 DAD （重复地址检测），次数最多为 3 次。
- 接口 eth0 每隔 1,000 毫秒重新发送 ND 报文。
- 接口 eth0 维持 Web 服务器的邻居可达性状态时长约 10,000 毫秒。如果在该时间内没有收到 Web 服务器的可达性确认消息， eth0 将停止向其转发流量。
- 配置 eth0 接口的 IP 地址为 2001:1:1:2::2/64。稍后，接口的 IPv6 地址状态为 DUPLICATE。
- 配置接口 eth0 接口的 IP 地址为 2001:1:1:2::1/64 （该地址不与内网中的任一主机重复）。稍后，接口的 IPv6 地址状态为 PREFERRED。

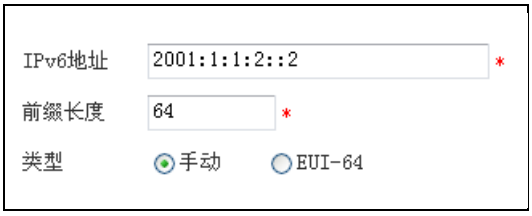
具体操作如下：

WebUI

1. 选择**网络 >IPv6> 邻居发现配置**。
2. 在**邻居发现 / 路由器通告列表**中点击 eth0 所对应的 ，进入 eth0 的编辑页面，进行如下配置：

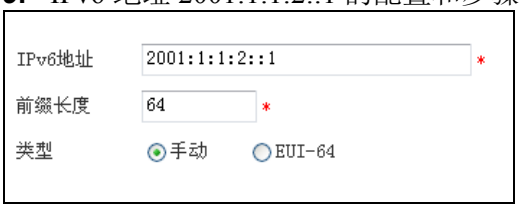


3. 点击**确定。**
4. 选择**网络 > 接口**。
5. 在**接口列表**中点击 eth0 所对应的 ， 进入 eth0 的编辑页面。
6. 点击 **IP 地址列表**中的**添加**，进行如下配置：



7. 点击**确定。**
8. 在**接口列表**中点击 eth0 所对应的 ，进入 eth0 的编辑页面。查看接口状态，为“ 重复（DUP） ”：

9. IPv6 地址 2001:1:1:2::1 的配置和步骤 6 相同。



10. 点击**确定**。
11. 在**接口列表**中点击 eth0 所对应的 ，进入 eth0 的编辑页面。查看接口状态，为“首选（PREFER）”：

12. 点击**确定**。
13. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] interface ethernet 0
NetEye@root-system-if-eth0] ipv6 enable
NetEye@root-system-if-eth0] ipv6 nd dad detect 3
NetEye@root-system-if-eth0] ipv6 nd retrans-timer 1000
NetEye@root-system-if-eth0] ipv6 nd reachable-time 10000
NetEye@root-system-if-eth0] ipv6 address 2001:1:1:2::2/64
NetEye@root-system-if-eth0] ipv6 address 2001:1:1:2::1/64
NetEye@root-system-if-eth0] end
NetEye@root> save config
```

完成上述操作后，运行 **show interface ethernet 0** 命令。可以查看到如下信息：

- DAD 已启用，重复检测次数为3次；ND报文的重新发送间隔为1,000毫秒；基础可达时间为 10,000 毫秒。

```
ND DAD is enabled, number of DAD attempts 3
ND retransmit time is 1000 milliseconds
ND base reachable time is 10000 milliseconds
```

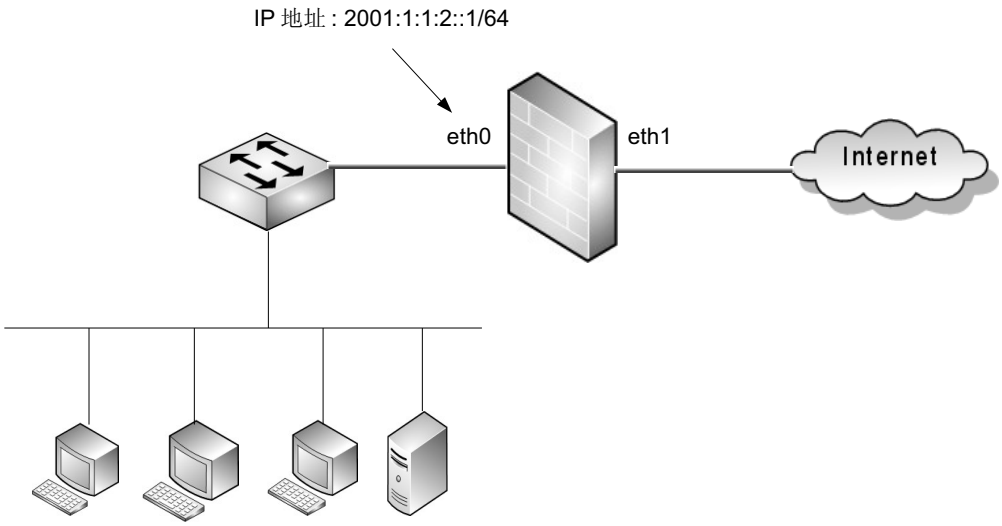
- IPv6地址2001:1:1:2::2处于DUP状态，表明已为网络中其他接口所使用；2001:1:1:2::1则处于 PREFER 状态，可以配置到 eth0 接口上。

```
Global unicast address(es):
  2001:1:1:2::2 , subnet is 2001:1:1:2::/64    [DUP]
  2001:1:1:2::1 , subnet is 2001:1:1:2::/64    [PREFER]
```

范例 2：路由器通告 （RA）配置

NISG 的 eth0 接口连接内网，其 IP 地址为 2001:1:1:2::1/64。

图 14 配置 RA



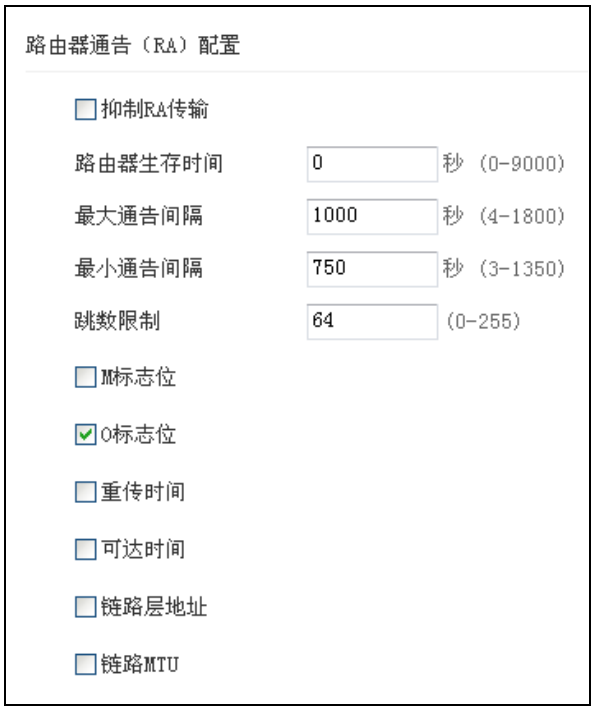
本范例需完成如下设置：

- 手动配置 eth0 接口的 IP 地址为 2001:1:1:2::1/64。
- 编辑 eth0 的 RA 相关属性：
  - 通告 （RA）参数：
    - 允许 eth0 向内网发布 RA 通告，内网主机不将 eth0 作为默认路由器。
    - RA 消息发布的时间间隔为 750~1000 秒。
    - 跳数限制为 64。
    - 内网主机只通过无状态地址自动配置获取 IPv6 地址，内网主机可以通过无状态 DHCPv6 配置获取其他网络配置信息。
    - RA 消息中不携带 eth0 的链路层地址和 MTU。
  - 前缀信息：
    - 通告前缀 2001:1:1:2::/64。
    - 内网主机可利用前缀进行无状态地址自动配置。
    - 不进行在链判定。

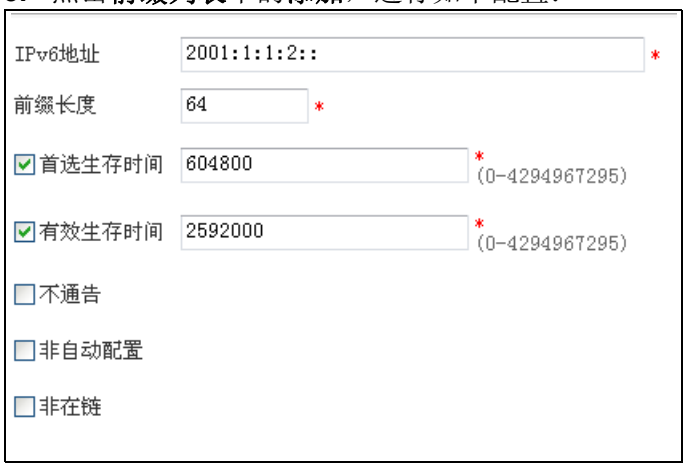
具体操作如下：

WebUI

1. 选择**网络 >IPv6> 邻居发现配置**。
2. 在**邻居发现 / 路由器通告列表**中点击 eth0 所对应的 ，进入 eth0 的编辑页面，进行如下配置：



3. 点击**前缀列表**中的**添加**，进行如下配置：



4. 点击**确定**。
5. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] interface ethernet 0
NetEye@root-system-if-eth0] ipv6 enable
NetEye@root-system-if-eth0] unset ipv6 nd ra suppress
NetEye@root-system-if-eth0] ipv6 nd ra router-lifetime 0
NetEye@root-system-if-eth0] ipv6 nd ra interval 750 1000
NetEye@root-system-if-eth0] ipv6 nd ra hop-limit 64
NetEye@root-system-if-eth0] ipv6 nd ra managed-flag off
NetEye@root-system-if-eth0] ipv6 nd ra other-flag on
NetEye@root-system-if-eth0] ipv6 nd ra link-address off
NetEye@root-system-if-eth0] ipv6 nd ra advlinkmtu off
NetEye@root-system-if-eth0] ipv6 nd ra prefix 2001:1:1:2::/64 valid-
lifetime default preferred-lifetime default no-adv off no-autoconf
ig off off-link off
NetEye@root-system-if-eth0] exit
NetEye@root> save config
```

4.20.4 配置参数说明

表 127 ND 配置属性

配置信息	说明
重复地址检测（DAD）重试次数	进行 DAD 检测时，发送 NS 消息的次数。取值范围为 0~600，缺省值为 1。
重传时间	进行 DAD 检测时，发送 NS 消息的间隔时间。取值范围为 1000~3600000 毫秒，缺省值为 1000 毫秒。 如果在设置的间隔时间内没有收到响应，则继续发送 NS 消息。当发送的次数达到所设置的 DAD 检测重试次数后，仍未收到响应，则认为待检测的地址可用。
基础可达时间	用于计算可达时间的基准值。可达时间即接口保持某个邻居可达状态的时间长度；在可达时间范围内，接口向该邻居转发流量。 取值范围为 1~3600000 毫秒，缺省值为 30000 毫秒。

表 128 RA 配置属性

配置信息	说明
抑制 RA 传输	抑制接口的 RA 通告。该功能缺省为启用，表示不允许在某个特定接口上进行 RA 通告。 在初始化向导的过程中，如果选择了透明模式，则该功能缺省为启用；如果选择了路由模式，则该功能缺省为禁用。
路由器生存时间	RA 消息发布的路由器生存时间，即作为缺省路由器的时间。取值范围为 0~9000 秒，缺省值为 1800 秒。当该值为 0 时，表示 NISG 将不作为缺省路由器。 主机根据接收到的 RA 消息中的该值，就可以确定是否将发布该 RA 消息的设备作为默认路由器。

表 128 RA 配置属性 (*续*)

配置信息	说明
最大通告间隔	未请求的 RA 消息发布的最大时间间隔。取值范围为 4-1800 秒，缺省值为 600 秒。该值必须小于或等于路由器生存时间的值。 配置 RA 消息发布的最大 / 最小时间间隔后，设备将在这两个时间间隔值之间随机选择一个值，作为周期性发布 RA 消息的时间间隔。
最小通告间隔	未请求的 RA 消息发布的最小时间间隔。取值范围为 3-1350 秒，缺省值为 200 秒。该值必须小于或等于最大时间间隔值的 0.75 倍。
跳数限制	在 RA 报文中发布的跳数限制。取值范围为 0~255，缺省值为 64。
M 标志位	当启用该功能时，表示接收到 RA 消息的接口除了通过无状态地址自动配置外，还可以通过有状态地址配置获取 IPv6 地址。禁用该功能时，表示接收到 RA 消息的接口只可以通过无状态地址自动配置获取 IPv6 地址。该功能缺省为禁用。
O 标志位	当启用该功能时，表示接收到 RA 消息的接口可以通过无状态 DHCPv6 配置获取 IPv6 地址以外的网络配置信息。禁用该功能时，表示接收到 RA 消息的接口不能通过无状态 DHCPv6 配置获取 IPv6 地址以外的网络配置信息。该功能缺省为禁用。
重传时间	表示是否在 RA 报文中携带重传时间。如果启用该功能，则 RA 报文中将携带 ND 配置中所设置的重传时间的值。 设备发送 NS 消息后，如果未在指定的时间间隔内收到响应，则会重新发送 NS 消息。该功能缺省为禁用。
可达时间	表示是否在 RA 报文中携带可达时间。如果启用该功能，则 RA 报文中将携带 ND 配置中所设置的可达时间的值。 当通过邻居可达性检测确认邻居可达后，在所设置的可达时间内，设备认为邻居可达；超过设置的时间后，如果需要向邻居发送报文，会重新确认邻居是否可达。该功能缺省为禁用。
链路层地址	表示是否在 RA 报文中携带链路层地址。如果启用该功能，则 RA 报文中将携带通告接口的源链路层地址。该功能缺省为启用。
链路 MTU	表示是否在 RA 报文中携带 MTU。如果启用该功能，则 RA 报文中将携带通告接口自身的 MTU 值。该功能缺省为启用。
前缀列表	通过配置该列表，可以指定 RA 报文中通告的前缀的相关信息，配置项包括： • **IPv6 地址**：RA 通告前缀。 • **前缀长度**：通告前缀的长度。 • **首选生存时间**：通告前缀的首选时间。取值范围为 0-4294967295 秒，缺省值为 604800 秒。缺省为启用。 • **有效生存时间**：通告前缀的有效时间。取值范围为 0-4294967295 秒，缺省值为 2592000 秒。缺省为启用。 • **不通告**：不在 RA 消息中通告该前缀。该功能缺省为禁用，表示在 RA 消息中通告该前缀。 • **非自动配置**：不用该前缀进行无状态地址自动配置。该功能缺省为禁用，表示该前缀可以用于无状态地址自动配置。 • **非在链**：该前缀非直连可达。从 NISG 收到 RA 报文的接口将根据 RA 报文中的 L 标志位判断其自身是否与 NISG 的 RA 通告接口处于同一链路。该功能缺省为禁用，表示该前缀是直连可达的。 管理员可以添加最多 32 条通告前缀，且各通告前缀不可以重叠。另外，添加的通告前缀不可以是本地链路前缀、全 0 前缀或者多播前缀。

5 路由

本章阐述 NISG 路由和多播的相关特性。

- 5.1. 概述。简单介绍相关的基本概念。
- 5.2. 基本配置步骤。详细介绍使用 UI 或命令行方式进行基本配置的步骤。
- 5.3. 基础范例。举例介绍单播及多播的基础配置。
- 5.4. 高级范例。举例介绍较为复杂场景下的配置步骤。
- 5.5. 参数说明。路由配置中相关参数的解释。

5.1. 概述

当 NISG 收到数据包后，如果该数据包属于，

1. 已存在会话：该数据包将直接按照指定路由被转发。
2. 不存在的会话：NISG 为该数据包指定转发路径。

本节介绍 NISG 路由、交换的概念。

- 5.1.1 单播
- 5.1.2 三层多播
- 5.1.3 二层多播

5.1.1 单播

5.1.1.1 缺省策略路由
5.1.1.2 负载均衡和链路探测
5.1.1.3 策略路由

5.1.1.1 缺省策略路由

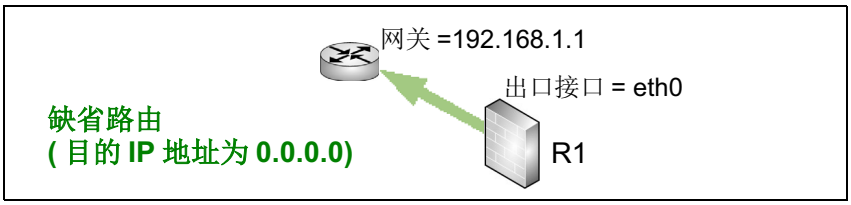
依据目的 IP 地址，缺省路由表决定以下参数：

1. 出口接口（可以设置路由的出口接口为 “Null” 来丢弃数据包，这样可以防止路由环路）。
2. 网关。

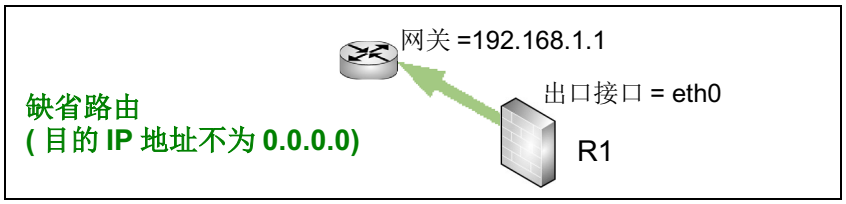
如果数据包没有匹配任何配置的策略路由，则会按照缺省策略路由转发。（策略路由为规定了流量的入口接口、源 IP 地址、服务及 TOS 的路由）。

系统可提供两种类型的缺省路由。

1. 数据包如无其他缺省路由可选，则选择目的 IP 地址为 0.0.0.0/0 的路由。

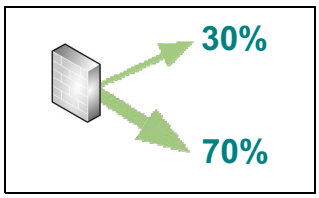


2. 数据包目的IP地址为所配置的IP地址或IP地址段时，根据目的IP地址选取缺省路由。

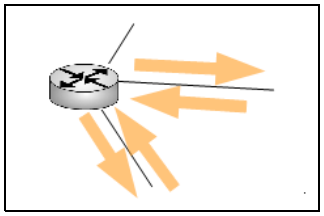


5.1.1.2 负载均衡和链路探测

负载均衡：一个新建会话会将数据包按权重分配到多条链路上。如果该条链路断开，该会话会重新选择一条新的链路进行通信。



链路探测：开启时， NISG 在每个探测周期会发送探测数据包到下一跳设备。



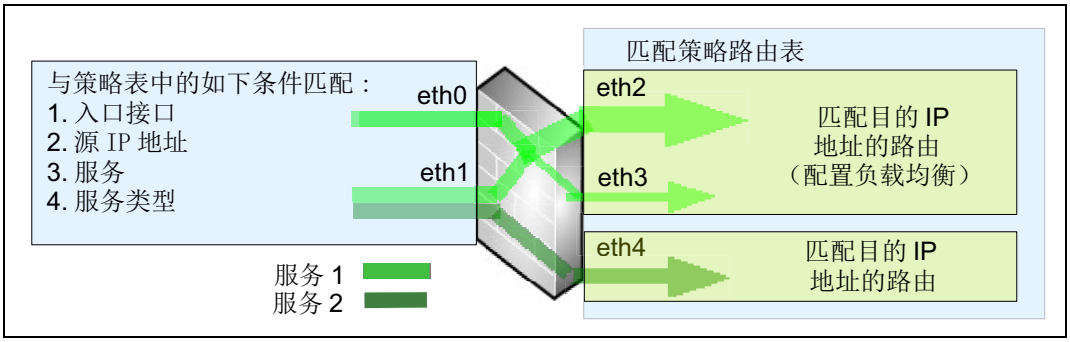
下列情况属链路故障：

- 探测次数达到阈值且在每个探测周期内都没有收到对端响应报文。
- 出口接口故障或已被关闭。

NISG 提供如下链路探测类型

探测类型	地址类型	发送的探测报文	应收到的响应报文
ARP Ping (ARP probe)	IPv4	ARP 请求报文	含 MAC 地址的 ARP 回复报文
TCP Ping (TCP probe)	IPv4 & IPv6	TCP SYN 报文	TCP SYN/ACK 报文
Ping (ICMP probe)	IPv4 & IPv6	通过 ping 或 ping6 命令发送的 ICMP 请求报文	ICMP 回复报文
NS Ping (NS probe)	IPv6	邻居请求报文	邻居通告报文

5.1.1.3 策略路由



策略表显示策略内容包含：

1. 入口接口
2. 源 IP 地址
3. 服务
4. TOS

每条策略都有自己的路由表。这些路由与缺省策略路由相似，通过数据包的目的 IP 地址确定以下参数：

1. 出口接口
2. 网关
3. 是否为负载均衡选路

所选的策略为：

1. 匹配相关参数的策略中优先级最高的一条。
2. 在该条策略中路由表有对应的出口路由。

路由选路：如果一张路由表中有多条到达同一目的 IP 地址的路由，系统根据以下三个条件，优先级由高到底，进行选路。

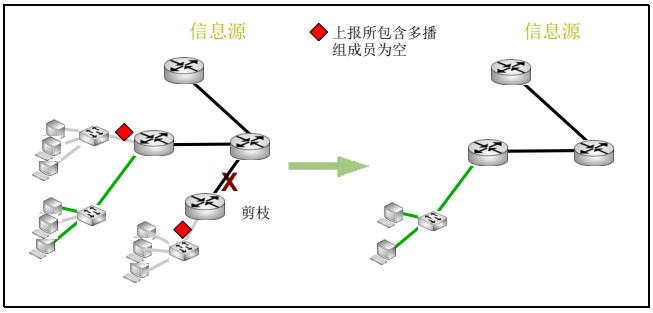
a. 最长掩码长度或前缀长度。
b. 最小 metric 值。
c. 最先添加路由。

5.1.2 三层多播

- 5.1.2.1 三层动态多播
- 5.1.2.2 三层静态多播

5.1.2.1 三层动态多播

- **路由决策：**系统基于 DVMRP 协议，为多播组接口动态输出包含距离的路由表。Metric 值用于路由选路，系统会选取 Metric 值较低的路径进行路由。
- **缓存有效时间：**动态多播路由在缓存中存在的时间长度。
- **阈值：**阈值为系统对转发多播数据包的 TTL 值的限制。只有数据包在入口接口处的 TTL 的值大于该接口阈值，才能被转发。
- **裁剪有效时间：**通过“广播与剪枝”方式，DVMRP 建立并维护从数据源到多播组的分发树。如果叶节点路由器发现与其直连的子网中没有多播主机，它将发送剪枝信息给数据源，并暂时从分发树上剪掉此部分。如果叶节点路由器发现有新组员要添加的多播组，DVMRP 会嫁接新枝到分发树中。下图展示了剪枝的过程。



5.1.2.2 三层静态多播

静态多播路由中配置有源 IP 地址、多播组 IP 地址、入口接口和出口接口等信息，多播数据包依据以下三点匹配静态路由，进而选择出口接口：

1. 源 IP 地址。
2. 多播组 IP 地址。
3. 入口接口。

在静态路由场景下，入口接口和转发接口的 DVMRP 功能必须处于开启状态。

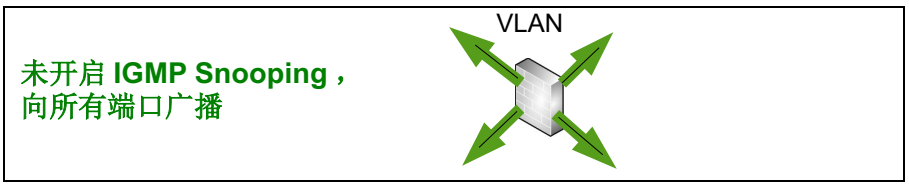
5.1.3 二层多播

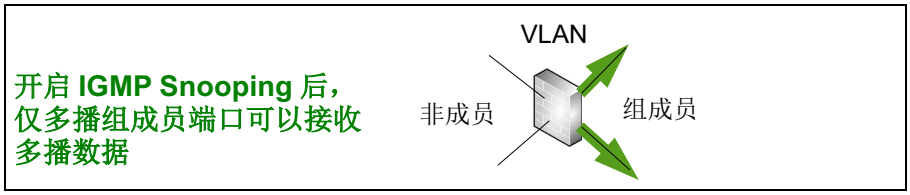
本节描述以下内容：

- 5.1.3.1 二层动态多播
- 5.1.3.2 二层静态多播

5.1.3.1 二层动态多播

主机通过 IGMP 协议动态加入多播组中。 NISG 支持 IGMPv1 和 IGMPv2。

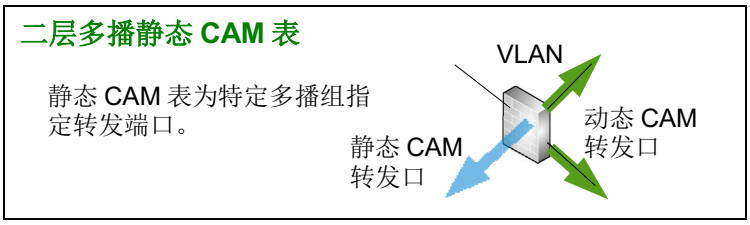




5.1.3.2 二层静态多播

二层多播转发表包含多播 IP 地址和转发接口的 MAC 地址的对应关系，多播数据包根据该表确定出口接口。

IGMP snooping 功能必须开启。



5.2. 基本配置步骤

5.2.1 单播
5.2.2 三层多播
5.2.3 二层多播

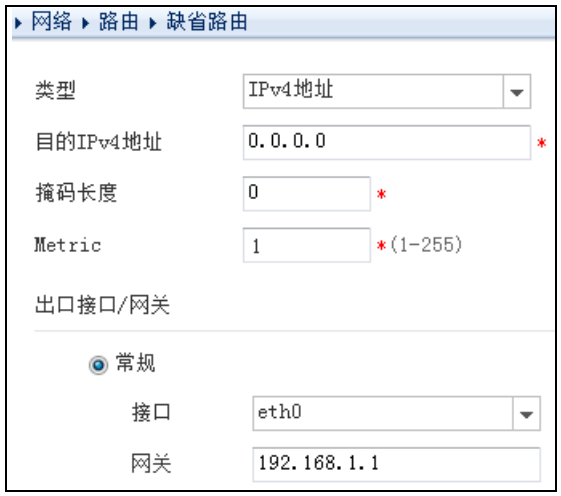
5.2.1 单播

- 5.2.1.1 缺省策略和缺省路由
- 5.2.1.2 负载均衡
- 5.2.1.3 策略路由

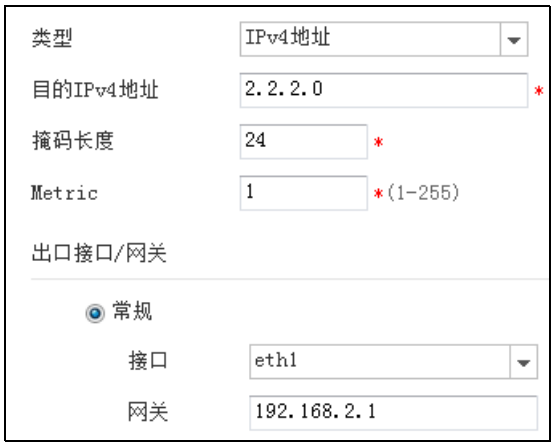
5.2.1.1 缺省策略和缺省路由

1. 选择**网络** > **路由** > **缺省路由** > **新建**指定缺省路由。

在地址栏中输入 0.0.0.0，并指定掩码长度 0， metric 值，出口接口和网关地址。



2. 选择**网络**> **路由**> **缺省路由**> **新建**为去往特定的目的IP地址或IP地址段的数据包指定缺省路由。



缺省策略路由会显示在缺省路由表中。

表 129 配置缺省路由相关命令

route	添加缺省路由。
show route	显示缺省路由信息。
unset route	删除缺省路由。

5.2.1.2 负载均衡

设置负载均衡策略。此处以配置缺省路由的负载均衡功能为例进行介绍，策略路由和非缺省路由负载均衡配置方法与其相似。

- 关闭探测。

- 开启探测。

配置完成后，缺省路由表中显示如下内容：

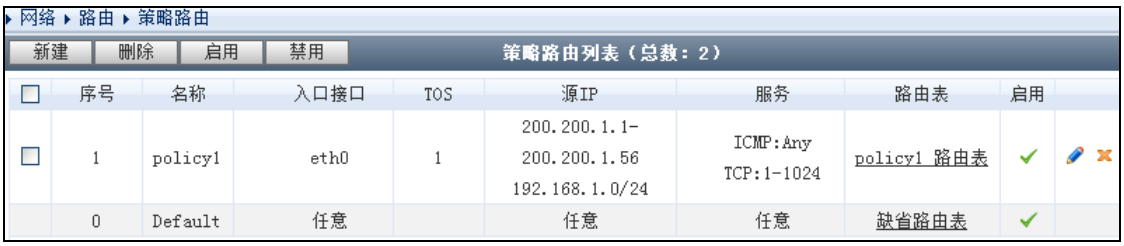
表 130 配置负载均衡相关命令

route {**default** | *ipv4 netmask*} **load-balancing**	为 IPv4 目的地址的数据包添加具有负载均衡功能的路由。
route {**default-v6** | *ipv6 prefix_length*} load-balancing	为 IPv6 目的地址的数据包添加具有负载均衡功能的路由。

5.2.1.3 策略路由

1. 依次选择**网络** > **路由** > **策略路由** > **新建**。
2. 配置入口接口、TOS、源 IP 地址和服务。

3. 点击**确定**，点击 。检查策略。



缺省情况下，添加后的路由策略会是开启状态。如果您删除一条路由策略，它所对应的路由表也将被删除。

4. 点击 **policy1 路由表**，配置匹配该策略的数据包的路由。配置方法与 5.2.1.1 缺省策略和缺省路由相同。

每条策略都有自己的路由表，策略路由表与缺省策略路由表相似。

路由包含如下信息：

1. 出口接口。
2. 网关。
3. 是否采用负载均衡方式。

如果在同一路由表中有到达同一目的 IP 地址多条路由，系统则会根据以下参数，优先级由高到低，选取最优路由。

a. 最长掩码或前缀。

b. 最小 metric 值。

c. 最先添加路由。

.

表 131　配置策略路由相关命令

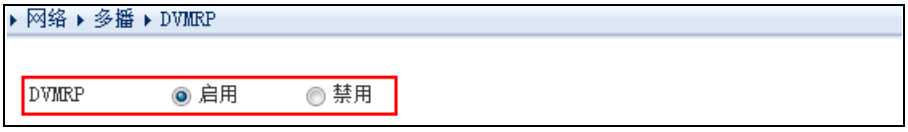
policy route *policy_name* [**number** *pri*]	添加策略。
matching	添加判断数据包是否匹配策略的标准。
policy route *policy_name* {**enable** | **disable**}	开启或关闭策略。
show policy route [*policy_name*]	显示策略信息。

5.2.2 三层多播

- 5.2.2.1 三层动态多播
- 5.2.2.2 三层静态多播

5.2.2.1 三层动态多播

1. 选择**网络** > **多播** > **DVMRP**。
2. 开启 DVMRP 服务。



3. 选择转发多播数据包的接口和入口接口，点击**添加**，为启用的 DVMRP 接口配置阈值和 metric 值。

4. 输入缓存有效时间 （缓存有效时间指系统动态自学习的多播路由信息在缓存中保存的时间）。

5. 输入裁剪有效时间 （裁剪有效时间指 NISG 保持分发树某分支处于裁剪状态下的时间）。

6. 点击**确定**，点击 。

表 132　配置 DVMRP 接口相关命令

dvmrp {enable | disable}	启用或禁用 DVMRP 服务。
dvmrp cache-lifetime *time*	设置 DVMRP 路由在多播缓存中的保存时间。
dvmrp prune-lifetime *time*	设置 NISG 保持裁剪状态的有效时间。
dvmrp metric {*metric_value* | **default**}	设置三层接口 DVMRP 的 metric 值。
dvmrp {on | off}	启用或禁用三层接口的 DVMRP 功能。
dvmrp pim {enable | disable}	启用或禁用 PIM 邻居发现功能。
dvmrp threshold {*threshold_value* | **default**}	设置三层接口的 TTL 阈值。
show dvmrp {interface | neighbor | timer}	显示 DVMRP 监控信息。
show dvmrp state	显示 DVMRP 配置信息。

5.2.2.2 三层静态多播

1. 选择**网络** > **路由** > **多播路由** > **新建**来增加路由。

TTL 决定数据包是否可以从接口中转发出去。当多播数据包的 TTL 值大于您所配置的阈值时，该数据包可以被转发。

2. 点击**确定**，点击 。

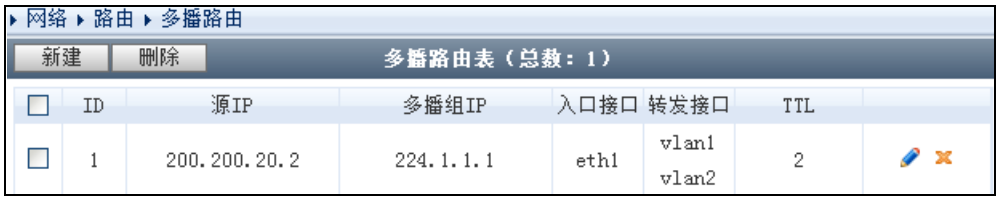


表 133 配置静态多播路由命令

dvmrp route	添加静态多播路由。
show dvmrp route	显示多播路由信息。
unset dvmrp route	删除静态多播路由。

5.2.3 二层多播

- 5.2.3.1 二层动态多播
- 5.2.3.2 二层静态多播

5.2.3.1 二层动态多播

1. 选择**网络** > **多播** > **IGMP Snooping**。点击 vlan1 对应的 。

2. 点击**开**，开启 IGMP Snooping 功能。
3. 点击任意接口项设置该接口的 IGMP 版本和模式。

4. 点击**确定**，点击 。
5. 如想查看 IGMP snooping 状态，可以点击 **IGMP Snooping 状态**链接，或者选择**监控** > **多播** > **IGMP Snooping** 状态进行查看。如需更多信息，可参见 14.16.2 IGMP Snooping 状态。

5.2.3.2 二层静态多播

1. 选择**网络** > **多播** > **IGMP Snooping**。点击 vlan1 对应的 。

2. 开启 IGMP Snooping。

3. 点击链接 vlan1 的**多播 CAM 表**。点击**新建**，建立一条多播 CAM 条目。

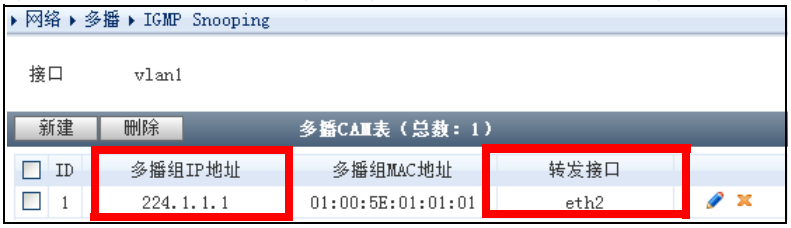


表 134 配置 IGMP Snooping 相关命令

igmp-snooping {on | off}	开启或关闭 IGMP snooping 功能。
igmp-snooping interface-flags	设置 VLAN 中二层接口所连接的网络类型。
igmp-snooping version	设置 IGMP 版本。
multicast cam-table	添加静态多播 CAM 条目。
show igmp-snooping state [**vlan** *vlan_id*]	显示 IGMP Snooping 状态。
unset multicast cam-table	删除静态多播 CAM 条目。

5.3. 基础范例

本节举例介绍如何配置路由和多播功能。

5.3.1 单播
5.3.2 三层多播
5.3.3 二层多播

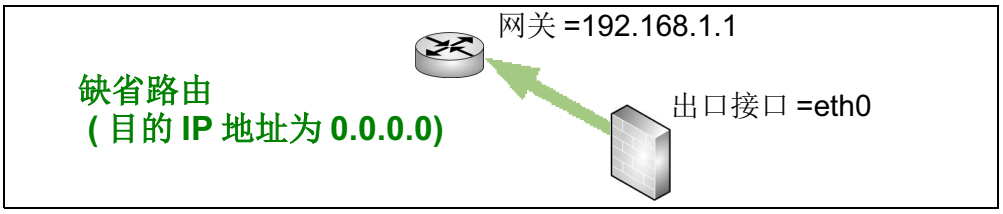
5.3.1 单播

本节举例介绍如何进行配置单播路由。

- 5.3.1.1 缺省路由
- 5.3.1.2 配置负载均衡
- 5.3.1.3 策略路由

5.3.1.1 缺省路由

本节介绍如何配置缺省路由。



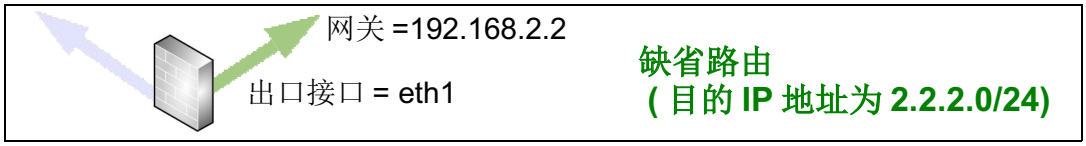
1. 点击**新建**，建立一条新的缺省路由。

2. 点击**确定**，点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] route 0.0.0.0 0.0.0.0 interface eth0 gateway
192.168.1.1 2
NetEye@root-system] exit
NetEye@root> save config
```

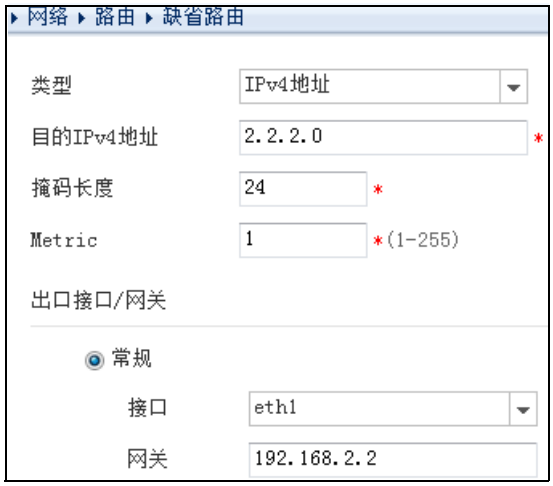
举例说明如何添加如下缺省策略路由 （目的 IP 地址不为 0 的缺省路由）。



为满足如下特征的数据包指定出口接口和网关。

- 不匹配任何策略。
- 有指定的目的 IP 地址。
- 在缺省路由表中没有其他更高优先级的路由。

进行如下参数配置：

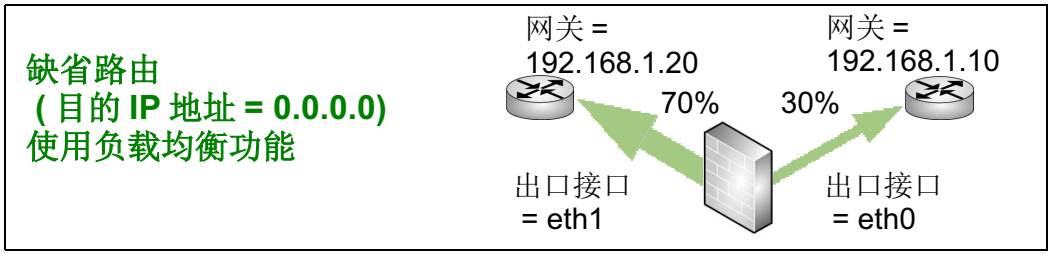


CLI

```
NetEye@root> configure mode override
NetEye@root-system] route 2.2.2.0 255.255.255.0 interface eth1 gateway
192.168.2.2 1
NetEye@root-system] exit
NetEye@root-system> save config
```

5.3.1.2 配置负载均衡

举例说明如何为缺省路由配置负载均衡。



1. 在负载均衡策略列表中点击**添加**，添加如下图的两条负载均衡策略。

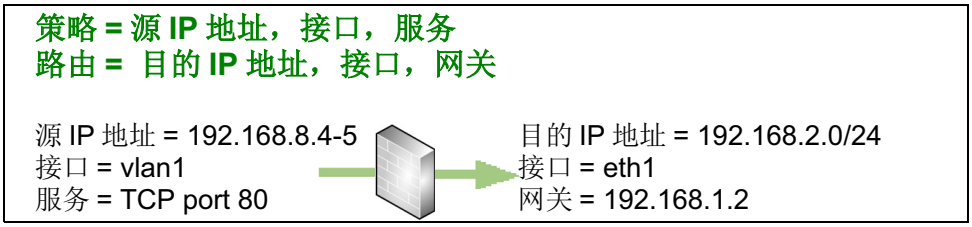
2. 点击**确定**，点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] route 0.0.0.0 0.0.0.0 load-balancing interface eth0 gateway 192.168.1.10 3 ip-track ping 192.168.1.10 15 5 1
NetEye@root-system] route 0.0.0.0 0.0.0.0 load-balancing interface eth1 gateway 192.168.1.20 7 ip-track ping 192.168.1.20 10 5 1
NetEye@root-system] exit
NetEye@root> save config
```

5.3.1.3 策略路由

举例说明如何创建一条策略路由。



1. 选择**网络** > **路由** > **策略路由** > **新建**。
2. 填写如下参数创建新的策略。

3. 点击**确定**。
4. 点击 Policy2 **路由表**，点击**新建**，新建一条静态路由。

5. 点击**确定**，点击 。

CLI

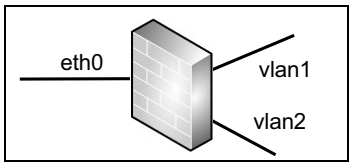
```
NetEye@root> configure mode override
NetEye@root-system] policy route policy2 enable
NetEye@root-system-routepolicy-policy2] matching input-interface vlan1
NetEye@root-system-routepolicy-policy2] matching sip 192.168.8.4
192.168.8.5
NetEye@root-system-routepolicy-policy2] matching protocol tcp 80
NetEye@root-system-routepolicy-policy2] route 192.168.2.0 255.255.255.0
interface eth1 gateway 192.168.1.2 1
NetEye@root-system-routepolicy-policy2] end
NetEye@root> save config
```

5.3.2 三层多播

- 5.3.2.1 配置三层动态多播
- 5.3.2.2 配置三层静态多播

5.3.2.1 配置三层动态多播

举例说明如何配置下图所示组网的动态多播。



1. 选择**网络** > **多播** > **DVMRP**。
2. 开启 DVMRP 功能。
3. 点击**添加**，对 DVMRP 接口做如下配置：
   a. 选择 vlan1 进行多播数据包的转发。
   b. 设置 vlan1 的阈值为 1。
   c. 设置 vlan1 的 metric 值为 1。点击**确定**。

4. 同样方式配置 vlan2。
5. 设置系统自学习的DVMRP路由在缓存中保存时间为7200秒。如果这条路由在7200秒中没有被用到，则它会被从缓存中删除。
6. 设置裁剪有效时间为 7200 秒。如支路被裁剪，则会被裁剪掉 7200 秒后，恢复向其转发多播数据包。
7. 点击**确定**，点击 。
8. 选择**监控** > **多播** >**DVMRP 邻居**，进行相关数据监控。

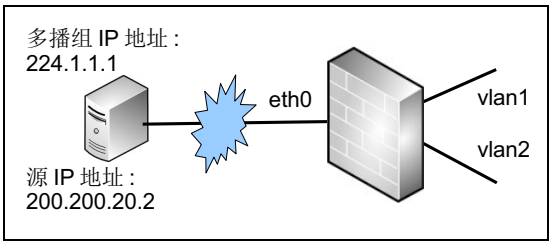
CLI

```
NetEye@root> configure mode
NetEye@root-system] dvmrp enable
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] dvmrp on
NetEye@root-system-vlan1] vlan 2
NetEye@root-system-vlan2] dvmrp on
NetEye@root-system-vlan2] exit
```

```
NetEye@root-system] dvmrp cache-lifetime 7200
NetEye@root-system] dvmrp prune-lifetime 7200
NetEye@root-system] dvmrp pim enable
NetEye@root-system] exit
NetEye@root> save config
```

5.3.2.2 配置三层静态多播

新建到 vlan1 的静态多播路由。



1. 点击**多播路由**链接或选择**网络** > **路由** > **多播路由**。
2. 点击**新建**，按照如下参数设定静态多播路由。

如果多播数据包的 TTL 值为大于 1，则该数据数据包能够被转发。

3. 点击**确定**，点击 。

CLI

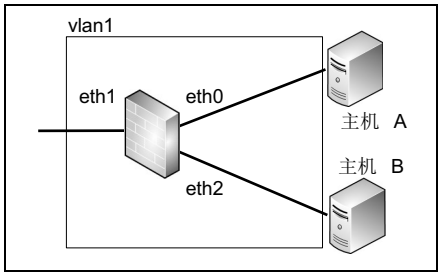
```
NetEye@root> configure mode
NetEye@root-system] dvmrp route 200.200.20.2 224.1.1.1 input eth0
forwarding vlan1 threshold 2
NetEye@root-system] exit
NetEye@root> save config
```

5.3.3 二层多播

- 5.3.3.1 二层动态多播
- 5.3.3.2 二层静态多播

5.3.3.1 二层动态多播

举例说明如何为下图中组网配置动态多播。



1. 选择**网络** > **多播** >**IGMP Snooping**，点击 vlan1 对应的 。
2. 在状态栏中点击**开**，开启 IGMP snooping。

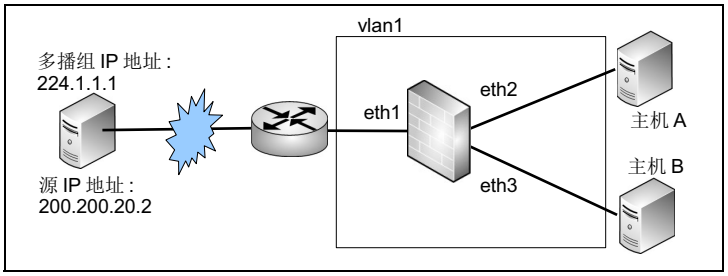
3. 点击**确定**，点击 。
4. 选择**监控** >**CAM**。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] igmp-snooping on
NetEye@root-system-vlan1] igmp-snooping version ethernet 0 v2
NetEye@root-system-vlan1] igmp-snooping version ethernet 1 v2
NetEye@root-system-vlan1] igmp-snooping version ethernet 2 v2
NetEye@root-system-vlan1] igmp-snooping interface-flags ethernet 0
host
NetEye@root-system-vlan1] igmp-snooping interface-flags ethernet 1
multicast-router
NetEye@root-system-vlan1] igmp-snooping interface-flags ethernet 2
host
NetEye@root-system-vlan1] end
NetEye@root> save config
```

5.3.3.2 二层静态多播

举例说明如何配置将多播 IP 地址为 224.1.1.1 的数据包转发到主机 A。



1. **选择** > **多播** >**IGMP Snooping**。
2. 点击链接 **vlan1 的多播 CAM 表**。
3. 点击**新建**，创建以下静态多播 CAM 项。

4. 点击**确定**，点击 。
5. 选择**监控** > **CAM**。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] multicast cam-table 224.1.1.1 eth1
NetEye@root-system-vlan1] end
NetEye@root> save config
```

5.4. 高级范例

本节以范例的形式介绍如何配置路由和多播：

- 5.4.1 范例 1：创建带有负载均衡的静态路由
- 5.4.2 范例 2：创建策略路由策略
- 5.4.3 范例 3：静态多播路由应用
- 5.4.4 范例 4：动态 DVMRP 多播路由应用
- 5.4.5 范例 5：IGMP Snooping 和静态多播 CAM 表项应用
- 5.4.6 范例 6：IGMP Snooping 和动态多播 CAM 表项应用

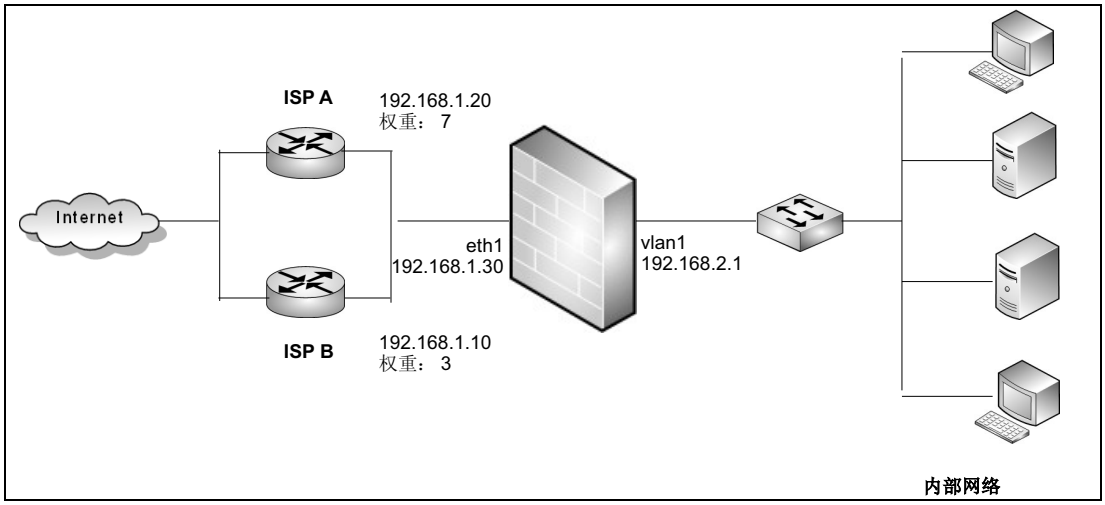
在每个场景中，您必须先完成一些配置：

1. 选择**网络 > 接口**，配置 NISG 接口。参见第 4 章，网络配置。
2. 如需使用安全域，选择**网络 > 安全域**，创建安全域。参见 4.12 安全域。
3. 选择**防火墙 > 缺省策略设置**，将缺省域间策略设置为**允许**；或选择**防火墙 > 访问策略**，创建允许任何数据流的访问策略。参见第 8 章，策略。

5.4.1 范例 1：创建带有负载均衡的静态路由

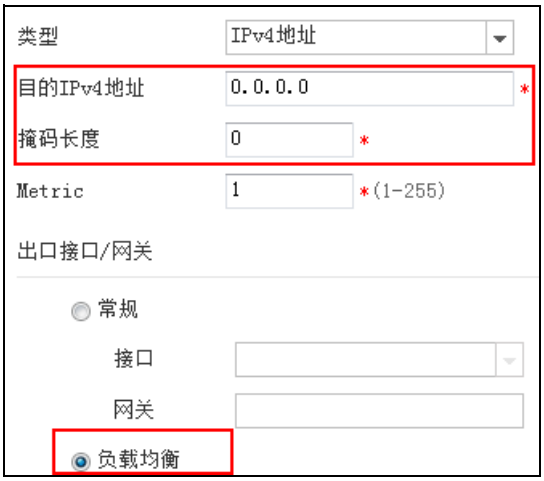
某企业的内部网络通过两家网络服务提供商接入互联网。由于网络服务提供商 A 的带宽和服务质量优于提供商 B，管理员将提供商 A 的权重设置为 7，将提供商 B 的权重设置为 3，可以适当地分配流量。同时，管理员也希望 NISG 对通往两家网络服务提供商的链路进行探测，以保证在一条链路出现故障的情况下，流量仍然能够通过另一条链路转发。

图 15 企业网络拓扑图



WebUI

1. 选择**网络** > **路由** > **缺省路由**。
2. 点击**新建**，创建一条 IPv4 缺省路由。



3. 在**负载均衡列表**中，点击**添加**，添加以下两条负载均衡策略：

4. 点击**确定**。
5. 点击 。

CLI

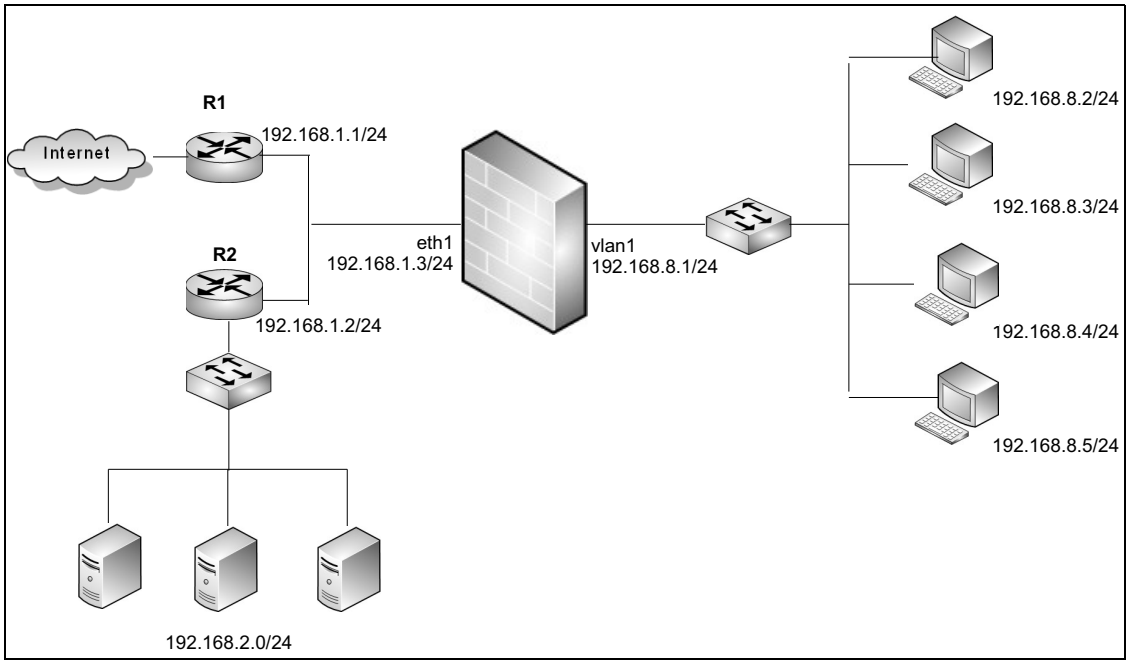
```
NetEye@root> configure mode override
NetEye@root-system] route 0.0.0.0 0.0.0.0 load-balancing interface eth1 gateway 192.168.1.20 7 ip-track ping 192.168.1.20 10 5 1
NetEye@root-system] route 0.0.0.0 0.0.0.0 load-balancing interface eth1 gateway 192.168.1.10 3 ip-track ping 192.168.1.10 15 5 1
NetEye@root-system] exit
NetEye@root>save config
```

5.4.2 范例 2：创建策略路由策略

一个内部网络的四台主机通过 NISG 与互联网和另一个内网相连。

- IP 地址为 192.168.8.2/24 和 192.168.8.3/24 的主机可以访问任意网络。
- IP 地址为 192.168.8.4/24 和 192.168.8.5/24 的主机只能访问端口号为 80 的内网服务器的 TCP 服务。

图 16 网络拓扑图



为前两台主机创建策略路由策略：

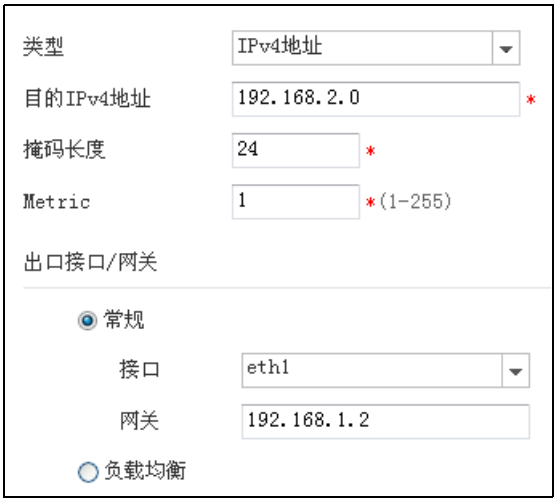
WebUI

1. 选择**网络** > **路由** > **策略路由**。
2. 点击**新建**，设置策略名称和接收数据包的接口。

3. 在**源 IP 地址**区域，点击**源 IP 地址列表**。点击**添加**，添加一段 IPv4 地址范围，点击**确定**。

4. 在**服务**区域，选择**任意**。

5. 点击**确定**。
6. 点击 **policy1 路由表**。点击**新建**，创建一条静态路由。



7. 点击**确定**。

8. 点击**新建**，创建一条缺省路由。

9. 点击**确定**。

10. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy route policy1 enable
NetEye@root-system-routepolicy-policy1] matching input-interface vlan1
NetEye@root-system-routepolicy-policy1] matching sip 192.168.8.2
192.168.8.3
NetEye@root-system-routepolicy-policy1] matching protocol any
NetEye@root-system-routepolicy-policy1] route 192.168.2.0 255.255.255.0
interface eth1 gateway 192.168.1.2 1
NetEye@root-system-routepolicy-policy1] route 0.0.0.0 0.0.0.0 interface
eth1 gateway 192.168.1.1 2
NetEye@root-system-routepolicy-policy1] exit
NetEye@root> save config
```

为另两台主机创建一条策略路由策略：

WebUI

1. 选择**网络** > **路由** > **策略路由**。
2. 点击**新建**，创建以下策略路由策略：

3. 点击**确定**。
4. 点击 **policy2 路由表**。点击**新建**，创建一条静态路由。

5. 点击**确定**。
6. 点击 。

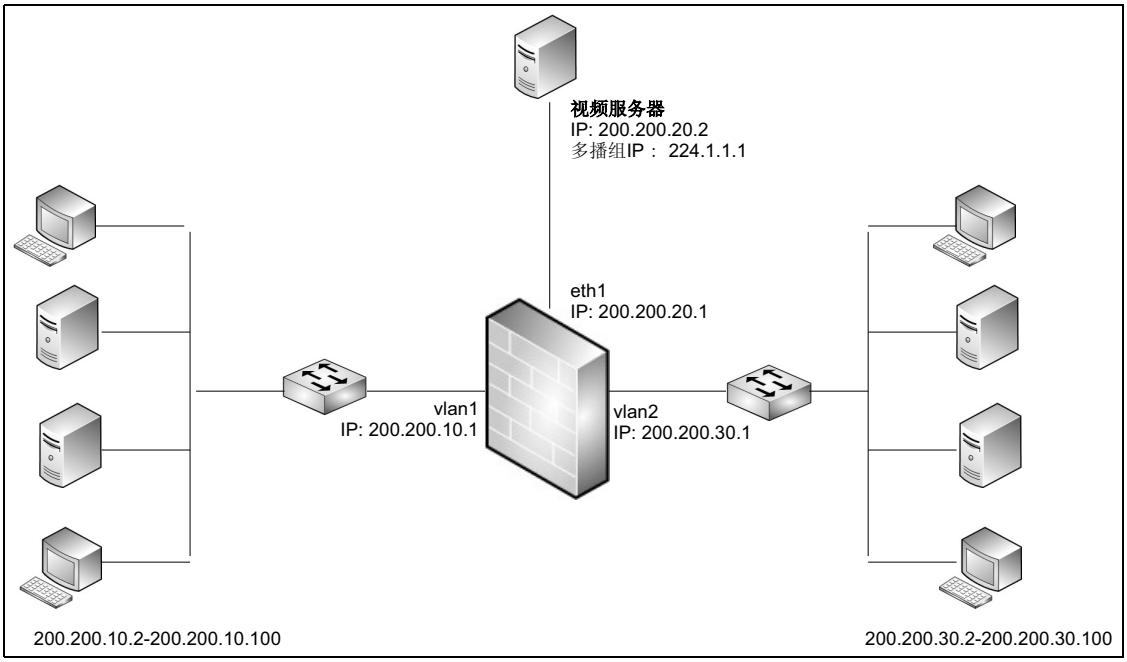
CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy route policy2 enable
NetEye@root-system-routepolicy-policy2] matching input-interface vlan1
NetEye@root-system-routepolicy-policy2] matching sip 192.168.8.4
192.168.8.5
NetEye@root-system-routepolicy-policy2] matching protocol tcp 80
NetEye@root-system-routepolicy-policy2] route 192.168.2.0 255.255.255.0
interface eth1 gateway 192.168.1.2 1
NetEye@root-system-routepolicy-policy2] end
NetEye@root> save config
```

5.4.3 范例 3：静态多播路由应用

视频服务器使用多播组 IP 地址 224.1.1.1 播放视频节目。多播数据包的 TTL 值为 5。管理员配置 NISG 以使 vlan1 和 vlan2 中的主机能够观看视频服务器播放的节目。

图 17 网络拓扑图



请先创建多播策略，允许多播数据流在接口间转发。参见 3.3 创建多播策略。

配置步骤如下：

- 5.4.3.1 3.1 配置 DVMRP
- 5.4.3.2 3.2 创建静态多播路由

5.4.3.1 3.1 配置 DVMRP

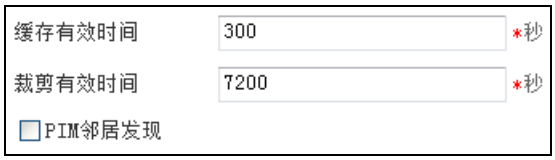
WebUI

1. 选择**网络** > **多播** >**DVMRP**。
2. 点击**启用**，开启 NISG 上的 DVMRP 功能。只有启用该功能，多播路由才会生效。

3. 在**启用的 DVMRP 接口**列表中，添加以下接口：

阈值和 Metric 在静态路由中不会生效。

4. 其他三个参数可以保持缺省配置，并且在静态路由中它们不会生效。



5. 点击**确定**。
6. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] dvmrp enable
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] dvmrp on
NetEye@root-system-vlan1] dvmrp metric 1
NetEye@root-system-vlan1] dvmrp threshold 1
NetEye@root-system-vlan1] exit
NetEye@root-system] interface ethernet 1
NetEye@root-system-if-eth1] dvmrp on
NetEye@root-system-if-eth1] dvmrp metric 1
NetEye@root-system-if-eth1] dvmrp threshold 1
NetEye@root-system-if-eth1] exit
NetEye@root-system] vlan 2
NetEye@root-system-vlan2] dvmrp on
NetEye@root-system-vlan2] dvmrp metric 1
NetEye@root-system-vlan2] dvmrp threshold 1
NetEye@root-system-vlan2] exit
NetEye@root-system] dvmrp cache-lifetime 300
NetEye@root-system] dvmrp prune-lifetime 7200
NetEye@root-system] dvmrp pim disable
NetEye@root-system] exit
NetEye@root> save config
```

5.4.3.2 3.2 创建静态多播路由

WebUI

1. 点击**多播路由**超链接。
2. 点击**新建**，创建以下静态多播路由：

因为多播数据包的 TTL 值是 5，要使 NISG 转发多播数据包，需要将静态路由的 TTL 设置为小于 5 的值 （在本范例中，设置为 2）。

3. 点击**确定**。
4. 点击 。

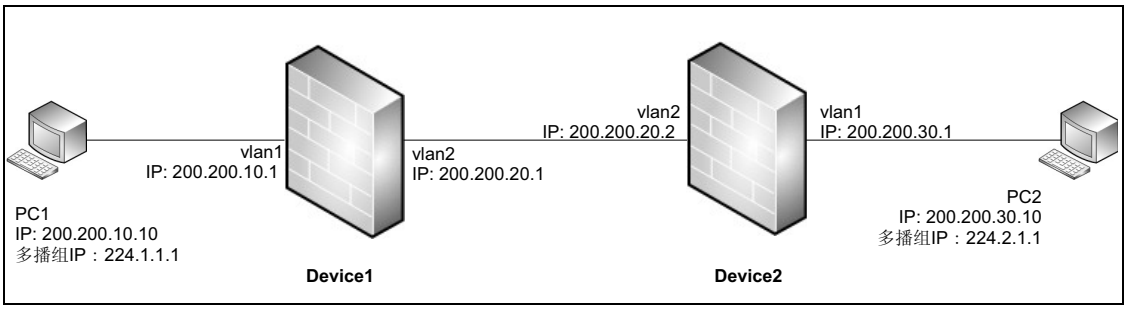
CLI

```
NetEye@root> configure mode
NetEye@root-system] dvmrp route 200.200.20.2 224.1.1.1 input eth1
forwarding vlan1,vlan2 threshold 2
NetEye@root-system] exit
NetEye@root> save config
```

5.4.4 范例 4：动态 DVMRP 多播路由应用

使用 PC1 和 PC2 的两个用户想要进行视频会议。 PC1 和 PC2 分别通过多播组 IP 地址 224.1.1.1 和 224.2.1.1 播放视频。多播数据包的 TTL 值为 3。管理员在 Device1 和 Device2 上配置 DVMRP 功能，使两个用户可以进行视频会议。

图 18 网络拓扑图



请先在 Device1 和 Device2 上完成以下配置：

- 创建访问策略，允许两台 NISG 设备的域间访问。参见 范例 2：创建访问策略。
- 创建多播策略，允许多播数据流转发。参见 3.3 创建多播策略。

5.4.4.1 Device1

WebUI

1. 选择**网络** > **多播** >**DVMRP**。
2. 点击**启用**，启用 DVMRP 功能。
3. 点击**添加**并配置以下 DVMRP 接口：
   a. 选择转发多播数据包的接口 vlan1.
   b. 将 vlan1 的阈值设置为 1，使 TTL 为 3 的多播数据包可以被接口转发。
   c. 将 vlan1 的 Metric 设置为 1，用于路由交换和更新。
   d. 点击**确定**。

   以同样的方式设置 vlan2。

4. 将从 Device2 学到的动态路由的缓存有效时间设置为 7200 秒。

   路由将在 Device1 的缓存中保留 2 个小时。如果在此期间，路由未被使用， 2 个小时后，该路由将被删除。

5. 将 Device1 的裁剪有效时间设置为 7200 秒。

   - 在此期间， Device1 裁剪发往 Device2 的多播数据包；
   - 2 个小时后， Device1 将恢复向 Device2 转发多播数据包。

6. （可选）勾选 **PIM 邻居发现**，使 Device1 支持 PIM 协议。
7. 点击**确定**。
8. 点击 。

如需监控动态多播路由或 DVMRP 邻居，选择**监控** > **路由**或**监控** > **多播** >**DVMRP 邻居**。更多信息，参见 14.16.1 DVMRP 邻居。

CLI

```
NetEye@root> configure mode
NetEye@root-system] dvmrp enable
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] dvmrp on
NetEye@root-system-vlan1] dvmrp metric 1
NetEye@root-system-vlan1] dvmrp threshold 1
NetEye@root-system-vlan1] exit
NetEye@root-system] vlan 2
NetEye@root-system-vlan2] dvmrp on
NetEye@root-system-vlan2] dvmrp metric 1
NetEye@root-system-vlan2] dvmrp threshold 1
NetEye@root-system-vlan2] exit
NetEye@root-system] dvmrp cache-lifetime 7200
NetEye@root-system] dvmrp prune-lifetime 7200
NetEye@root-system] dvmrp pim enable
NetEye@root-system] policy default inter-zone access permit
NetEye@root-system] exit
NetEye@root> save config
```

5.4.4.2 Device2

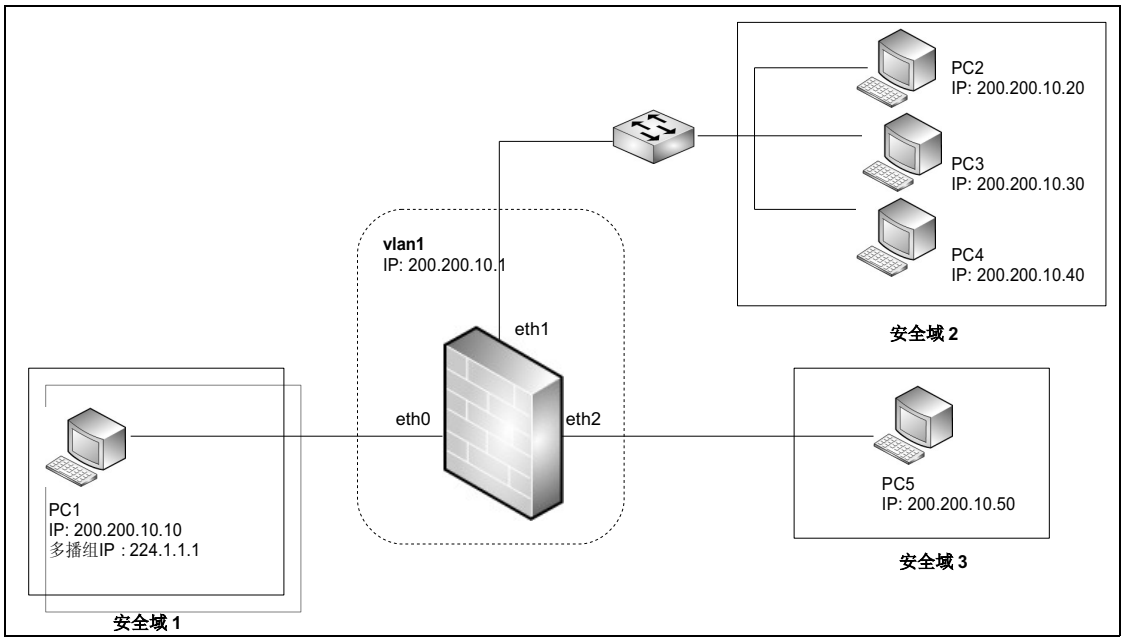
使用相同的方式配置 Device2。在完成所有配置后，使用 PC1 和 PC2 的两个用户可以进行视频会议。

5.4.5 范例 5：IGMP Snooping 和静态多播 CAM 表项应用

VLAN 接口 vlan1 包含三个二层以太网接口 eth0、 eth1 和 eth2。 PC1 为多播源，通过多播组 IP 地址 224.1.1.1 播放视频数据。

管理员在 vlan1 中配置 IGMP Snooping。创建一条静态多播 CAM 表项以使 PC2、 PC3、PC4 能一直接收到多播视频数据流；而 PC5 只有在点播后，才能收到多播数据流。

图 19 网络拓扑图



请先创建多播策略，允许多播数据流在三个安全域间转发。参见 范例 3：安全域间多播策略的应用。

配置步骤如下：

- 5.4.5.1 5.1 配置 vlan1 的 IGMP Snooping 属性
- 5.4.5.2 5.2 创建静态多播 CAM 表项

5.4.5.1 5.1 配置 vlan1 的 IGMP Snooping 属性

WebUI

1. 选择**网络** > **多播** >**IGMP Snooping**，点击 vlan1 对应的 。
2. 在**状态**区域点击**开**，启用 IGMP Snooping 功能，设置二层接口的 IGMP 版本和模式:

3. 点击**确定**。
4. 点击 。

如需查看 IGMP Snooping 状态，点击 **IGMP Snooping 状态**超链接或选择**监控** > **多播** >**IGMP Snooping 状态**。关于 IGMP Snooping 状态信息，请参见 14.16.2 IGMP Snooping 状态。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] igmp-snooping on
NetEye@root-system-vlan1] igmp-snooping version ethernet 0 v2
NetEye@root-system-vlan1] igmp-snooping version ethernet 1 v2
NetEye@root-system-vlan1] igmp-snooping version ethernet 2 v2
NetEye@root-system-vlan1] igmp-snooping interface-flags ethernet 0
host
NetEye@root-system-vlan1] igmp-snooping interface-flags ethernet 1
multicast-router
NetEye@root-system-vlan1] igmp-snooping interface-flags ethernet 2
host
NetEye@root-system-vlan1] end
NetEye@root> save config
```

5.4.5.2 5.2 创建静态多播 CAM 表项

WebUI

1. 选择**网络** > **多播** >**IGMP Snooping**。
2. 在**多播 CAM 表**列内点击 vlan1 对应的多播 CAM 表的超链接。

3. 点击**新建**，创建如下静态多播 CAM 表项：

4. 点击**确定**。
5. 点击 。

如需监控静态和动态多播 CAM 表项，选择**监控** >**CAM**。更多信息，请参见 14.8 CAM。

CLI

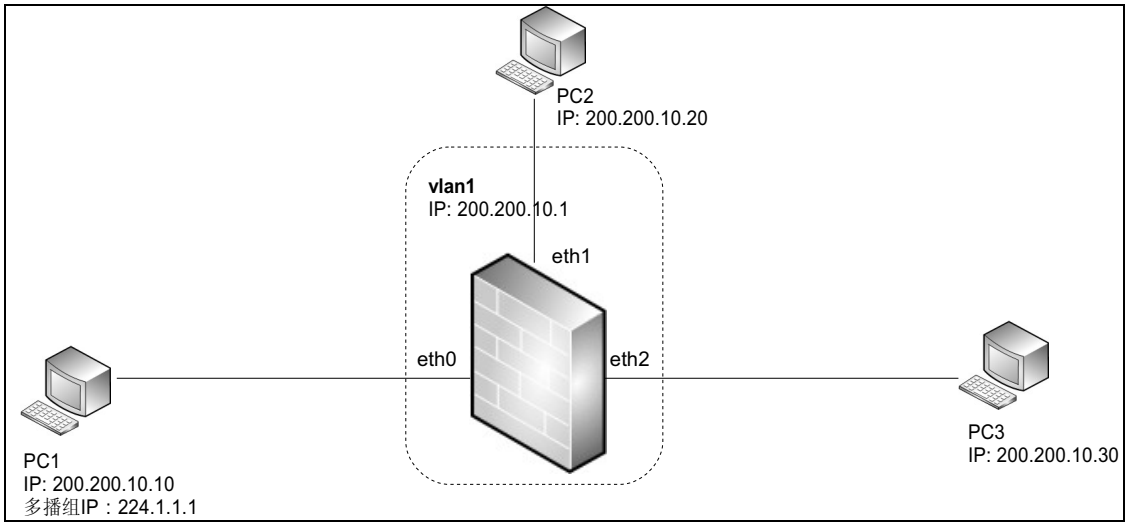
```
NetEye@root> configure mode override
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] multicast cam-table 224.1.1.1 eth1
NetEye@root-system-vlan1] end
NetEye@root> save config
```

5.4.6 范例 6：IGMP Snooping 和动态多播 CAM 表项应用

VLAN 接口 vlan1 包含三个二层以太网接口 eth0、 eth1 和 eth2。 PC1 为多播源，通过多播组 IP 地址 224.1.1.1 播放视频数据。

管理员配置 vlan1 的 IGMP Snooping 功能。当用户从 PC2 和 PC3 进行点播时， PC2 和 PC3 将向 224.1.1.1 发送 IGMP 成员报告， NISG 可以通过监听报告创建动态 CAM 表项，而后 PC2 和 PC3 的用户能够观看多播视频。当任意一个用户关闭视频，发送离开组消息时， NISG 会删除对应的动态 CAM 表项。

图 20 网络拓扑图



请先创建多播策略，允许多播数据流的转发。参见 3.3 创建多播策略。

WebUI

1. 选择**网络** > **多播** >**IGMP Snooping**，点击 vlan1 对应的 。
2. 在**状态**区域点击**开**，启用 IGMP Snooping 功能，并进行如下配置。

3. 点击**确定**。
4. 点击 。

如需查看 IGMP Snooping 状态，点击 **IGMP Snooping 状态**超链接或选择**监控** > **多播** >**IGMP Snooping 状态**。关于 IGMP Snooping 状态信息，请参见 14.16.2 IGMP Snooping 状态。

创建动态 CAM 表项后，可以选择**监控** >**CAM** 监控表项。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] igmp-snooping on
NetEye@root-system-vlan1] igmp-snooping version ethernet 0 v2
NetEye@root-system-vlan1] igmp-snooping version ethernet 1 v2
NetEye@root-system-vlan1] igmp-snooping version ethernet 2 v2
NetEye@root-system-vlan1] igmp-snooping interface-flags ethernet 0
host
NetEye@root-system-vlan1] igmp-snooping interface-flags ethernet 1
host
NetEye@root-system-vlan1] igmp-snooping interface-flags ethernet 2
host
NetEye@root-system-vlan1] end
NetEye@root> save config
```

5.5. 参数说明

本节介绍配置路由或多播功能时用到的参数的含义 :

- 5.5.1 单播路由参数
- 5.5.2 单播策略路由参数
- 5.5.3 三层动态多播 （DVMRP）参数
- 5.5.4 三层静态多播参数
- 5.5.5 二层动态多播参数 （IGMP Snooping）
- 5.5.6 二层静态多播 CAM 条目参数

5.5.1 单播路由参数

表 135 单播路由参数说明

参数	说明
类型	IP 地址的类型。 IPv4 地址或 IPv6 地址。
目的 IPv4 地址 / 目的 IPv6 地址	数据包要被发送到的目的主机或目的网络的地址。 缺省路由的目的 IPv4 和 IPv6 地址分别是 0.0.0.0 和 ::。
掩码长度 / 前缀长度	目的 IPv4 地址的掩码长度或目的 IPv6 地址的前缀长度。 缺省路由的掩码长度和前缀长度都为 0。 掩码长度的取值范围是 0 ～ 32 ；前缀长度的取值范围为 0 ～ 128。
Metric	指路由的优先级。取值范围为 1 ～ 255。 Metric 值越小，优先级越高。
出口接口 / 网关	用于为静态路由设置一个出口接口、网关或两者均设置。 您可以配置常规的静态路由，也可以配置带有负载均衡策略的静态路由。
常规	用于配置不带负载均衡功能的静态路由。 管理员至少需要设置以下一项： **接口**：用于将数据包转发出去的三层接口。如果管理员选择 Null 接口，则不允许输入网关地址，数据包会被丢弃。 **网关**：对端网络无法直达时的下一跳路由设备的 IP 地址。
负载均衡	用于配置具有负载均衡功能的静态路由。 管理员可以为负载均衡策略配置以下参数： **接口**：转发数据包的三层接口。 **网关**：对端网络无法直达时的下一跳路由设备的 IP 地址。 **权重**：下一跳路由设备所能分到的会话比例。 权重越大，端口所获得的会话就越多。 权重的取值范围为 1 ～ 255，缺省值为 1。 **探测类型**：用于探测 IP 地址的方式，包括 ARP Ping、 Ping、 TCP Ping 和 NS Ping。也可以将探测类型设置为 None，即不进行探测。 None 为缺省的探测类型。 ARP Ping 只用于探测内网的 IPv4 地址； NS Ping 只用于探测 IPv6 地址。 **探测 IPv4 地址 / 探测 IPv6 地址**：所探测的路由设备的 IPv4 或 IPv6 地址。 **探测端口**：使用 TCP 探测时，所探测的路由设备的端口。端口的取值范围为 1 ～ 65535。 **探测周期**：两次链路探测之间的时间间隔，取值范围为 1 ～ 30000 秒，缺省值为 3 秒。 **探测重试次数**：NISG 探测 IP 地址时允许连续失败的最大次数。如果探测失败次数达到了此阈值，但是在探测周期内未得到回复，则认为链路不通。探测重试次数的取值范围为 1 ～ 999 次，缺省值为 3。 您最多可以为一条静态路由配置 8 个负载均衡策略。

5.5.2 单播策略路由参数

表 136 策略路由相关参数说明

参数	说明
序号	表示策略路由策略的优先级。数值越小，优先级越高。如果在创建策略时未指定其序号，那么此策略的优先级将自动变成最小。
名称	名称为策略路由唯一标识。 长度 1 ～ 15 字节， UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & #。
入口接口	用于接收数据包的三层接口。入口接口可以是任意一个可用的三层接口。
TOS	用于定义数据包中的交付服务 （吞吐量、延迟、可靠性及经济成本）。 TOS 的取值范围为 0 ～ 15： 0 表示不要求任何服务。 1 表示要求最低的时延。 2 表示要求最高的吞吐量。 4 表示要求最高的可靠性。 8 表示要求最小的代价。
源 IP 地址	发送数据包的 IP 地址。源 IP 地址可以是以下任意类型： **任意**：包括所有 IPv4 和 IPv6 地址。 **任意 IPv4 地址**：包括所有 IPv4 地址。 **任意 IPv6 地址**：包括所有 IPv6 地址。 **使用下表 —** 包括 IP 地址对象，对象组， IPv4 地址， IPv4 地址段， IPv4 地址及掩码， IPv6 地址， IPv4 地址段， IPv4 地址及前缀。 您最多可以配置 32 个源 IP 地址条目。
服务	数据包使用的传输层服务。服务类型可以是以下任意一种： **任意**：包括所有协议类型。 **使用下表**：包括对象、对象组以及自定义协议。 自定义协议包括 ICMP、 ICMPv6、 TCP、 UDP 和 Other。 当设置 ICMP 协议时，管理员可以选择以下任意类型：ECHO_and_ECHOREPLY，INFO_REQUEST_and_INFO_REPLY， TIMESTAMP_and_TIMESTAMPREPLY，ADDRESS_and_ADDRESSREPLY， ROUTER_ADVERTISEMENT，ROUTER_SOLICITATION，DEST_UNREACH，SOURCE_QUENCH，REDIRECT，TIME_EXCEEDED， PARAMETERPROB 和 Any （表示任意 ICMP 协议类型）。 当设置 ICMPv6 协议时，管理员可以选择以下任意类型：DEST_UNREACH，PACKET_TOO_BIG， TIME_EXCEEDED， PARAMETERPROB，ECHO_and_ECHOREPLY 和 Any （表示任意 ICMPv6 协议类型）。 TCP 和 UDP 协议的目的端口号范围为 1 ～ 65535。其他协议号范围为 1 ～ 255。 您可以最多配置 32 个服务条目。
路由表	策略路由策略所对应的路由表。

5.5.3 三层动态多播 （DVMRP）参数

表 137 DVMRP 参数说明

参数	说明
DVMRP	用于在 NISG 设备上启用或禁用 DVMRP 功能。 DVMRP 缺省为禁用。
启动的 DVMRP 接口	启用 DVMRP 功能的三层接口 （除环回接口和隧道接口）。只有 DVMRP 接口才能参与多播信息的处理与转发。 **接口**：三层接口名称。最多可以选择 32 个 DVMRP 接口。 **阈值**：DVMRP 接口的阈值，用于控制数据包是否能从此接口转发出去。只适用于动态多播路由。 只有当多播数据包的 TTL 值大于接收数据包的 DVMRP 接口的阈值时，数据包才会从接口转发出去。阈值的取值范围为 1 ～ 255，缺省值是 1。 数据包的 TTL 值 （单位为跳数）是指数据包最多可以经过的路由设备数量。当数据包经过一个 DVMRP 路由设备，它的 TTL 值就会减 1。当 TTL 值为 0 时，数据包就会被丢弃。 **Metric**：DVMRP 接口的路由度量值，用于多播路由交换和更新，只适用于动态多播路由。 取值范围是 1 ～ 32，缺省值是 1。
缓存有效时间	动态学习到的多播路由在缓存中的存在时间，必须是 5 的整数倍。取值范围 60 ～ 7200 秒，缺省值是 300 秒。 对于未被使用的动态多播路由，超出该时间后，其信息将从 NISG 删除。
裁剪有效时间	NISG 保持裁剪状态的时间，必须是 5 的整数倍。取值范围是 120 ～ 7200 秒，缺省值是 7200 秒。 超过此时间， NISG 则恢复向下游路由器转发多播数据包。
PIM 邻居发现	如果启用，则 NISG 可以监听 PIM 消息，与运行 PIM 协议的多播路由器建立邻居关系。 此功能缺省为禁用。

5.5.4 三层静态多播参数

表 138 静态多播路由参数说明

参数	说明
源 IP 地址	发送多播数据包的 IP 地址。
多播组 IP 地址	目的多播组的 IP 地址。
入口接口	接收多播数据包的 DVMRP 接口。入口接口不可以与任何转发接口相同。
转发接口	将多播数据包转发出去的 DVMRP 接口。
TTL	控制数据包是否能从 DVMRP 接口转发出去。 TTL 相当于 DVMRP 的阈值，更多信息，参见表 137 DVMRP 参数说明中的 “ 阈值 ”。

5.5.5 二层动态多播参数 （IGMP Snooping）

所有 VLAN 都支持 IGMP Snooping。如果需要在 VLAN 内支持多播并使用 IGMP Snooping 功能，必须启用 IGMP Snooping ； 否则，多播数据包将会被转发给 VLAN 内的所有接口。

表 139 IGMP Snooping 参数说明

参数	说明
VLAN	VLAN 接口名称。 管理员只可以为 VLAN 接口配置 IGMP Snooping 功能。 IGMP Snooping 最多支持 1024 个 VLAN。
状态	用于在 VLAN 内启用或禁用 IGMP Snooping 功能： **开**：启用 IGMP Snooping 功能。 **关**：禁用 IGMP Snooping 功能。 IGMP 缺省为禁用。 启用 IGMP Snooping 后，该功能在 255 秒后生效。
二层接口	VLAN 内包含的二层接口。每个 VLAN 中最多可以包含 32 个接口。
IGMP 版本	VLAN 中二层接口支持的 IGMP 的版本，可以将其设置为： **自动**：接口通过分析接收的报文动态地识别 IGMP 的版本。**自动**为缺省设置。 **v1**：IGMP 版本 1。 NISG 不处理 IGMPv2 独有的报文，如离开组报文。 **v2**：IGMP 版本 2。 NISG 既可以处理 IGMPv2 的报文也可以处理 IGMPv1 的报文。 处于同一个网段的路由设备必须使用相同的 IGMP 版本。
IGMP 模式	与 VLAN 中二层接口连接的网络的类型，可以将其设置为： **自动**：接口通过接收的报文动态地识别网络类型。**自动**为缺省设置。 **多播路由器**：与接口相连的是多播路由器。 **主机**：与接口相连的是主机。

5.5.6 二层静态多播 CAM 条目参数

表 140 多播 CAM 表参数说明

参数	说明
多播组 IP 地址	目的多播组的 IP 地址。
多播组 MAC 地址	目的多播组的 IP 地址所对应的 MAC 地址。系统根据 IP 地址自动计算 MAC 地址。
转发接口	VLAN 中用于转发多播数据包的接口。必须为静态多播 CAM 条目设置至少一个转发口。如果某个出口接口是处于禁用的状态，那么不向此接口转发多播数据包。每个多播 CAM 条目最多支持 32 个转发接口。

6 地址转换

本章介绍 NISG 的地址转换特性并介绍如何在 NISG 上配置地址转换规则。章节结构如下：

- 6.1 地址转换概述，描述 NAT 概念和基本原理。
- 6.2 基本配置步骤，描述基本配置步骤和 UI 对话框信息。实际使用场景不一定会用到所有配置步骤。
- 6.3 范例，描述如何配置不同的 NAT 类型。
- 6.4 配置参数说明，详细描述相关参数。

6.1 地址转换概述

本节介绍 NAT 基本概念。 NAT 规则定义了哪些数据包 IP 地址会被转换以及转换方法。

- 6.1.1 NAT 规则创建和选择描述了 NAT 规则以及如何选择数据包转换规则。
- NISG 提供以下三种 NAT 类型：
  - 6.1.2 SNAT 规则
  - 6.1.3 DNAT 规则
  - 6.1.4 MIP 规则
- 6.1.5 导入 / 导出描述导入导出 NAT 配置。

6.1.1 NAT 规则创建和选择

- 6.1.1.1 规则列表
- 6.1.1.2 规则策略
- 6.1.1.3 规则优先级 （序号）

6.1.1.1 规则列表

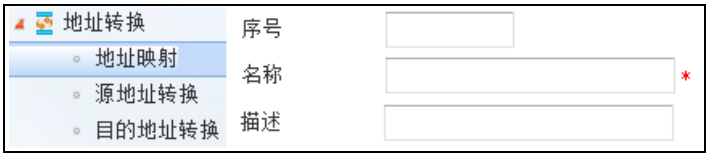
可以创建 SNAT、 DNAT 和 MIP 规则，定义数据包的处理方式。

6.1.1.2 规则策略

可以为 NAT 规则设定策略，根据数据包的参数匹配特定的 NAT 规则 （例如入口接口或源 IP 地址等）。

6.1.1.3 规则优先级 （序号）

序号越小， NAT 规则优先级越高。 MIP 规则的优先级高于 SNAT 和 DNAT 规则。



6.1.2 SNAT 规则

源地址转换 （SNAT）将数据包的源 IP 地址进行转换。 SNAT 主要应用于从被保护的内网访问外网的情况。

- 6.1.2.1 策略和优先级
- 6.1.2.2 NAPT
- 6.1.2.3 保留时间
- 6.1.2.4 一对一
- 6.1.2.5 多对一
- 6.1.2.6 多对多

6.1.2.1 策略和优先级

接收到来自内网的数据包，如果不属于已有会话，不匹配任何 MIP 规则， NISG 会将其与所有 SNAT 规则匹配，并根据与数据包匹配的最高优先级的规则对其进行源 IP 地址转换。所有来自同一会话的后续数据包都会根据此规则进行转换。

SNAT 规则的匹配条件包括：

- 方向
- 目的 IP 地址
- 服务

6.1.2.2 NAPT

网络地址端口转换。不启用 NAPT, 只对地址进行转换，端口号保持不变。启用 NAPT，地址和端口号都会进行转换，转换后端口号不可以手动设置。对于每个转换后的 IP 地址，源端口号从 65534 到 1024 降序分配，循环使用。

- 一对一 SNAT：NAPT 可选。
- 多对一 SNAT：必须启用 NAPT。
- 多对多 SNAT：建议启用 NAPT。

6.1.2.3 保留时间

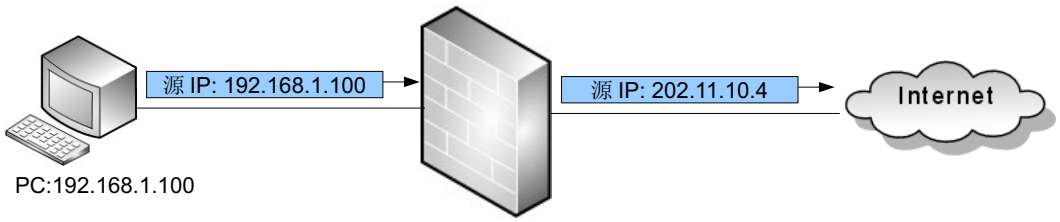
映射关系对应的所有会话都断开后，映射关系保持的时间。

未启用 NAPT 时必须设置保留时间。

6.1.2.4 一对一

将单个源 IP 地址转换为单个 IP 地址或指定接口的 IP 地址。

图 21 一对一 SNAT

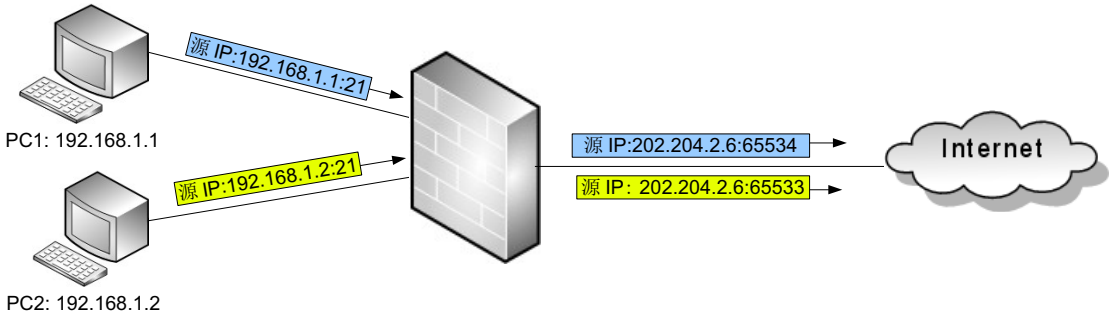


6.1.2.5 多对一

将多个 源 IP 地址转换为单个 IP 地址或指定接口的 IP 地址。

对于 TCP 和 UDP 数据包，此类 SNAT 需开启 NAPT，以实现多个源 IP 地址同时转换。

图 22 多对一源地址转换

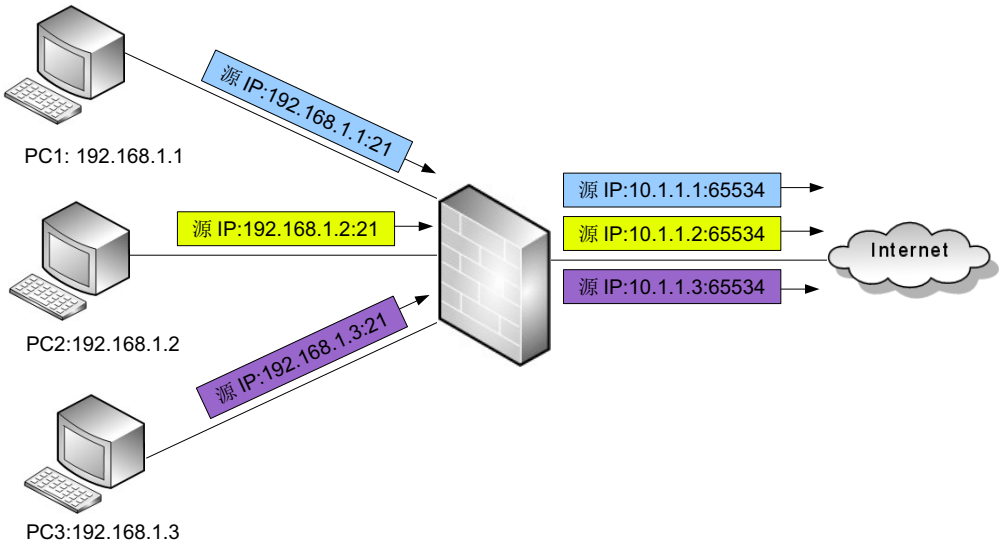


6.1.2.6 多对多

将多个 源 IP 地址转换为多个 IP 地址或指定接口的多个 IP 地址。

对于 TCP 和 UDP 数据包，此类 SNAT 建议开启 NAPT。一个或多个源 IP 地址可以使用同一个转换后 IP 地址，避免转换后 IP 地址分配不足。

图 23 多对多源地址转换



6.1.3 DNAT 规则

目的地址转换 （DNAT）将数据包的目的 IP 地址进行转换。 DNAT 主要应用于从外网访问受保护的内网的情况。

- 6.1.3.1 策略和优先级
- 6.1.3.2 NAPT
- 6.1.3.3 一对一
- 6.1.3.4 一对多
- 6.1.3.5 负载均衡
- 6.1.3.6 链路探测
- 6.1.3.7 域名服务 （DNS 重写）

6.1.3.1 策略和优先级

接收到来自外网的数据包，如果不属于已有会话，不匹配任何 MIP 规则， NISG 会将其与所有 DNAT 规则匹配，并根据与数据包匹配的最高优先级的规则对其进行目的 IP 地址转换。所有来自同一会话的后续数据包都会根据此规则进行转换。

DNAT 规则的匹配条件包括：

- 方向
- 源 IP 地址

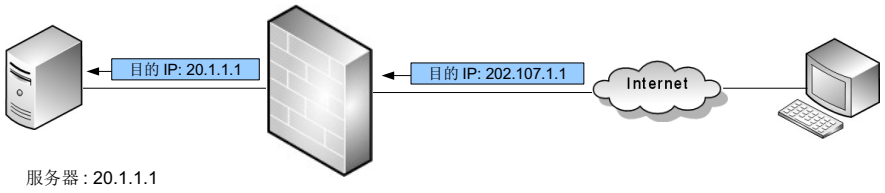
6.1.3.2 NAPT

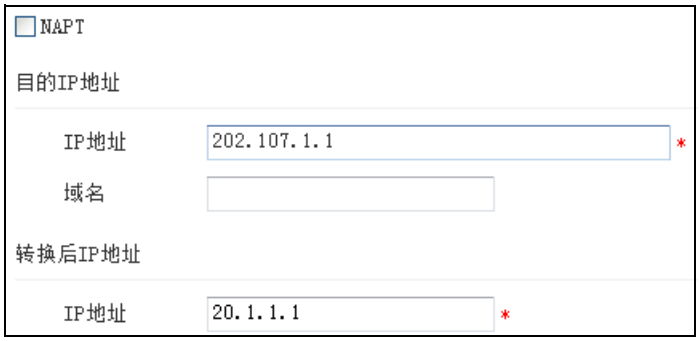
不启用 NAPT, 只对地址进行转换，端口号保持不变。启用 NAPT，地址和端口号都会进行转换，管理员可以手动设置转换后端口号。

- 一对一 DNAT：NAPT 可选。
- 一对多 DNAT：必须启用 NAPT。

6.1.3.3 一对一

将单个目的 IP 地址转换为单个 IP 地址。

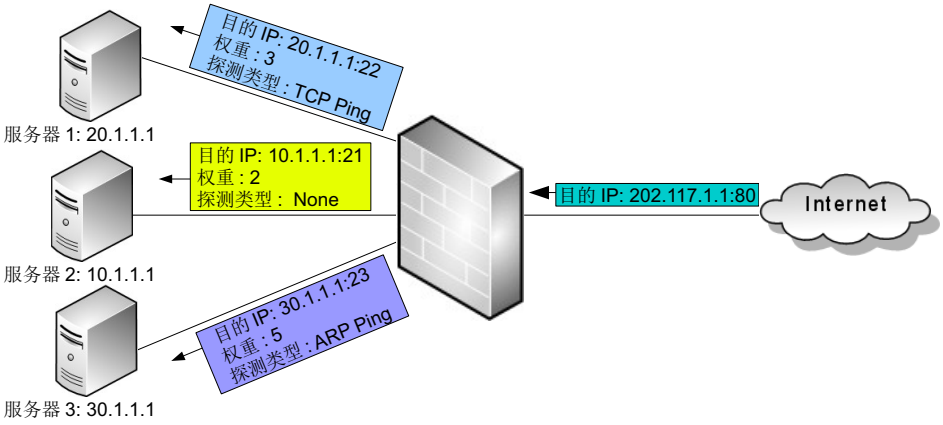


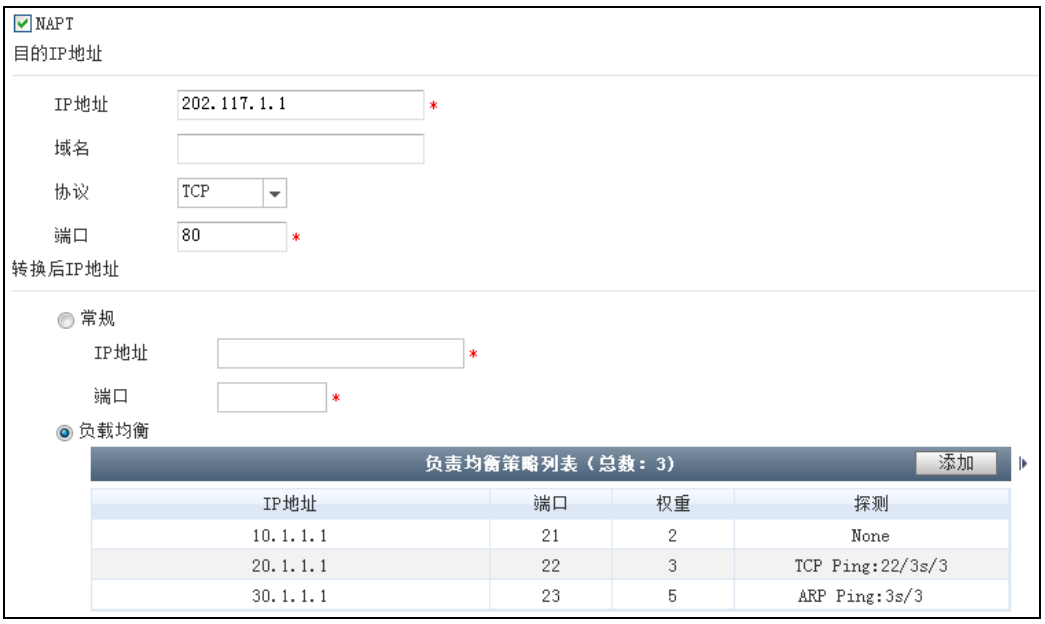


6.1.3.4 一对多

将一个目的 IP 地址转换为多个 IP 地址。

对于 TCP 和 UDP 数据包，此类 DNAT 需开启 NAPT，以实现负载均衡。





6.1.3.5 负载均衡

基于 DNAT 的负载均衡根据服务器的权重分流会话，避免单一服务器负载过重或链路故障导致的服务不可用。

6.1.3.6 链路探测

启用基于 DNAT 的负载均衡后， NISG 通过链路探测确定其与各服务器之间的链路是否畅通。如果与某服务器的链路不通，会话通过其他链路进行，该服务器的权重变为 0。链路恢复后，服务器权重恢复原值。

NISG 支持以下四种链路探测类型：

- ARP 探测
- TCP 探测
- ICMP 探测
- NS 探测

关于链路探测类型的更多信息，请参见 5.1.1.2 负载均衡和链路探测。

6.1.3.7 域名服务 （DNS 重写）

可以在 DNAT 规则中设置要转换的目的 IP 地址对应的域名。设置域名后， NISG 在收到来自 DNS 服务器的数据包后，会将域名对应的数据包的目的 IP 地址与所有 DNAT 规则匹配。如果发现匹配规则， NISG 将把域名对应的外部 IP 地址转换为 DNAT 规则中的内部 IP 地址。

6.1.4 MIP 规则

地址映射 （Mapped IP， MIP）是指一个内网 IP 地址与一个公网 IP 地址的一对一的映射，不涉及端口转换。地址映射具有双向性。

- 6.1.4.1 策略和优先级
- 6.1.4.2 域名服务 （DNS 重写）

6.1.4.1 策略和优先级

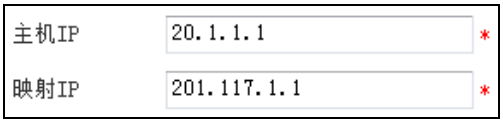
接收到的数据包，如果不属于已有会话， NISG 会将其与所有 MIP 规则匹配，并根据与数据包匹配的最高优先级的规则对其进行地址转换。所有来自同一会话的后续数据包都会根据此规则进行转换。

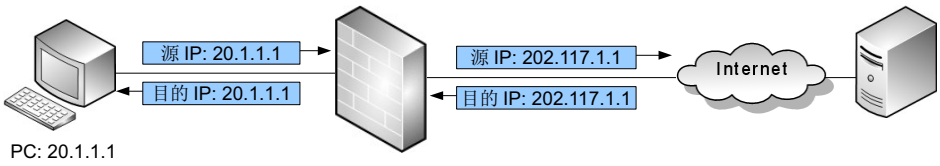
MIP 规则的优先级高于 SNAT 规则和 DNAT 规则。当收到来自内网或外网的新数据包时， NISG 会将数据包与所有启用的 MIP 规则进行匹配，如果没有匹配任何 MIP 规则，NISG 会继续将数据包与 SNAT 规则或 DNAT 规则进行匹配。

MIP 规则的匹配条件包括：

- 方向
- 目的 IP 地址
- 服务

映射关系通过设置主机 IP 地址和映射 IP 实现。





6.1.4.2 域名服务 （DNS 重写）

可以在 MIP 规则中设置要转换的目的 IP 地址对应的域名。设置域名后， NISG 在收到来自 DNS 服务器的数据包后，会将域名对应的数据包的目的 IP 地址与所有 MIP 规则匹配。如果发现匹配规则， NISG 将把域名对应的外部 IP 地址转换为 MIP 规则中的内部 IP 地址。

6.1.5 导入 / 导出

可以导入现有的 NAT 规则或将目前的 NAT 配置导出到文本文档。

6.2 基本配置步骤

本节描述基本配置步骤，在实际应用场景中，您可能只需要进行下面列出的一项或几项配置步骤（请参见 6.3 范例中的场景）。

- 6.2.1 创建 SNAT 规则
- 6.2.2 创建 DNAT 规则
- 6.2.3 创建 MIP 规则

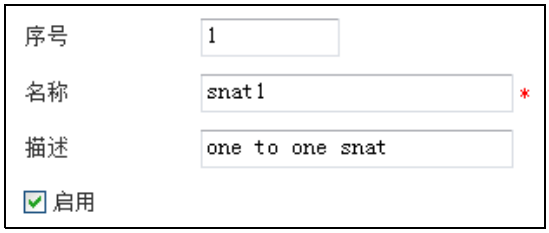
提示：IPv4 和 IPv6 地址不能同时在一条规则中出现。

6.2.1 创建 SNAT 规则

- 6.2.1.1 创建规则
- 6.2.1.2 高级设置
- 6.2.1.3 一对一 SNAT（不启用 NAPT）
- 6.2.1.4 多对一 SNAT（启用 NAPT）
- 6.2.1.5 多对多 SNAT（启用 NAPT）

6.2.1.1 创建规则

1. 选择**网络** > **地址转换** > **源地址转换**。
2. 点击**新建**创建新规则。设置规则名称、描述及序号（优先级），启用或禁用规则。



6.2.1.2 高级设置

在**高级设置**区域，输入数据包匹配的条件。只有所有条件都匹配的数据包才会被转换。

6.2.1.3 一对一 SNAT （不启用 NAPT）

1. 取消勾选 **NAPT**，设置保留时间。

2. 添加源 IP 地址。

3. 添加转换后 IP 或选择任一接口。

6.2.1.4 多对一 SNAT （启用 NAPT）

1. 勾选 **NAPT**。
2. 在**源 IP 地址列表**中添加多个 IP 地址。
3. 从**接口**下拉框中选择一个接口或者添加一个 IP 地址作为转换后 IP 地址。

6.2.1.5 多对多 SNAT （启用 NAPT）

1. 勾选 **NAPT**。
2. 在**源 IP 地址列表**中添加多个 IP 地址。
3. 添加多个 IP 地址作为转换后 IP 地址。

表 141 SNAT 规则命令

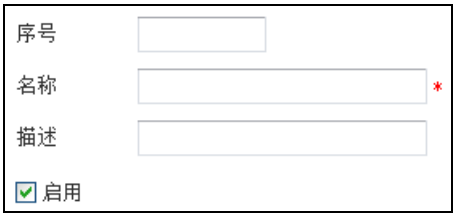
policy snat *policy_name*	添加 SNAT 规则。
policy snat *policy_name* **append**	添加源 / 转换后 IP 地址。
policy snat *policy_name* **description**	添加规则的描述。
policy snat *policy_name* {**enable** | **disable**}	启用或禁用规则。
policy snat *policy_name* **matching**	添加数据包匹配条件。
policy snat *policy_name* **number** *pri*	更改规则优先级。
show policy snat [*policy_name*]	显示规则信息。
unset policy snat [*policy_name*]	删除规则。
unset policy snat *policy_name* **matching**	删除数据包匹配条件。

6.2.2 创建 DNAT 规则

- 6.2.2.1 创建规则
- 6.2.2.2 高级设置
- 6.2.2.3 一对一 DNAT （不启用 NAPT）
- 6.2.2.4 一对一 DNAT （启用 NAPT）
- 6.2.2.5 一对多 DNAT （启用 NAPT）

6.2.2.1 创建规则

1. 选择**网络** > **地址转换** > **目的地址转换**。
2. 点击**新建**创建规则。设置 DNAT 规则名称、描述及序号 （优先级），启用或禁用规则。



6.2.2.2 高级设置

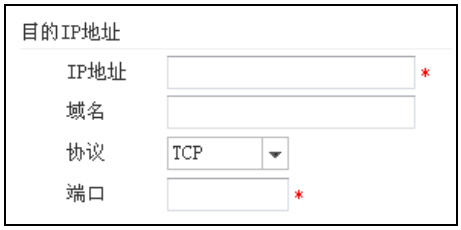
在**高级设置**区域，输入数据包匹配的条件。只有所有条件都匹配的数据包才会被转换。

6.2.2.3 一对一 DNAT （不启用 NAPT）

1. 取消勾选 **NAPT**。
2. 输入目的 IP 地址 （或域名）和转换后 IP 地址。

6.2.2.4 一对一 DNAT （启用 NAPT）

1. 勾选 **NAPT**。
2. 在**目的 IP 地址**区域，添加目的 IP 地址或域名，设置端口号和协议类型。



3. 在**转换后 IP 地址**区域，选择**常规**，输入 IP 地址和对应端口。

6.2.2.5 一对多 DNAT （启用 NAPT）

1. 勾选 **NAPT**。
2. 在**目的 IP 地址**区域，添加目的 IP 地址或域名，设置端口号和协议类型。

在**转换后 IP 地址**区域，选择**负载均衡**，添加负载均衡策略 （IP 地址、端口、权重及探测方式）至列表。

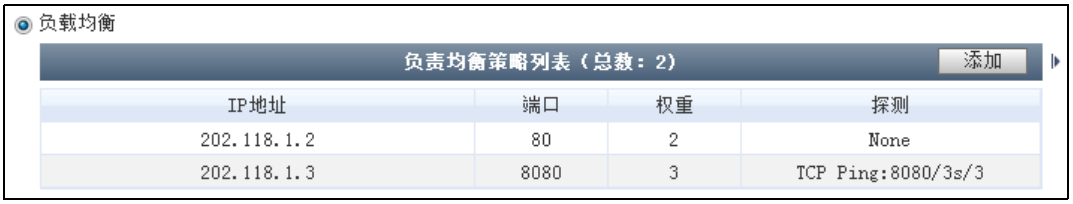


表 142 DNAT 规则命令

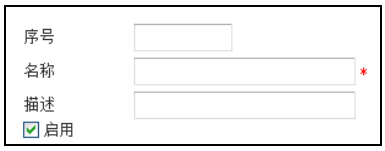
policy dnat *policy_name*	添加 DNAT 规则。
policy dnat *policy_name* **load-balancing**	添加负载均衡规则。
policy dnat *policy_name* **description**	添加规则描述。
policy dnat *policy_name* {**enable** | **disable**}	启用或禁用规则。
policy dnat *policy_name* **matching**	添加数据包匹配条件。
policy dnat *policy_name* **number** *pri*	更改规则优先级。
show policy dnat [*policy_name*]	显示规则信息。
unset policy dnat [*policy_name*]	删除规则。
unset policy dnat *policy_name* **matching**	删除数据包匹配条件。

6.2.3 创建 MIP 规则

- 6.2.3.1 创建规则
- 6.2.3.2 高级设置
- 6.2.3.3 一对一映射

6.2.3.1 创建规则

1. 选择**网络** > **地址转换** > **地址映射**。
2. 点击**新建**创建规则。设置 MIP 规则名称、描述及序号（优先级），启用或禁用规则。



6.2.3.2 高级设置

在**高级设置**区域，输入数据包匹配的条件。只有所有条件都匹配的数据包才会被转换。

6.2.3.3 一对一映射

输入主机 IP 和对应的转换后 IP（或域名）。

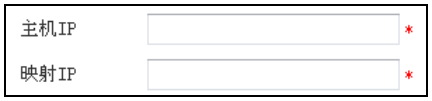


表 143 MIP 规则命令

policy mip *policy_name*	添加 MIP 规则。
policy mip *policy_name* **description**	添加规则描述。
policy mip *policy_name* {**enable** | **disable**}	启用或禁用规则。
policy mip *policy_name* **matching**	添加数据包匹配条件。
policy mip *policy_name* **number** *pri*	更改规则优先级。
show policy mip [*policy_name*]	显示规则信息。
unset policy mip [*policy_name*]	删除规则。
unset policy mip *policy_name* **matching**	删除数据包匹配条件。

6.3 范例

本节包括配置 NAT 规则的如下范例：

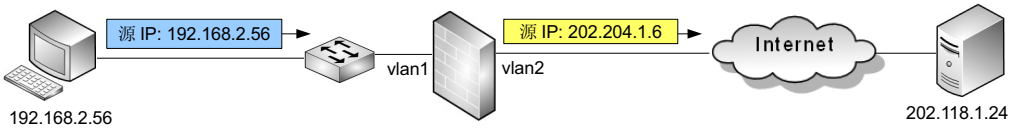
- 范例 1：一对一 SNAT
- 范例 2：多对一 SNAT （启用 NAPT）
- 范例 3：一对一 DNAT
- 范例 4：一对多 DNAT （启用 NAPT）
- 范例 5：MIP
- 范例 6：DNAT 和 DNS 重写

范例 1：一对一 SNAT

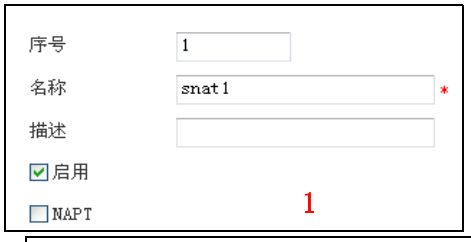
IP 地址为 192.168.2.56 的内部主机通过公网 IP 202.204.1.6 访问 Internet。配置一对一源地址转换规则，对满足以下条件的数据包进行源地址转换：

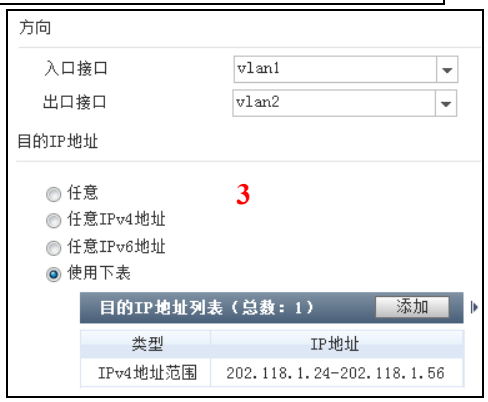
1. 内部主机的目的 IP 地址在 202.118.1.24 ～ 202.118.1.56 之间。
2. 入口接口为 vlan1，出口接口为 vlan2。
3. 内部数据包使用的服务类型为自定义，协议类型为 ICMP 任意。

图 24 一对一源地址转换



1. 选择**网络** > **地址转换** > **源地址转换**。点击**新建**，创建一条 SNAT 规则。





2. 点击**确定**。
3. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy snat snat1 iplist 192.168.2.56 iplist 202.204.1.6 napt enable
NetEye@root-system] policy snat snat1 matching input-interface vlan1
NetEye@root-system] policy snat snat1 matching output-interface vlan2
NetEye@root-system] policy snat snat1 matching dip 202.118.1.24 202.118.1.56
NetEye@root-system] policy snat snat1 matching protocol icmp any
NetEye@root-system] exit
NetEye@root> save config
```

从外网查看源地址转换结果：

Source	Destination	Protocol	Info
202.204.1.6	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	202.204.1.6	ICMP	Echo (ping) reply
202.204.1.6	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	202.204.1.6	ICMP	Echo (ping) reply

从内网查看源地址转换结果：

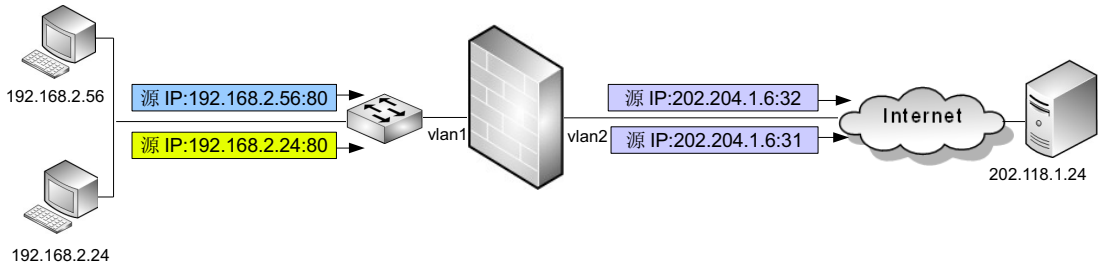
Source	Destination	Protocol	Info
192.168.2.56	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	192.168.2.56	ICMP	Echo (ping) reply
192.168.2.56	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	192.168.2.56	ICMP	Echo (ping) reply

范例 2：多对一 SNAT （启用 NAPT）

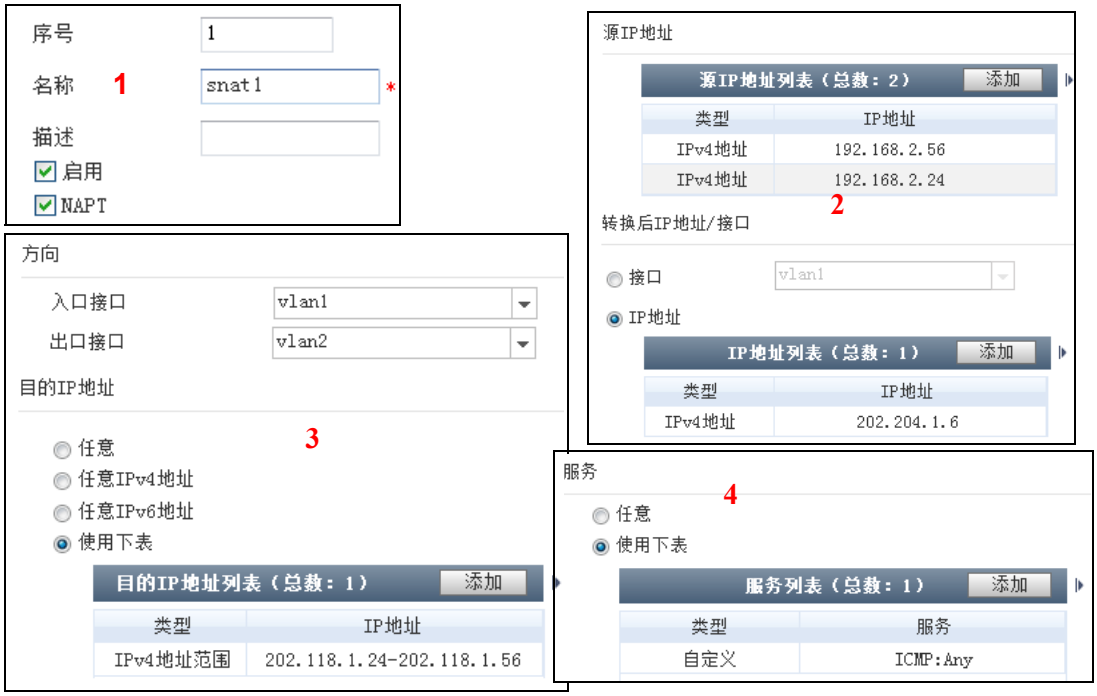
IP 地址分别为 192.168.2.56 和 192.168.2.24 的两台内部主机通过同一公网 IP 202.204.1.6 访问 Internet。配置多对一源地址转换规则，启用 NAPT。对满足规则中以下条件的数据包进行源地址转换：

1. 内部主机的目的 IP 地址在 202.118.1.24 ～ 202.118.1.56 之间。
2. 入口接口为 vlan1，出口接口为 vlan2。
3. 内部数据包使用的服务类型为自定义，协议类型为 ICMP 任意。

图 25 基于端口的多对一源地址转换



1. 选择**网络** > **地址转换** > **源地址转换**。点击**新建**，创建一条 SNAT 规则：



2. 点击**确定**。
3. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy snat snat1 iplist
192.168.2.24,192.168.2.56 iplist 202.204.1.6 napt enable
NetEye@root-system] policy snat snat1 matching input-interface vlan1
NetEye@root-system] policy snat snat1 matching output-interface vlan2
NetEye@root-system] policy snat snat1 matching dip 202.118.1.24
202.118.1.56
NetEye@root-system] policy snat snat1 matching protocol icmp any
NetEye@root-system] exit
NetEye@root> save config
```

从外网查看源地址转换结果：

Source	Destination	Protocol	Info
202.204.1.6	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	202.204.1.6	ICMP	Echo (ping) reply
202.204.1.6	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	202.204.1.6	ICMP	Echo (ping) reply

从内网查看源地址转换结果：

Source	Destination	Protocol	Info
192.168.2.56	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	192.168.2.56	ICMP	Echo (ping) reply
192.168.2.56	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	192.168.2.56	ICMP	Echo (ping) reply

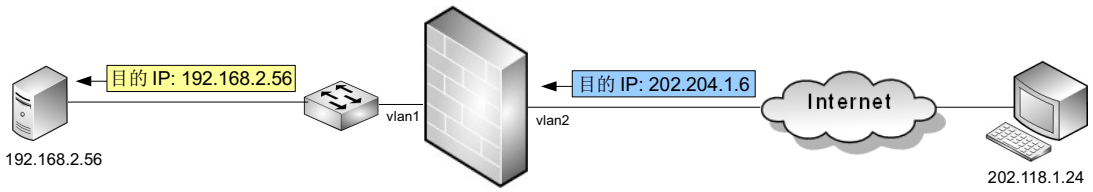
Source	Destination	Protocol	Info
192.168.2.24	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	192.168.2.24	ICMP	Echo (ping) reply
192.168.2.24	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	192.168.2.24	ICMP	Echo (ping) reply

范例 3：一对一 DNAT

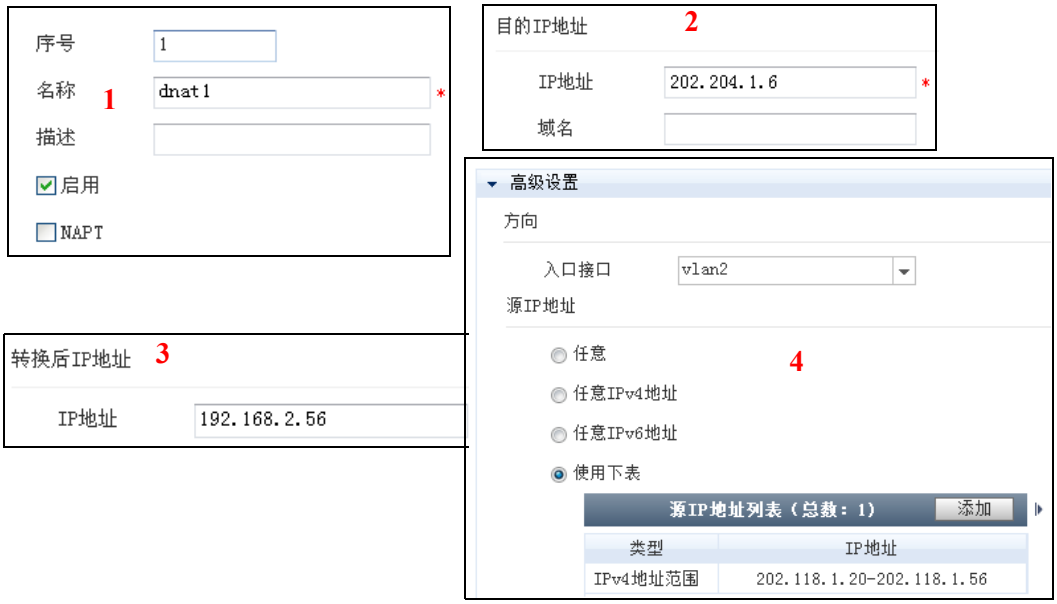
外部主机通过公网 IP 202.204.1.6 来访问内部服务器 192.168.2.56。配置一对一目的地址转换规则，对满足以下条件的数据包进行目的地址转换：

1. 外部主机的源 IP 地址在 202.118.1.20 ～ 202.118.1.56 之间。
2. 入口接口为 vlan2。

图 26 配置目的地址转换规则



1. 选择**网络** > **地址转换** > **目的地址转换**。点击**新建**，创建一条 DNAT 规则：



2. 点击**确定**。
3. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy dnat dnat1 202.204.1.6 192.168.2.56 enable
NetEye@root-system] policy dnat dnat1 matching input-interface vlan2
NetEye@root-system] policy dnat dnat1 matching sip 202.118.1.20
202.118.1.56
NetEye@root-system] exit
NetEye@root> save config
```

从外部主机查看目的地址转换结果：

Source	Destination	Protocol	Info
202.118.1.24	202.204.1.6	ICMP	Echo (ping) request
202.204.1.6	202.118.1.24	ICMP	Echo (ping) reply
202.118.1.24	202.204.1.6	ICMP	Echo (ping) request
202.204.1.6	202.118.1.24	ICMP	Echo (ping) reply

从内网查看目的地址转换结果：

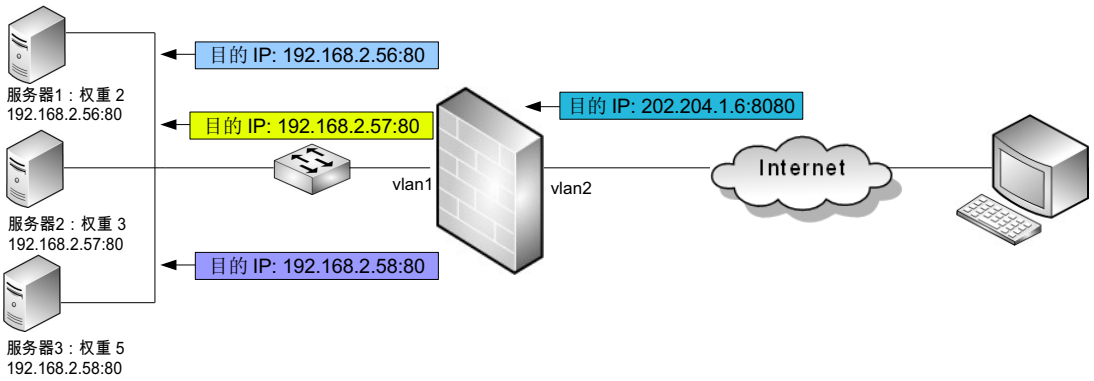
Source	Destination	Protocol	Info
202.118.1.24	192.168.2.56	ICMP	Echo (ping) request
192.168.2.56	202.118.1.24	ICMP	Echo (ping) reply
202.118.1.24	192.168.2.56	ICMP	Echo (ping) request
192.168.2.56	202.118.1.24	ICMP	Echo (ping) reply

范例 4：一对多 DNAT （启用 NAPT）

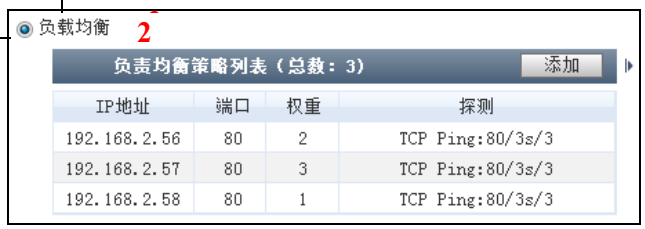
外部主机使用公网 IP 202.204.1.6 访问内网的 Web 服务，内网设有三个 Web 服务器。设置一对多目的地址转换规则，启用 NAPT，使外网流量合理分配给内网服务器。对满足以下条件的数据包进行目的地址转换：

1. 外部主机的源 IP 地址在 202.118.1.20 ～ 202.118.1.56 之间。
2. 入口接口为 vlan2。

图 27 基于目的地址转换的负载均衡



1. 选择**网络** > **地址转换** > **目的地址转换**。点击**新建**，创建一条 DNAT 规则：



2. 点击**确定**。
3. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy dnat dnat2 load-balancing 202.204.1.6 tcp 8080 192.168.2.56 80 2 ip-track tcpping port 80 3 3 enable
NetEye@root-system] policy dnat dnat2 matching load-balancing 192.168.2.57 80 3 ip-track tcpping port 80 3 3
NetEye@root-system] policy dnat dnat2 matching load-balancing 192.168.2.58 80 5 ip-track tcpping port 80 3 3
NetEye@root-system] policy dnat dnat2 matching sip 202.118.1.20 202.118.1.56
NetEye@root-system] policy dnat dnat2 matching input-interface vlan2
NetEye@root-system] exit
NetEye@root> save config
```

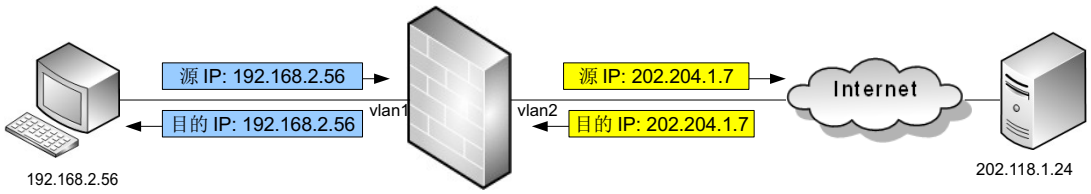
访问 http://202.204.1.6，NISG 根据权重将会话分流至服务器 3，服务器权重变为 2:3:4，再次访问， NISG 继续根据权重将会话分流至服务器 3。当服务器权重变为 2:3:2 后，新的会话将被分流至服务器 2。NISG 根据权重继续分流会话至服务器 1、2、3，服务器权重递减。当服务器权重变为 0:0:0 后， NISG 将根据服务器权重 2:3:5 重新分流会话。

范例 5：MIP

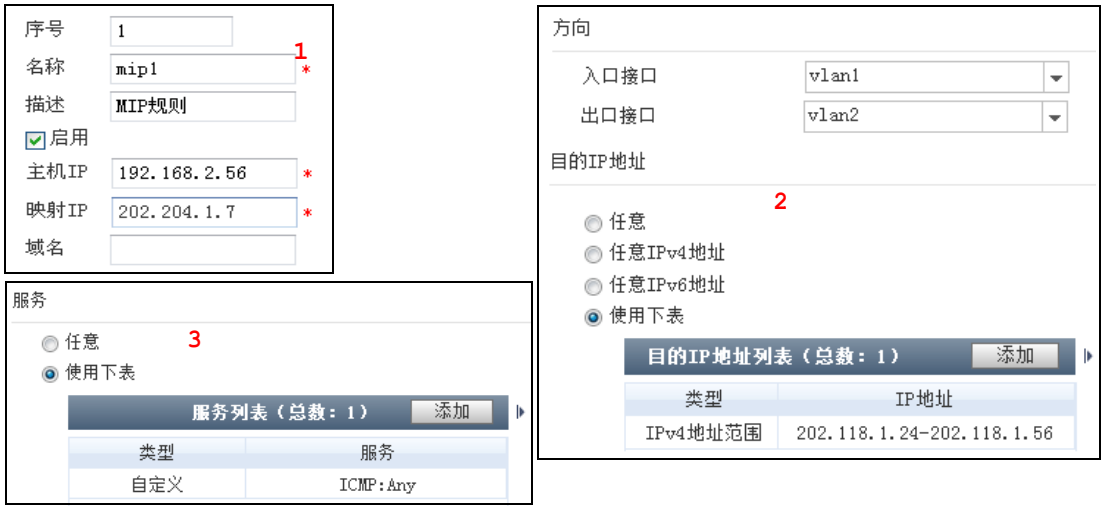
在本范例中，

1. 当内网主机向外网服务器发送数据包时，NISG将数据包的源IP地址192.168.2.56转换为202.204.1.7。
2. 当外网服务器回应内网主机时， NISG 将数据包的目的 IP 地址 202.204.1.7 转换为 192.168.2.56。

图 28 配置地址映射规则



1. 选择**网络** > **地址转换** > **地址映射**。点击**新建**，创建一条 MIP 规则：



2. 点击**确定**。
3. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy mip mip1 192.168.2.56 202.204.1.7 enable
NetEye@root-system] policy mip mip1 matching input-interface vlan1
NetEye@root-system] policy mip mip1 matching output-interface vlan2
NetEye@root-system] policy mip mip1 matching dip 202.118.1.24
202.118.1.56
NetEye@root-system] policy mip mip1 matching protocol icmp any
NetEye@root-system] exit
NetEye@root> save config
```

当内网主机向外网发送数据包时，从内网查看地址映射结果：

Source	Destination	Protocol	Info
192.168.2.56	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	192.168.2.56	ICMP	Echo (ping) reply
192.168.2.56	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	192.168.2.56	ICMP	Echo (ping) reply

从外网查看地址映射结果：

Source	Destination	Protocol	Info
202.204.1.7	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	202.204.1.7	ICMP	Echo (ping) reply
202.204.1.7	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	202.204.1.7	ICMP	Echo (ping) reply

当外网服务器回应时，从内网查看地址映射结果：

Source	Destination	Protocol	Info
202.118.1.24	192.168.2.56	ICMP	Echo (ping) request
192.168.2.56	202.118.1.24	ICMP	Echo (ping) reply
202.118.1.24	192.168.2.56	ICMP	Echo (ping) request
192.168.2.56	202.118.1.24	ICMP	Echo (ping) reply

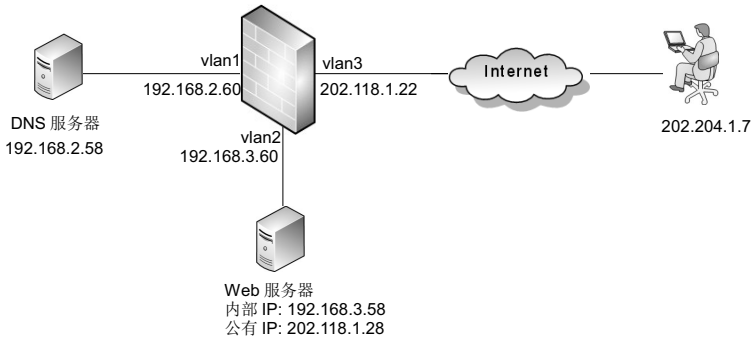
从外网查看地址映射结果：

Source	Destination	Protocol	Info
202.118.1.24	202.204.1.7	ICMP	Echo (ping) request
202.204.1.7	202.118.1.24	ICMP	Echo (ping) reply
202.118.1.24	202.204.1.7	ICMP	Echo (ping) request
202.204.1.7	202.118.1.24	ICMP	Echo (ping) reply

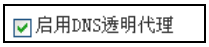
范例 6：DNAT 和 DNS 重写

用户向 DNS 服务器发起请求， DNS 服务器应答指明域名 www.test.com 对应 IP 地址 202.118.1.28， NISG 收到 DNS 应答后，根据配置的 DNAT 策略将 202.118.1.28 转换成内网 Web 服务器的 IP 地址 192.168.3.58，用户访问 Web 服务器。

图 29 DNAT 中的 DNS 重写

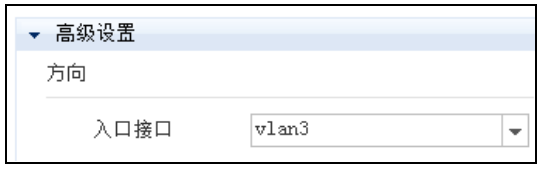


1. 选择**防火墙** > **访问策略**。创建全通访问策略 policy1 并选择**启用 DNS 透明代理**。



2. 选择**网络** > **DNS** > **DNS 代理**。点击**新建**设置 DNS 代理。

3. 选择**网络** > **地址转换** > **目的地址转换**。点击**新建**创建 DNAT 规则。



4. 点击**确定**。
5. 点击 。

CLI

```
NetEye@root> configure mode
NetEye@root-system] policy access policy1 any any any any any any
permit enable
NetEye@root-system] policy access policy1 dns-proxy enable
NetEye@root-system] dns server-select www.test.com output-interface
any primary 192.168.3.58
NetEye@root-system] policy dnat dnat1 202.118.1.28 domain
www.test.com 192.168.3.58 enable
NetEye@root-system] policy dnat dnat1 matching input-interface vlan3
NetEye@root-system] exit
NetEye@root> save config
```

6.4 配置参数说明

- 6.4.1 源地址转换规则参数
- 6.4.2 目的地址转换规则参数
- 6.4.3 地址映射规则参数

6.4.1 源地址转换规则参数

表 144 源地址转换规则配置信息

参数	说明
序号	设定源地址转换规则的优先级，取值范围为 1-80000。序号越小，优先级越高。 如果在创建规则时未指定其序号，那么此规则将获得最大序号，优先级最低。
名称	源地址转换规则名称。长度 1-63 字节， UTF-8 字符。不能包含以下字符：? , " ' \ < > & # 和空格。 同一个虚拟系统内的 SNAT 规则名称不能相同。
描述	源地址转换规则描述信息。长度 0-255 个字节。 UTF-8 字符。不能包含以下字符：? " ' \ < > &
启用	用于启用或禁用源地址转换规则。源地址转换规则缺省为启用，启用后才进行匹配。
NAPT	用于启用或禁用网络地址端口转换功能。 NAPT 缺省为启用。
保留时间	指映射关系对应的所有会话都断开后，映射关系保持的时间。 取值范围为 30-99999999 秒。
源 IP 地址	数据包发出的源 IP 地址。 管理员最多可以配置 32 个源 IP 地址条目。
转换后 IP 地址 / 接口	数据包经过源地址转换后的 IP 地址，可以是以下任一类型： • 接口：系统任一三层接口，此接口的 IP 地址将被用作转换后 IP 地址。 • IP 地址：IPv4 或 IPv6 地址。 管理员最多可以配置 8 个转换后 IP 地址条目。
高级设置	用于设置匹配数据包的条件。当数据包匹配所有的条件时， NISG 会根据指定的源地址规则对其进行源地址转换。匹配条件包括： • 方向：包括 NISG 接收数据包的入口接口和转发数据包的出口接口。 • 目的 IP 地址：NISG 转发数据包的目的 IPv4 或 IPv6 地址。 管理员最多可以配置 32 个目的 IP 地址条目。 • 服务：数据包使用的传输层服务，可以是对象、对象组以及自定义协议 (ICMP、ICMPv6、 TCP、 UDP 和 Other)。 管理员最多可以配置 32 个服务条目。

6.4.2 目的地址转换规则参数

表 145 目的地址转换规则配置信息

参数	说明
序号	设定目的地址转换规则的优先级。取值范围为 1-80000。数值越小，优先级越高。 如果在创建规则时未指定其序号，那么此规则将获得最大序号，优先级最低。
名称	目的地址转换规则名称。长度 1-63 字节， UTF-8 字符。不能包含以下字符：? , " ' \ < > & # 和空格。 同一个虚拟系统内的 DNAT 规则名称不能相同。
描述	目的地址转换规则描述信息。长度 0-255 个字节。 UTF-8 字符。不能包含以下字符：? " ' \ < > &
启用	用于启用或禁用目的地址转换规则。目的地址转换规则缺省为启用，启用后才进行匹配。
NAPT	用于启用或禁用网络地址端口转换功能。 NAPT 缺省为启用。
目的 IP 地址	数据包初始要到达的 IP 地址。 管理员可以配置以下参数： • IP 地址：数据包要到达的初始 IPv4 或 IPv6 地址。 • 域名：与初始目的 IP 地址相对应的域名。域名长度为 2-255 字节。 • 协议：数据包使用的协议，有 TCP 和 UDP 两种。缺省为 TCP。 如果启用了网络地址端口转换，则必须设置此项。 • 端口：进行端口转换之前的原始目的端口。 如果启用了网络地址端口转换，则必须设置此项。 目的端口号的范围为 1-65535。
转换后 IP 地址	用于设置一个或多个转换后 IP 地址。可设置为以下任一类型： • 常规：设置一个转换后 IPv4 或 IPv6 地址及端口。 • 负载均衡：设置有多个转换后 IP 的负载均衡策略。
负载均衡	管理员需设置以下负载均衡和链路探测参数： • 转换后目的 IP 地址及端口 • 权重：服务器所能分到的会话比例。取值范围为 1-255，缺省值为 1。 • 探测类型：包括 ARP Ping、 TCP Ping、 ICMP Ping、 NS Ping 和 None。 None 为缺省探测类型。 • 探测端口：使用 TCP Ping 时，所探测的服务器的端口。端口的取值范围为 1-65535。 • 探测周期：两次链路探测之间的时间间隔，取值范围为 1-30000 秒，缺省值为 3 秒。 • 探测重试次数：NISG 探测 IP 地址时允许连续失败的最大次数。如果探测失败次数达到了此阈值，但是在探测周期内未得到回复，则认为链路不通。探测重试次数的取值范围为 1-999 次，缺省值为 3 次。 管理员最多可以为一条目的地址转换规则配置 8 个负载均衡策略。
高级设置	用于设置数据包匹配的条件。当数据包匹配所有的条件时， NISG 会根据指定的目的地址转换规则对其进行目的地址转换。匹配条件包括： • 方向：NISG 接收数据包的入口接口。 • 源 IP 地址：发送数据包的 IPv4 或 IPv6 地址。 管理员最多可以配置 32 个源 IP 地址条目。
描述	目的地址转换规则描述信息。长度 0-255 个字节。 UTF-8 字符。不能包含以下字符：? " ' \ < > &

6.4.3 地址映射规则参数

表 146 地址映射规则配置信息

参数	说明
序号	设置地址映射规则的优先级。取值范围为 1 ～ 80000。数值越小，优先级越高。 如果在创建规则时未指定其序号，那么此规则的序号将自动变成最大。
名称	地址映射规则名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & # 同一个虚拟系统内的 MIP 规则名称不能相同。
描述	地址映射规则的描述信息。长度 0 ～ 255 个字节。 UTF-8 字符。不能包含以下字符：? " ' \ < > &
启用	用于启用或禁用地址映射规则。地址映射规则的状态缺省为启用，启用后才进行匹配。
主机 IP	内网主机的私有 IPv4 或 IPv6 地址。 当数据包从内部网络发起且目的是外部网络时，主机 IP 地址是数据包的源 IP 地址。当数据包从外部网络发起且目的是内部网络时，主机 IP 地址是数据包经过地址转换后的目的 IP 地址。
映射 IP	与内网主机的私有 IPv4 或 IPv6 地址相对应的公网 IPv4 或 IPv6 地址。 当数据包从内部网络发起且目的是外部网络时，映射 IP 地址是数据包经过地址转换后的源 IP 地址。当数据包从外部网络发起且目的是内部网络时，映射 IP 地址是数据包的初始目的 IP 地址。
域名	与映射 IP 地址相对应的域名，长度为 2 ～ 255 字节。 当需要应用 DNS 重写时，管理员可以输入域名。
高级设置	用于设置匹配数据包的条件。当数据包匹配地址映射规则中的所有条件时， NISG 会根据规则对其进行地址转换。匹配条件包括： • 方向：包括入口接口和出口接口。 当数据包从内部网络发起且目的是外部网络时，入口接口是接收数据包的接口。当数据包从外部网络发起且目的是内部网络时，入口接口是转发数据包的接口。 当数据包从内部网络发起且目的是外部网络时，出口接口是转发数据包的接口。当数据包从外部网络发起且目的是内部网络时，出口接口是接收数据包的接口。 • 目的 IP 地址：当会话从内部网络发起且目的是外部网络时，目的 IP 地址是数据包要到达的 IP 地址。当会话从外部网络发起且目的是内部网络时，目的 IP 地址是发送数据包的 IP 地址。 可以是 IP 地址对象或对象组、 IPv4 或 IPv6 地址、 IPv4 或 IPv6 地址范围、 IPv4 地址 / 掩码或 IPv6 地址 / 前缀。 管理员最多可以配置 32 个目的 IP 地址条目。 • 服务：数据包使用的传输层服务，可以是对象、对象组以及自定义协议。自定义协议包括 ICMP、 ICMPv6、 TCP、 UDP 和 Other。TCP 和 UDP 协议的目的端口号范围为 1 ～ 65535。其它协议号范围为 1 ～ 255。 管理员最多可以配置 32 个服务条目。

7 服务质量

本章介绍服务质量 （Quality of Service， QoS）的功能特性，包含以下内容：

- 7.1. 基本概念，描述 QoS 的相关概念和基本原理。
- 7.2. 基本配置步骤，描述基本配置步骤和 WebUI 截图。客户场景可能不需要配置所有步骤。
- 7.3. 范例，给出详细的范例配置步骤。
- 7.4. 配置参数说明，详细描述 QoS 配置参数。

7.1. 基本概念

QoS 指网络带宽有限的情况下，为指定网络流量提供更优服务的一种能力。本节介绍 QoS 相关的一些基本概念：

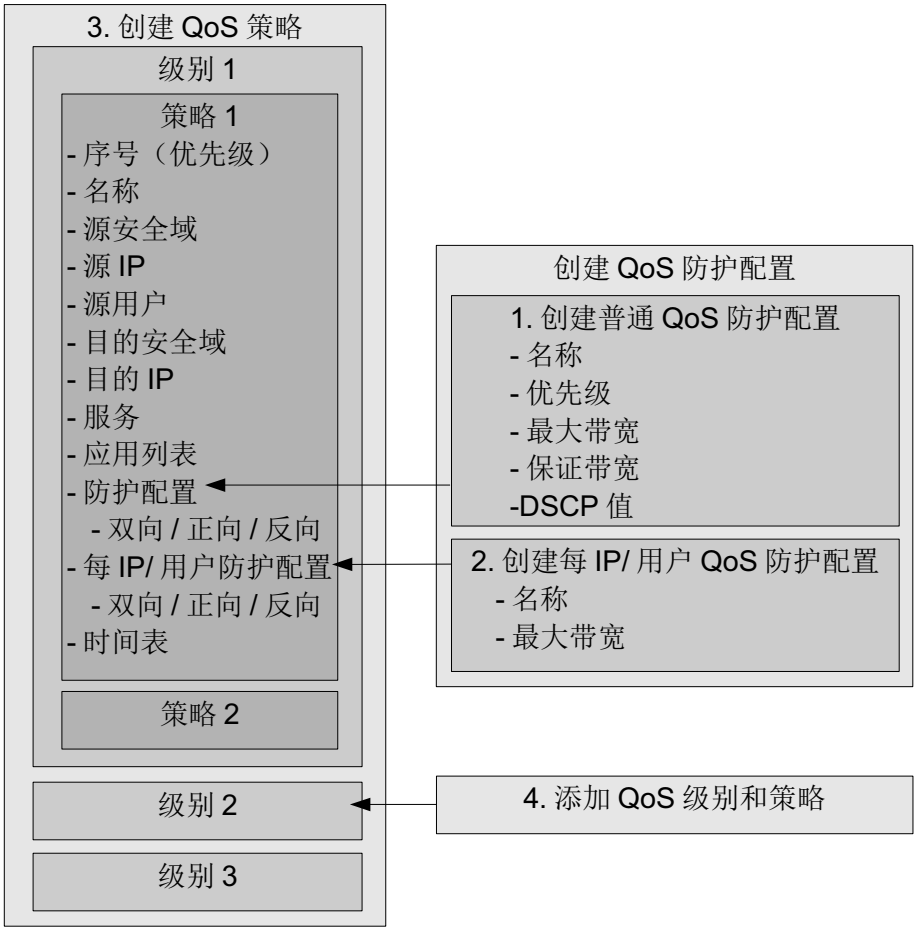
- **策略序号**：QoS 策略的优先级。
- **匹配条件**包括：
  - 源安全域 /IP
  - 目的安全域 /IP
  - 源用户
  - 服务
  - 应用列表
- **普通 QoS 防护配置**：指定所有 IP/ 用户流量的最大带宽、保证带宽、优先级和 DSCP 值。
- **每 IP/ 用户 QoS 防护配置**：指定每 IP/ 用户流量可占用的最大带宽。
- **时间表**：QoS 策略的生效时间。
- **多级 QoS**: 用于从不同维度指定多条策略的串联的 QoS 模块。数据流依次通过每一级 QoS 带宽控制。

7.2. 基本配置步骤

本节包含以下内容：

- 7.2.1 创建普通 QoS 防护配置
- 7.2.2 创建每 IP/ 用户 QoS 防护配置
- 7.2.3 创建 QoS 策略

图 30 QoS 配置步骤



提示：QoS 只能通过 WebUI 进行配置。

7.2.1 创建普通 QoS 防护配置

1. 选择 **UTM>QoS>QoS 防护配置**。
2. 点击**新建**，创建普通 QoS 防护配置。

3. 点击**确定**。

4. 点击 克隆 QoS 防护配置。点击 查看引用该防护配置的策略。

7.2.2 创建每 IP/ 用户 QoS 防护配置

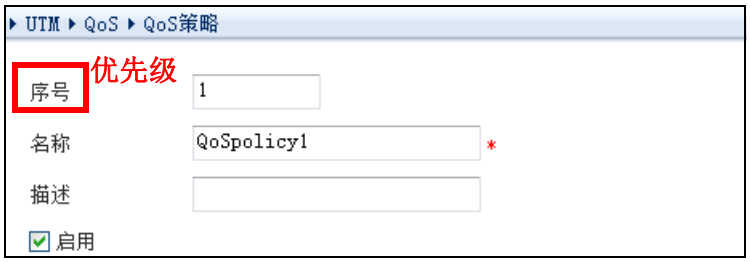
1. 选择 **UTM>QoS> 每 IP/ 用户 QoS 防护配置**。
2. 点击**新建**，创建每 IP/ 用户 QoS 防护配置。

3. 点击**确定**。

4. 点击 克隆 QoS 防护配置。点击 查看引用该防护配置的策略。

7.2.3 创建 QoS 策略

1. 选择 **UTM>QoS>QoS 策略**。
2. 点击**新建**，创建 QoS 策略。
   a. 设置策略优先级、名称和启用状态：



   b. 设置源安全域、源 IP 和源用户：

c. 设置目的安全域和目的 IP：

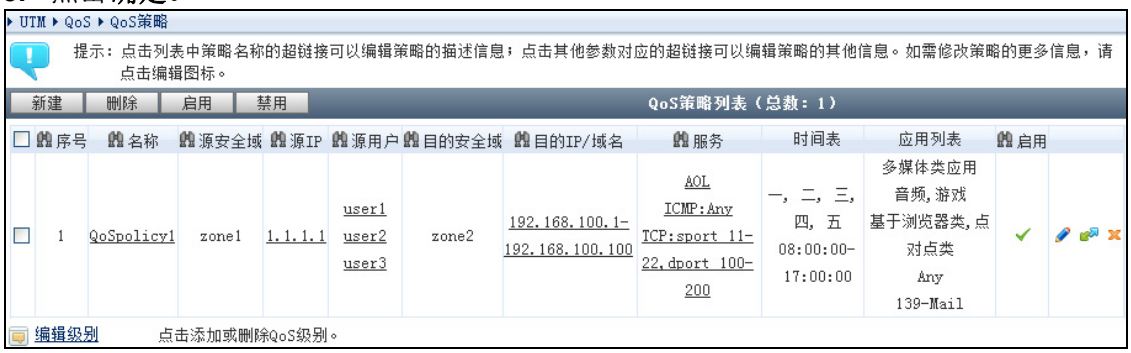
d. 设置服务和应用。关于如何添加应用到应用列表，请参见 10.2.1.2.3. 创建应用控制防护配置 （2c）。

e. 指定普通 QoS 防护配置和每 IP/ 用户 QoS 防护配置：

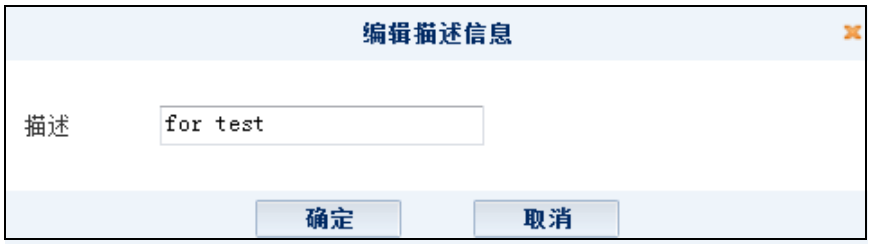
f. 指定：

g. 设置策略生效时间：

3. 点击**确定**。

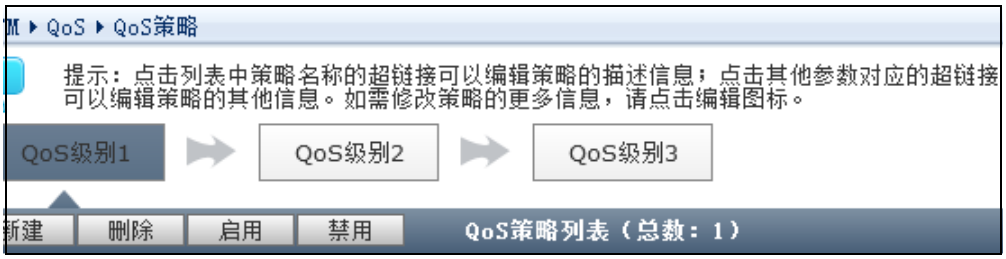


- 点击 移动策略位置以改变其优先级（同级别内的优先级）。
- 点击 设置查找 QoS 策略的筛选条件。
- 点击策略名称链接编辑策略的描述信息：



- 点击对应的链接编辑以下参数信息：源 IP、源用户、目的 IP/ 域名、服务。

4. 要配置多级 QoS，点击**编辑级别**，添加 QoS 级别和相应用级别的 QoS 策略。

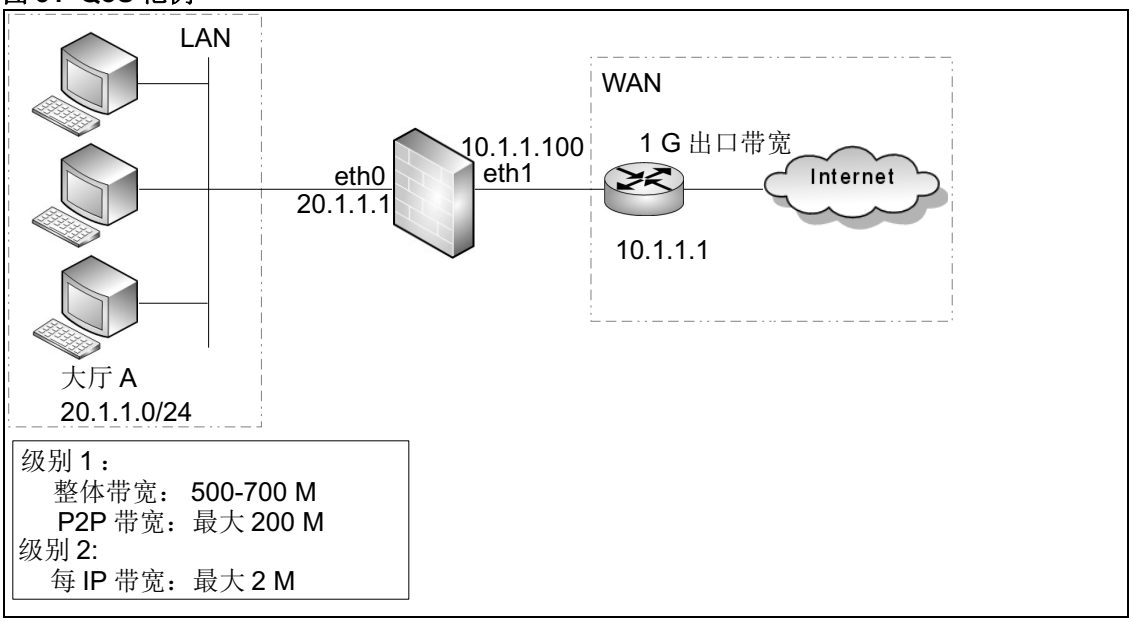


7.3. 范例

如下图所示，某部门大厅 A 的员工为开发团队，对 P2P 应用流量的需求较小。该部门网络管理员希望：

- 保证大厅 A 的整体上网带宽 （IP 流量）在 500-700M ；
- 限制 P2P 流量不超过 200M，以免影响其他大厅 P2P 流量带宽；
- 每位员工上网流量不超过 2M （每位员工仅分配一个 IP）。

图 31 QoS 范例



配置步骤包括：

- 7.3.1. 创建普通 QoS 防护配置 （最大带宽 / 保证带宽）
- 7.3.2. 创建每 IP QoS 防护配置 （最大带宽）
- 7.3.3. 编辑 QoS 级别
- 7.3.4. 创建多级 QoS 策略

7.3.1. 创建普通 QoS 防护配置 （最大带宽 / 保证带宽）

1. 选择 **UTM>QoS>QoS 防护配置**。
2. 点击**新建**，为大厅 A 创建 QoS 防护配置 qosprofile1：

3. 点击**确定**。
4. 点击**新建**，为大厅 A 创建 QoS 防护配置 qosprofile2。**最大带宽**：204800 Kbps (200M)。
5. 点击 。

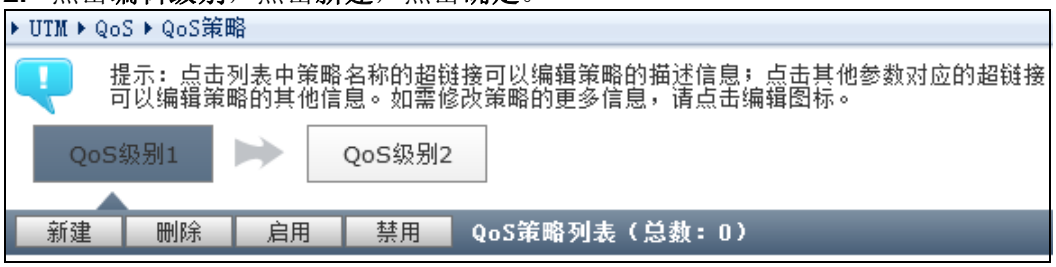
7.3.2. 创建每 IP QoS 防护配置 （最大带宽）

1. 选择 **UTM>QoS> 每 IP/ 用户防护配置**。
2. 创建每 IP QoS 防护配置 peripprofile1：

3. 点击**确定**。点击 。

7.3.3. 编辑 QoS 级别

1. 选择 **UTM>QoS>QoS 防护配置**。
2. 点击**编辑级别**，点击**新建**，点击**确定**。



7.3.4. 创建多级 QoS 策略

1. 选择 **UTM>QoS>QoS 策略**。
2. 点击 **QoS 级别 1**，为大厅 A 创建 QoS 策略 lev1p1forA：

3. 点击**确定**。
4. 选择 **QoS 级别 2**，点击**新建**，创建 QoS 策略 lev2p1forA：
   - **源安全域**：zone2
   - **目的全域**：zone1
   - **双向 QoS 防护配置**：qosprofile2
5. 点击**确定**。点击 。

7.4. 配置参数说明

本节介绍以下内容的配置参数：

- 7.4.1. QoS 策略
- 7.4.2. QoS 防护配置
- 7.4.3. 每 IP/ 用户 QoS 防护配置

7.4.1. QoS 策略

表 147 QoS 策略参数

参数	描述
序号	QoS 策略的优先级，序号越小，优先级越高。取值范围为 1-80000。
名称	QoS 策略的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?,"'\<>&#
源安全域	QoS 策略要控制的数据包的发起安全域，缺省为**任意**。
源 IP	每条 QoS 策略支持 4096 个源 IP 地址或地址段。
源用户	类型包括： • **任意**：包括已进行身份认证和未进行身份认证的所有用户。缺省为**任意**。 • **任意认证用户**：包括已进行身份认证的所有用户。 • **使用下表**：可以选择包括未在 NISG 上创建的、外部认证服务器上的用户。 每条 QoS 策略支持 4096 个源用户。
目的安全域	QoS 策略要控制的数据包发往的安全域，缺省为**任意**。
目的 IP/ 域名	每条 QoS 策略支持 4096 个目的 IP 地址、地址段或域名。
服务	QoS 策略要控制的数据包的源和目的端口。 管理员最多可添加 32 条服务 （4096 个端口号），协议列表内不允许出现重复的条目。
应用列表	QoS 策略要控制的数据包所属应用的类型。 管理员可通过选择应用名称或过滤条件添加应用。
时间表	QoS 策略的生效时间。管理员可以选择设置周期性或一次性时间表。 如果当前访问策略未设置时间表，并且其状态为启用，则表示它在任何时间内都生效。
启用	QoS 策略缺省为启用。
描述	QoS 策略的描述信息。长度 0~255 字节， UTF-8 字符。不能包含以下字符：?"' \<>&

表 147 QoS 策略参数 (*续*)

参数	描述
（普通）防护配置	QoS 策略引用的普通 QoS 防护配置。 QoS 策略通过指定普通 QoS 防护配置定义整体流量的保证带宽、最大带宽、优先级和 DSCP 值。 QoS 策略中可以指定双向和单向两种 QoS 防护配置： • **双向 QoS 防护配置**：对双向的流量进行带宽控制。 • **正向 QoS 防护配置**：对从源到目的的流量进行带宽控制。仅当管理员勾选**反向 QoS 防护配置**时可见。 • **反向 QoS 防护配置**：对反向流量进行控制。 一个 QoS 防护配置可以被多条策略引用。
每 IP/ 用户防护配置	QoS 策略引用的每 IP/ 用户 QoS 防护配置。 QoS 策略通过指定每 IP/ 用户 QoS 防护配置定义每 IP 或每用户流量的最大带宽。 QoS 策略中可以为每 IP/ 用户 QoS 防护配置指定以下内容： • **防护配置类型**：包括**每 IP** 和**每用户**。 • **双向每 IP/ 用户 QoS 防护配置**：对双向的流量进行每 IP/ 用户带宽控制。 • **正向每 IP/ 用户 QoS 防护配置**：对从源到目的的流量进行每 IP/ 用户带宽控制。仅当管理员勾选**反向每 IP/ 用户 QoS 防护配置**时可见。 • **反向每 IP/ 用户 QoS 防护配置**：对反向流量进行每 IP/ 用户带宽控制。

7.4.2. QoS 防护配置

表 148 （普通） QoS 防护配置参数

参数	描述
名称	普通 QoS 防护配置的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?,"'\ < > & #
引用	点击 查看引用该普通 QoS 防护配置的 QoS 策略。 一个普通 QoS 防护配置可以被多个 QoS 策略引用，被引用的防护配置不能被删除。
优先级	指定流量的转发优先权级别。 当实际产生的带宽总和达到策略允许的最大带宽或达到系统处理能力上限时，优先级高的流量将被优先转发。 优先级分为保证带宽和未保证带宽的优先级，保证带宽的优先级整体高于未保证带宽的优先级。保证带宽的优先级分为高、中、低三个等级，未保证带宽的优先级也分为高、中、低三个等级，保证带宽的低优先级也高于未保证带宽的高优先级。
最大带宽	最大可使用带宽。 指定服务占用的流量不能超过此限制。如果此阈值大于系统吞吐量， NISG 会尽最大努力转发流量。
保证带宽	NISG 保证定义的流量能够享受到对应的带宽。保证带宽必须小于等于最大带宽。
DSCP	对流经 NISG 的数据包添加的标记，表示数据包在后续的网络设备上需要继续进行流量控制。关于差分服务代码点 （Differentiated Services Code Point， DSCP）的详细信息，请参见 RFC 2474。

7.4.3. 每 IP/ 用户 QoS 防护配置

表 149 每 IP/ 用户 QoS 防护配置参数

参数	描述
名称	每 IP/ 用户 QoS 防护配置的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?,"'\<>&#
引用	点击 查看引用当前每 IP/ 用户 QoS 防护配置的 QoS 策略。 一个每 IP/ 用户 QoS 防护配置可以被多个 QoS 策略引用，被引用的防护配置不能被删除。
最大带宽	每 IP 或用户可以使用的最大带宽。

8 策略

策略用于对流经 NISG 的数据包实施访问控制。NISG 访问控制的主要原则是“禁止未经许可的访问”。本章内容包括：

- 8.1 概述，介绍 NISG 策略的概念和原理。
- 8.2 基本配置，介绍策略的基本配置步骤和 UI。
- 8.3 范例，描述如何配置 IP-MAC 绑定策略、访问策略、多播策略和会话策略。
- 8.4 配置参数说明，详细介绍 NISG 策略的各项配置参数。

8.1 概述

本节介绍 NISG 的策略特性，章节结构如下所示：

- 8.1.1 IP-MAC 绑定
- 8.1.2 访问策略
- 8.1.3 缺省访问策略
- 8.1.4 多播策略
- 8.1.5 会话策略

8.1.1 IP-MAC 绑定

NISG 的 IP-MAC 地址绑定特性能够将主机的 IP 地址及其网卡的 MAC 地址绑定到一起。由于 MAC 地址的唯一性， IP-MAC 绑定可以防止非法主机冒用合法主机的 IP 地址。本节包括：

- 8.1.1.1 IP-MAC 地址绑定策略
- 8.1.1.2 IP-MAC 绑定策略包处理流程

8.1.1.1 IP-MAC 地址绑定策略

在缺省情况下， NISG 不对数据包的源 IP 地址与 MAC 地址是否匹配进行检查。管理员可以将源 IPv4 或 IPv6 地址与 MAC 地址进行绑定。 NISG 将根据 IP-MAC 地址绑定策略中定义的绑定关系，验证数据包是否来自合法的 MAC 地址。

8.1.1.2 IP-MAC 绑定策略包处理流程

当 NISG 接收到 IP 数据包时，将根据其源 IP 地址和源 MAC 地址查询所有已启用的 IP-MAC 地址绑定策略。匹配流程如下：

- 如果数据包的源IP与IP-MAC绑定策略中的源IP匹配，而数据包的源MAC与策略中的MAC 不匹配，则丢弃数据包。
- 如果数据包的源IP与IP-MAC绑定策略中的源IP不匹配，而数据包的源MAC与策略中的 MAC 匹配，则丢弃数据包。
- 如果数据包的源 IP 和源 MAC 与 IP-MAC 绑定策略中的源 IP 与 MAC 都不匹配，且 IP-MAC 绑定的缺省动作为拒绝，则丢弃数据包。

8.1.2 访问策略

访问策略对从特定源发往特定目的的数据包进行控制。

8.1.2.1 策略元素

访问策略的元素包括：

- 基本元素：序号 (优先级）、名称、描述信息、启用状态 （启用、禁用）、产生日志状态。
- 匹配条件：源安全域、源用户、源 IP、目的安全域、目的 IP、服务、时间表。
- 处理数据包的动作包括：允许和拒绝、 VPN 隧道、启用 DNS 透明代理。
- 特定超时时间。

8.1.2.2 访问策略包处理流程

当收到数据包时， NISG 将数据包中的会话信息与会话表进行匹配，匹配流程如下：

表 150 访问策略包处理流程

与会话表匹配（是 / 否）	与访问策略匹配（是 / 否）	访问策略动作（允许 / 拒绝	NISG 采取的动作
是	N/A	N/A	根据会话表对数据包进行状态检测。只要数据包的会话状态与会话表中的状态匹配，则转发数据包。
否	是	允许	将数据包的会话信息保存在会话表中并转发数据包。
否	是	拒绝	丢弃
否	否	N/A	应用缺省访问策略 （安全域内 / 域间访问策略）

8.1.3 缺省访问策略

缺省访问策略包括：

- 安全域间缺省访问策略：安全域间缺省访问策略控制不同安全域之间的 IP 数据流。在 NISG 未被划分安全域前，所有数据流都被认为是域间数据流。
- 安全域内缺省访问策略控制同一安全域内不同的 NISG 接口间的 IP 数据流。

缺省访问策略的动作可以设置为**允许**或**拒绝**。安全域间缺省访问策略的缺省动作为**拒绝**，安全域内缺省访问策略的缺省动作为**允许**。

缺省访问策略的优先级低于 NISG 中已存在的访问策略。

8.1.4 多播策略

在 NISG 上，管理员可以设置特定的条件控制多播数据信息流的转发。这些条件统称为多播策略。 NISG 只转发匹配多播策略中所有条件的多播数据包。在 NISG 上，可以设置多播策略将来自于特定源 IP 的多播数据包转发和路由到指定的目的 IP 地址。

如果配置了多播路由，而没有配置相应的多播策略， NISG 不转发此条路由的多播数据包。

8.1.5 会话策略

NISG 的会话策略特性通过限制具有某些特征的会话的数量，可以防止会话表泛滥的发生。 NISG 提供三种类型的会话策略：

- 8.1.5.1 基于源 IP 地址的会话限制
- 8.1.5.2 基于目的 IP 地址的会话限制
- 8.1.5.3 基于策略的会话限制

8.1.5.1 基于源 IP 地址的会话限制

限制每源 IP 地址的并发会话数。NISG 将根据如下条件拒绝来自指定 IP 地址的后续连接请求：

- 当来自源 IP 地址的会话匹配了基于源 IP 的会话策略中定义的如下条件：
  - 源 IP 地址
  - 源和目的安全域
  - 服务
- 来自于源 IP 地址的并发会话数目达到 NISG 允许的最大会话数目 （阈值）。

8.1.5.2 基于目的 IP 地址的会话限制

限制每目的 IP 地址的并发会话数目。NISG 依据如下条件拒绝发往指定 IP 地址的后续连接请求：

- 当发往指定目的 IP 地址的会话匹配了基于目的 IP 的会话策略中定义的如下条件：
  - 目的 IP 地址
  - 源和目的安全域
  - 服务
- 并发会话数目到达 NISG 允许的最大会话数目 （阈值）。

8.1.5.3 基于策略的会话限制

限制所有符合指定源和目的 IP 地址条件的并发会话的总数。 NISG 依据如下条件拒绝匹配此策略的后续连接请求：

- 当来自指定源IP地址且发往指定目的IP地址的会话匹配了基于策略的会话策略中定义的如下条件：
  - 源和目的 IP 地址
  - 源和目的安全域
  - 服务
- 并发会话数目到达 NISG 允许的最大会话数目 （阈值）。

8.2 基本配置

本节介绍了 NISG 策略的基本配置步骤，包括：

- 8.2.1 配置 IP-MAC 绑定
- 8.2.2 创建访问策略
- 8.2.3 配置缺省访问策略
- 8.2.4 创建多播策略
- 8.2.5 创建会话策略

在配置以上策略之前，您需要先完成如下配置：

- 安全域：选择**网络** > **安全域**。
- 用户：选择**系统** > **认证** > **用户**。
- IP 地址对象或对象组：选择**系统** > **对象** > **IP 地址** > **IP 地址对象** /**IP 地址对象组**。

提示：IP-MAC 绑定策略可以同时包含 IPv4 地址和 IPv6 地址，而其他策略都不允许。

- 服务对象或对象组：选择**系统** > **对象** > **服务** > **服务对象** / **服务对象组**。

8.2.1 配置 IP-MAC 绑定

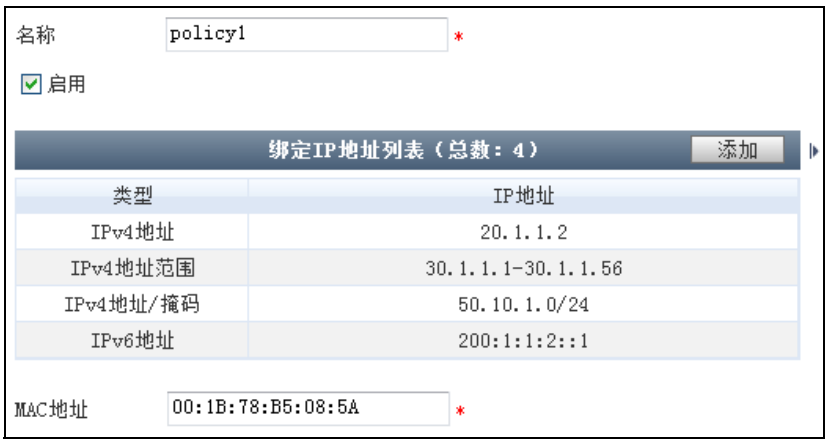
IP-MAC 绑定配置包括：

- 8.2.1.1 创建 IP-MAC 绑定策略
- 8.2.1.2 配置缺省动作

8.2.1.1 创建 IP-MAC 绑定策略

选择**防火墙** > **IP-MAC 绑定** > **新建**。

1. 设置策略名称。
2. 添加源 IP 地址。
3. 添加源 MAC 地址。



提示：每个 IP-MAC 绑定策略只能包含一个 MAC 地址，但是可以包含多个 IP 地址或范围。

8.2.1.2 配置缺省动作

当数据包没有匹配到任何 IP-MAC 绑定策略时， NISG 将会根据 IP-MAC 绑定缺省动作对其进行处理。

选择**防火墙 > IP-MAC 绑定**，在**与下列 IP-MAC 绑定策略不匹配的连接**区域，设置**允许**或**拒绝**。

注意：在 WebUI 上，将 “ **与下列 IP-MAC 绑定策略不匹配的连接 ”** 的动作设置为**拒绝**前，必须配置一条 IP-MAC 绑定策略将管理主机的 IP 与 MAC 地址绑定且保证该策略成功启用。否则会因为缺省动作生效而导致网络连接失败。

表 151 IP-MAC 绑定策略命令

policy ip-mac *policy_name*	添加 IP-MAC 绑定策略
policy default ip-mac {**permit** | **deny**}	修改缺省动作
unset policy ip-mac [*policy_name*]	删除 IP-MAC 绑定策略
show policy ip-mac	查看 IP-MAC 绑定策略配置信息

8.2.2 创建访问策略

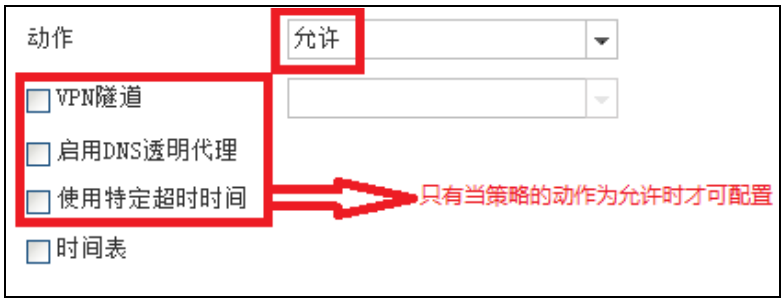
选择**防火墙** > **访问策略** > **新建**。

1. 设置策略基本元素。

2. 指定数据包的源。

3. 设置数据包的目的地址和服务类型。

4. 设置访问策略的动作。



- 勾选 **VPN 隧道**复选框，选择 VPN 隧道或隧道组。
- 勾选**启用 DNS 透明代理**启用 DNS 透明代理功能。
- 勾选**使用特定超时时间**设置 TCP 会话、 UDP 和 ICMP 模拟会话的超时时间。

选择**防火墙** > **缺省策略设置**，设置会话超时时间的缺省值。

5. 设置策略的生效时间。

表 152 访问策略命令

policy access *policy_name*	添加访问策略
policy access *policy_name* **description**	设置备注信息
policy access *policy_name* **log** {**on** | **off**}	启用或禁用日志功能
policy access *policy_name* **number** *pri*	修改策略优先级
policy access *policy_name* **protocol**	添加服务
policy access *policy_name* **schedule**	设置访问策略生效时间
policy access *policy_name* **sourceip**	添加源 IP 地址
policy access *policy_name* **desip**	添加目的 IP 地址
policy access *policy_name* **timeout**	设置会话超时时间
policy access *policy_name* **tunnel**	设置 VPN 隧道
policy access *policy_name* [**user** *user_list*]	添加源用户
unset policy access [*policy_name*]	删除访问策略
show policy access	查看访问策略的配置信息
timeout	设置会话缺省超时时间
timeout reset	设置会话缺省超时时间为缺省值

8.2.3 配置缺省访问策略

选择**防火墙** > **缺省策略设置**，可以设置安全域间和安全域内缺省策略的动作。

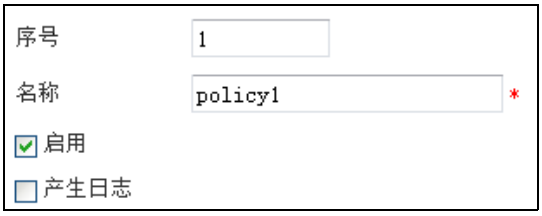
表 153 缺省策略设置命令

policy default inter-zone access {permit | deny}	设置域间缺省策略的动作
policy default intra-zone *zone_name* **{permit | deny}**	设置域内缺省策略的动作
show policy default	显示缺省策略的信息

8.2.4 创建多播策略

选择**防火墙** > **多播策略** > **新建**。

1. 设置策略的基本元素。



2. 设置数据包的源地址。

3. 设置数据包的目的多播组 IP 地址和允许的安全域。

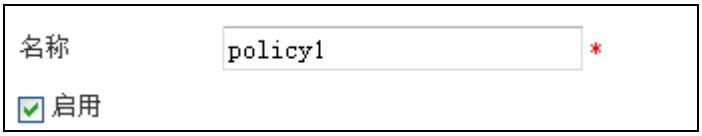
表 154 多播策略命令

policy multicast *policy_name*	添加多播策略
policy multicast *policy_name* **groupip**	添加多播组 IP 地址
policy multicast *policy_name* **log {on | off}**	启用或禁用日志功能
policy multicast *policy_name* **sourceip**	添加源 IP 地址
policy multicast *policy_name* **allowedzone**	添加目的安全域
policy multicast *policy_name* **{enable | disable}**	启用或禁用多播策略
policy multicast *policy_name* **number** *pri*	修改策略优先级
show policy multicast [*policy_name*]	查看多播策略的配置信息
unset policy multicast [*policy_name*]	删除多播策略

8.2.5 创建会话策略

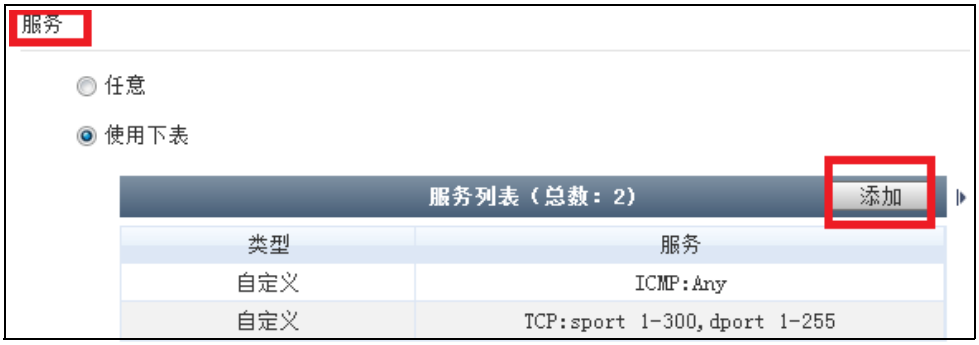
选择**防火墙** > **会话策略** > **新建**。

1. 设置策略基本元素。



2. 设置数据包的源和目的地址。

3. 设置数据包的服务类型。



4. 设置会话策略的类型、允许的最大连接数及动作。

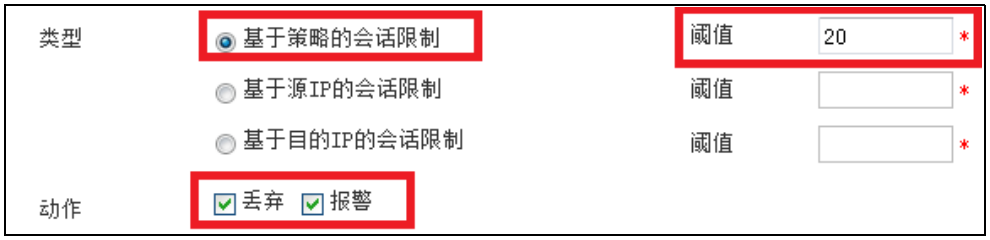


表 155 会话策略命令

policy session *policy_name*	添加会话策略
policy session *policy_name* **sourceip**	为会话策略添加源 IP 地址
policy session *policy_name* **desip**	为会话策略添加目的 IP 地址
policy session *policy_name* {**enable** | **disable**}	启用或禁用会话策略
policy session *policy_name* **protocol**	为会话策略追加服务
policy session *policy_name* **type**	为会话策略修改策略类型和阈值
show policy session [*policy_name*]	查看策略的配置信息
unset policy session [*policy_name*]	删除会话策略

8.3 范例

本节列出了策略配置的范例，包括：

- 范例 1：创建 IP-MAC 绑定策略
- 范例 2：创建访问策略
- 范例 3：安全域间多播策略的应用
- 范例 4：创建基于目的 IP 的会话策略

在配置每条范例之前，都需要先完成如下配置：

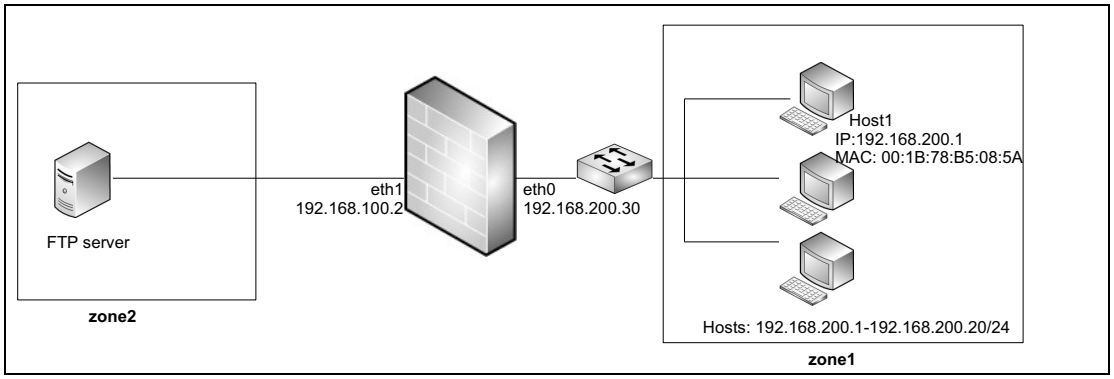
- 选择**网络** > **接口**，进入**接口**页面对 NISG 的接口进行配置。详细信息请参见 4.2.3 范例：以太网接口。
- 如果范例中涉及到安全域，选择**网络** > **安全域** > **新建**，创建新的安全域。详细信息请参见 4.12.3 范例：安全域应用。
- 如果范例中涉及到用户，选择**系统** > **认证** > **用户** > **新建**，创建新用户。详细信息请参见 3.14 网络用户。
- 如果范例中涉及到对象或对象组，选择**系统** > **对象**，创建 IP 地址对象或服务对象。详细信息请参见 3.24 对象。
- 选择**防火墙** > **缺省策略设置**，将安全域间缺省策略的动作设置为**允许**，或者选择**防火墙** > **访问策略**，创建一条允许所有数据流通过的访问策略。请参见 8.2.2 创建访问策略。

范例 1：创建 IP-MAC 绑定策略

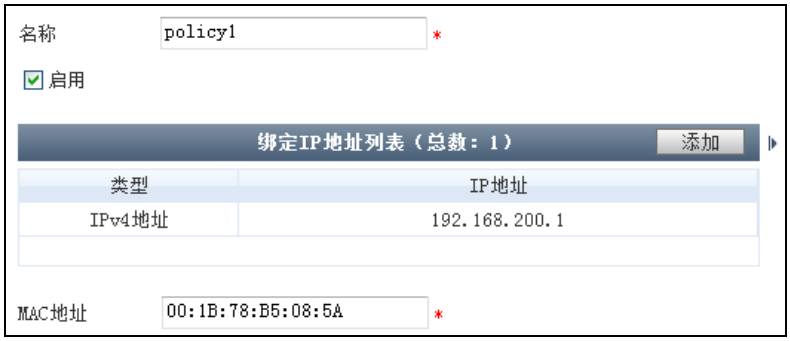
在本范例中，安全域 zone2 中部署了 FTP 服务器。为了防止 IP 地址欺骗，管理员创建 IP-MAC 绑定策略 policy1：

- 将 Host1 的 IP 地址 192.168.200.1 与其 MAC 地址 00:1B:78:B5:08:5A 绑定，只允许 zone1 中的 Host1 访问 zone2 中的 FTP 服务器。
- 当其他主机试图访问 zone2 中的 FTP 服务器，而其 IP 和 MAC 地址不匹配任何 IP-MAC 绑定策略时，阻止此主机访问服务器。

图 32 网络拓扑图



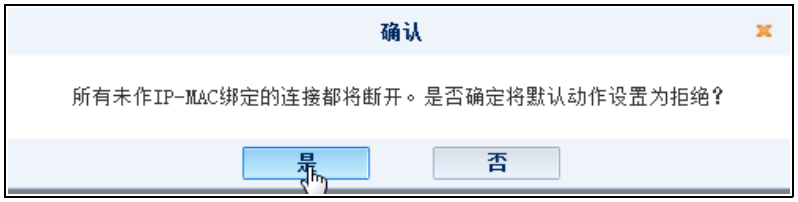
1. 选择**防火墙** > **IP-MAC 绑定** > **新建**，添加一条 IP-MAC 绑定策略。



2. 点击**确定**。
3. 在**与下列 IP-MAC 绑定策略不匹配的连接**区域，点击**拒绝**。

注意：在将动作设置为**拒绝**前，必须配置一条 IP-MAC 绑定策略将管理主机的 IP 与 MAC 地址绑定且保证该策略成功启用。否则会因为缺省动作生效而导致网络连接失败。

4. 在下列的对话框中点击**是**。



5. 点击 。

CLI

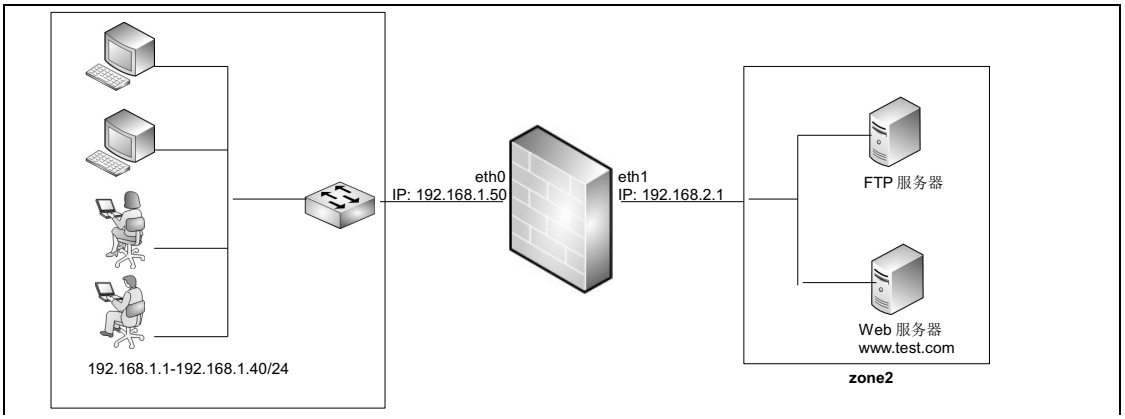
```
NetEye@root> configure mode override
NetEye@root-system] policy ip-mac policy1 192.168.200.1
00:1B:78:B5:08:5A enable
NetEye@root-system] policy default ip-mac deny
NetEye@root-system] exit
NetEye@root> save config
```

范例 2：创建访问策略

在本范例中，管理员在 zone2 中部署一台 Web 服务器 （域名为 www.test.com）和 FTP 服务器。管理员要求 NISG 对从 zone1 到 zone2 的数据流进行以下访问控制：

- 策略 1：允许安全域 zone1 内 IP 地址范围在 192.168.1.1-192.168.1.20 中的主机访问安全域 zone2 内的 FTP 服务器，并对其访问情况进行记录。同时，为避免 FTP 服务器的并发连接数过大，在已建立的 FTP 会话上，如果用户在 300 秒内未进行操作，会话能够超时断开。
- 策略 2：不允许安全域 zone1 内 IP 地址范围在 192.168.1.21-192.168.1.40 中的用户 user1、user2 以及所有未在 NISG 本地创建的外部用户在工作时间 (08:30:00-17:30:00，周一至周五) 访问 zone2 中的 Web 服务器。

图 33 网络拓扑图



1. 选择**防火墙 > 访问策略**。点击**新建**创建访问策略 policy1。

2. 点击**确定**。

3. 点击**新建**创建访问策略 policy2。

4. 点击**确定**。

5. 点击 。

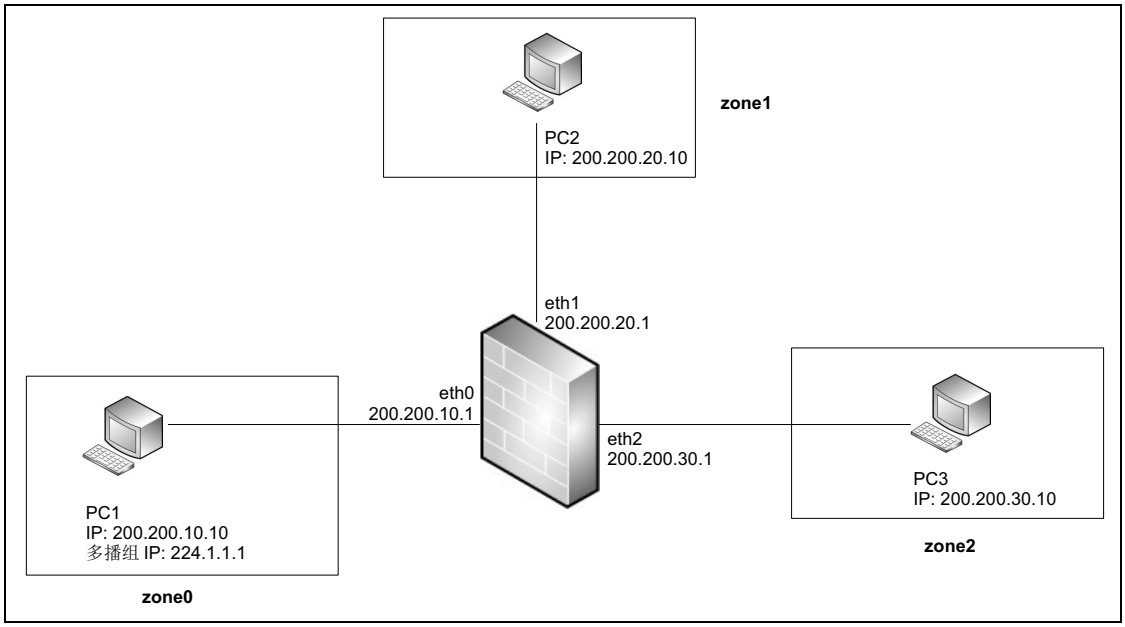
CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy access policy1 zone1 192.168.1.1-
192.168.1.20 zone2 any protocol-object FTP any permit enable 1
NetEye@root-system] policy access policy1 timeout tcp ested 300
NetEye@root-system] policy access policy1 log on
NetEye@root-system] policy access policy2 zone1 192.168.1.21-
192.168.1.40 zone2 DomainName www.test.com protocol-object DNS user
user1,user2 include-external-users deny enable 2
NetEye@root-system] policy access policy2 schedule start-week 1 end-
week 5 08:30:00-17:30:00
NetEye@root-system] exit
NetEye@root> save config
```

范例 3：安全域间多播策略的应用

在本范例中， PC1 为多播源，通过多播组 IP 地址 224.1.1.1 将多播数据流发送给 PC2 和 PC3。管理员创建一条多播策略只允许 PC2 接收来自 PC1 的多播数据流。

图 34 网络拓扑图



配置步骤如下：

- 3.1 启用 DVMRP
- 3.2 创建静态多播路由
- 3.3 创建多播策略

3.1 启用 DVMRP

1. 选择**网络** > **多播** > **DVMRP**。配置 DVMRP，如下所示：

2. 点击**确定**。
3. 点击 。

CLI

```
NetEye@root>configure mode
NetEye@root-system]dvmrp enable
NetEye@root-system]interface ethernet 0
NetEye@root-system-if-eth0]dvmrp on
NetEye@root-system-if-eth0]dvmrp metric 1
NetEye@root-system-if-eth0]dvmrp threshold 1
NetEye@root-system-if-eth0]exit
NetEye@root-system]interface ethernet 1
NetEye@root-system-if-eth1]dvmrp on
NetEye@root-system-if-eth1]dvmrp metric 1
NetEye@root-system-if-eth1]dvmrp threshold 1
NetEye@root-system-if-eth1]exit
NetEye@root-system]interface ethernet 2
NetEye@root-system-if-eth2]dvmrp on
NetEye@root-system-if-eth2]dvmrp metric 1
NetEye@root-system-if-eth2]dvmrp threshold 1
NetEye@root-system-if-eth2]exit
NetEye@root-system]dvmrp cache-lifetime 300
NetEye@root-system]dvmrp prune-lifetime 7200
NetEye@root-system]dvmrp pim disable
NetEye@root-system] exit
NetEye@root> save config
```

3.2 创建静态多播路由

1. 在 **DVMRP** 页面点击**多播路由**超链接或选择**网络** > **路由** > **多播路由**。点击**新建**创建如下静态多播路由：

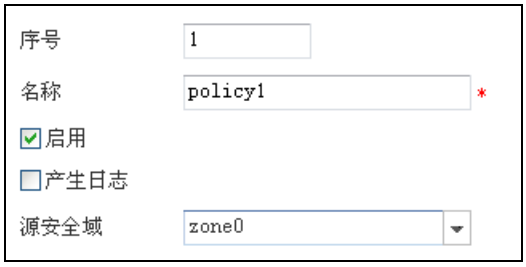
2. 点击**确定**。
3. 点击 。

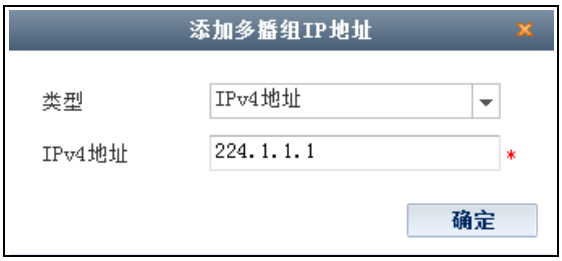
CLI

```
NetEye@root>configure mode
NetEye@root-system]dvmrp route 200.200.10.10 224.1.1.1 input eth0
forwarding eth1,eth2 threshold 2
NetEye@root-system]exit
NetEye@root>save config
```

3.3 创建多播策略

1. 选择**防火墙** > **多播策略**。点击**新建**，创建一条名为 policy1 的多播策略，允许 PC2 接收来自 PC1 的多播数据流。





2. 点击**确定**。
3. 点击 。

CLI

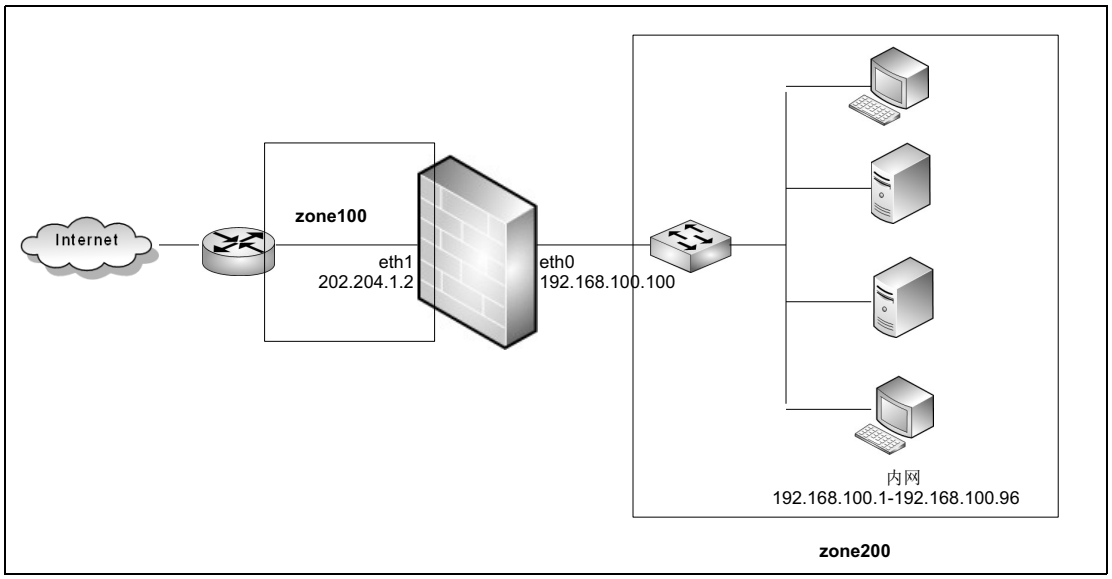
```
NetEye@root> configure mode override
NetEye@root-system] policy multicast policy1 zone0 200.200.10.10
224.1.1.1 zone1 enable 1
NetEye@root-system] end
NetEye@root> save config
```

范例 4：创建基于目的 IP 的会话策略

在本范例中，某公司的网络中存在大量的无用的 TCP 连接。为防止 DoS 攻击，管理员要求 NISG 丢弃满足以下条件的数据包并发送报警事件：

- 来自安全域 zone100。
- 目的IP地址是zone200内192.168.100.1-192.168.1.96 范围中的任一IP地址，且最大并发会话数超过 20。
- 使用的服务为 TCP， TCP 端口号范围为 1-65535。

图 35 网络拓扑图



1. 选择**防火墙** > **会话策略**。点击**新建**创建新的会话策略。

2. 点击**确定**。
3. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy session policy1 zone100 zone200 any
192.168.100.1-192.168.100.96 tcp 1-65535 1-65535 20 type dstip
enable drop alert
NetEye@root-system] end
NetEye@root> save config
```

8.4 配置参数说明

本节详细介绍了策略配置过程中的参数信息，包括：

- 8.4.1 IP-MAC 绑定策略参数
- 8.4.2 访问策略参数
- 8.4.3 多播策略参数
- 8.4.4 会话策略参数

8.4.1 IP-MAC 绑定策略参数

表 156 IP-MAC 绑定策略的配置信息

配置信息	说明
名称	IP-MAC 地址绑定策略名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & # 同一个虚拟系统内部的 IP-MAC 地址绑定策略不允许配置相同的名称。
启用	用于启用或禁用 IP-MAC 地址绑定策略。 IP-MAC 地址绑定策略缺省为启用。
绑定 IP 地址列表	用于设置发送数据包的源 IP 地址。 IP 地址可以是以下任一类型： • IP 地址对象 • 对象组 • IPv4 地址 • IPv4 地址范围 • IPv4 地址 / 掩码长度 • IPv6 地址 • IPv6 地址范围 • IPv6 地址 / 前缀长度 **IP 地址对象**为缺省设置。管理员最多可以添加 4096 个地址条目。 IP 地址列表内的条目不允许出现完全相同的情况。
MAC 地址	用于设置发送数据包的源 MAC 地址。 管理员只可以为每条 IP-MAC 地址绑定策略设置一个 MAC 地址。 **IP 地址绑定列表**中的每个 IPv4 和 IPv6 地址都与此 MAC 地址绑定。

8.4.2 访问策略参数

表 157 访问策略的配置信息

配置信息	说明
序号	访问策略的优先级。取值范围为 1 ～ 80000 之间的整数。数值越小，优先级越高。 如果在创建策略时未指定其序号，那么此策略的序号将自动成为最大的。如果将已存在策略的序号指定给新建的策略，则已存在策略的序号将在原序号的基础上加 1。
名称	访问策略的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & # 同一个虚拟系统内部的访问策略不允许配置相同的名称。
描述	访问策略的描述信息。长度 0 ～ 255 个字节。UTF-8 字符。不能包含以下字符：？" ' \ < > &
启用	用于启用或禁用访问策略。访问策略的状态缺省为启用。
产生日志	NISG 是否为匹配访问策略的数据包记录日志。此功能缺省为禁用。
源安全域	发送数据包的安全域。缺省为 **Any**，即所有安全域。
源 IP 地址	发送数据包的 IP 地址，可以是以下任一类型： • 任意：包括所有 IPv4 和 IPv6 地址。**任意**为缺省设置。 • 任意 IPv4 地址：包括所有 IPv4 地址。 • 任意 IPv6 地址：包括所有 IPv6 地址。 • 使用下表：包括 IP 地址对象、对象组、 IPv4 地址、 IPv4 地址范围、 IPv4 地址 / 掩码、IPv6 地址、 IPv6 地址范围和 IPv6 地址 / 前缀。 **IP 地址对象**为缺省设置。 管理员最多可以配置 4096 个源 IP 地址条目。源 IP 地址列表内的条目不允许出现完全相同的情况。
源用户	发送数据包的用户，可以是以下任一类型： • 任意：包括所有网络用户，包括已经通过身份认证和未通过身份认证的用户。**任意**为缺省设置。 • 任意认证用户：包括已经通过身份认证的所有网络用户。 • 使用下表：包括管理员选择的网络用户。管理员可以根据自身的需求选择是否包含未在 NISG 中配置的外部用户。 管理员最多可以选择 4096 个源用户。源用户列表内的条目不允许出现完全相同的情况。 关于用户的信息，请参见 3.14 网络用户。
目的安全域	数据包要到达的安全域。缺省为 **Any**，即所有安全域。
目的 IP 地址	数据包要到达的 IP 地址，可以是以下任一类型： • 任意：包括所有 IPv4 和 IPv6 地址。**任意**为缺省设置。 • 任意 IPv4 地址：包括所有 IPv4 地址。 • 任意 IPv6 地址：包括所有 IPv6 地址。 使用下表：包括 IP 地址对象、对象组、 IPv4 地址、 IPv4 地址范围、 IPv4 地址 / 掩码、IPv6 地址、 IPv6 地址范围、 IPv6 地址 / 前缀和域名。 **IP 地址对象**为缺省设置。 域名的长度范围为 2 ～ 255 个字节。管理员最多可以设置 4096 个目的 IP 地址条目。目的 IP 地址列表内的条目不允许出现完全相同的情况。

表 157 访问策略的配置信息 (*续*)

配置信息	说明
服务	数据包使用的传输层服务，可以是以下任一类型： • 任意：包括所有协议类型。**任意**为缺省设置。 • 使用下表：包括服务对象、服务对象组以及自定义协议。**对象 AOL** 为缺省配置。 自定义协议包括 ICMP、 ICMPv6、 TCP、 UDP 和 Other。 当设置 ICMP 协议时，管理员可以选择以下任一类型：ECHO_and_ECHOREPLY，INFO_REQUEST_and_INFO_REPLY， TIMESTAMP_and_TIMESTAMPREPLY，ADDRESS_and_ADDRESSREPLY， ROUTER_ADVERTISEMENT，ROUTER_SOLICITATION，DEST_UNREACH， SOURCE_QUENCH， REDIRECT，TIME_EXCEEDED， PARAMETERPROB 和 Any （表示任意 ICMP 协议类型）。 当设置 ICMPv6 协议时，管理员可以选择以下任一类型：DST_UNREACH， PACKET_TOO_BIG， TIME_EXCEEDED， PARAM_PROB，ECHO_and_ECHOREPLY 和 Any （表示任意 ICMPv6 协议类型）。 TCP 和 UDP 协议的源和目的端口号范围为 1 ～ 65535。其它协议号范围为 1 ～ 255。 管理员最多可以配置 32 个服务条目 （共 4096 个端口号）。服务列表内的条目不允许出现完全相同的情况。
动作	描述 NISG 如何处理匹配访问策略的数据包： • 允许：发数据包并更新其所属会话的状态。动作缺省为**允许**。 • 拒绝：丢弃数据包并取消其会话。
VPN 隧道	当访问策略的动作为**允许**时，可以选择启用或禁用 VPN 隧道功能。此功能缺省为禁用。启用后，可以将数据包引入到指定的 VPN 隧道或隧道组。
启用 DNS 透明代理	当访问策略的动作为**允许**时，可以启用或禁用透明代理功能。此功能缺省为禁用。 关于透明代理的信息，请参见 4.14 DNS 代理。
使用特定超时时间	当访问策略的动作为**允许**时，可以启用或禁用特定超时时间。此功能缺省为禁用。 启用后，可以为 TCP 会话状以及 ICMP 和 UDP 的模拟会话设置超时时间。超时时间范围为 1 ～ 99999999 秒。禁用该功能时， NISG 将采用系统提供的缺省状态超时时间设置。

时间表	用于启用或禁用访问策略的生效时间。此功能缺省为禁用。
	如果没有为启用的访问策略设置时间表，那么此条访问策略在任何时间都生效。
	• 循环：用于设置访问策略的循环生效时间。在循环生效时间范围内，访问策略在每周指定的具体时间生效。
	  • 每周：可以从周一至周日中选择。
	  • 时间列表：可以设置每天生效时间的起始时间和终止时间。格式为：HH:MM:SS ；可选范围：00:00:00 ～ 23:59:59。最多可以将 8 个时间条目添加到时间表内。时间范围允许重叠但不允许完全相同。
	• 单次：用于设置访问策略的单次生效时间。访问策略只在设置的时间段内生效，而不会在其他时间段重复生效。日期的格式为： YYYY-MM-DD ；可选择范围为 1970-01-01 ～ 2037-12-31。
	必须设置一个起始日期和时间以及终止日期和时间。

8.4.3 多播策略参数

表 158 多播策略的配置信息

配置信息	说明
序号	表示多播策略的优先级。取值范围为 1 ～ 80000 之间的整数。数值越小，优先级越高。 如果在创建策略时未指定其序号，那么此策略的序号将自动成为最大的。如果将已存在策略的序号指定给新建的策略，则已存在策略的序号将在原序号的基础上加 1。
名称	多播策略的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & # 同一个虚拟系统内部的多播策略不允许配置相同的名称。
启用	用于启用或禁用多播策略。多播策略缺省为启用。
产生日志	NISG 是否为匹配多播策略的数据包记录日志。此功能缺省为禁用。
源安全域	NISG 接收多播数据包的入口安全域。缺省为 **Any**，即任意安全域。
源 IP 地址	发送多播数据包的 IP 地址，可以是以下任一类型： • 任意：包括所有 IPv4 多播地址。缺省为**任意**。 • 使用下表：包括 IP 地址对象、对象组、 IPv4 地址、 IPv4 地址范围和 IPv4 地址 / 掩码。缺省为 **IP 地址对象**。 管理员最多可以配置 4096 个源 IP 地址条目。源 IP 地址列表内的条目不允许出现完全相同的情况。
多播组 IP 地址	多播数据包的目的多播组的 IP 地址，可以是以下任一类型： • 任意：包括所有 IPv4 多播组地址。缺省为**任意**。 • 使用下表：包括 IP 地址对象、对象组、 IPv4 地址、 IPv4 地址范围和 IPv4 地址 / 掩码。缺省为 **IP 地址对象**。 管理员最多可以配置 4096 个多播组 IP 地址条目。多播组 IP 地址列表内的条目不允许出现完全相同的情况。
允许安全域	允许转发多播数据包的出口安全域。缺省为 **Any**，即所有安全域。

8.4.4 会话策略参数

表 159 会话策略的配置信息

配置信息	说明
名称	会话策略的名称。长度 1-63 字节，UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & # 同一个虚拟系统内部的会话策略不允许配置相同的名称。
启用	用于启用或禁用会话策略。会话策略缺省为启用。
源安全域	发送数据包的安全域。缺省为 **Any**，即所有安全域。
目的安全域	数据包要到达的安全域。缺省为 **Any**，即所有安全域。
源 IP 地址	发送数据包的 IP 地址，可以是以下任一类型： • 任意：包括所有 IPv4 和 IPv6 地址。**任意**为缺省设置。 • 任意 IPv4 地址：包括所有 IPv4 地址。 • 任意 IPv6 地址：包括所有 IPv6 地址。 • 使用下表：包括 IP 地址对象、对象组、 IPv4 地址、 IPv4 地址范围、 IPv4 地址 / 掩码、IPv6 地址、 IPv6 地址范围和 IPv6 地址 / 前缀。 **IP 地址对象**为缺省设置。管理员最多可以配置 4096 个源 IP 地址条目。源 IP 地址列表内的条目不允许出现完全相同的情况。
目的 IP 地址	数据包要到达的 IP 地址，可以是以下任一类型： • 任意：包括所有 IPv4 和 IPv6 地址。**任意**为缺省设置。 • 任意 IPv4 地址：包括所有 IPv4 地址。 • 任意 IPv6 地址：包括所有 IPv6 地址。 • 使用下表：包括 IP 地址对象、对象组、 IPv4 地址、 IPv4 地址范围、 IPv4 地址 / 掩码、IPv6 地址、 IPv6 地址范围和 IPv6 地址 / 前缀。 **IP 地址对象**为缺省设置。 管理员最多可以配置 4096 个目的 IP 地址条目。目的 IP 地址列表内的条目不允许出现完全相同的情况。
服务	数据包使用的传输层服务，可以是以下任一一种： • 任意：包括所有协议类型。**任意**为缺省设置。 • 使用下表：包括对象、对象组以及自定义协议。对象 AOL 为缺省设置。 自定义协议包括 ICMP、 ICMPv6、 TCP、 UDP 和 Other。 当设置 ICMP 协议时，管理员可以选择以下任一类型：ECHO_and_ECHOREPLY，INFO_REQUEST_and_INFO_REPLY， TIMESTAMP_and_TIMESTAMPREPLY，ADDRESS_and_ADDRESSREPLY， ROUTER_ADVERTISEMENT，ROUTER_SOLICITATION，DEST_UNREACH， SOURCE_QUENCH， REDIRECT，TIME_EXCEEDED， PARAMETERPROB 和 Any （表示任意 ICMP 协议类型）。 当设置 ICMPv6 协议时，管理员可以选择以下任一类型：DST_UNREACH，PACKET_TOO_BIG， TIME_EXCEEDED， PARAM_PROB，ECHO_and_ECHOREPLY 和 Any （表示任意 ICMPv6 协议类型）。 TCP 和 UDP 协议的目的端口号范围为 1 ～ 65535。其它协议号范围为 1 ～ 255。 管理员最多可以配置 32 个服务条目 （共 4096 个端口号）。服务列表内的条目不允许出现完全相同的情况。
类型	会话策略的类型： • 基于策略的会话限制 （缺省类型） • 基于源 IP 的会话限制 • 基于目的 IP 的会话限制

表 159 会话策略的配置信息 (*续*)

配置信息	说明
阈值	会话策略允许的最大并发会话数目。取值范围是 1 ～ 99999999。
动作	指 NISG 如何处理匹配到会话策略的数据包，包括： • 报警：发送报警事件。 • 丢弃：丢弃攻击数据包。 缺省为**报警 + 丢弃**。

9 攻击防御

本章介绍安全域级的攻击检测和防御机制。

- 9.1. 基本概念，介绍攻击防御的概念和基本原理。
- 9.2. 攻击类型 / 方式 / 解决措施，描述常见的攻击类型以及 NISG 针对这些攻击采取的措施。
- 9.3. 基本配置步骤，配置防火墙攻击防御时使用的各项基本步骤。
- 9.4. 配置参数说明，参数详细信息。

9.1. 基本概念

本节包括：

- 9.1.1. 攻击目的
- 9.1.2. 攻击威胁类型
- 9.1.3. 应对措施

9.1.1. 攻击目的

攻击目的包括：

- 获取机密数据
- 获取主机系统的相关信息
- 损坏目标系统

9.1.2. 攻击威胁类型

攻击可以分为以下几个类型：

- DoS 攻击
- 探测攻击
- TCP 逃避控制
- IP 选项校验
- ICMP 攻击

9.1.3. 应对措施

可以通过**防火墙** > **攻击防御**指定攻击防御措施。

大部分的防御措施中会要求设置阈值，用于判定攻击行为的产生时机 （例如一个时间段内发送的数据包数量）。

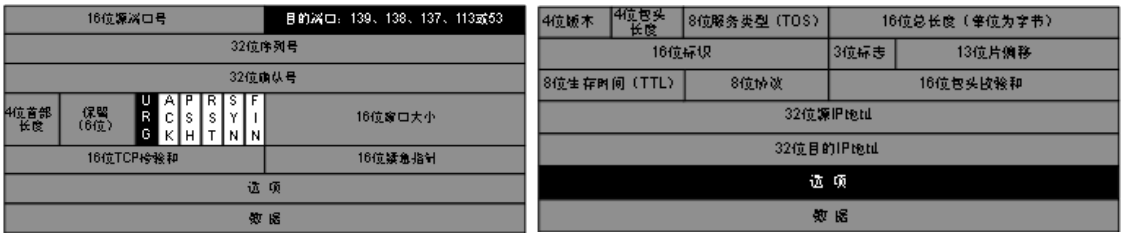
9.2. 攻击类型 / 方式 / 解决措施中描述了 NISG 中针对各类攻击的应对措施：

- **丢弃**：丢弃数据包。
- **报警**：产生一个报警事件，通知管理员检测到攻击行为。报警事件内容包含如下信息：
  - 攻击类型
  - 攻击数据包的源 / 目的 IP 地址和源 / 目的端口
  - 攻击数据包所属的虚拟系统
  - 协议
  - 源 / 目的安全域 （仅对策略级攻击防御有效）

9.2. 攻击类型 / 方式 / 解决措施

本节列出常见的攻击类型，和 NISG 针对这些攻击采取的解决措施。如想深入了解该特性，您需要了解 TCP 和 IP 数据包包头结构。 TCP/IP 数据包头的信息列出，如图 36 所示。

图 36 TCP/IP 数据包包头



NISG 支持防护的攻击类型分类如下：

- 9.2.1. DoS 防御
- 9.2.2. 探测防御
- 9.2.3. TCP 逃避控制
- 9.2.4. IP 选项校验
- 9.2.5. ICMP 攻击防御

9.2.1. DoS 防御

DoS 攻击的攻击类型、方式及解决措施如表 160 所示。

表 160 DoS 防御的类型、方式和解决措施

攻击类型	攻击方式	NISG 解决措施
ICMP 泛滥	在短时间内向受害主机发送大量 ICMP echo 请求包，耗尽主机资源。	限制每秒钟允许通过的 ICMP Echo 数据包个数 （即阈值）。
TCP SYN 泛滥	在短时间内向受害主机发送带有虚假源 IP 地址的 TCP SYN 数据包。迫使受害主机回应大量 SYN/ACK 数据包。由于这些数据包的源 IP 地址对应的主机往往是不存在或不可达的，所以 ACK 数据包得不到回应，导致 TCP 连接无法建立，使受害主机系统中堆积大量的半连接，直至资源耗尽。	限制每秒内允许通过的 TCP SYN 数据包数 （阈值）。
UDP 泛滥	在短时间内向受害主机发送大量 UDP 包，耗尽主机资源。	限制每秒钟允许通过的 UDP 数据包个数 （即阈值）。
DNS 泛滥	在短时间内向受害主机发送大量 DNS 请求，耗尽主机资源。	限制每秒钟允许通过的来自某安全域的 （基于 UDP 的） DNS 查询请求数量 （即阈值）。 DNS 请求报文是一种 UDP 报文。因此，对于 DNS 请求报文的策略，遵从防 DNS 泛滥和 UDP 泛滥的两个阈值中较小的。 如果设置的 DNS 泛滥的阈值大于 UDP 泛滥阈值，则根据 UDP 泛滥策略对其进行处理。如果设置的 DNS 泛滥阈值小于或等于 UDP 泛滥阈值，则根据 DNS 泛滥策略对其进行处理。
TCP RST 扫描	向目标主机发送大量带有虚假源 IP 的 TCP RST 数据包，使该主机中正常的连接被恶意关闭，服务也因此被迫中断。	接收到 TCP RST 数据包时，会检查此数据包是否属于 NISG 中已存在的任何一个会话，如果不属于，将认定此数据包具有 TCP RST 扫描行为，并按照管理员设置的动作对其进行处理。
WinNuke	向使用 Windows 操作系统的主机的 53、 113、137、 138 或 139 端口发送 TCP URG 数据包，造成 NetBIOS 碎片重叠，并导致系统崩溃。	当 NISG 中存在目的端口为 139、 138、 137、 113 或 53 的 TCP 会话时，如果接收到属于这个会话的 TCP URG 数据包，将认定此数据包具有 WinNuke 攻击的特征，并按照管理员设置的动作对其进行处理。
LAND	在短时间内向受害主机发送大量源、目的 IP 相同的 TCP SYN 数据包，使受害者系统中存在大量的无用连接 （也被称为空连接），耗尽受害主机的资源，导致拒绝服务。	当接收到 TCP SYN 数据包时，会验证此数据包的源 IP 地址和目的 IP 地址是否相同，如果相同，会按照管理员设置的动作对其进行处理。
Smurf	伪造大量的源 IP 地址为受害主机 IP 且目的 IP 地址为广播地址的 ICMP Echo 请求包，使网络中的所有主机都不断地向受害主机发送应答数据包，导致受害主机乃至整个网络发生拥塞。	接收到 ICMP Echo 数据包时，会检查此数据包的目的 IP 地址是否为广播地址，如果是，将认定此数据包具有 Smurf 攻击行为，并按照管理员设置的动作对其进行处理。

表 160 DoS 防御的类型、方式和解决措施 (*续*)

攻击类型	攻击方式	NISG 解决措施
Ping of Death	IP 数据包的最大长度规定为 65535 字节。如果某主机接收到大于规定长度的 IP 数据包，无论它使用哪一种操作系统，都可能引发无法预料的后果，使系统无法正常运行。 在 Ping of Death 攻击中，攻击者通常会将过大的 IP 数据包分解成 IP 碎片发送给受害主机。受害主机接收到这些 IP 碎片包时会对其进行重组，当这些碎片被重组到一定大小时，受害主机就会因系统崩溃而拒绝服务。	NISG 会对 IP 碎片数据包进行重组，如果重组后 IP 数据包的长度大于 65535，将认定这些 IP 碎片数据包具有 Ping of Death 攻击特征，并将这些数据包丢弃。
TearDrop	网络中较大的 IP 数据包会被分解成多个较小的 IP 数据包 （即 IP 碎片）进行传输。每个 IP 碎片包的包头中都有一个偏移字段，表示该碎片在原来未分片数据包中的起始位置。当这些 IP 碎片到达目的地后，目的主机会根据它们的偏移值，将这些 IP 碎片重组为原来的 IP 数据包。 如果某些 IP 碎片覆盖了位于它前面的碎片，重组这样的 IP 碎片时会使操作系统产生无法预料的后果，尤其是一些旧版本的操作系统。 在 Teardrop 攻击中，攻击者通过修改偏移字段，使 IP 碎片数据包发生重叠。当目的主机尝试重组这些 IP 碎片数据包时，就会引起系统崩溃，导致拒绝服务。	NISG 接收到 IP 碎片数据包后，会检查与这个 IP 碎片数据包相邻的 IP 碎片数据包，比较偏移值和数据的长度，来判断是否有数据重叠。 NISG 将会把 IP 碎片数据包中重叠的部分删掉，然后进行重组。
TCP SYN Cookie		主要防御 TCP SYN 泛滥攻击。通过 SYN 代理功能，NISG 能够代替它所保护的服务器处理正常的 SYN 请求， NISG 无需保留连接的状态信息，只需检查 ACK 序列号就可以确定三次握手的合法性，节约系统资源。

9.2.2. 探测防御

探测攻击的攻击类型、方式及解决措施如表 161 所示。

表 161 探测防御的类型、方式和解决措施

攻击类型	攻击方式	NISG 解决措施
IP 地址扫描	将 ICMP Echo 请求包发送给多个主机，如果其中某个主机对 Echo 请求进行应答，那么说明这个主机是活动的，从而让攻击者知道有哪些主机是可以进一步入侵的。 当检测到同一源主机指定时间间隔 （阈值）内向其他目的主机发送 10 个以上的 ICMP Echo 请求包时，视为 IP 地址扫描攻击。	检测到 IP 地址扫描攻击时，按照管理员设置的动作对其进行处理。
TCP SYN 端口扫描	向同一主机的不同端口发送 TCP SYN 数据包来扫描可用的服务。根据端口应答信息的不同，攻击者可以判断出哪些端口是开放的，从而确定进一步攻击目标主机的哪些服务。 检测到同一源主机在指定时间间隔 （阈值）内将 TCP SYN 数据包发送给同一目的主机的 16 个以上不同端口时，视为 TCP SYN 端口扫描攻击。	检测到 TCP SYN 端口扫描攻击时，按照管理员设置的动作对其进行处理。
TCP FIN 扫描	将 TCP FIN 数据包发送给目标主机的某个端口，然后根据是否返回信息来判断这个端口是否开放 （若返回一个 RST 数据包，说明该端口是关闭的；若什么都不返回，说明该端口是开放的）。由于不同的操作系统对这种数据包的应答信息有所不同，所以攻击者还可以根据返回信息的差异，进一步判断出目标主机正在使用的操作系统类型。	如果接收到 TCP FIN 数据包，而且该数据包不属于当前任何一个连接信息，那么就认定这个数据包具有 TCP FIN 扫描攻击的特征并按照管理员设置的动作进行处理。
XMAS 扫描	将同时设置了 FIN、 URG 和 PSH 标志位的 TCP 数据包发送给目标主机的某个端口，然后根据是否返回信息来判断这个端口是否是开放的 （若返回一个 RST 数据包，说明该端口被禁用；若什么都不返回，说明该端口启用）。由于同时设置了 FIN、 URG 和 PSH 标志位的 TCP 数据包是一个异常包，不同的操作系统对这种异常包的应答信息有所不同，所以攻击者还可以根据返回信息的差异，进一步判断出目标主机正在使用的操作系统类型。	如果接收到同时设置了 FIN、 URG 和 PSH 标志位的 TCP 数据包，那么就认定这个数据包具有 TCP XMAS 扫描攻击的特征并按照管理员设置的动作进行处理。
TCP NULL 扫描	将未设置任何标志位的 TCP 数据包发送给目标主机的某个端口，然后根据是否返回信息来判断这个端口是否启用 （若返回一个 RST 数据包，说明该端口被禁用；若什么都不返回，说明该端口启用）。由于未设置任何标志位的 TCP 数据包是一个异常包，不同的操作系统对这种异常包的应答信息有所不同，所以攻击者还可以根据返回信息的差异，进一步判断出目标主机正在使用的操作系统类型。	如果接收到未设置任何标志位的 TCP 数据包，那么就认定这个数据包具有 TCP NULL 扫描攻击的特征并按照管理员设置的动作进行处理。

表 161 探测防御的类型、方式和解决措施 (*续*)

攻击类型	攻击方式	NISG 解决措施
SYN&FIN 标志	因为 SYN 标志和 FIN 标志的用途截然相反，所以正常情况下， SYN 标志和 FIN 标志不能同时出现在一个 TCP 数据包中，同时设置了 SYN 和 FIN 标志位的 TCP 数据包是一个异常包。由于不同的操作系统对这种异常包的应答信息有所不同，攻击者将这种数据包发送给目标主机，就可以根据返回信息的差异，判断出目标主机正在使用的操作系统类型。	如果 NISG 接收到同时设置了 SYN 和 FIN 标志位的 TCP 数据包，那么就认定这个数据包具有攻击的特征，并将其丢弃。
无 ACK 标志的 FIN 标志	正常情况下，设置了 FIN 标志位的 TCP 数据包也要同时设置 ACK 标志位，仅设置了 FIN 标志位而未设置 ACK 标志位的 TCP 数据包是一个异常包。攻击者将这种数据包发送给目标主机，然后根据不同的操作系统对这种异常包的不同反应 （有的会直接丢弃该数据包，有的会返回一个 RST 数据包），判断目标主机正在使用哪种操作系统。	如果 NISG 接收到仅设置了 FIN 标志位而未设置 ACK 标志位的 TCP 数据包，那么就认定这个数据包具有攻击的特征，并将其丢弃。
非 SYN 标志	发起会话的第一个数据包是有 SYN 标记的数据包，如果没有，则视为异常数据包。攻击者有时会在未建立连接的情况下，向目标主机的某个端口发送这种异常数据包，并根据目标主机是否返回信息来判断这个端口是否是开放的（若返回一个 RST 数据包，说明该端口是关闭的；若什么都不返回，说明该端口是开放的）。	NISG 每接收到一个数据包，都会进行会话 （即连接）的查找。如果该数据包属于已存在的会话，NISG 将更新这个会话，并转发该数据包；如果该数据包不属于已存在的会话， NISG 将会对其进行 SYN 标志检查。如果该数据包设置了 SYN 标志位， NISG 将建立新的会话，然后将其转发；如果该数据包未设置 SYN 标志位， NISG 就认定这个数据包具有攻击的特征，并将其丢弃。
IP 欺骗	攻击者在数据包包头中设置虚假的源地址信息，冒用合法用户的身份向目标网络发送数据包，从而让攻击者获得网络中受限区域的访问权限。 NISG 有两种检测 IP 欺骗的方法：一种是路由正确性检查，另一种是 IP 地址和 MAC 地址绑定。	当 NISG 上的接口工作在路由或 NAT 模式下时，要应用路由条目对数据包的路由正确性进行检查来实现对 IP 欺骗行为的检测。即当接收数据包的接口与其源 IP 地址在路由条目中所对应的接口不同时，认为该数据包有 IP 欺骗行为。 当 NISG 上的接口工作在 “ 透明 ” 模式下时，要应用 IP 地址和 MAC 地址绑定来实现对 IP 欺骗行为的检测。即当接收数据包的接口与其 MAC 地址所对应的接口不同时，认为该数据包有 IP 欺骗行为。

9.2.3. TCP 逃避控制

TCP 逃避的攻击类型、方式及解决措施如表 162 所示。

表 162 TCP 逃避的类型、方式和解决措施

攻击类型	攻击方式	NISG 解决措施
TCP 逃避控制 / 伪造 TCP 重置	TCP RST 数据包用于复位因某种原因引起的错误连接，接收到这种数据包的主机，会清空缓存中已经建立好的连接，如果要继续发送数据，就必须重新开始建立连接。攻击者经常利用这一点，向目标主机发送大量带有虚假源 IP 的 TCP RST 数据包，使该主机中正常的连接被恶意关闭，造成数据丢失和服务中断。	通过检测每个连接在规定的时间间隔内允许通过的最大 RST 数据包个数（即阈值），当达到阈值时，在规定的阻断时间内阻断后续的 RST 数据包，来防止虚假的 TCP RST 数据包对连接造成的破坏和系统资源的损耗。
TCP 逃避控制 /Small PMTU	路径 MTU （Path Maximum Transmission Unit， PMTU）表示因特网上任意一条路径的 MTU。主机可以利用 PMTU Discovery 功能，探测出与目标主机之间的最小 MTU 值，从而确定发送数据包的大小。主机一般根据自身的 MTU 值发出一个 IP 数据包，并且标记该数据包在传输过程中不可分片，当该数据包在传输过程中遇到某一数据链路段的 MTU 值小于该数据包，则该段的路由器会回应给主机一个 ICMP 目的不可达的响应报文，主机会根据这个报文中提供的数据来修改本身的 MTU 值。 Small PMTU 是一种带宽攻击方式，攻击者通过伪造 ICMP 应答包，欺骗受害主机将 MTU 设置成一个较小的值，使目标主机以小包的形式发送大量的数据，进而消耗目标主机的资源，以达到攻击的目的。	通过设置最小 MTU 值，与返回的 ICMP 目标不可达报文中的下一跳 MTU 值进行比较，如果前者大于后者，则丢弃此 ICMP 应答报文。
TCP 逃避控制 /TCP 控制位异常	TCP 控制位异常校验用于在 TCP 连接建立及关闭过程中检查数据包中的 SYN、ACK、FIN 位是否正确置位。TCP 连接的每一个环节数据包包头中的控制位都有着不同的状态，初始建立 TCP 连接时，客户端会向服务端发送带有 SYN 标志的数据包来请求连接，服务端接收到这个包以后会将同时带有 SYN 和 ACK 标志位的数据包回送给客户端，最后客户端发送 ACK 标志数据包确认，以此完成三次握手。结束连接时，会发送带有 FIN 的数据包用来结束一个 TCP 会话。	NISG 会在 TCP 连接的建立和关闭时，检查数据包包头中的控制位是否正确置位，如果控制位的置位有误，则阻断该连接，以防止恶意的攻击和对连接的破坏。

表 162 TCP 逃避的类型、方式和解决措施 (*续*)

攻击类型	攻击方式	NISG 解决措施
TCP 逃避控制 /TCP 数据重叠	当 TCP 数据包在网络中传输时，会由于传输的错误或者人为的修改，使 TCP 数据包中的数据产生重叠，主机接受到这种数据包将会导致系统崩溃。	NISG 可以对数据包中的数据进行校验，系统会自动去掉数据包中重叠的部分。
TCP 保护	TCP 协议本身的一些漏洞可能会被攻击者利用，存在安全隐患。	TCP 保护功能通过校验 TCP 校验和与 TCP 序列号，可有效地对协议应用提供增强的安全保障。 校验 TCP 校验和：探测带有非法校验和的数据包。如果数据包的校验和非法，那么将丢弃该数据包。 校验 TCP 序列号：探测不符合连接状态的数据包。将当前 TCP 数据包的序列号与 TCP 连接状态进行比对，如果数据包匹配 TCP 会话连接但是序列号错误，那么将丢弃该数据包。

9.2.4. IP 选项校验

IP 选项校验的攻击类型、方式及解决措施如表 163 所示。

表 163 IP 选项校验的类型、方式和解决措施

攻击类型	攻击方式	NISG 解决措施
IP 记录路由选项	记录 IP 数据包在传输过程中经过的网络设备的 IP 地址。当目的主机接收到设置了记录路由选项的 IP 数据包后，可以获取其记录的路由信息。 攻击者可以利用记录路由选项的这种特性，对网络进行侦查。如果目标网络中的某台主机已被攻击者控制，那么攻击者向该主机发送设置了记录路由选项的 IP 数据包，就可以提取并利用该数据包所记录的路由信息，了解目标网络的拓扑及编址方案。	接收到设置了记录路由选项的 IP 数据包后，首先根据预先设置的动作对其进行处理。如果 NISG 允许其通过，则再检验其选项格式是否正确。如果格式正确， NISG 需要把转发接口的 IP 地址记录在这个 IP 数据包的记录路由选项中，并将数据包转发；如果格式错误，会将数据包丢弃。
IP 时间戳选项	记录路由器处理数据包的时间，一般在调试网络时用于对路由器的行为进行跟踪。当某个目的主机接收到设置了 IP 时间戳选项的 IP 数据包后，就可以获取该数据包途经路由器的 IP 地址列表，及其在各个路由器之间的传输时间。 攻击者可以利用 IP 时间戳选项的这种特性，来对网络进行探测。如果目标网络中的某台主机已被攻击者控制，那么攻击者向该主机发送设置了 IP 时间戳选项的 IP 数据包，就可以提取并利用该数据包所记录的地址及时间信息，了解目标网络的拓扑及寻址方案。	接收到设置了 IP 时间戳选项的 IP 数据包后，首先根据预先设置的动作对其进行处理。如果 NISG 允许其通过，则再检验其选项格式是否正确。如果格式正确， NISG 需要把时间记录在 IP 时间戳选项中，并将数据包转发；如果格式错误， NISG 会将数据包丢弃。

表 163 IP 选项校验的类型、方式和解决措施 (*续*)

攻击类型	攻击方式	NISG 解决措施
IP 宽松源路由选项	与 IP 严格源路由选项相似，但前者相对于后者对数据包在网络中选路的要求进行了放宽。设置了 IP 宽松源路由选项的数据包必须经过在选项中指定的所有路由器，并按指定的地址顺序前进，但允许数据包经过选项指定范围以外的路由器。 攻击者通常会利用 IP 宽松源路由选项的这种特性，使用所指定的路由来隐藏数据包的真实来源，从而非法获得一些受保护网络的访问权限。	接收到设置了 IP 宽松源路由选项的 IP 数据包后，则首先根据预先设置的动作对其进行处理。如果 NISG 允许其通过，则再检验其选项格式是否正确。如果格式正确， NISG 使用转发出口的 IP 地址来替换选项中对应的 IP 地址，并将数据包转发；如果格式错误， NISG 会将数据包丢弃。
IP 严格源路由选项	使发送端可以预先确定数据包在网络中传输时的路由。这样，发送端根据需要就可以选择延时最小或吞吐量最大的路由，也可以选择更加安全或更加可靠的路由。 设置 IP 严格源路由选项的数据包在选路过程中必须经过其包头选项中指定的所有路由器，且不能经过未指定的路由器。若数据包经过未指定的路由器或到达终点时仍未经过某些指定的路由器，该数据包将会被丢弃。 攻击者通常会利用严格 IP 源路由选项的这种特性，使用所指定的路由来隐藏数据包的真实来源，从而非法获得一些受保护网络的访问权限。	接收到设置了 IP 严格源路由选项的 IP 数据包后，则首先根据预先设置的动作对其进行处理。如果 NISG 允许其通过，则再检验其选项格式是否正确。如果格式正确， NISG 使用转发出口的 IP 地址来替换选项中对应的 IP 地址，并将数据包转发；如果格式错误， NISG 会将数据包丢弃。
IP 跟踪路由选项	用于跟踪一个数据包从源到目的的选路路径。如果一个源主机向某个目的主机发送一个设置了 IP 跟踪路由选项的 ICMP Echo 请求数据包，则该请求包在到达目的主机前经过的每个路由器都会向源主机回应一个 ICMP TraceRoute 数据包。假设从源主机到目的主机共经过了 n（n 为正整数）个路由器，则源主机将接收到 n 个 ICMP TraceRoute 数据包和目的主机回应的 ICMP 应答数据包，从而达到跟踪路由的目的。 如果目的主机回应的 ICMP 应答包同样保留了 IP 跟踪路由选项，则目的主机还可以跟踪该应答包所经过的路由。 攻击者通常会利用 IP 跟踪路由选项的上述特性，来收集目标网络的拓扑和编址方案。	接收到设置了 IP 跟踪路由选项的 IP 数据包后，则首先根据预先设置的动作对其进行处理。如果 NISG 允许其通过，则再检验其选项格式是否正确。如果格式正确， NISG 需要给这个选项数据包的源端发送一个 ICMP TraceRoute 消息，并将数据包转发；如果格式错误， NISG 会将数据包丢弃。
其他 IP 选项	除了以上介绍的几种 IP 选项攻击， NISG 还可以检测并防御携带其他 IP 选项的数据包。	接收到设置了其他 IP 选项的数据包后，首先根据预先设置的动作对其进行处理。如果 NISG 允许其通过，则再检验其选项格式是否正确。如果格式正确， NISG 会将其转发；如果格式错误， NISG 会将其丢弃。
IP 分片与重组	IP 碎片攻击是指攻击者利用数据包重组代码中的漏洞，向目标主机发送内容被恶意篡改的 IP 碎片数据包。当目标主机接收到这些数据包时，由于无法对其进行正确处理，而导致系统出现异常甚至崩溃。	如果 NISG 接收到 IP 碎片数据包，会首先检查其是否合法，对于合法的 IP 碎片数据包， NISG 会将其重组为一个完整的数据包；对于非法的 IP 碎片数据包， NISG 会将其丢弃。从而达到防御 IP 碎片攻击的目的。

9.2.5. ICMP 攻击防御

ICMP 攻击的攻击类型、方式及解决措施如表 164 所示。

表 164 ICMP 的攻击类型、方式和解决措施

攻击类型	攻击方式	NISG 解决措施
ICMP ISS Pinger	互联网安全扫描器 （Internet Security Scanner，ISS），可以扫描主机信息及系统漏洞。	检测到此类攻击时，按照管理员设置的动作进行处理。
ICMP L3retriever Ping	利用 ICMP Echo 方式，发现网络上主机的状态。	检测到此类攻击时，按照管理员设置的动作进行处理。
ICMP Nemesis v1.1 Echo	通过 Nemesis v1.1 软件发送的 ICMP 请求包。	检测到此类攻击时，按照管理员设置的动作进行处理。
ICMP Ping NMAP	网络映射器 （Network Mapper， NMAP）扫描，NMAP 可以快速扫描大型网络及单个主机，发现网络上所运行的主机，获取主机的运行信息。	检测到此类攻击时，按照管理员设置的动作进行处理。
ICMP Icmpenum v1.1.1	用于扫描目标主机的 IP 地址。	检测到此类攻击时，按照管理员设置的动作进行处理。
ICMP Redirect Host	对主机重定向，可以修改主机的路由表，进而影响数据包的发送。	检测到此类攻击时，按照管理员设置的动作进行处理。
ICMP Redirect Net	对网络重定向。	检测到此类攻击时，按照管理员设置的动作进行处理。
ICMP Superscan Echo	利用 Superscan ICMP 请求回显来测试网络中主机的活动状态。	检测到此类攻击时，按照管理员设置的动作进行处理。
ICMP Traceroute IPOPTs	发送 ICMP 包并且对所经过的路径进行记录。	检测到此类攻击时，按照管理员设置的动作进行处理。
ICMP Webtrends Scanner	扫描网络中的主机及其运行状态。	检测到此类攻击时，按照管理员设置的动作进行处理。
ICMP Source Quench	一种流控制信息，攻击者可以利用其造成的低带宽来发动 DoS 攻击。	检测到此类攻击时，按照管理员设置的动作进行处理。
ICMP Broadscan Smurf Scanner	通过发送特定的 ICMP 来扫描网络中活动的主机。	检测到此类攻击时，按照管理员设置的动作进行处理。
ICMP Ping Speedera	使用 Speedera ping 占用主机资源。	检测到此类攻击时，按照管理员设置的动作进行处理。
ICMP TJPingPro1.1Build 2 Windows	可以获取网络中主机的路径。	检测到此类攻击时，按照管理员设置的动作进行处理。
ICMP Ping WhatsUp Gold Windows	可以获取网络中主机的用户名、 IP 地址等信息。	检测到此类攻击时，按照管理员设置的动作进行处理。
ICMP Ping CyberKit 2.2 Windows	可以检测网络连接及记录路由功能。	检测到此类攻击时，按照管理员设置的动作进行处理。
ICMP Ping Sniffer Pro/NetXRay Network Scan	通过发送 ping 来获取网络中活动的主机。	检测到此类攻击时，按照管理员设置的动作进行处理。
ICMP 目标不可达 - 访问被禁止	目标不可访问。	检测到此类攻击时，按照管理员设置的动作进行处理。
ICMP 目标不可达 - 访问目的主机被禁止	目标主机不可访问。	检测到此类攻击时，按照管理员设置的动作进行处理。

表 164 ICMP 的攻击类型、方式和解决措施 (*续*)

攻击类型	攻击方式	NISG 解决措施
ICMP 目标不可达 - 访问目的网络被禁止	目标网络不可访问。	检测到此类攻击时，按照管理员设置的动作进行处理。
ICMP 数据孤岛带宽查询	用于收集连接的网络带宽。	检测到此类攻击时，按照管理员设置的动作进行处理。
ICMP 路径 MTU 拒绝服务攻击	ICMP 协议路径 MTU 拒绝服务，可以获取网络的 MTU，进而发动 DoS 攻击。	检测到此类攻击时，按照管理员设置的动作进行处理。

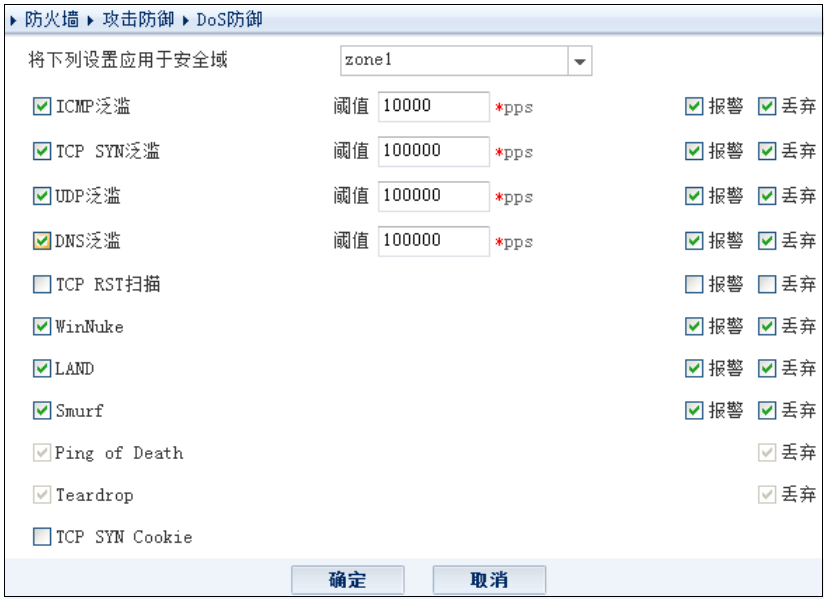
9.3. 基本配置步骤

本节介绍 NISG 中攻击防御的基本配置步骤，包括 WebUI 操作和 CLI。

- 9.3.1. DoS 防御
- 9.3.2. 探测防御
- 9.3.3. TCP 逃避控制
- 9.3.4. IP 选项校验
- 9.3.5. ICMP 攻击防御

9.3.1. DoS 防御

1. 选择**防火墙** > **攻击防御** >**DoS 防御**，进行相关配置。



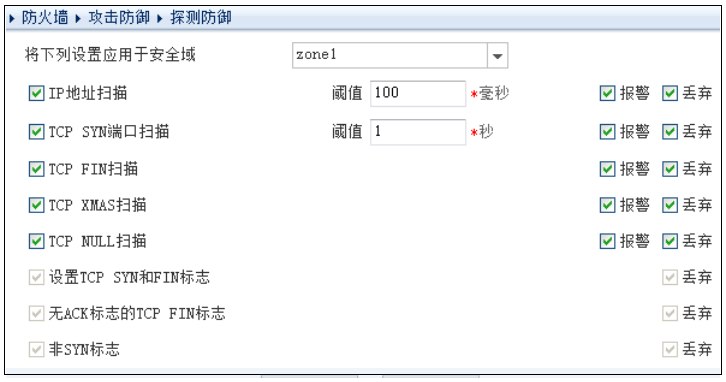
2. 点击**确定**。
3. 点击 。

表 165 DoS 防御相关命令

attack-defense *zone_name* **tcp-syn-cookie active** {**on** | **off**}	启用或禁用指定安全域内 SYN Cookie 的检测和防御。

9.3.2. 探测防御

1. 选择**防火墙** > **攻击防御** > **探测防御**，进行相关配置。



2. 点击**确定**。
3. 点击 。

9.3.3. TCP 逃避控制

1. 选择**防火墙** > **攻击防御** >**TCP 逃避控制**，进行相关配置。

2. 点击**确定**。
3. 点击 。

表 166 TCP 逃避控制相关命令

attack-defense *zone_name* **spoofed-reset**	设置 TCP 逃避控制的伪造重置保护阈值。
attack-defense *zone_name* **small-pmtu parameter** *threshold_value*	设置 TCP 逃避控制的最小 MTU 值。
attack-defense *zone_name* **tcp-checksum** [**alert**]	启用或禁用对带有非法校验和的数据包的报警功能。
attack-defense tcp-sequence-track	设置 TCP 序列号检验功能。

9.3.4. IP 选项校验

1. 选择**防火墙** > **攻击防御** >**IP 选项校验**，进行相关配置。

2. 点击**确定**。
3. 点击 。

表 167 IP 选项校验相关命令

customize-the-size-of-IP-datagrams-to-send active {on | off} threshold *threshold_ip_datagram*	启用或禁用自定义重组后发送数据包大小功能并设置阈值。
show customize-the-size-of-IP-datagrams-to-send	查看自定义重组后发送的数据包大小功能的设置。

9.3.5. ICMP 攻击防御

1. 选择**防火墙 > 攻击防御 >ICMP 攻击防御**，进行相关配置。

2. 点击**确定**。
3. 点击 。

9.4. 配置参数说明

- 9.4.1. DoS 防御参数
- 9.4.2. ICMP 防御参数
- 9.4.3. IP 选项校验参数
- 9.4.4. 探测防御参数
- 9.4.5. TCP 逃避控制

9.4.1. DoS 防御参数

下表是 NISG 中 DoS 防御相关参数。

表 168 DoS 防御参数

攻击防御类型	启用	报警	丢弃	阈值 范围 / 默认值	其他参数
ICMP 泛滥	Y/N	Y/N	Y/N	1 - 1,000,000 pps / 10,000	
TCP SYN 泛滥	Y/N	Y/N	Y/N	1 - 1,000,000 pps / 100,000	
UDP 泛滥	Y/N	Y/N	Y/N	1 - 1,000,000 pps / 100,000	
DNS 泛滥	Y/N	Y/N	Y/N	1 - 1,000,000 pps / 100,000	
TCP RST 扫描	Y/N	Y/N	Y/N		
WinNuke	Y/N	Y/N	Y/N		
LAND	Y/N	Y/N	Y/N		
Smurf	Y/N	Y/N	Y/N		IPv6 中不存在广播地址，所以 IPv6 中没有 Smurf 攻击。
Ping of Death	Y		Y		
Teardrop	Y		Y		
TCP SYN Cookies	Y/N				

9.4.2. ICMP 防御参数

下表是 NISG 中 ICMP 防御相关参数。

表 169 ICMP 相关参数

攻击防御类型	启用	报警	丢弃	阈值 范围 / 默认值	其他参数
ICMP ISS Pinger	Y/N	Y/N	Y/N		
ICMP L3retriever Ping	Y/N	Y/N	Y/N		
ICMP Nemesis v1.1 Echo	Y/N	Y/N	Y/N		
ICMP Ping NMAP	Y/N	Y/N	Y/N		
ICMP Icmpenum v1.1.1	Y/N	Y/N	Y/N		
ICMP Redirect Host	Y/N	Y/N	Y/N		
ICMP Redirect Net	Y/N	Y/N	Y/N		
ICMP Superscan Echo	Y/N	Y/N	Y/N		
ICMP Traceroute IPOPTs	Y/N	Y/N	Y/N		
ICMP Webtrends Scanner	Y/N	Y/N	Y/N		
ICMP Source Quench	Y/N	Y/N	Y/N		
ICMP Broadscan Smurf Scanner	Y/N	Y/N	Y/N		
ICMP Ping Speedera	Y/N	Y/N	Y/N		
ICMP TJPingPro1.1Build 2 Windows	Y/N	Y/N	Y/N		
ICMP Ping Whatsup Gold Windows	Y/N	Y/N	Y/N		
ICMP Ping CyberKit 2.2 Windows	Y/N	Y/N	Y/N		
ICMP Ping Sniffer Pro/ NetXRay Network Scan	Y/N	Y/N	Y/N		
ICMP 目标不可达 - 访问被禁止	Y/N	Y/N	Y/N		
ICMP 目标不可达 - 访问目的主机被禁止	Y/N	Y/N	Y/N		
ICMP 目标不可达 - 访问目的网络被禁止	Y/N	Y/N	Y/N		
ICMP 数据孤岛带宽查询	Y/N	Y/N	Y/N		
ICMP 路径 MTU 拒绝服务攻击	Y/N	Y/N	Y/N		

9.4.3. IP 选项校验参数

下表是 NISG 中 IP 选项校验相关参数。

表 170 IP 选项校验参数

攻击防御类型	启用	报警	丢弃	阈值 范围 / 默认值	其他参数
IP 记录路由选项	Y/N	Y/N	Y/N		
IP 时间戳选项	Y/N	Y/N	Y/N		
IP 严格源路由选项	Y/N	Y/N	Y/N		
IP 宽松源路由选项	Y/N	Y/N	Y/N		
IP 跟踪路由选项	Y/N	Y/N	Y/N		
其他 IP 选项	Y/N	Y/N	Y/N		
IP 分片	Y				
IP 重组	Y				
自定义待发送 IP 报文的大小	Y/N			30-1460/ 1400 字节	

9.4.4. 探测防御参数

下表是 NISG 中探测防御相关参数。

表 171 探测防御参数

攻击防御类型	启用	报警	丢弃	阈值 范围 / 默认值	其他参数
IP 地址扫描	Y/N	Y/N	Y/N	100 - 10,000 毫秒 （100 的整数倍） / 100	
TCP SYN 端口扫描	Y/N	Y/N	Y/N	1 - 7,200 秒 / 1	
TCP FIN 扫描	Y/N	Y/N	Y/N		
TCP XMAS 扫描	Y/N	Y/N	Y/N		
TCP NULL 扫描	Y/N	Y/N	Y/N		
设置 TCP SYN 和 FIN 标志	Y		Y		
无 ACK 标志的 TCP FIN 标志	Y		Y		
非 SYN 标志	Y		Y		

9.4.5. TCP 逃避控制

下表是 NISG 中 TCP 逃避控制相关参数。

表 172 TCP 逃避控制参数

攻击防御类型	启用	报警	丢弃	阈值 范围 / 默认值	其他参数
伪造 TCP 重置	Y/N	Y/N	Y/N	2 - 10,000 / 5	时间间隔 = 2 - 10,000 秒 / 15 阻断间隔 = 2 - 10,000 秒 / 120
Small PMTU	Y/N	Y/N	Y/N	68 - 512 字节 / 350	
TCP 控制位异常	Y		Y		
TCP 数据重叠	Y		Y		
校验 TCP 校验和	Y	Y/N	Y		
校验 TCP 序列号	Y	Y/N	Y		探测不符合连接状态的数据包。将当前 TCP 数据包的序列号与 TCP 连接状态进行比对，如果数据包匹配 TCP 会话连接但是序列号错误，那么将丢弃该数据包。管理员可以配置对如下数据包进行探测。 • 所有：对所有数据包进行不符合连接状态探测，并记录序列校验对数据包采用的每个处理动作（包括 ACK 号正确但序列号错误的非 RST 数据包）。 • 异常 ：对异常数据包进行不符合连接状态探测，并只记录导致丢包并有攻击可能的重大事件 （包括无效的 ACK 号和无效的序列号）。 • 可疑 ：对可疑数据包进行不符合连接状态探测，并只记录导致丢包的重大事件 （包括不同序列的 SYN 重传和不同窗口扩展的 SYN/SYN-ACK 重传）。

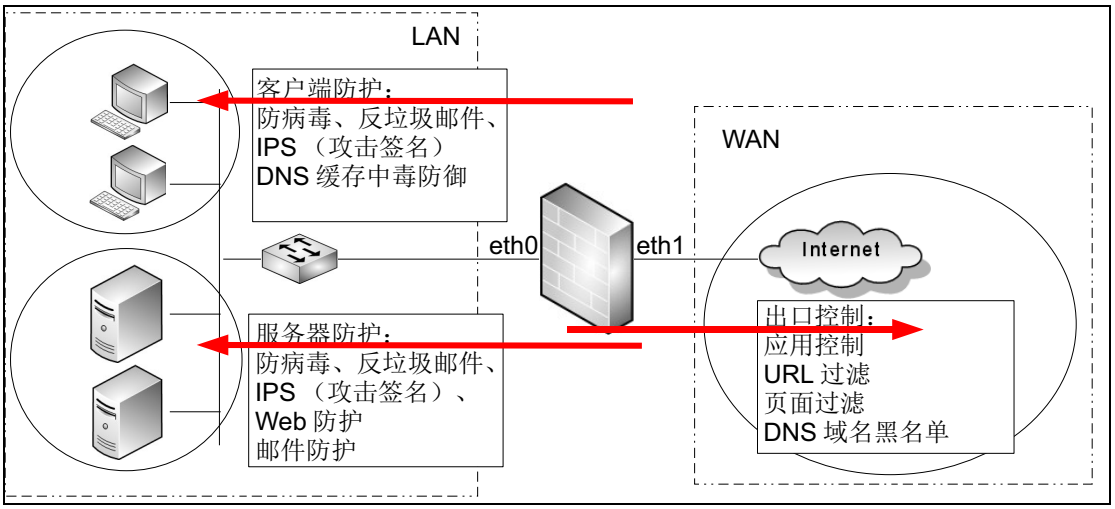
10 统一威胁管理

本章介绍统一威胁管理 （Unified Threat Management， UTM）功能。

- 10.1. 概述，描述 UTM 的基本概念。
- 10.2. 基本配置步骤，介绍 UTM 特性的基本配置步骤。用户场景不需要配置所有步骤。
- 10.3.UTM 范例，给出详细的范例配置步骤。
- 10.4. 配置参数说明，详细描述 UTM 配置参数。
- 10.5.UTM 缺省设置，列出 UTM 功能模块的一些缺省设置。

10.1. 概述

图 37 UTM 典型应用场景



UTM 提供三种安全策略：

- 10.1.1. 出口控制
- 10.1.2. 客户端防护
- 10.1.3. 服务器防护

如果数据包匹配到任意一种安全策略，将进行相应的 UTM 检测，包括：

- 协议识别。
- 依照 RFC 规范进行协议异常检测。
- 根据用户配置进行协议限制 （协议限制的优先级高于协议异常检测。当用户配置和 RFC 规范冲突时，以用户配置为准）。
- 对数据包进行内容级检测。

UTM 对客户端和服务器的防护包括：

- 10.1.2.3. 防病毒
- 10.1.2.4. 反垃圾邮件
- 10.1.2.2.IPS

UTM 还支持：

- 实时更新应用知识库、 URL 分类、防病毒规则、反垃圾邮件规则和攻击签名规则。
- 当 UTM 检测到病毒、垃圾邮件或攻击时，返回给客户端通知消息。
- 监控。参见第 14 章 , 监控。

10.1.1. 出口控制

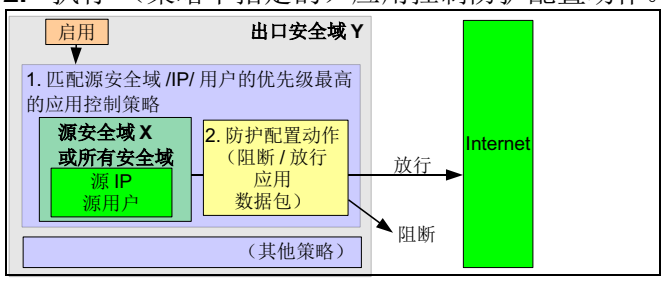
出口控制针对出口安全域阻断来自多个内网安全域的非法流量。

- 10.1.1.1. 应用数据包处理流程
- 10.1.1.2. HTTP 数据包处理流程
- 10.1.1.3. DNS 数据包处理流程

10.1.1.1. 应用数据包处理流程

UTM 出口控制中，应用数据包处理流程如下图所示：

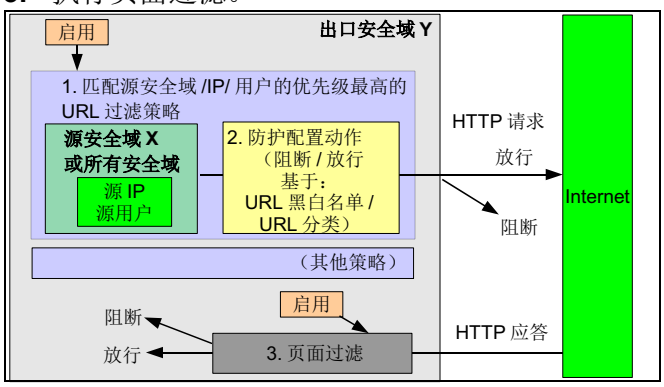
1. 根据源安全域 /IP/ 用户确定优先级最高的匹配策略。
2. 执行 （策略中指定的）应用控制防护配置动作。



10.1.1.2. HTTP 数据包处理流程

UTM 出口控制提供 URL 过滤 （针对 HTTP 请求）和页面过滤 （针对 HTTP 响应）功能， HTTP 数据包处理流程如下图所示：

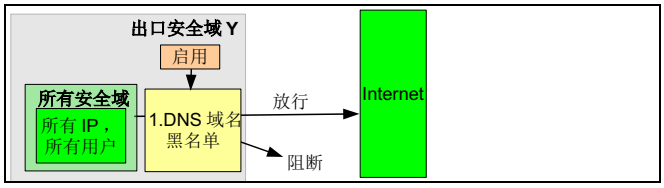
1. 根据源安全域 /IP/ 用户确定优先级最高的匹配策略。
2. 执行 （策略中指定的） URL 过滤防护配置动作。
3. 执行页面过滤。



10.1.1.3. DNS 数据包处理流程

UTM 出口控制提供 DNS 域名黑名单过滤 DNS 请求。 DNS 数据包处理流程如下所示：

1. 阻断匹配黑名单的 DNS 请求。



10.1.2. 客户端防护

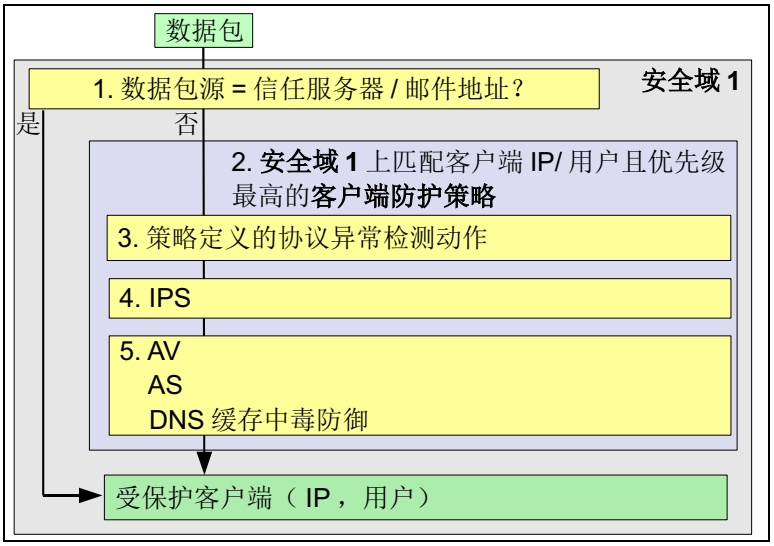
UTM 针对每安全域开启客户端防护功能，阻断到指定客户端 IP/ 用户的非法流量。

- 10.1.2.1. 基本步骤
- 10.1.2.2. IPS
- 10.1.2.3. 防病毒
- 10.1.2.4. 反垃圾邮件

10.1.2.1. 基本步骤

UTM 客户端防护数据包处理流程如下图所示：

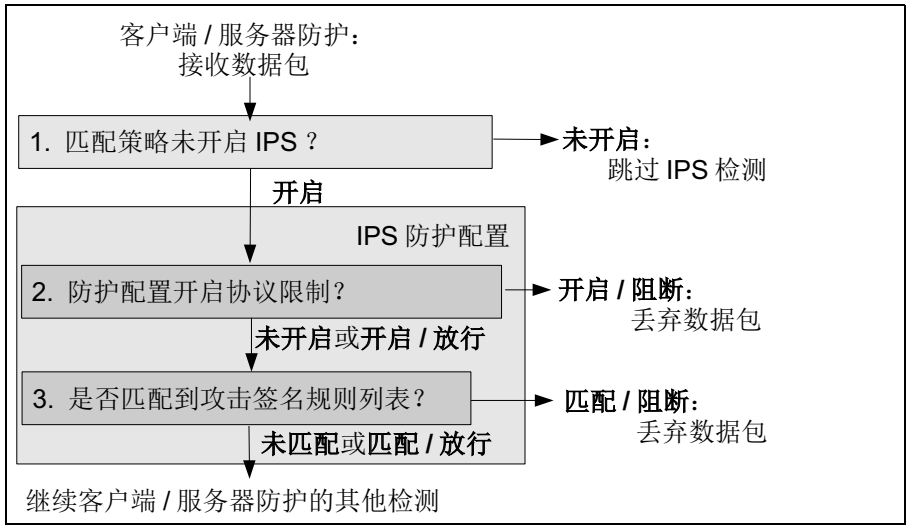
1. 如果来自信任服务器或邮件地址 （每安全域定义）：放行。
2. 根据客户端 IP/ 用户确定目的安全域上优先级最高的匹配策略。
3. 执行协议异常检测 （策略中定义）。
4. 执行 （策略中指定的） IPS 防护配置动作，参见 10.1.2.2. IPS。
5. 根据协议不同，选择执行 AV 扫描、 AS 检测或 DNS 缓存中毒防御检测。
   - 对于 POP3、IMAP、FTP 或 HTTP 协议数据包，执行（策略中指定的）AV 防护配置动作 （如果来自 AV 信任源：跳过 AV 扫描），参见 10.1.2.3. 防病毒。
   - 对于 POP3 协议数据包，执行（策略中指定的）AS 防护配置动作（如果匹配 AS 允许列表：跳过 AS 检测；如果匹配 AS 阻断列表：丢弃数据包；如果未匹配允许 / 阻断列表：匹配自定义垃圾邮件关键字列表），参见 10.1.2.4. 反垃圾邮件。
   - 对于 DNS 协议数据包，执行 DNS 缓存中毒防御动作 （全局配置）。



10.1.2.2. IPS

IPS 定义攻击签名检测和协议限制，并且需要在客户端 / 服务器防护策略中指定。 IPS 数据包处理流程如下图所示：

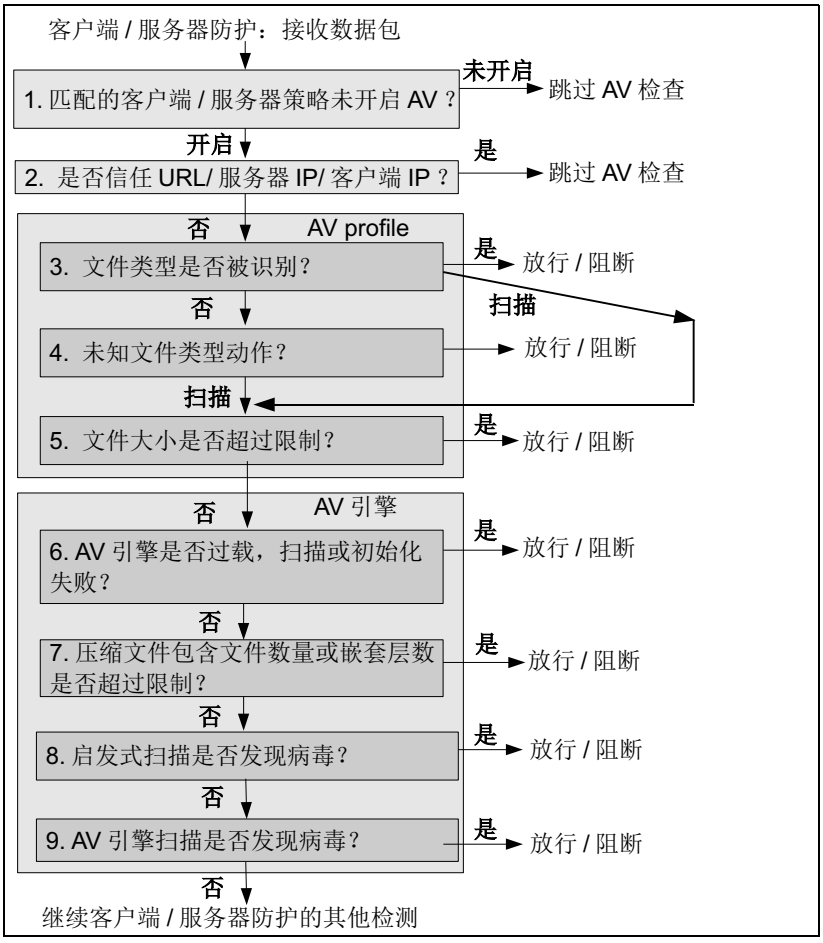
1. 如果策略中未开启 IPS：忽略 IPS 检测。
2. 如果防护配置中开启协议限制，指定客户端 / 服务器类型的协议限制。如果匹配限制条件，则根据管理员最后选择的协议限制级别中定义的动作进行放行或阻断。
3. 如果匹配到攻击签名规则列表，则根据防护配置中定义的规则动作放行或阻断。



10.1.2.3. 防病毒

防病毒在客户端 / 服务器防护中指定。防病毒数据包处理流程如下图所示：

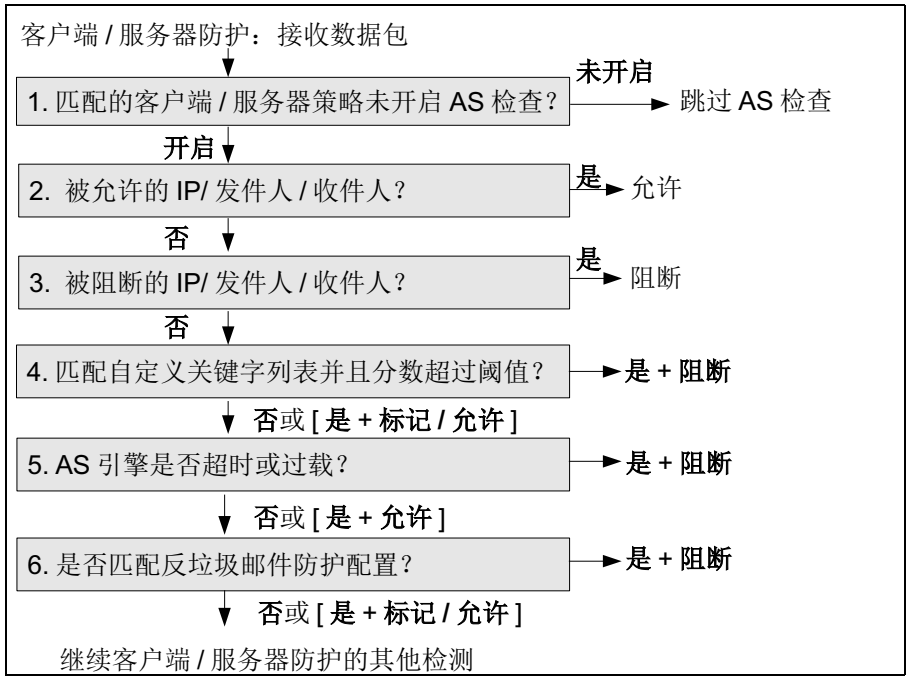
1. 如果策略中未开启防病毒，则跳过防病毒扫描。
2. 如果来自信任 URL、 Web 服务器或客户端，则直接放行文件，不进行病毒扫描。
3. 如果匹配到文件类型，则根据防护配置中定义的动作放行、阻断或扫描。
4. 如果文件类型不可识别，则根据防护配置中定义的动作放行、阻断或扫描。
5. 如果文件大小超过扫描限制，则根据防护配置中定义的动作放行或阻断。
6. 如果 AV 引擎过载、扫描失败、初始化失败，则根据扫描设置放行或阻断文件。
7. 如果检测到压缩文件并且压缩文件大小超出限制，则根据压缩文件扫描设置放行或阻断。
8. 如果开启了启发式扫描并且检测到病毒，则根据启发式扫描中设置放行或阻断文件。
9. 如果 AV 引擎检测到病毒，则根据扫描设置放行或阻断文件。



10.1.2.4. 反垃圾邮件

反垃圾邮件在客户端 / 服务器防护中指定。反垃圾邮件数据包处理流程如下图所示：

1. 如果策略中未开启反垃圾邮件，则跳过反垃圾邮件检测。
2. 如果匹配到反垃圾邮件 IP/ 发件人 / 收件人允许列表：放行邮件。
3. 如果匹配到反垃圾邮件 IP/ 发件人 / 收件人阻断列表：阻断邮件。
4. 如果匹配到自定义垃圾邮件关键字列表并且分数超出阈值，则根据匹配动作阻断或放行邮件 （也可选择标记邮件）。
5. 如果反垃圾邮件引擎超时或过载，则根据匹配动作放行 （不经扫描直接放行）或阻断邮件。
6. 如果匹配到反垃圾邮件防护配置，则根据匹配动作阻断或放行邮件 （也可选择标记邮件）。



10.1.3. 服务器防护

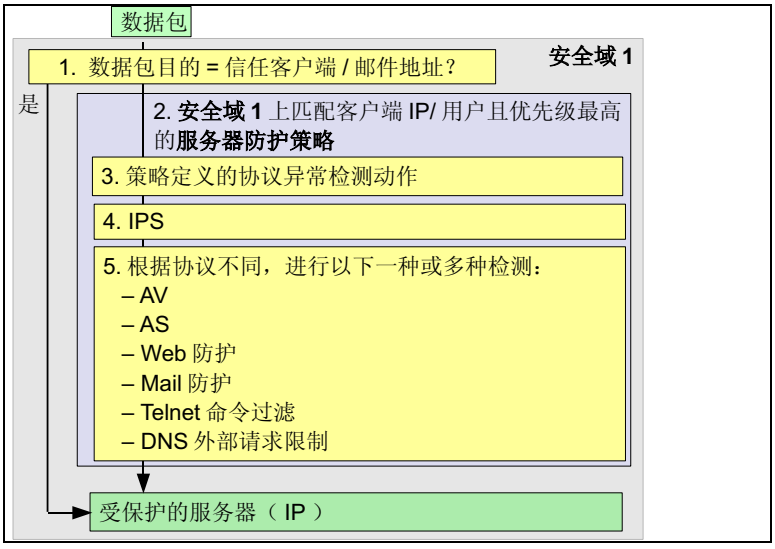
服务器防护只保护客户端发往指定安全域中服务器的流量，如上传和发邮件等。

- 10.1.2.1. 基本步骤
- 10.1.3.2. IPS，防病毒和反垃圾邮件 （同客户端防护）

10.1.3.1. 基本步骤

UTM 服务器防护数据包处理流程如下图所示：

1. 如果来自信任客户端或邮件地址 （每安全域定义）：放行。
2. 根据服务器 IP 地址，确定目的安全域上优先级最高的匹配策略。
3. 执行协议异常检测 （策略中定义）。
4. 执行 IPS 检测 （在 IPS 防护配置中指定），包括协议限制和攻击签名检测，参见 10.1.2.2. IPS。
5. 根据协议不同，选择执行以下一种或多种检测：
   - 对于 SMTP 或 FTP 协议数据包，执行防病毒扫描。如果来自 AV 信任源：跳过防病毒扫描。执行 （策略中指定的）AV 防护配置动作。具体参见 10.1.2.3. 防病毒。
   - 对于 SMTP 协议数据包，执行反垃圾邮件检测。如果匹配到 AS 允许列表：跳过反垃圾邮件检测。如果匹配到 AS 阻断列表：丢弃数据包。执行 AS 关键字列表 （全局配置）动作。执行 （策略中指定的）AS 防护配置动作。具体参见 10.1.2.4. 反垃圾邮件。
   - 对于 HTTP 协议数据包，执行 Web 防护 （全局配置）动作。
   - 对于 SMTP 协议数据包，执行邮件防护 （全局配置）动作。
   - 对于 Telnet 协议数据包，执行 Telnet 命令过滤。（策略中定义）
   - 对于 DNS 协议数据包，执行 DNS 外部请求限制。（策略中定义）



10.1.3.2. IPS，防病毒和反垃圾邮件

同客户端防护。

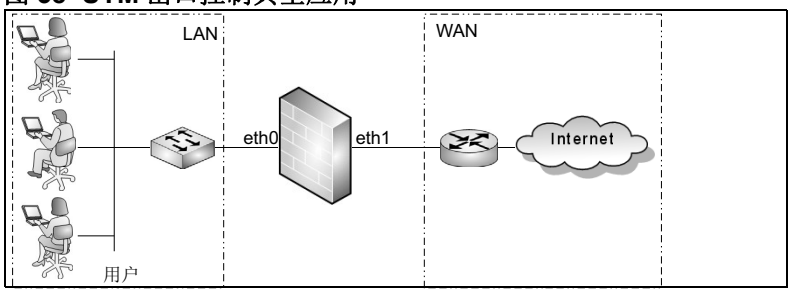
10.1.4. 应用场景

出口控制、客户端防护和服务器防护的典型应用场景如下所示。

场景 1：出口控制

如下图所示，安全域 LAN 包含以太网接口 eth0、 WAN 包含 eth1，公司想控制内网用户到 Internet 的访问流量。那么，您可以通过 NISG 的应用控制、 URL 过滤、 DNS 域名黑名单和页面过滤功能实现该目的。

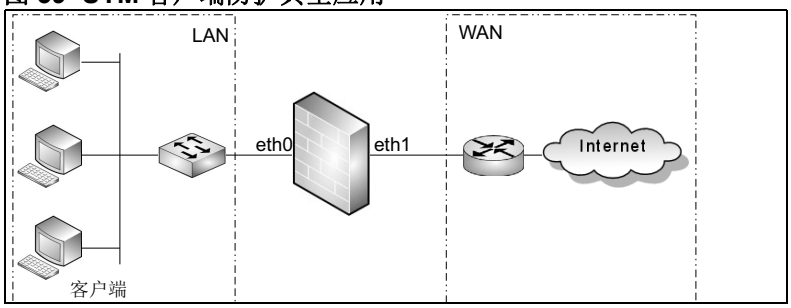
图 38 UTM 出口控制典型应用



场景 2：客户端防护

如下图所示，NISG 上有两个安全域 LAN 和 WAN，LAN 包含以太网接口 eth0、WAN 包含 eth1，公司想保护 LAN 内的客户端不受外网威胁。那么，您可以在 LAN 上配置客户端防护功能来实现该目的。

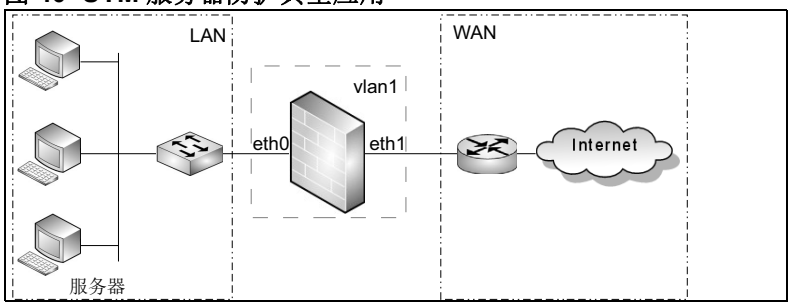
图 39 UTM 客户端防护典型应用



场景 3：服务器防护

如下图所示，NISG 上有两个安全域 LAN 和 WAN，LAN 包含以太网接口 eth0、WAN 包含 eth1，公司想保护 LAN 内的服务器不受外网威胁。那么，您可以在 LAN 上配置服务器防护功能来实现该目的。

图 40 UTM 服务器防护典型应用



10.2. 基本配置步骤

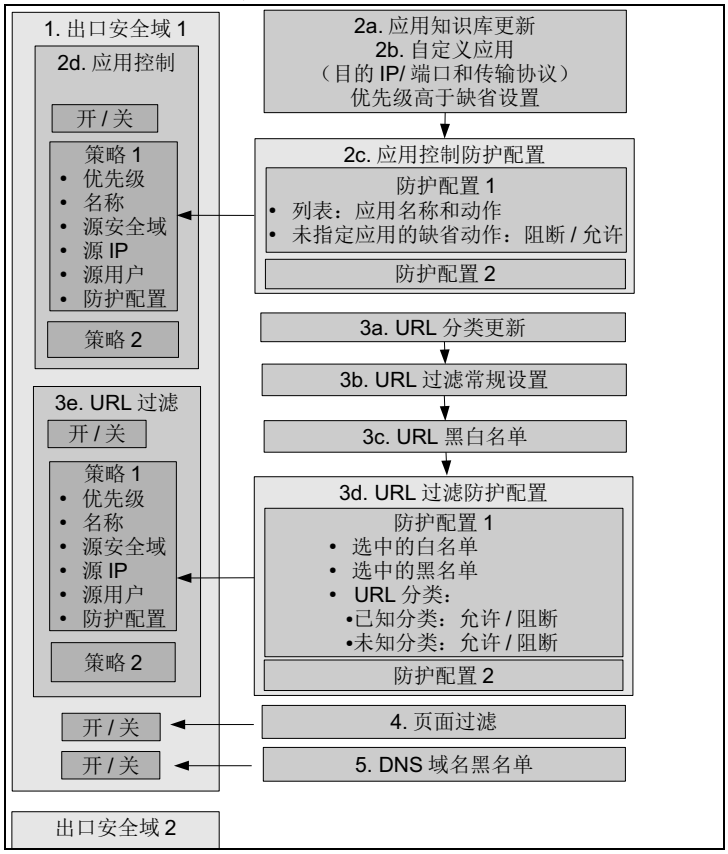
本节描述以下功能的基本配置步骤：

- 10.2.1. 出口控制
- 10.2.2. 客户端防护
- 10.2.3. 服务器防护
- 10.2.4. 通知消息
- 10.2.5. 概要信息页面

提示：UTM 只能通过 WebUI 进行配置，不支持 CLI。

10.2.1. 出口控制

图 41 出口控制配置步骤



基本设置：

- 10.2.1.1. 创建安全域 / 访问策略 / 缺省路由 /NAT 规则

出口控制配置：

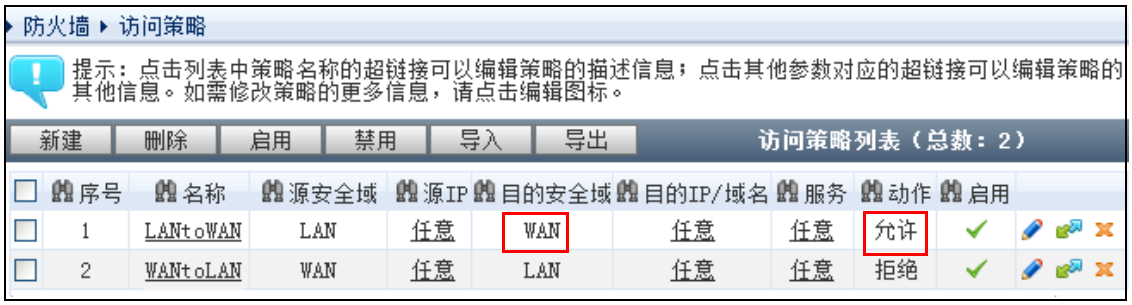
- 10.2.1.2. 配置应用控制：
  - 10.2.1.2.1. 更新应用知识库 （2a）
  - 10.2.1.2.2. 添加自定义应用 （2b）
  - 10.2.1.2.3. 创建应用控制防护配置 （2c）
  - 10.2.1.2.4. 创建应用控制策略 （2d）
- 10.2.1.3. 配置 （HTTP 请求） URL 过滤：
  - 10.2.1.3.1. 更新 URL 分类库 （3a）
  - 10.2.1.3.2. 配置 URL 过滤常规设置 （3b）
  - 10.2.1.3.3. 创建 URL 过滤防护配置：黑白名单 （3c）
  - 10.2.1.3.4. 创建 URL 过滤动作防护配置 （3d）
  - 10.2.1.3.5. 创建 URL 过滤策略 （3e）
- 10.2.1.4. 配置 （HTTP 应答）页面过滤
- 10.2.1.5. 配置 DNS 域名黑名单

10.2.1.1. 创建安全域 / 访问策略 / 缺省路由 /NAT 规则

出口控制用于控制一个出口安全域和多个入口安全域之间的流量。根据需要创建安全域、访问策略、缺省路由和 NAT 规则。详细信息请参见 4.12 安全域， 8.2.2 创建访问策略， 5.2.1 单播和 6.2.1 创建 SNAT 规则。

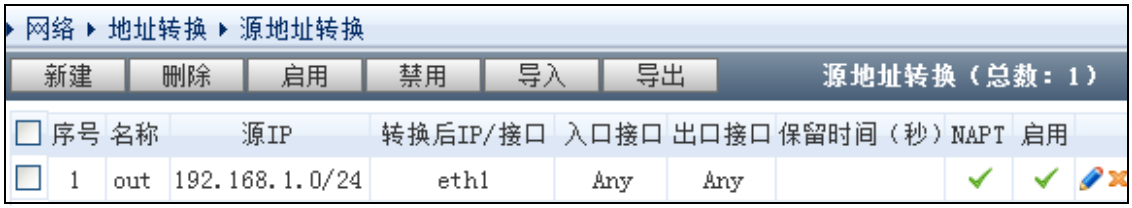
1. 选择**网络 > 安全域**，创建安全域（至少创建一个出口安全域）。下图中 LAN 是入口安全域，WAN 是出口安全域。

2. 选择**防火墙 > 访问策略**，创建访问策略允许内网到外网的访问。



3. 选择**网络 > 路由 > 缺省路由**，根据需要添加缺省路由。

4. 如果NISG工作在路由模式，选择**网络>地址转换>源地址转换**，添加如下源地址转换规则：



10.2.1.2. 配置应用控制

- 10.2.1.2.1. 更新应用知识库 （2a）
- 10.2.1.2.2. 添加自定义应用 （2b）
- 10.2.1.2.3. 创建应用控制防护配置 （2c）
- 10.2.1.2.4. 创建应用控制策略 （2d）

10.2.1.2.1. 更新应用知识库 （2a）

详细信息请参见 10.4.2.2.4. （应用知识库）更新。

1. 选择 **UTM> 出口控制 > 应用控制 > 更新**。

2. 根据需要选择手动更新或从 Internet 更新。

10.2.1.2.2. 添加自定义应用 （2b）

详细信息请参见 10.4.2.2.3. 应用知识库和 10.4.2.2.2. 自定义应用。

1. 选择 **UTM> 出口控制 > 应用控制 > 应用知识库**。
2. 根据分类、技术、风险等级和 / 或应用名称查找应用。当鼠标指向应用名称时，会出现该应用的描述信息。

3. 选择 **UTM> 出口控制 > 应用控制 > 自定义应用**。
4. 根据需要添加自定义应用，自定义条件主要包括 IP 地址、协议和端口。

提示：添加页面**应用**下拉框支持自动补齐。例如，如果您输入字母 G，下拉框将显示所有名称以 G 开头的应用供您选择。

10.2.1.2.3. 创建应用控制防护配置 （2c）

详细信息请参见 10.4.2.2.1. （应用控制）防护配置。

1. 选择 **UTM> 出口控制 > 应用控制 > 防护配置**。
2. 点击**新建**，创建应用控制防护配置：
   a. 通过过滤条件或应用名称添加应用。

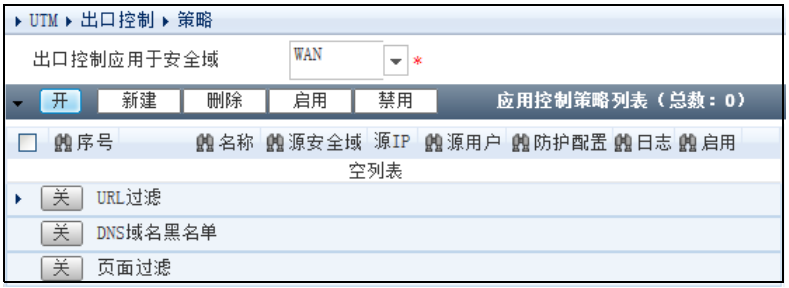
   b. 点击**确定**，将应用添加到新建防护配置中。

   c. 点击**确定**，查看新建防护配置。可点击 克隆已有防护配置。

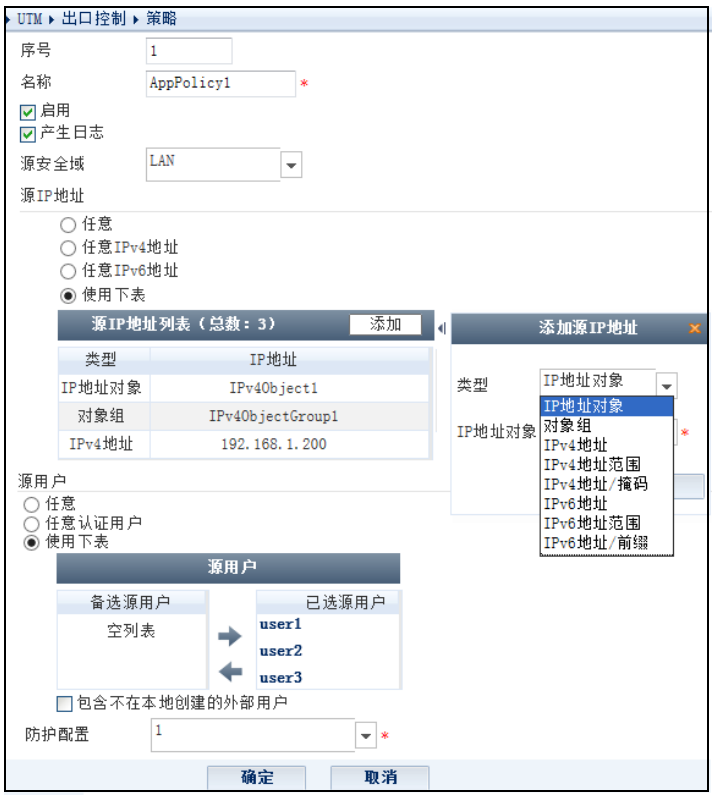
10.2.1.2.4. 创建应用控制策略 （2d）

详细信息请参见 10.4.2.1.1. 应用控制策略。

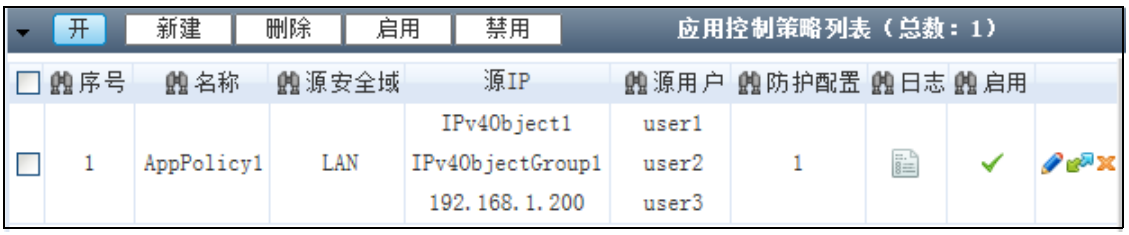
1. 选择 **UTM> 出口控制 > 策略**。
2. 选择出口安全域，开启应用控制功能。



3. 点击**应用控制**展开配置区域，点击**新建**，创建应用控制策略。



4. 点击**确定**。



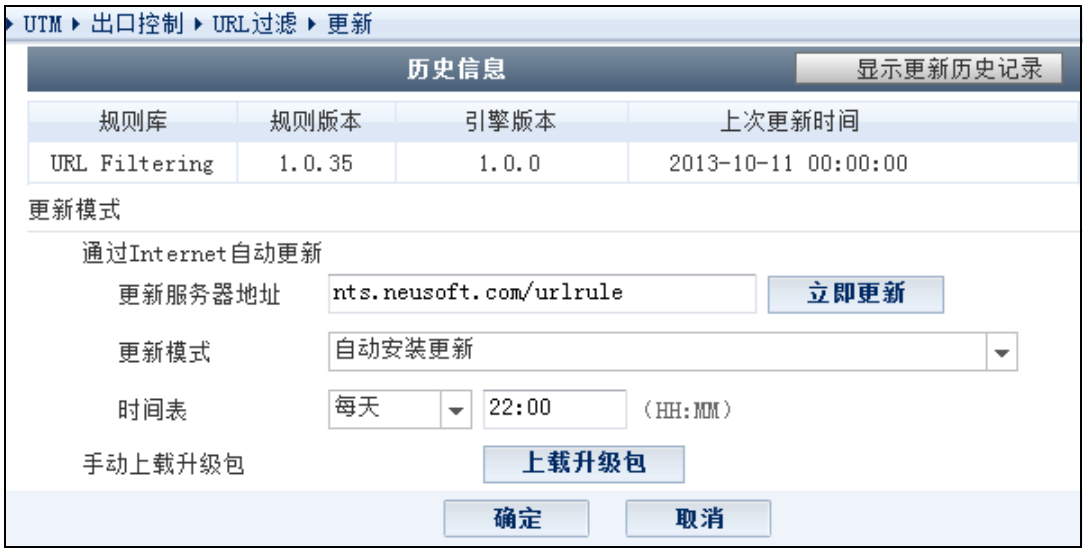
10.2.1.3. 配置 （HTTP 请求） URL 过滤

- 10.2.1.3.1. 更新 URL 分类库 （3a）
- 10.2.1.3.2. 配置 URL 过滤常规设置 （3b）
- 10.2.1.3.3. 创建 URL 过滤防护配置：黑白名单 （3c）
- 10.2.1.3.4. 创建 URL 过滤动作防护配置 （3d）
- 10.2.1.3.5. 创建 URL 过滤策略 （3e）

10.2.1.3.1. 更新 URL 分类库 （3a）

详细信息请参见 10.4.2.3.4. （URL 分类）更新。

1. 选择 **UTM> 出口控制 >URL 过滤 > 更新**。

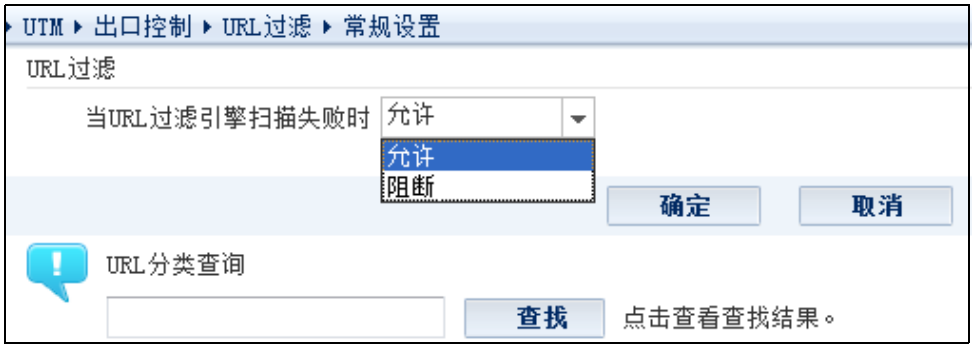


2. 根据需要选择手动更新或从 Internet 更新。

10.2.1.3.2. 配置 URL 过滤常规设置 （3b）

详细信息请参见 10.4.2.3.1. （URL 过滤）常规设置。

1. 选择 **UTM> 出口控制 >URL 过滤 > 常规设置**，设置 URL 过滤引擎失败时的动作。



2. 点击**确定**。
3. 根据需要查询 URL 分类。

10.2.1.3.3. 创建 URL 过滤防护配置：黑白名单 （3c）

详细信息请参见 10.4.2.3.3.URL 黑白名单。

1. 选择 **UTM> 出口控制 >URL 过滤 > 黑白名单**。
2. 点击**新建**，创建 URL 白名单：

3. 点击**确定**。
4. 点击**新建**，创建 URL 黑名单。

d. 点击**确定**，查看新建防护配置。可点击 克隆已有黑白名单。

10.2.1.3.4. 创建 URL 过滤动作防护配置 （3d）

详细信息请参见 10.4.2.3.2. （URL 过滤）防护配置。

1. 选择 **UT> 出口控制 >URL 过滤 > 防护配置**。

2. 点击**新建**，创建 URL 过滤防护配置。

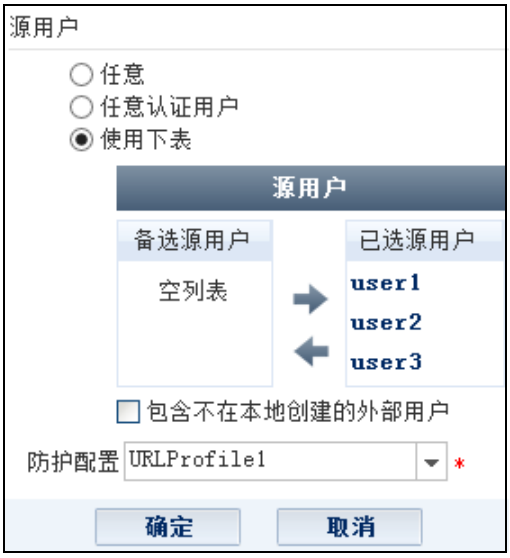
3. 点击**确定**，查看新建防护配置。可点击 克隆已有防护配置创建新的防护配置。

10.2.1.3.5. 创建 URL 过滤策略 （3e）

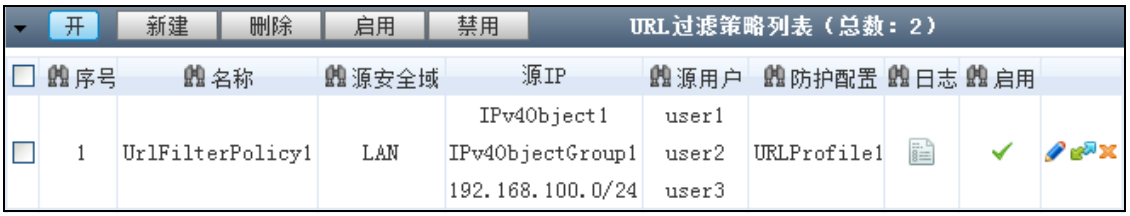
详细信息请参见 10.4.2.1.2.URL 过滤策略。

1. 选择 **UTM> 出口控制 > 策略**。
2. 选择出口安全域，开启 URL 过滤功能。

3. 点击 **URL 过滤**展开配置区域，点击**新建**，创建 URL 过滤策略。



4. 点击**确定**。



10.2.1.4. 配置 （HTTP 应答）页面过滤

详细信息请参见 10.4.2.5. 页面过滤。

1. 选择 **UTM> 出口控制 > 页面过滤**。
2. 配置页面过滤功能阻断含有指定关键字的 HTTP 响应页面。

3. 点击**确定**。
4. 选择 **UTM> 出口控制 > 策略**。
5. 选择出口安全域，开启页面过滤功能。

10.2.1.5. 配置 DNS 域名黑名单

详细信息请参见 10.4.2.4.DNS 域名黑名单。

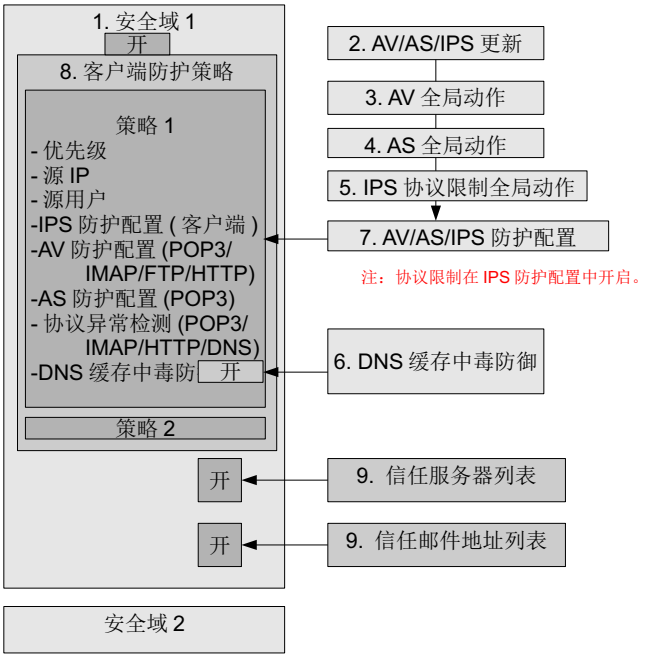
1. 选择 **UTM> 出口控制 >DNS 域名黑名单**。
2. 配置 DNS 域名黑名单。

3. 点击**确定**。
4. 选择 **UTM> 出口控制 > 策略**。
5. 选择出口安全域，开启 DNS 域名黑名单功能。

10.2.2. 客户端防护

客户端配置步骤如下图所示：

图 42 客户端防护配置步骤



基本设置：

- 10.2.2.1. 创建安全域 / 访问策略 / 缺省路由 /NAT 规则

常规设置 （AV/AS/IPS 规则更新）：

- 10.2.2.2. 更新 AV/AS/IPS 规则

全局动作：

- 10.2.2.3. 配置 AV 全局动作 （信任列表 / 病毒检测动作 / 启发式扫描 / 扫描限制）
- 10.2.2.4. 配置 AS 全局动作 （允许 / 阻断列表，关键字列表，扫描设置）
- 10.2.2.5. 配置 IPS SMTP/POP3/IMAP/DNS 协议限制 （客户端）
- 10.2.2.6. 配置 DNS 缓存中毒防御全局动作

动作防护配置：

- 10.2.2.7. 创建 AV/AS/IPS 防护配置

目的安全域动作和策略：

- 10.2.2.8. 创建客户端防护策略
- 10.2.2.9. 创建信任服务器 / 邮件列表

10.2.2.1. 创建安全域 / 访问策略 / 缺省路由 /NAT 规则

1. 选择**网络 > 安全域**，创建客户端防护安全域。详细信息请参见 4.12 安全域。
2. 选择**防火墙 > 访问策略**，创建访问策略。详细信息请参见 8.2.2 创建访问策略。
3. 选择**网络 > 路由 > 缺省路由**，修改缺省路由。详细信息请参见 5.2.1 单播。
4. 如果 NISG 工作在路由模式，选择**网络 > 地址转换 > 源地址转换**，添加源地址转换规则。详细信息请参见 6.2.1 创建 SNAT 规则。

10.2.2.2. 更新 AV/AS/IPS 规则

- 10.2.2.2.1. 更新防病毒规则
- 10.2.2.2.2. 更新反垃圾邮件规则
- 10.2.2.2.3. 更新攻击签名规则

10.2.2.2.1. 更新防病毒规则

更新防病毒规则库。详细信息请参见 10.4.5.6. （防病毒规则）更新。

1. 选择 **UTM> 防病毒 > 更新**。
2. 根据需要手动更新或从 Internet 更新。

10.2.2.2.2. 更新反垃圾邮件规则

更新反垃圾邮件规则库。详细信息请参见 10.4.6.6.（反垃圾邮件规则）更新。

1. 选择 **UTM> 反垃圾邮件 > 更新**。
2. 根据需要手动更新或从 Internet 更新。

10.2.2.2.3. 更新攻击签名规则

更新攻击签名规则库。详细信息请参见 10.4.7.3.（攻击签名规则）更新。

1. 选择 **UTM>IPS> 更新**。
2. 根据需要手动更新或从 Internet 更新。

10.2.2.3. 配置 AV 全局动作 （信任列表 / 病毒检测动作 / 启发式扫描 / 扫描限制）

配置以下防病毒全局设置：

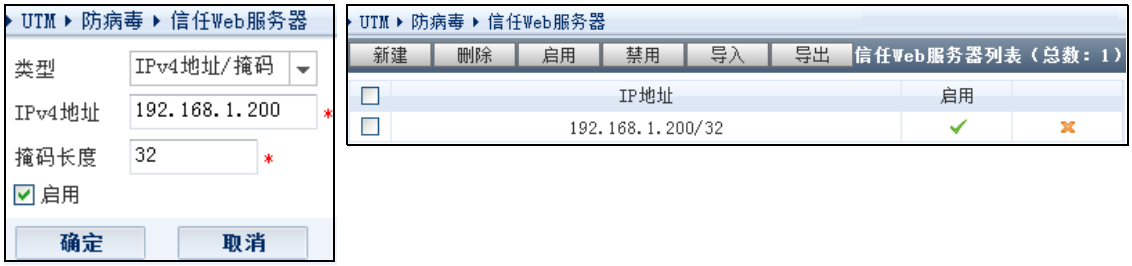
- 10.2.2.3.1. 创建 AV 信任 URL/Web 服务器 / 客户端
- 10.2.2.3.2. 设置 AV 引擎常规设置

10.2.2.3.1. 创建 AV 信任 URL/Web 服务器 / 客户端

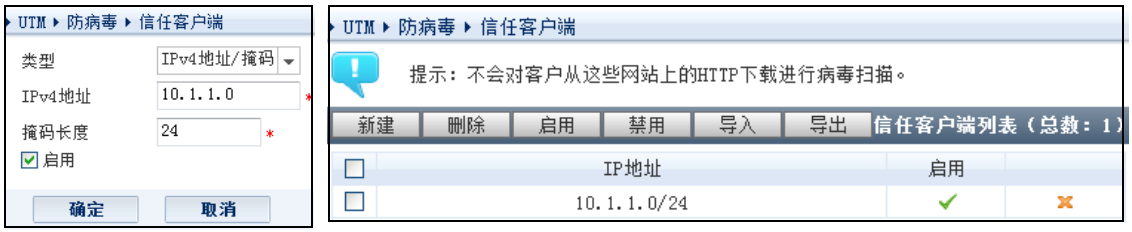
详细信息请参见 10.4.5.2. 信任 URL， 10.4.5.3. 信任 Web 服务器和 10.4.5.4. 信任客户端。

1. 选择 **UTM> 防病毒 > 信任 URL**。

2. 选择 **UTM> 防病毒 > 信任 Web 服务器**。



3. 选择 **UTM> 防病毒 > 信任客户端**。



10.2.2.3.2. 设置 AV 引擎常规设置

配置以下常规设置：

- 检测到病毒时：阻断 / 放行
- 启发式扫描检测到病毒：阻断 / 放行
- 扫描限制：
  - 压缩文件扫描
  - 滴流
  - AV 引擎过载 / 扫描失败
  - AV 引擎初始化失败

详细信息请参见 10.4.6.1.（反垃圾有邮件）常规设置。

1. 选择 **UTM> 防病毒 > 常规设置**。
2. 设置发现病毒时采取的处理动作。

3. 设置启发式扫描。

4. 设置压缩文件扫描、滴流、 AV 引擎过载或失效时的处理动作。

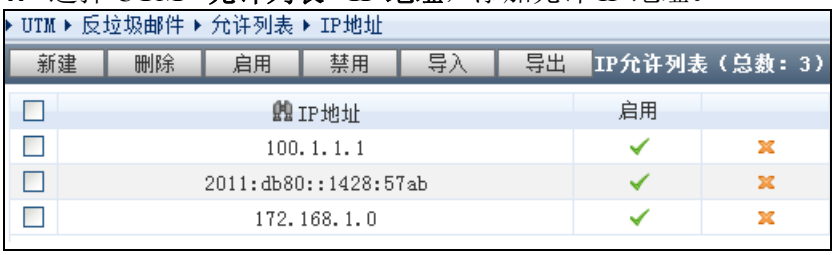
10.2.2.4. 配置 AS 全局动作 （允许 / 阻断列表，关键字列表，扫描设置）

配置以下反垃圾邮件的全局设置：

- 10.2.2.4.1. 创建 IP/ 发件人 / 收件人允许 / 阻断列表
- 10.2.2.4.2. 配置自定义垃圾邮件关键字列表
- 10.2.2.4.3. 设置反垃圾邮件规则和全局动作 （常规设置）

10.2.2.4.1. 创建 IP/ 发件人 / 收件人允许 / 阻断列表

1. 选择 **UTM> 允许列表 >IP 地址**，添加允许 IP 地址。



2. 选择 **UTM> 允许列表 > 发件人**，添加允许发件人。

3. 选择 **UTM> 允许列表 > 收件人**，添加允许收件人。

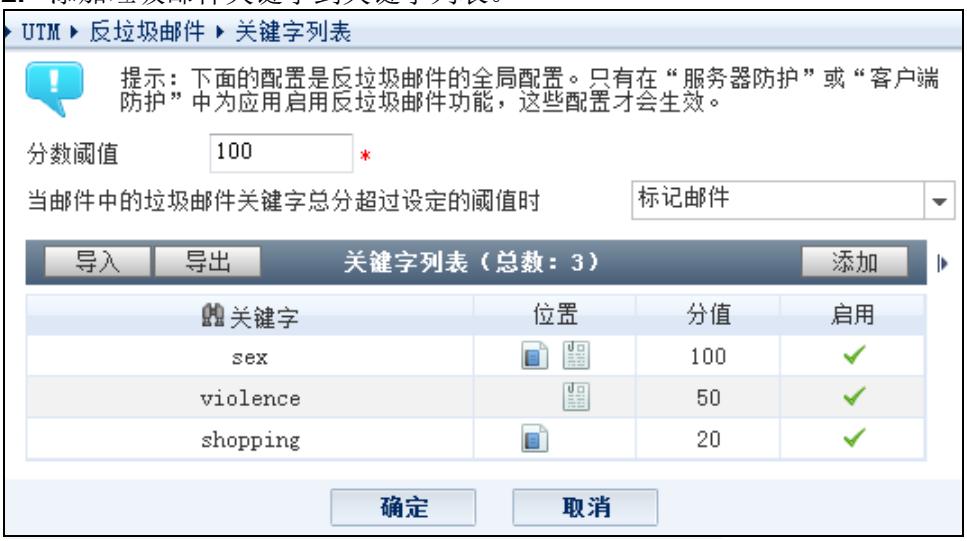
4. 选择 **UTM> 阻断列表 >IP 地址**，添加阻断 IP 地址。

5. 选择 **UTM> 阻断列表 > 发件人**，添加阻断发件人。

6. 选择 **UTM> 阻断列表**，添加阻断收件人。

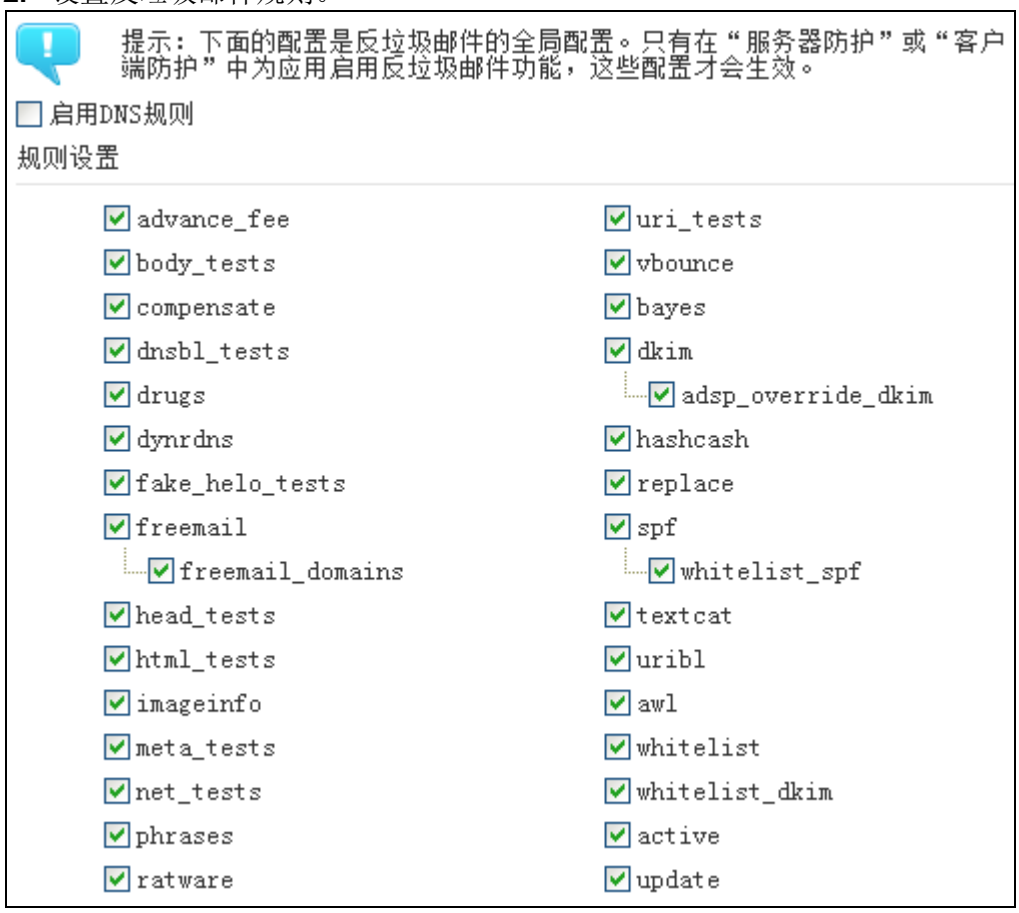
10.2.2.4.2. 配置自定义垃圾邮件关键字列表

1. 选择 **UTM> 反垃圾邮件 > 关键字列表**。
2. 添加垃圾邮件关键字到关键字列表。

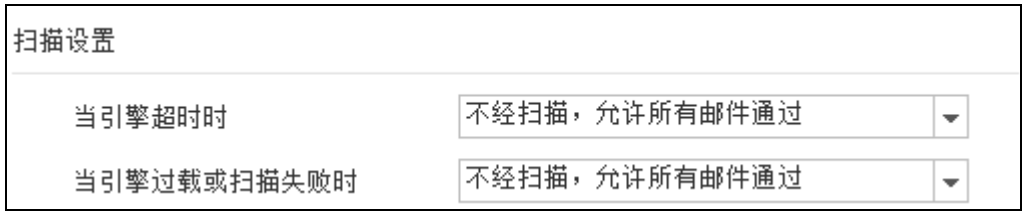


10.2.2.4.3. 设置反垃圾邮件规则和全局动作 （常规设置）

1. 选择 **UTM> 反垃圾邮件 > 常规设置**。
2. 设置反垃圾邮件规则。



3. 设置扫描超时或失效时的处理动作。



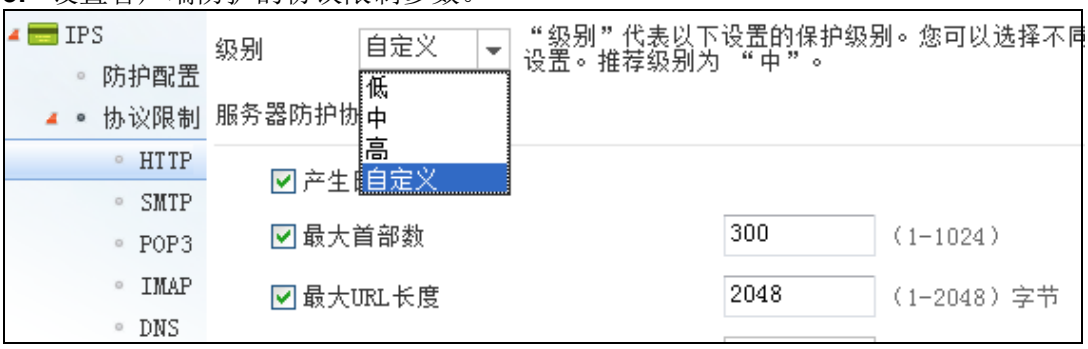
4. 点击**确定**。

10.2.2.5. 配置 IPS SMTP/POP3/IMAP/DNS 协议限制 （客户端）

IPS 协议限制的基本内容如下：

- **类型**：HTTP， SMTP， POP3， IMAP， DNS
- **级别**：低，中，高，自定义 （只有最后选中的级别生效。）
- **服务器端协议限制**：HTTP， SMTP， POP3， IMAP， DNS
- **客户端协议限制**：SMTP， POP3， IMAP， DNS

1. 选择协议限制类型（客户端类型的 IPS 防护配置中可以选择 SMTP、POP3、IMAP 和 DNS）。例如选择 **UTM>IPS> 协议限制 >SMTP**。
2. 选择协议限制级别 （如选择**高**级别）。
3. 设置客户端防护的协议限制参数。



4. 点击**确定**。

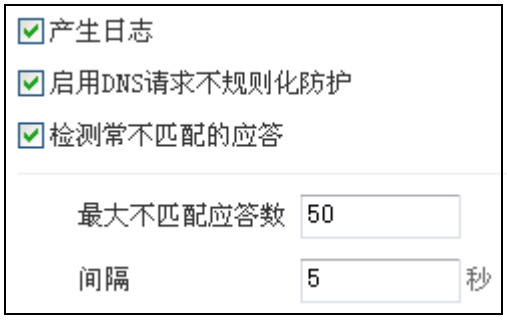
提示：最后选择的级别即生效级别。

5. 在客户端 IPS 防护配置中启用协议限制 （如 SMTP）。

10.2.2.6. 配置 DNS 缓存中毒防御全局动作

设置 DNS 缓存中毒防御 （CPD）。详细信息请参见 10.4.3.4.DNS 缓存中毒防御。

1. 选择 **UTM> 客户端防护 >DNS 缓存中毒防御**。



2. 点击**确定**。

10.2.2.7. 创建 AV/AS/IPS 防护配置

- 10.2.2.7.1. 查看缺省 AV 防护配置
- 10.2.2.7.2. 自定义 AV 防护配置并在策略中指定
- 10.2.2.7.3. 查看缺省反垃圾邮件防护配置
- 10.2.2.7.4. 自定义 AS 防护配置并在策略中指定
- 10.2.2.7.5. 查看缺省 IPS 防护配置 （概要）
- 10.2.2.7.6. 创建 IPS 防护配置
- 10.2.2.7.7. 启用 / 配置协议限制

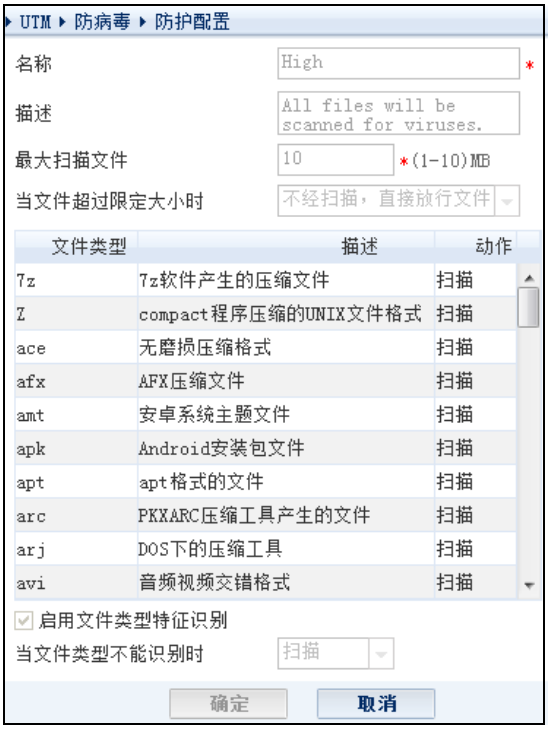
10.2.2.7.1. 查看缺省 AV 防护配置

详细信息请参见表 236。

1. 选择 **UTM> 防病毒 > 防护配置。**
2. 查看缺省防护配置。

提示：系统提供三个缺省 AV 防护配置 （高、中、低），最多可添加 29 个自定义 AV 防护配置。

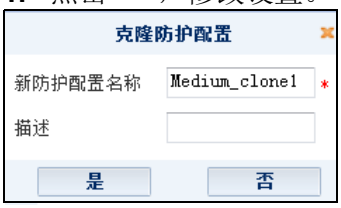
3. 点击缺省防护配置名称查看缺省配置。

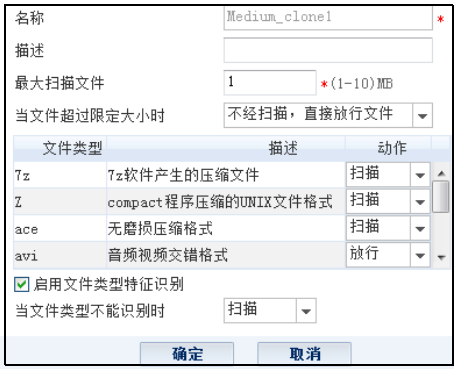


10.2.2.7.2. 自定义 AV 防护配置并在策略中指定

详细信息请参见 10.4.5.5. （防病毒）防护配置。

1. 点击 ，修改设置。

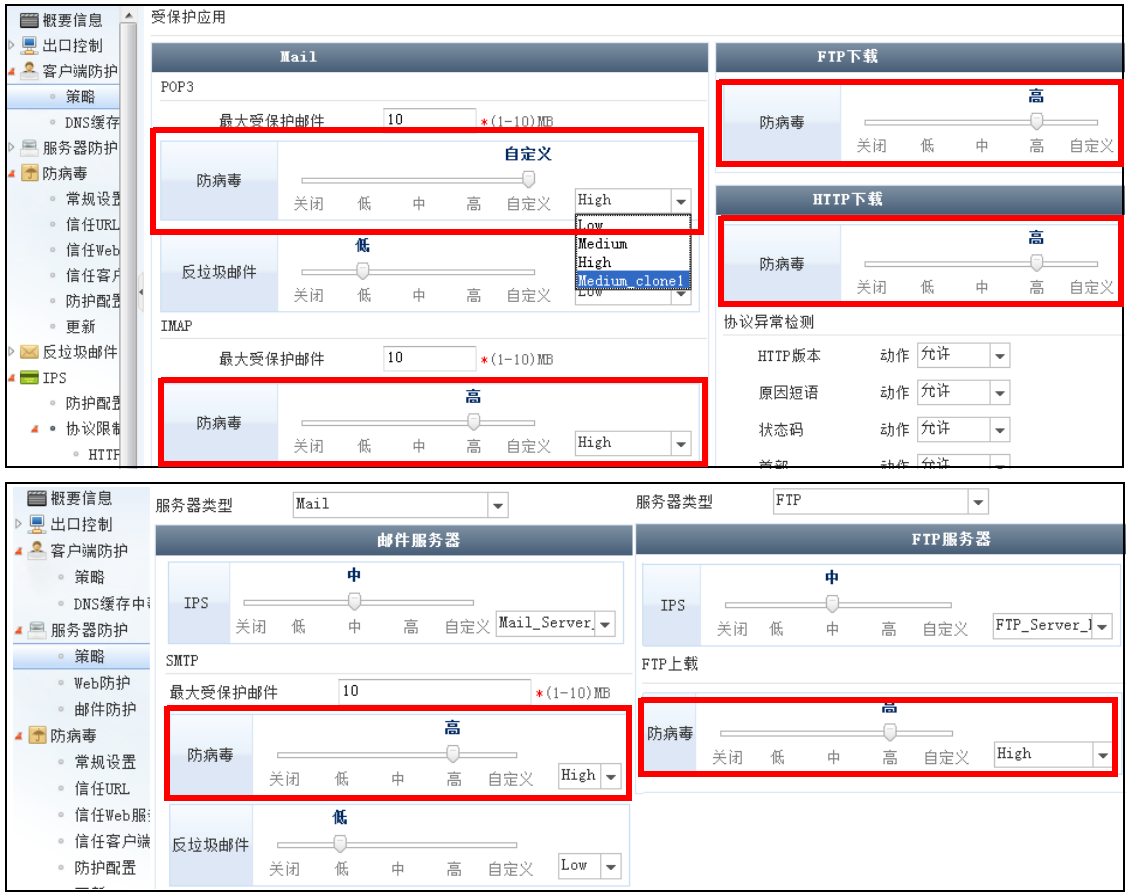




2. 如果点击**新建**，缺省配置同缺省防护配置 Medium。

提示：防护配置名称是防护配置的唯一标识，可通过防护配置名称在客户端 / 服务器防护策略中指定防护配置。

3. 在客户端 / 服务器防护策略中指定防病毒防护配置。



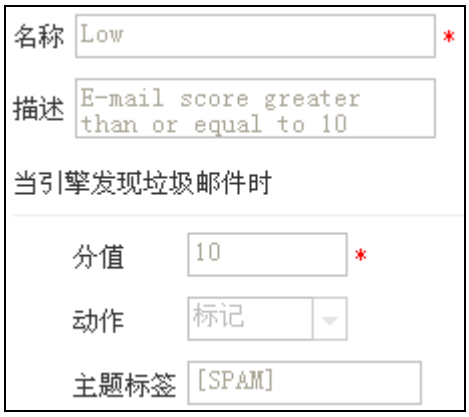
10.2.2.7.3. 查看缺省反垃圾邮件防护配置

详细信息请参见 10.4.6.5.（反垃圾邮件）防护配置。

1. 选择 **UTM> 反垃圾邮件 > 防护配置。**
2. 查看缺省防护配置。

提示：系统提供三个缺省反垃圾邮件防护配置（High、 Medium、 Low），最多可添加 29 个自定义反垃圾邮件防护配置。

3. 点击缺省反垃圾邮件防护配置名称，查看缺省设置。



10.2.2.7.4. 自定义 AS 防护配置并在策略中指定

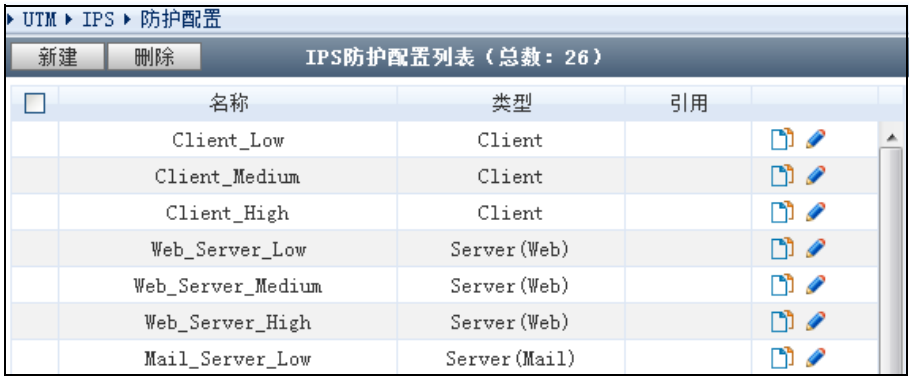
4. 点击 或点击**新建**创建防护配置，设置垃圾邮件分数阈值和处理动作。如果点击**新建**创建防护配置，缺省设置同缺省防护配置 Medium。

提示：防护配置名称是防护配置的唯一标识，可通过防护配置名称在客户端 / 服务器防护策略中指定防护配置。

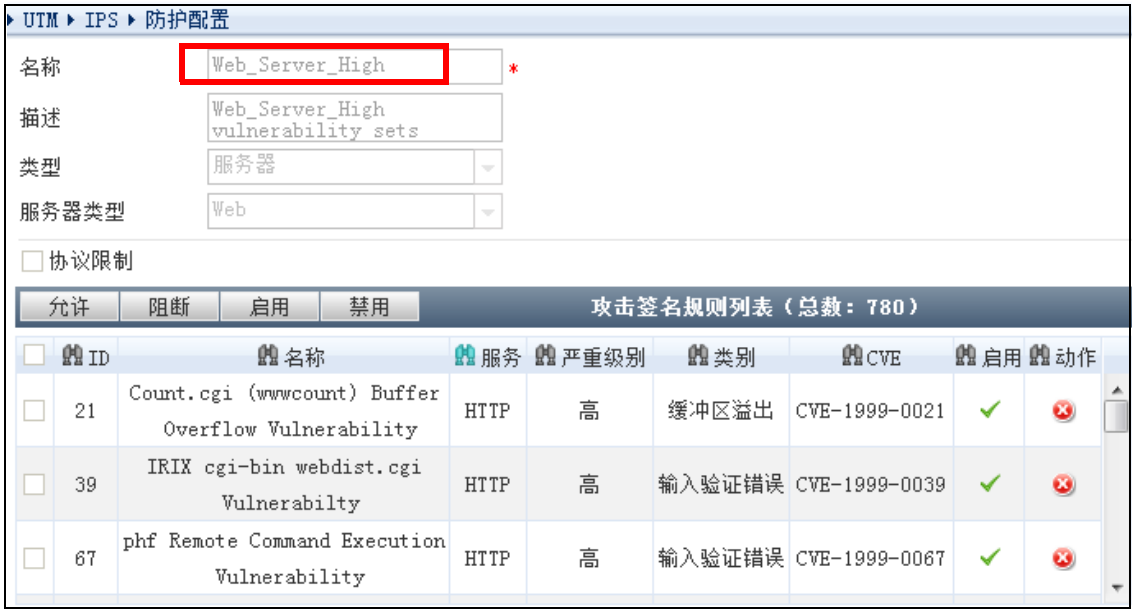
5. 在客户端 / 服务器防护策略中指定反垃圾邮件防护配置。

10.2.2.7.5. 查看缺省 IPS 防护配置 （概要）

1. 选择 **UTM>IPS> 防护配置。**
2. 查看缺省的 IPS 防护配置：



3. 点击缺省防护配置名称查看设置。



提示：将鼠标指向规则列表中的参数名称，会出现一个 ▼ 按钮，点击设置要显示的参数。

4. 下图演示了在客户端 / 服务器防护策略中如何选择 IPS 防护配置。

10.2.2.7.6. 创建 IPS 防护配置

IPS 防护配置的基本配置内容如下：

- **名称**：用于在客户端 / 服务器防护策略中选择防护配置
- **类型**：服务器 / 客户端
- **服务器类型**：Web/Mail/FTP/Telnet/DNS/ 其他
- **协议限制**：HTTP/SMTP/POP3/IMAP/DNS （只能在自定义防护配置中启用 / 禁用。）
- **攻击签名规则**：启用 / 禁用，允许 / 阻断

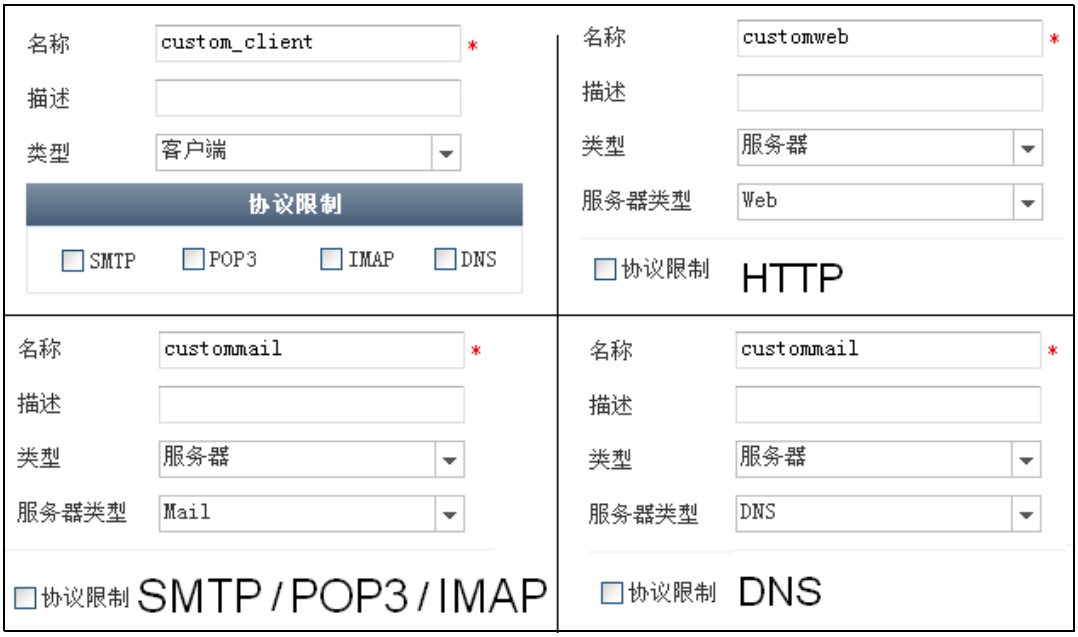
5. 点击 拷贝防护配置或点击**新建**创建新的防护配置。

6. 在攻击签名规则列表中，为防护配置指定要启用的规则和规则动作（允许 / 阻断）。

7. 防护配置名称作为防护配置的唯一标识，用于在客户端 / 服务器防护策略中指定防护配置。

10.2.2.7.7. 启用 / 配置协议限制

8. 启用特定类型的协议限制 （只能为自定义防护配置启用协议限制）。

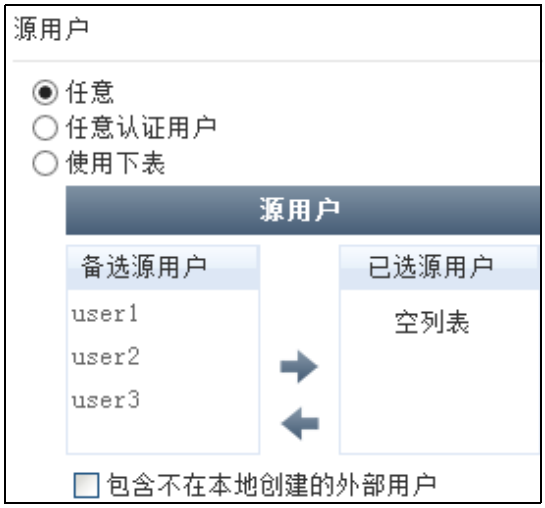


10.2.2.8. 创建客户端防护策略

创建客户端防护策略。详细信息请参见 10.4.3. 客户端防护。

1. 选择 **UTM> 客户端防护 > 策略**。
2. 选择入口安全域，为其开启客户端防护策略。

3. 点击**客户端防护策略列表**上方的**新建**按钮，创建客户端防护策略：
   a. 输入策略基本信息，设置受保护客户端的 IP 地址。



b. 选择 IPS 检测级别并设置 IPS 防护配置。

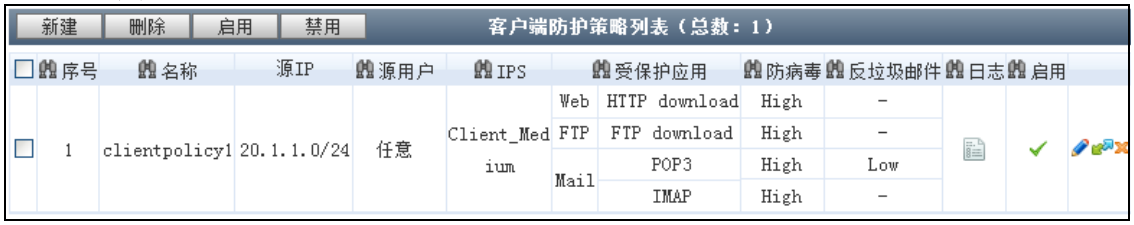
c. 启用 / 禁用邮件防护配置。

d. 为 FTP 下载流量设置防病毒检测级别并选择防病毒防护配置。

e. 为 HTTP 下载流量设置防病毒检测级别、选择防病毒防护配置并设置协议异常检测。

f. 为 DNS 客户端流量开启 DNS 缓存中毒防御功能，并设置协议异常检测处理动作。

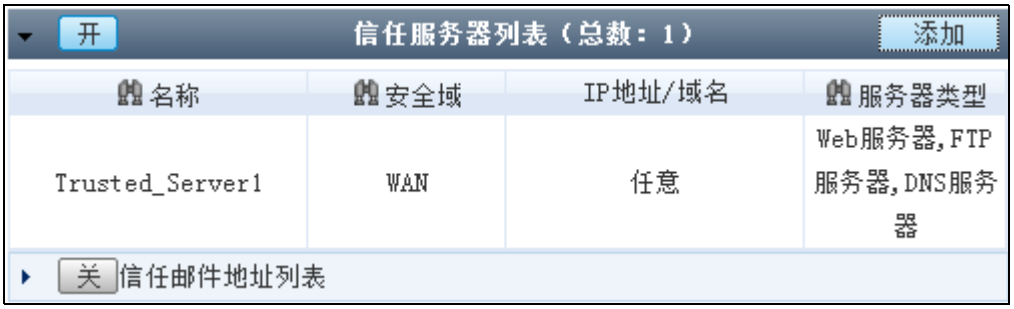
4. 点击**确定**。



10.2.2.9. 创建信任服务器 / 邮件列表

创建信任服务器列表。详细信息请参见 10.4.3.2. （客户端防护）信任服务器列表。

1. 选择 **UTM> 客户端防护 > 策略 > 信任服务器列表**。
2. 启用信任服务器列表，点击其后的空白区域展开列表。
3. 配置信任服务器列表。将鼠标指向列表条目，会出现一个 ✖ 图标，可以点击删除该条目。双击条目进行编辑。



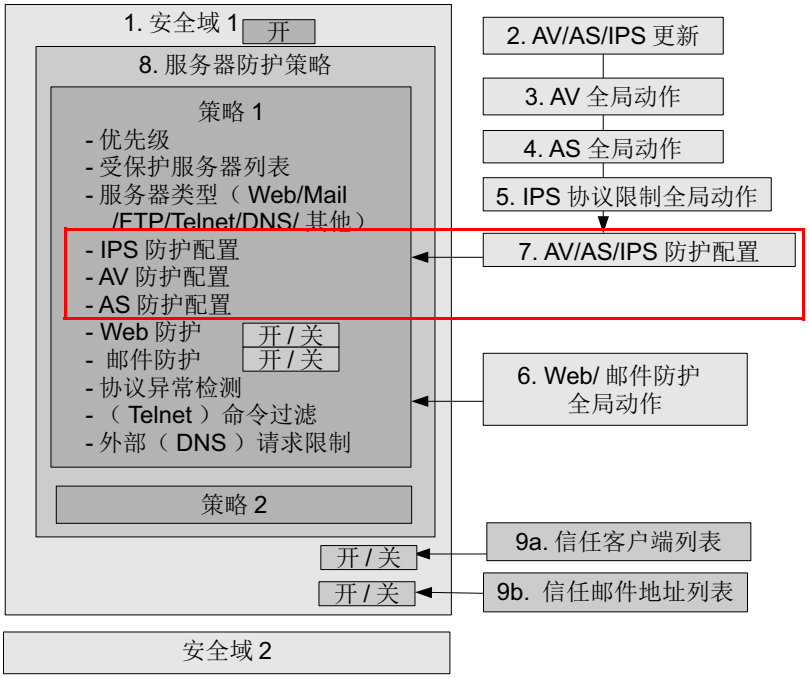
创建信任邮件地址列表。详细信息请参见 10.4.3.3. （客户端防护）信任邮件地址列表。

4. 选择 **UTM> 客户端防护 > 策略 > 信任邮件地址列表**。
5. 启用信任邮件地址列表。
6. 配置信任邮件地址列表。可以删除 / 编辑列表条目，方法同信任服务器列表。

10.2.3. 服务器防护

服务器防护的配置步骤如下图所示：

图 43 服务器防护配置步骤



基本设置：

- 10.2.3.1. 创建安全域 / 访问策略 / 缺省路由 /NAT 规则

常规设置 （AV/AS/IPS 规则更新）：

- 10.2.3.2. 更新 AV/AS/IPS 规则

全局动作：

- 10.2.3.3. 配置 AV 全局动作 （信任列表 / 病毒检测动作 / 启发式扫描 / 扫描限制）
- 10.2.3.4. 配置 AS 全局动作 （允许 / 阻断列表，关键字列表，扫描失败动作）
- 10.2.3.5. 配置 IPS 协议限制 （HTTP/SMTP/POP3/IMAP/DNS 服务器）
- 10.2.3.6. 配置 web/ 邮件防护全局动作

动作防护配置：

- 10.2.3.7. 创建 AV/AS/IPS 动作防护配置

目的安全域动作 / 策略：

- 10.2.3.8. 创建服务器防护策略
- 10.2.3.9. 创建信任客户端 / 邮件列表

10.2.3.1. 创建安全域 / 访问策略 / 缺省路由 /NAT 规则

同客户端防护，参见 10.2.2.1. 创建安全域 / 访问策略 / 缺省路由 /NAT 规则。

10.2.3.2. 更新 AV/AS/IPS 规则

同客户端防护，参见 10.2.2.2. 更新 AV/AS/IPS 规则。

10.2.3.3. 配置 AV 全局动作 （信任列表 / 病毒检测动作 / 启发式扫描 / 扫描限制）

同客户端防护，参见 10.2.2.3. 配置 AV 全局动作 （信任列表 / 病毒检测动作 / 启发式扫描 / 扫描限制）。

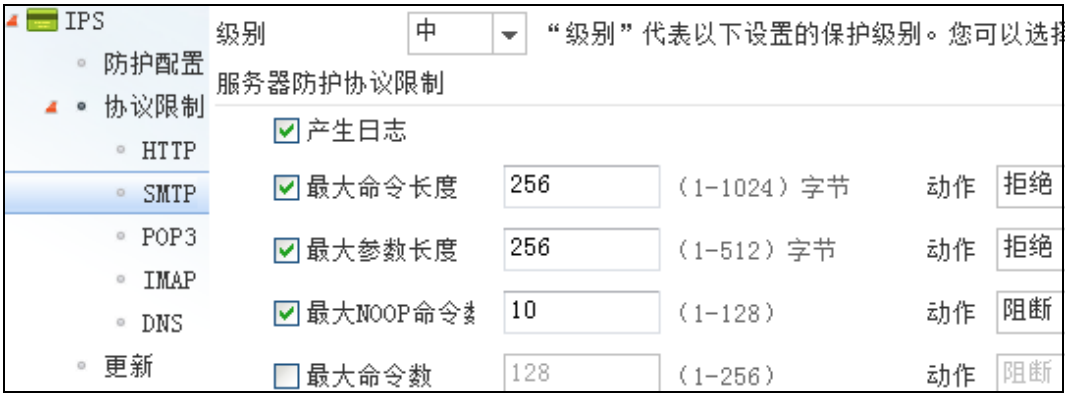
10.2.3.4. 配置 AS 全局动作 （允许 / 阻断列表，关键字列表，扫描失败动作）

同客户端防护，参见 10.2.2.4. 配置 AS 全局动作 （允许 / 阻断列表，关键字列表，扫描设置）。

10.2.3.5. 配置 IPS 协议限制 （HTTP/SMTP/POP3/IMAP/DNS 服务器）

关于客户端防护的协议限制配置，请参见 10.2.2.5. 配置 IPS SMTP/POP3/IMAP/DNS 协议限制 （客户端）。

1. 选择协议限制类型 （服务器类型的 IPS 防护配置中可以选择 HTTP、 SMTP、 POP3、 IMAP 和 DNS）。例如，选择 **UTM>IPS> 协议限制 >SMTP**。
2. 选择协议限制级别 （如选择**高**级别协议限制）。
3. 设置服务器防护的协议限制参数。



4. 点击**确定**。

提示：最后选择的级别即生效级别。

5. 选择相应的服务器 IPS 防护配置，并在 IPS 防护配置中启用协议限制。

10.2.3.6. 配置 web/ 邮件防护全局动作

设置 Web 防护。详细信息请参见 10.4.4.4.Web 防护。

1. 选择 **UTM> 服务器防护 >Web 防护**。
2. 分别启用 / 禁用**信息泄露防护**的各项功能，整体启用 / 禁用记录日志功能。

3. 点击**注入攻击防御**，配置相关信息。

4. 点击**确定**。

设置邮件防护。详细信息请参见 10.4.4.5. 邮件防护。

5. 选择 **UTM> 服务器防护 > 邮件防护**。

6. 启用 / 禁用邮件防护功能和记录日志功能。

7. 点击**确定**。

10.2.3.7. 创建 AV/AS/IPS 动作防护配置

同客户端防护，详细信息请参见 10.2.2.7. 创建 AV/AS/IPS 防护配置。

1. 服务器类型的防护配置如下所示：

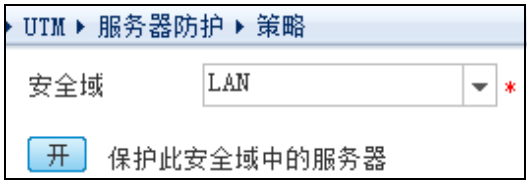
2. 点击 按钮，查看缺省防护配置。

3. 点击 按钮，通过拷贝和编辑缺省防护配置创建新的防护配置。

10.2.3.8. 创建服务器防护策略

详细信息请参见 10.4.4. 服务器防护。

1. 选择 **UTM> 服务器防护 > 策略**。
2. 选择入口安全域并为其开启服务器防护策略。



3. 点击**新建**创建 Web 服务器防护策略，并在策略中开启 **Web 防护**。

4. 点击**确定**。

5. 点击**新建**创建邮件服务器防护策略，并在策略中开启**邮件防护**。

6. 点击**确定**。

7. 创建 FTP 服务器防护策略。

8. 点击**确定**。

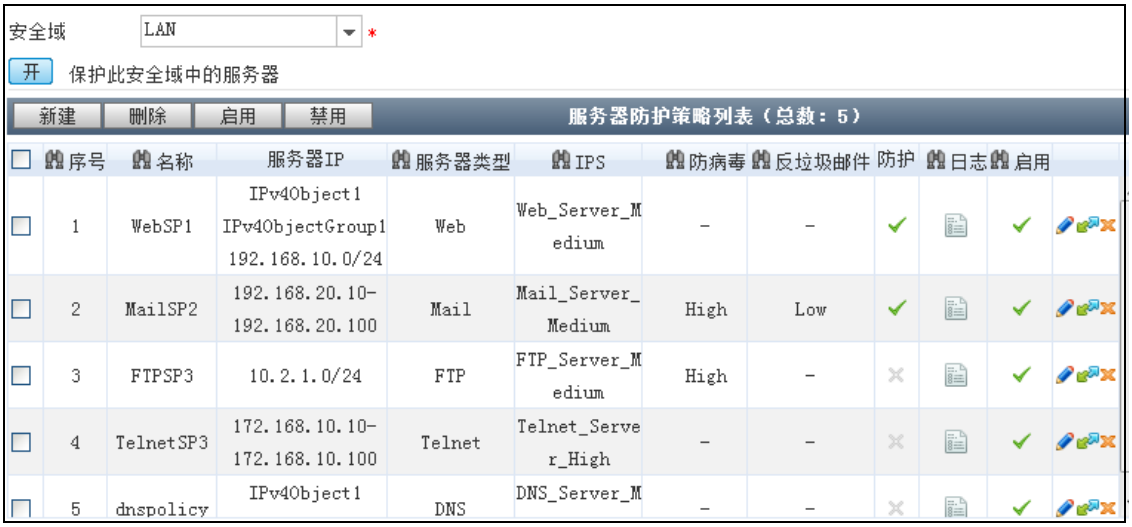
9. 创建 Telnet 服务器防护策略。

10. 点击**确定**。

11. 创建 DNS 服务器防护策略。

12. 点击**确定**。

13. 查看创建策略。



	序号	名称	服务器IP	服务器类型	IPS	防病毒	反垃圾邮件	防护	日志	启用	
☐	1	WebSP1	IPv4Object1 IPv4ObjectGroup1 192.168.10.0/24	Web	Web_Server_Medium	-	-	✓		✓	
☐	2	MailSP2	192.168.20.10- 192.168.20.100	Mail	Mail_Server_Medium	High	Low	✓		✓	
☐	3	FTPSP3	10.2.1.0/24	FTP	FTP_Server_Medium	High	-	✗		✓	
☐	4	TelnetSP3	172.168.10.10- 172.168.10.100	Telnet	Telnet_Server_High	-	-	✗		✓	
☐	5	dnspolicy	IPv4Object1	DNS	DNS_Server_M	-	-	✗		✓	

10.2.3.9. 创建信任客户端 / 邮件列表

创建信任客户端列表，详细信息请参见 10.4.4.2. （服务器防护）信任客户端列表。

1. 选择 **UTM> 服务器防护 > 策略**。
2. 启用并配置信任客户端列表。

创建信任邮件地址列表。配置同客户端防护，请参见 10.2.3.9. 创建信任客户端 / 邮件列表。配置参数信息请参见 10.4.4.3. （服务器防护）信任邮件地址列表。

10.2.4. 通知消息

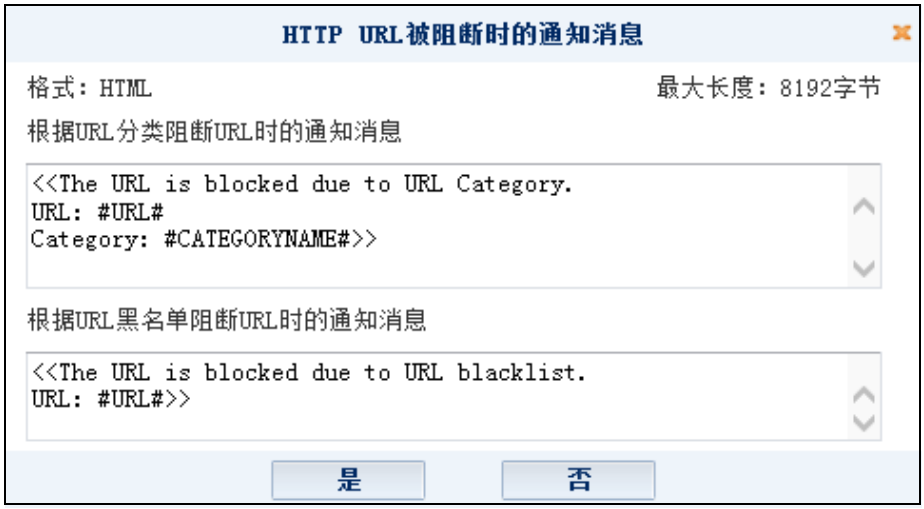
通知消息分为两类：

- **系统预定义通知消息**：不可修改。
- **用户自定义通知消息**：可通过 WebUI 进行配置。

详细信息请参见 10.4.8. 通知消息。

1. 选择 **UTM> 通知消息**。

2. 点击链接编辑通知消息显示内容。



3. 点击**是**。

10.2.5. 概要信息页面

概要信息页面给出了所有安全域的 UTM 信息。 UTM 策略应用域安全域。

1. 选择 **UTM> 概要信息**查看所有安全域的 UTM 信息。

2. 点击本页面图标到相应的页面进行配置。

10.3. UTM 范例

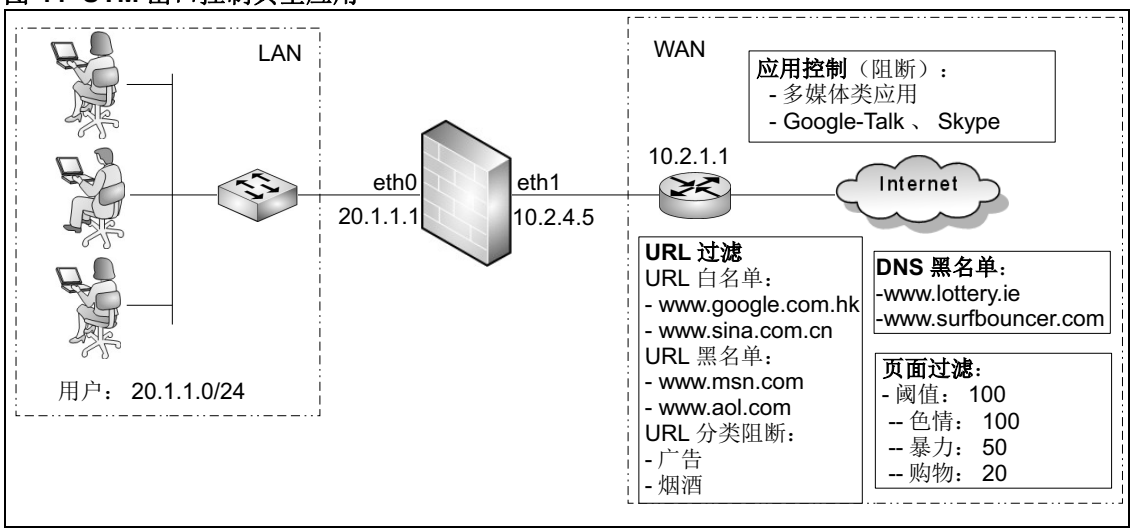
本节给出三个范例，描述如何将 NISG 应用于三个 UTM 典型场景：

- 范例 1：UTM 出口控制典型应用
- 范例 2：UTM 客户端防护典型应用
- 范例 3：UTM 服务器防护典型应用

范例 1：UTM 出口控制典型应用

如下图所示，某公司内网 LAN 中的员工通过 NISG 与互联网进行通讯，为了对员工的上网行为进行限制，管理员可以配置相应的应用控制策略、 URL 过滤策略、域名黑名单以及页面过滤。

图 44 UTM 出口控制典型应用



如果初次登录选择跳过初始化过程，配置 UTM 之前，需要先配置：

1. 创建安全域 / 缺省路由 / 访问策略 /NAT 规则

UTM 配置步骤包括：

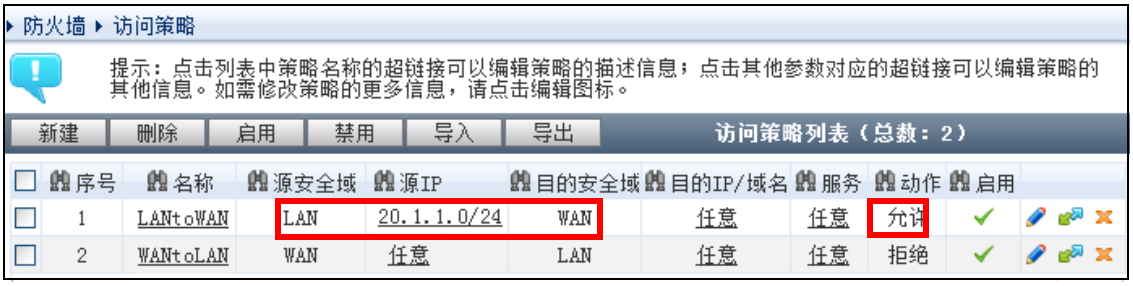
2. 配置应用控制
3. 配置 URL 过滤
4. 配置 DNS 域名黑名单
5. 配置页面过滤

1. 创建安全域 / 缺省路由 / 访问策略 /NAT 规则

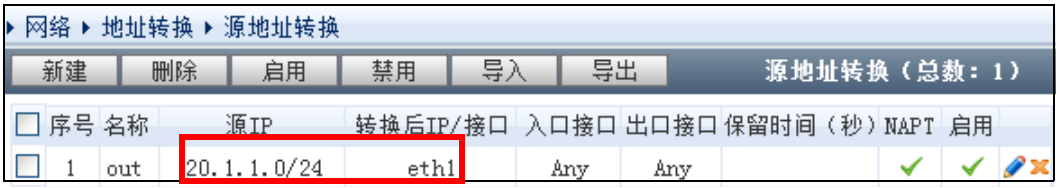
1. 选择**网络 > 接口**，设置 eth1 和 eth0 为三层接口，并设置其 IP 地址分别为 10.2.4.5/21 和 20.1.1.1/24。
2. 选择**网络 > 安全域**，创建两个三层安全域LAN和WAN，并将eth0划分给LAN、eth1划分给 WAN。

3. 选择**网络 > 路由 > 缺省路由**，修改缺省路由的网关为 10.2.1.1。

4. 选择**防火墙 > 访问策略**，创建访问策略，允许 LAN 中 20.1.1.0 网段到 WAN 的访问、拒绝 WAN 到 LAN 的访问：



5. 选择**网络>地址转换>源地址转换**，添加源地址转换规则，将源IP转换成eth1接口的IP地址：



2. 配置应用控制

应用控制配置包括创建应用控制防护配置和策略。

2.1. 创建应用控制防护配置

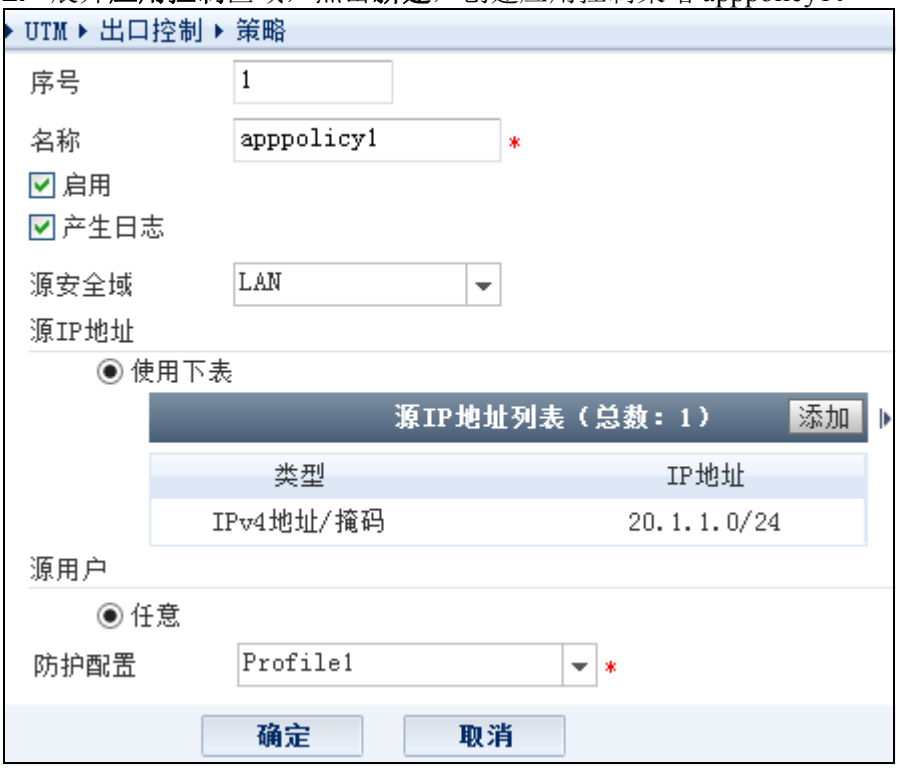
1. 选择 **UTM> 出口控制 > 应用控制 > 防护配置**。
2. 点击**新建**，创建应用控制防护配置 Profile1。

提示：通过名称添加应用到防护配置时，可以输入应用名称的首个或前两个字母，然后使用下拉框的自动补齐功能选择应用。

3. 点击**确定**。

2.2. 创建应用控制策略

1. 选择 **UTM> 出口控制 > 策略**。选择安全域 WAN，开启应用控制功能。
2. 展开**应用控制**区域，点击**新建**，创建应用控制策略 apppolicy1。



3. 点击**确定**。启用该策略之后，20.1.1.0 网段的用户将不能使用 Google-Talk 和 Skype 应用，不能访问 Internet 多媒体类应用。

2.3. 监控应用控制

1. 打开 Google-Talk 和 Skype 应用尝试登录，会发现登录失败。
2. 选择**监控 > 报警 / 日志 > 应用控制报警**，可以看到 Google-Talk、Skype 和多媒体类应用已被阻断。

- Google-Talk 被阻断的日志信息：

- Skype 被阻断的日志信息：

- 多媒体应用被阻断的日志信息：

3. 配置 URL 过滤

URL 过滤配置包括创建 URL 黑白名单、 URL 过滤防护配置和 URL 过滤策略。

3.1. 创建 URL 黑白名单

1. 选择 **UTM> 出口控制 >URL 过滤 > 黑白名单**。
2. 点击**新建**，创建 URL 白名单 Whitelist1。

3. 点击**确定**。
4. 点击**新建**，创建黑名单 Blacklist1。

5. 点击**确定**。

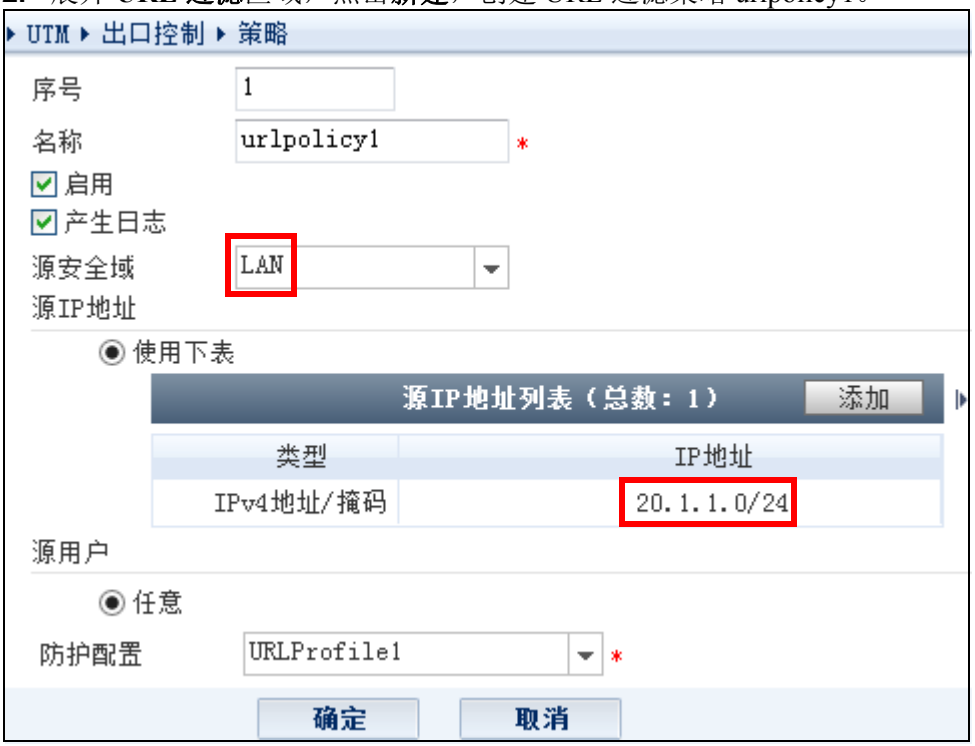
3.2. 创建 URL 过滤防护配置

1. 选择 **UTM> 出口控制 >URL 过滤 > 防护配置。**
2. 点击**新建**，创建 URL 过滤防护配置 URLProfile1 （设置**广告**和**烟酒**类 URL 动作为阻断）。

3. 点击**确定**。

3.3. 创建 URL 过滤策略

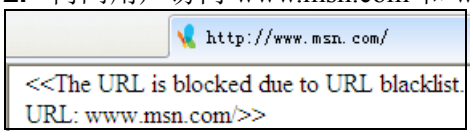
1. 选择 **UTM> 出口控制 > 策略**。选择安全域 WAN，开启 URL 过滤功能。
2. 展开 **URL 过滤**区域，点击**新建**，创建 URL 过滤策略 urlpolicy1。



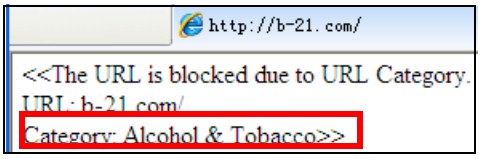
3. 点击**确定**。启用该策略之后， 20.1.1.0 网段的用户可以访问白名单中的网址以及被允许的 URL 分类，但是不能访问黑名单中的网址和被阻断的 URL 分类（广告和烟酒）。

3.4. 监控 URL 过滤

1. 内网用户可以成功访问 www.google.com.hk 和 www.sina.com.cn。
2. 内网用户访问 www.msn.com 和 www.aol.com 时提示 URL 被黑名单阻断：



3. 广告和弹出窗口类网页将被 URL 分类过滤功能阻断。



4. 选择**监控>报警/日志>URL过滤报警**，查看URL被黑白名单以及分类阻断或放行的日志信息。 URL 过滤支持模糊匹配。

   - 白名单放行的 URL：

   - 黑名单阻断的 URL：

   - 分类阻断的 URL：

4. 配置 DNS 域名黑名单

1. 选择 **UTM> 出口控制 >DNS 域名黑名单**。
2. 配置 DNS 域名黑名单，阻断 www.lottery.ie 和 www.surfbouncer.com 的域名请求：

3. 点击**确定**。
4. 选择 **UTM> 出口控制 > 策略**。
5. 选择安全域 WAN，开启 DNS 域名黑名单功能。内网用户将不能访问被域名黑名单阻断的网站。

6. 选择**监控 > 报警 / 日志 >IPS 报警**，可查看 DNS 黑名单阻断信息。对域名 www.lottery.ie 和 www.surfbouncer.com 的 DNS 请求将被阻断。

5. 配置页面过滤

1. 选择 **UTM> 出口控制 > 页面过滤**。
2. 配置页面过滤，阻断包含列表中关键字且总分超过阈值的页面。例如下面的设置，包含一个“色情”关键字的页面将被阻断，包含一个“暴力”关键字和 3 个“购物”关键字 (1*50+3*20=110%) 的页面也将被阻断。

3. 点击**确定**。
4. 选择 **UTM> 出口控制 > 策略**。
5. 选择安全域 WAN，开启页面过滤功能。

6. 点击 。当内网用户访问的网页包含指定关键字且累计分数达到阈值时，页面将被阻断。

7. 选择**监控 > 报警 / 日志 >IPS 报警**，可查看页面关键字过滤阻断信息。

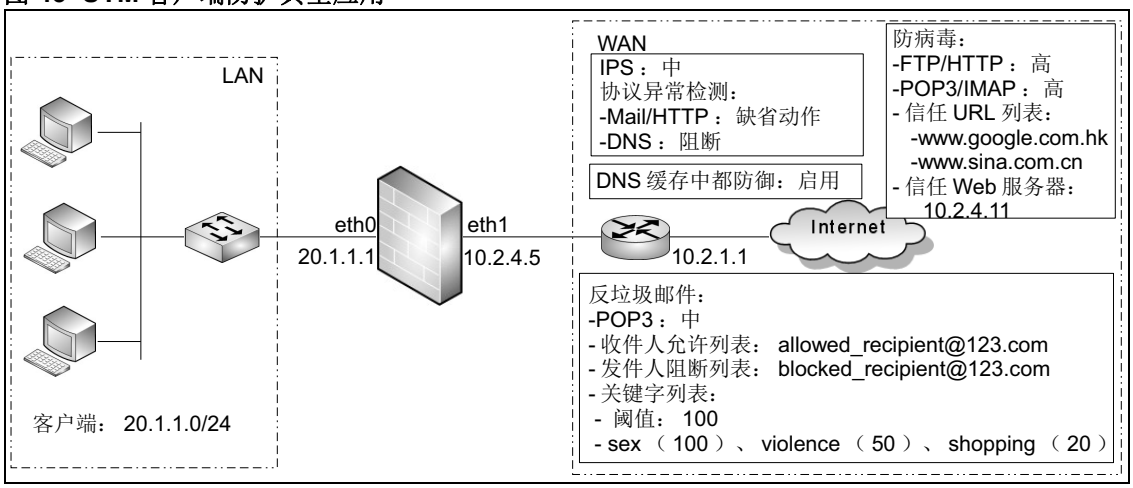
序号	日期时间	源IP	源端口	目的IP	目的端口	服务	规则ID	信息	动作
4	2014-04-08 22:01:50	20.1.1.100	1075	202.107.117.11	80	HTTP		URL=www.baidu.com/s 摘要=关键字 (色情) 总分 (4300) 超过 100。	阻断
5	2014-04-08 22:01:47	20.1.1.100	1075	210.83.210.155	80	HTTP		URL=www.baidu.com/s 摘要=关键字 (购物) 总分 (120) 超过 100。	阻断
6	2014-04-08 22:01:46	20.1.1.100	1075	202.107.117.11	80	HTTP		URL=www.baidu.com/s 摘要=关键字 (暴力) 总分 (350) 超过 100。	阻断

提示：有时候用户访问不了白名单中的 URL，是因为其响应页面包含的过滤关键字总分数达到了阈值而被阻断。若出现此种情况，请检查两者配置是否冲突。

范例 2：UTM 客户端防护典型应用

如下图所示，某公司内网客户端通过 NISG 与互联网进行通讯，为了对客户端的安全进行防护，管理员可以配置相应的客户端防护功能，包括防病毒、反垃圾邮件、攻击签名检测 （IPS）以及 DNS 缓存中毒防御。

图 45 UTM 客户端防护典型应用

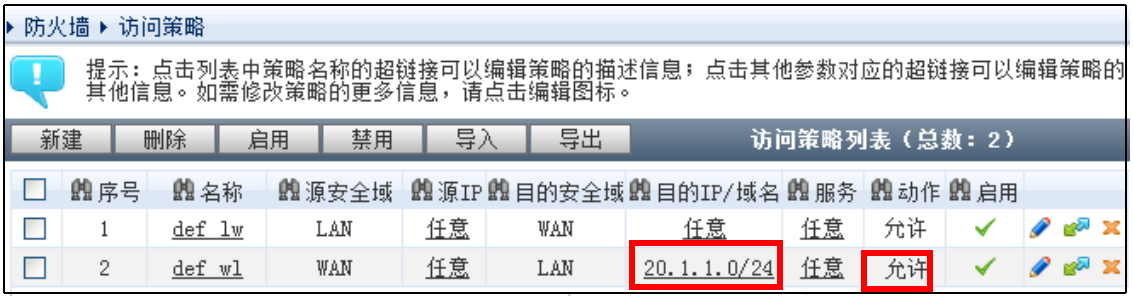


如果初次登录选择路由模式，则本范例配置步骤如下：

1. 修改访问策略
2. 配置防病毒功能
3. 配置反垃圾邮件功能
4. 配置 DNS 缓存中毒防御功能
5. 创建客户端防护策略
6. 监控客户端防护

1. 修改访问策略

1. 选择**防火墙 > 访问策略**。
2. 修改访问策略如下，允许客户端流量通过：



2. 配置防病毒功能

1. 选择 **UTM> 防病毒 > 信任 URL**，添加信任 URL 地址 www.google.com.hk 和 www.sina.com.cn。

2. 选择 **UTM> 防病毒 > 信任服务器**，添加信任服务器 10.2.4.11。

3. 配置反垃圾邮件功能

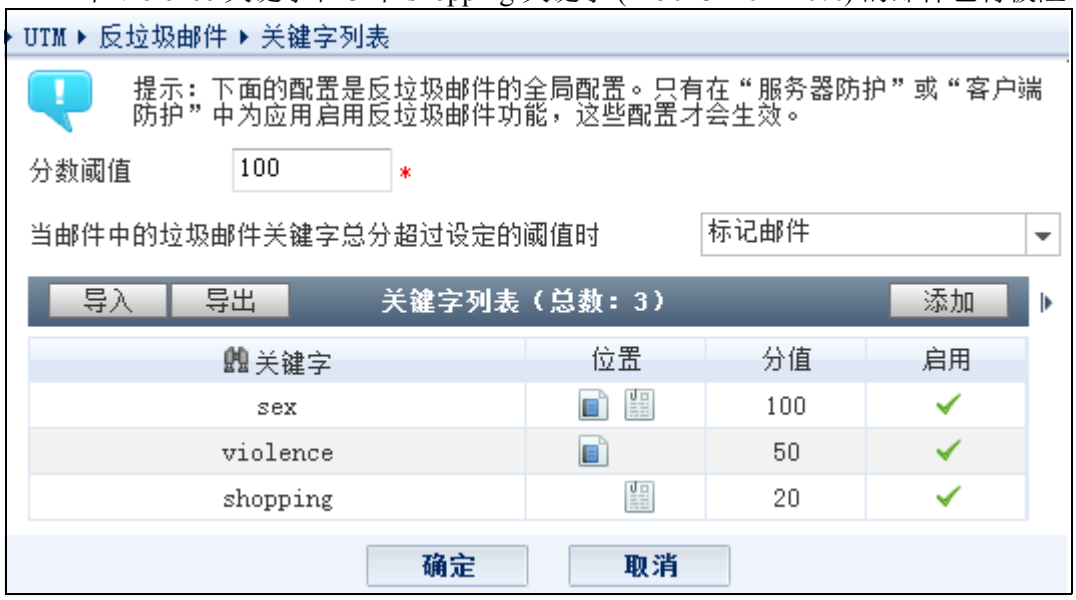
配置允许和阻断列表：

1. 选择 **UTM> 反垃圾邮件 > 允许列表 > 收件人**，添加允许收件人地址 allowed_recipient@123.com。

2. 选择 **UTM> 反垃圾邮件 > 阻断列表 > 收件人**，添加阻断收件人地址 blocked_recipient@123.com。

配置关键字列表：

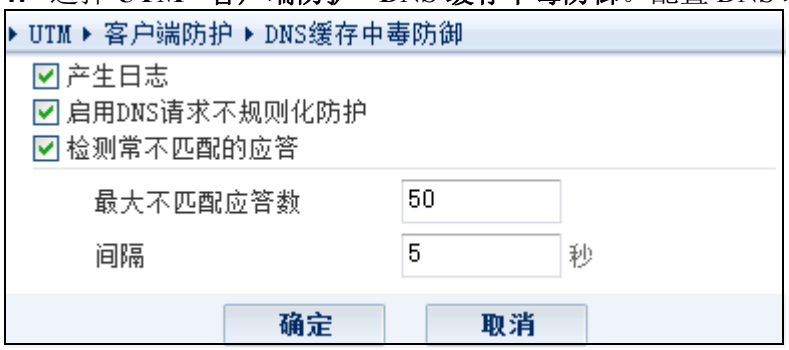
1. 选择 **UTM> 反垃圾邮件 > 关键字列表**。
2. 设置垃圾邮件分数阈值和动作，添加要过滤的关键字，阻断包含列表中关键字且总分超过阈值的邮件。例如下面的设置，包含一个 sex 关键字的邮件将被阻断，包含一个 violence 关键字和 3 个 shopping 关键字 (1*50+3*20=110%) 的邮件也将被阻断。



3. 点击**确定**。

4. 配置 DNS 缓存中毒防御功能

1. 选择 **UTM> 客户端防护 >DNS 缓存中毒防御**。配置 DNS 缓存中毒防御功能。



2. 点击**确定**。

5. 创建客户端防护策略

1. 选择 **UTM> 客户端防护 > 策略**。选择安全域 LAN，开启客户端防护功能。
2. 点击**新建**，进行如下基本配置：

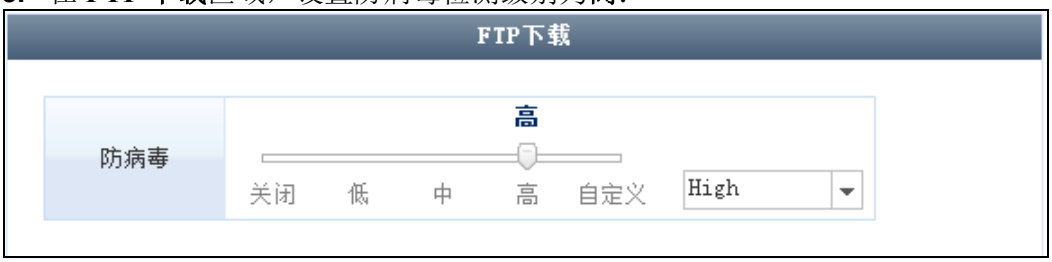
3. IPS 检测级别选取**中**。

提示：管理员可以选择 **UTM>IPS> 防护配置**，点击缺省防护配置 Client_Medium 查看设置，还可以新建自定义防护配置并在策略中引用。

4. 在 **Mail** 应用防护区域，进行如下设置：

提示：管理员可以选择 **UTM> 防病毒 / 反垃圾邮件 > 防护配置**，点击缺省防护配置 Medium 查看设置，还可以新建自定义防护配置并在策略中引用。

5. 在 **FTP 下载**区域，设置防病毒检测级别为**高**：



6. 在 **HTTP 下载**区域，设置防病毒检测级别为**高**，并使用协议异常检测的缺省设置：

7. 开启 DNS 缓存中毒防御功能，并使用协议异常检测的缺省配置。

8. 点击**确定**。

9. 点击 。

6. 监控客户端防护

- 6.1 监控 AV 功能
- 6.2 监控 AS 功能
- 6.3 监控 IPS 功能
- 6.4 监控 DNS 缓存中毒防御功能

6.1 监控 AV 功能

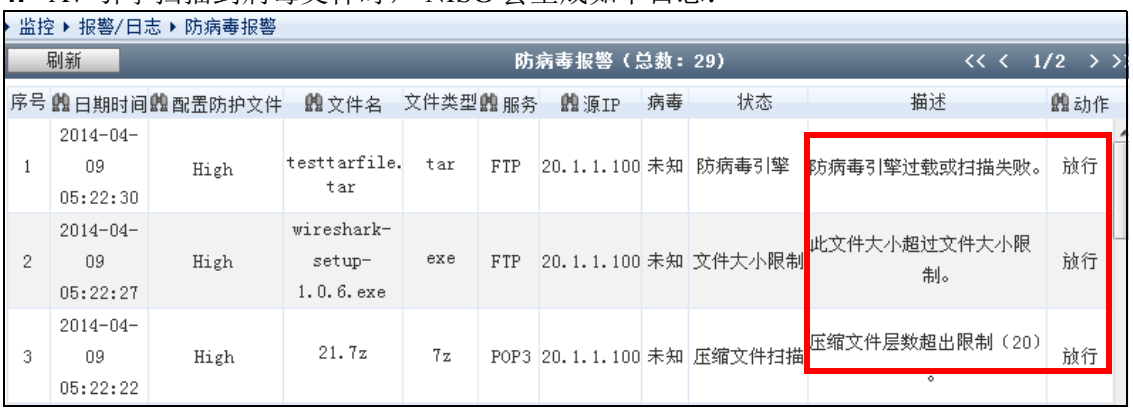
1. 选择**监控 > 报警 / 日志 > 防病毒报警**，查看防病毒监控信息。
2. 当客户端访问信任 URL 列表中的网址时， NISG 会生成如下日志：

序号	日期时间	配置防护文件	文件名	文件类型	服务	源IP	病毒	状态	描述	动作
5	2014-04-09 03:56:50	N/A	logo9w.png	未知	HTTP	20.1.1.100	未知	信任URL列表	文件来自于受信任URL列表（www.google.com.hk/images/srpr/logo9w.png）。	放行
6	2014-04-09 03:56:43	N/A	www.sina.com.cn/	未知	HTTP	20.1.1.100	未知	信任URL列表	文件来自于受信任URL列表（www.sina.com.cn/）。	放行

3. 当客户端访问信任 Web 服务器时， NISG 会生成如下日志：

序号	日期时间	配置防护文件	文件名	文件类型	服务	源IP	病毒	状态	描述	动作
1	2014-04-09 04:37:10	N/A	10.1.3.108/	未知	HTTP	20.1.1.100	未知	信任服务端列表	文件来自于受信服务端列表（10.2.4.11/32）。	放行

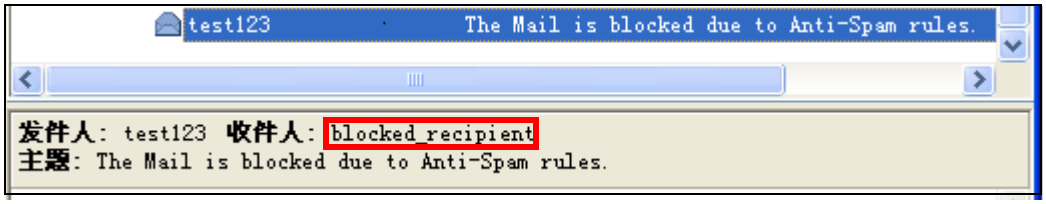
4. AV 引擎扫描到病毒文件时， NISG 会生成如下日志：



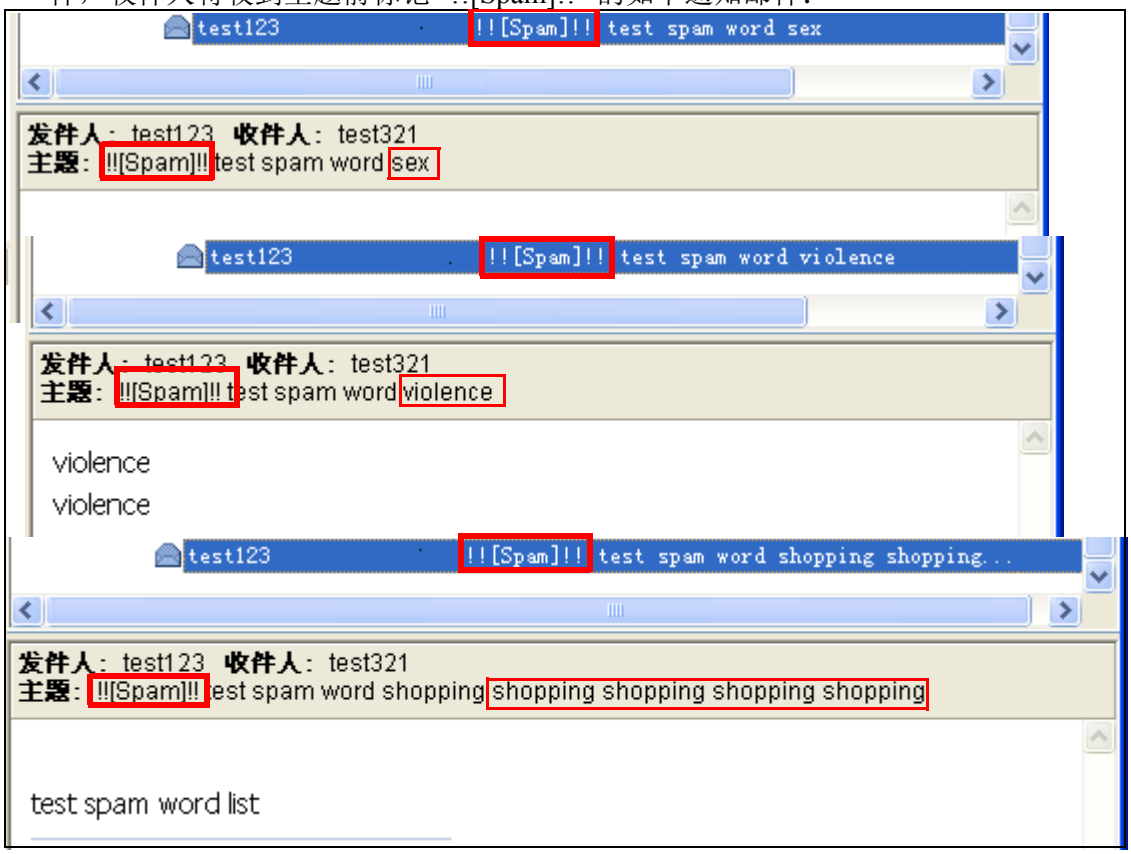
序号	日期时间	配置防护文件	文件名	文件类型	服务	源IP	病毒	状态	描述	动作
1	2014-04-09 05:22:30	High	testtarfile.tar	tar	FTP	20.1.1.100	未知	防病毒引擎	防病毒引擎过载或扫描失败。	放行
2	2014-04-09 05:22:27	High	wireshark-setup-1.0.6.exe	exe	FTP	20.1.1.100	未知	文件大小限制	此文件大小超过文件大小限制。	放行
3	2014-04-09 05:22:22	High	21.7z	7z	POP3	20.1.1.100	未知	压缩文件扫描	压缩文件层数超出限制（20）。	放行

6.2 监控 AS 功能

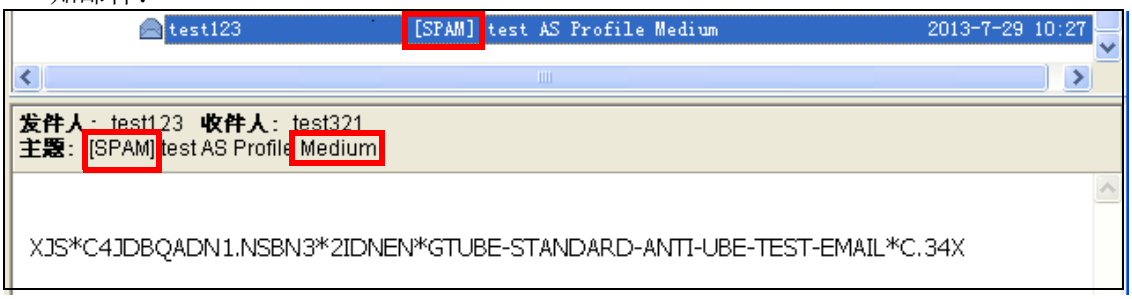
1. 发往允许收件人的邮件将被直接放行，发往阻断收件人的邮件将被阻断，同时 NISG 会生成相应的报警日志。
2. 发往阻断收件人的邮件被阻断时，收件人会收到主题如下的通知邮件：



3. 当发往客户端的邮件中包含指定关键字并且总分数达到阈值时， NISG 将会阻断该邮件，收件人将收到主题前标记 “!![Spam]!!” 的如下通知邮件：



4. NISG还将根据策略指定的缺省防护配置Medium中的反垃圾邮件规则扫描邮件，如果匹配规则，将丢弃邮件并生成报警日志，并返回收件人一封主题前标记 [Spam] 的通知邮件：



5. 选择**监控 > 报警 / 日志 > 反垃圾邮件报警**，查看生成的日志信息：

序号	日期时间	配置防护文件	服务	源IP	发件人	主题	附件	功能	信息	收件人	动作
1	2014-04-09 07:10:20	Medium	POP3	20.1.1.100	user666@123.com	test spam shopping	None	关键字过滤	关键字总分大于等于阈值(100)，已知的最高分关键字为(shopping)。		标记
2	2014-04-09 07:09:18	Medium	POP3	20.1.1.100	user666@123.com	test spam violence violence	None	关键字过滤	关键字总分大于等于阈值(100)，已知的最高分关键字为(violence)。		标记
3	2014-04-09 07:05:05	Medium	POP3	20.1.1.100	user888@123.com	未知	未知	收件人允许列表	命中收件人允许列表。	allowed_recipient@123.com	允许
4	2014-04-09 07:01:41	Medium	POP3	20.1.1.100	user888@123.com	test spam sex	None	关键字过滤	关键字总分大于等于阈值(100)，已知的最高分关键字为(sex)。		标记
5	2014-04-09 06:55:54	Medium	POP3	20.1.1.100	user555@123.com	未知	未知	收件人阻断列表	命中收件人阻断列表。	blocked_recipient@123.com	阻断
6	2014-04-09 07:01:41	Medium	POP3	20.1.1.100	user123@123.com	test AS Profile Medium	None	反垃圾邮件扫描	垃圾邮件分数为999.0>5。		标记

提示：如果发现配置错误，管理员可以点击监控页面的超链接编辑源 IP 或发件人地址。

6.3 监控 IPS 功能

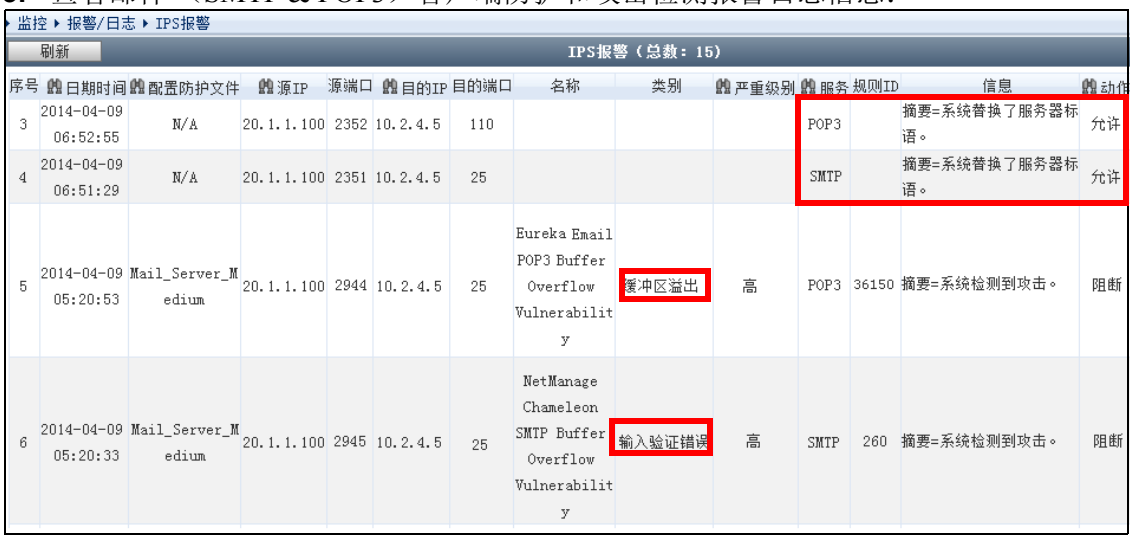
1. 选择**监控 > 报警 / 日志 >IPS 报警**，查看 IPS 监控信息。
2. 查看 HTTP 协议协议异常检测报警日志信息：

监控 ▸ 报警/日志 ▸ IPS报警

刷新 IPS报警（总数：15）

序号	日期时间	配置防护文件	源IP	源端口	目的IP	目的端口	服务	规则ID	信息	动作
5	2014-04-09 05:20:53	N/A	20.1.1.100	1817	123.126.42.251	80	HTTP		URL=php.weather.sina.com.cn/iframe/index/w_cl.php 摘要=检测到首部异常。	允许

3. 查看邮件 （SMTP & POP3）客户端防护和攻击检测报警日志信息：

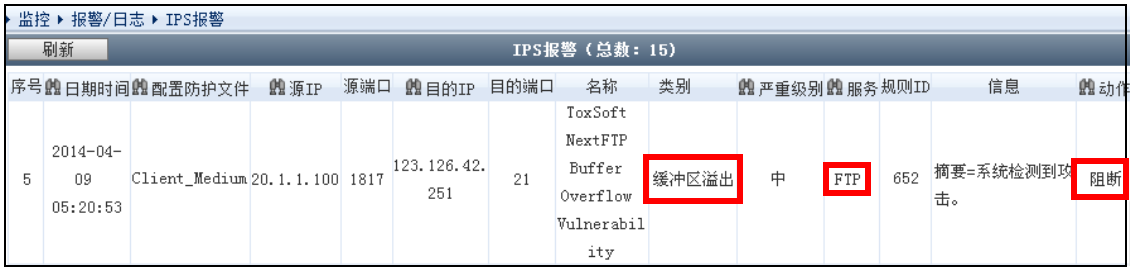


监控 ▸ 报警/日志 ▸ IPS报警

刷新 IPS报警（总数：15）

序号	日期时间	配置防护文件	源IP	源端口	目的IP	目的端口	名称	类别	严重级别	服务	规则ID	信息	动作
3	2014-04-09 06:52:55	N/A	20.1.1.100	2352	10.2.4.5	110				POP3		摘要=系统替换了服务器标语。	允许
4	2014-04-09 06:51:29	N/A	20.1.1.100	2351	10.2.4.5	25				SMTP		摘要=系统替换了服务器标语。	允许
5	2014-04-09 05:20:53	Mail_Server_Medium	20.1.1.100	2944	10.2.4.5	25	Eureka Email POP3 Buffer Overflow Vulnerability	缓冲区溢出	高	POP3	36150	摘要=系统检测到攻击。	阻断
6	2014-04-09 05:20:33	Mail_Server_Medium	20.1.1.100	2945	10.2.4.5	25	NetManage Chameleon SMTP Buffer Overflow Vulnerability	输入验证错误	高	SMTP	260	摘要=系统检测到攻击。	阻断

4. 查看 FTP 攻击报警日志信息：



监控 ▸ 报警/日志 ▸ IPS报警

刷新 IPS报警（总数：15）

序号	日期时间	配置防护文件	源IP	源端口	目的IP	目的端口	名称	类别	严重级别	服务	规则ID	信息	动作
5	2014-04-09 05:20:53	Client_Medium	20.1.1.100	1817	123.126.42.251	21	ToxSoft NextFTP Buffer Overflow Vulnerability	缓冲区溢出	中	FTP	652	摘要=系统检测到攻击。	阻断

5. 查看 DNS 协议异常检测报警日志信息：

监控 ▸ 报警/日志 ▸ IPS报警

刷新 IPS报警（总数：15）

序号	日期时间	源IP	源端口	目的IP	目的端口	服务	规则ID	信息	动作
9	2014-04-08 22:01:53	20.1.1.100	1075	210.83.210.155	53	DNS		摘要=检测到DNS异常。	阻断

6.4 监控 DNS 缓存中毒防御功能

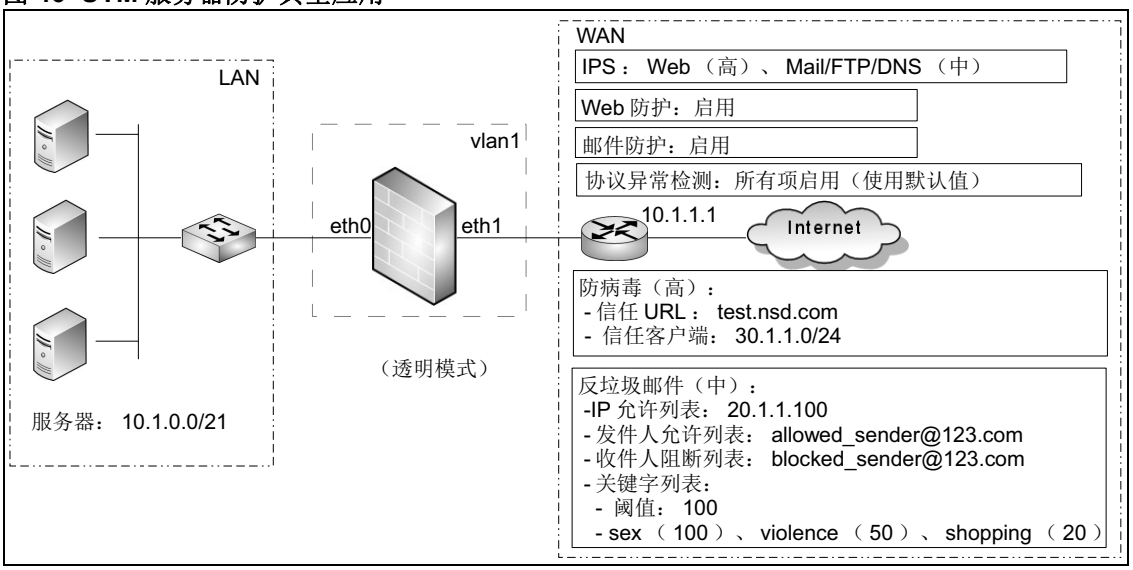
1. 受保护客户端发出的DNS请求ID将被不规则化，以防止攻击者利用DNS请求的ID编号规律进行攻击。
2. 指定时间内探测到的 DNS 不匹配应答数超过限制值时， DNS 请求将被阻断，同时产生日志。
3. 选择**监控 > 报警 / 日志 >IPS 报警**，查看生成的 DNS 日志信息：

序号	日期时间	源IP	源端口	目的IP	目的端口	服务	规则ID	信息	动作
9	2014-04-08 22:01:53	20.1.1.100	1075	210.83.210.155	53	DNS		摘要=DNS ID不规则化。	阻断
10	2014-04-08 22:01:53	20.1.1.100	1075	202.107.117.11	53	DNS		摘要=DNS ID不规则化。	阻断
11	2014-04-08 22:01:51	20.1.1.100	1075	210.83.210.155	53	DNS		域名=www.surfbouncer.com 摘要=请求域名在黑名单中。	阻断
12	2014-04-08 22:01:50	20.1.1.100	1075	202.107.117.11	53	DNS		域名=www.surfbouncer.com 摘要=请求域名在黑名单中。	阻断

范例 3：UTM 服务器防护典型应用

如下图所示，某公司内部网络 LAN 中部署多台服务器向外网提供服务，为对服务器的安全进行防护，管理员可以在 NISG 中配置相应的 Web、邮件、 FTP 和 DNS 服务器防护策略。

图 46 UTM 服务器防护典型应用

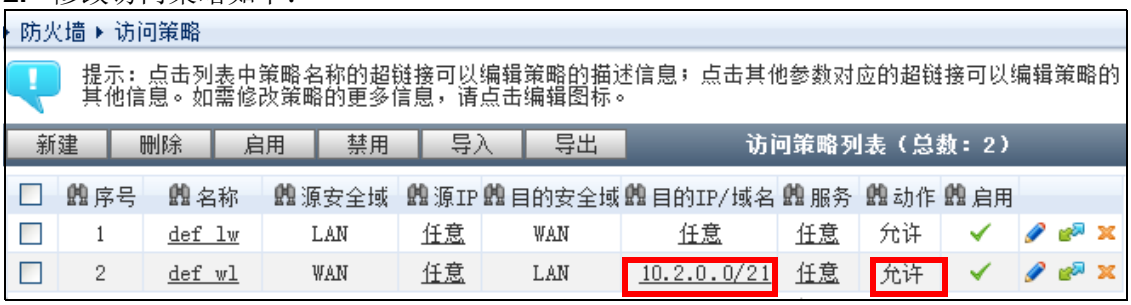


假设管理员初次登录时选择了透明模式，则本范例配置步骤如下：

1. 修改访问策略
2. 配置防病毒功能
3. 配置反垃圾邮件功能
4. 创建服务器防护策略
5. 配置 Web 防护
6. 配置邮件防护
7. 监控服务器防护

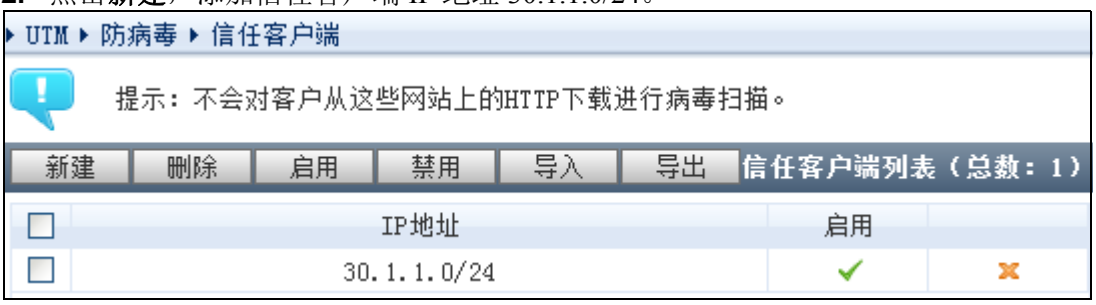
1. 修改访问策略

1. 选择**防火墙 > 访问策略**。
2. 修改访问策略如下：



2. 配置防病毒功能

1. 选择 **UTM> 防病毒 > 信任客户端**。
2. 点击**新建**，添加信任客户端 IP 地址 30.1.1.0/24。



3. 当添加启用了防病毒的服务器防护策略后，来自 30.1.1.0/24 网段的客户端访问将被直接放行，不进行防病毒检测。

3. 配置反垃圾邮件功能

1. 选择 **UTM> 反垃圾邮件 > 允许列表 >IP 地址**。
2. 添加允许 IP 地址 20.1.1.100：

3. 当相应的邮件服务器防护策略被启用后，发往和来自该允许 IP 的邮件将被直接放行。
4. 选择 **UTM> 反垃圾邮件 > 允许列表 > 发件人**。
5. 添加允许发件人地址 allowed_sender@123.com：

6. 当相应的邮件服务器防护策略被启用后，来自该允许发件人的邮件将被直接放行。
7. 选择 **UTM> 反垃圾邮件 > 阻断列表 > 发件人**。
8. 添加阻断发件人地址 blocked_sender@123.com：

9. 当相应的邮件服务器防护策略被启用后，发往该阻断收件人的邮件将被直接阻断。
10. 配置关键字列表。同范例 2。

4. 创建服务器防护策略

1. 选择 **UTM> 服务器防护 > 策略**。
2. 选择安全域 **LAN**，在 LAN 上开启服务器保护功能，创建以下策略：

- 4.1.Web 服务器防护策略
- 4.2. 邮件服务器防护策略
- 4.3.FTP 服务器防护策略
- 4.4.DNS 服务器防护策略

4.1.Web 服务器防护策略

3. 点击**新建**，创建 Web 服务器防护策略：

4. 点击**确定**。

4.2. 邮件服务器防护策略

5. 点击**新建**，创建邮件服务器防护策略：

6. 点击**确定**。

4.3.FTP 服务器防护策略

7. 点击**新建**，创建 FTP 服务器防护策略：

8. 点击**确定**。

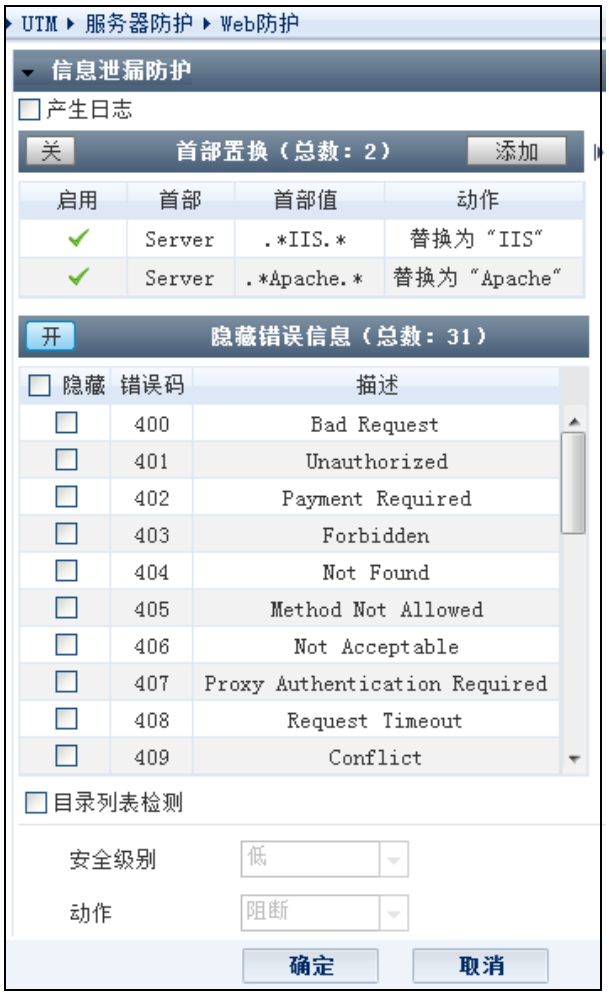
4.4.DNS 服务器防护策略

9. 点击**新建**，创建 DNS 服务器防护策略：

10. 点击**确定**。

5. 配置 Web 防护

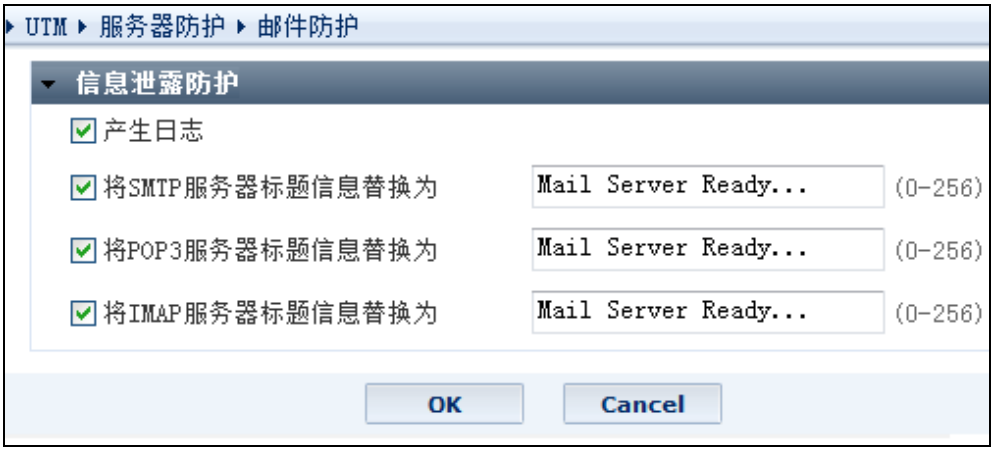
1. 选择 **UTM> 服务器防护 >Web 防护**。
2. 分别启用信息泄漏防护的各项功能，整体启用记录日志功能：



3. 点击**确定**。

6. 配置邮件防护

1. 选择 **UTM> 服务器防护 > 邮件防护**。
2. 启用邮件防护功能和记录日志功能：



3. 点击**确定**。点击 。

7. 监控服务器防护

- 7.1 监控 AV 功能
- 7.2 监控 AS 功能
- 7.3 监控 IPS 功能

7.1 监控 AV 功能

1. 当邮件附件被检测出病毒或超过限制时， NISG 会将该附件替换为系统预定义或自定义的通知消息附件：

- 如压缩包嵌套级别超过限定大小 （20）时，附件中通知消息内容如下：

```
The nesting levels of the archive file exceeds the limit(20). 21.7z is blocked.
```

- 如邮件附件检测出病毒时，附件中通知消息内容如下：

```
The attachment eicar.com is stripped.
<<Dangerous attachment has been stripped.   The file "eicar.com" has been stripped
because of a virus. It was infected with the "Eicar-Test-Signature.UNOFFICIAL" virus. >>
```

2. 当检测到邮件附件或 FTP 上载文件被病毒感染时，NISG 会根据指定动作处理邮件附件或 FTP 上载文件并产生相应的报警日志。除文件大小超过限制仍被放行外 （根据策略引用的 High 防护配置的定义），其他处理动作皆为阻断。

3. 选择**监控 > 报警 / 日志 > 防病毒报警**，查看防病毒监控信息。

序号	日期时间	配置防护文件	文件名	文件类型	服务	源IP	病毒	状态	描述	动作
1	2014-04-10 04:20:48	High	21.7z	7z	FTP	10.1.3.109	未知	压缩文件扫描	压缩文件层数超出限制（20）。	阻断
2	2014-04-10 04:15:31	High	wireshark-setup-1.0.6.exe	exe	FTP	10.1.3.109	未知	文件大小限制	此文件大小超过文件大小限制。	放行
3	2014-04-10 04:08:54	High	eicar.com	未知	SMTP	10.1.3.109	Eicar-Test-Signature.UNOFFICIAL	感染病毒	文件被病毒感染。	阻断
4	2014-04-10 04:07:54	High	eicar.com	未知	FTP	10.1.3.109	Eicar-Test-Signature.UNOFFICIAL	感染病毒	文件被病毒感染。	阻断

7.2 监控 AS 功能

1. 服务器防护中，匹配允许列表的邮件将被放行，匹配阻断列表的邮件将被阻断。但是与客户端防护不同的是， NISG 不会发送通知邮件给客户端。
2. 选择**监控 > 报警 / 日志 > 反垃圾邮件报警**，查看反垃圾邮件监控信息：

监控 ▸ 报警/日志 ▸ 反垃圾邮件报警

刷新　　反垃圾邮件报警（总数：12）

序号	日期时间	配置防护文件	服务	源IP	发件人	主题	附件	功能	信息	收件人	动作
1	2014-04-10 05:02:49	Medium	SMTP	10.1.3.109	blocked_sender@123.com	未知	未知	发件人阻断列表	命中发件人阻断列表。		阻断
2	2014-04-10 05:02:35	Medium	SMTP	10.1.3.109	allowed_sender@123.com	未知	未知	发件人允许列表	命中发件人允许列表。		允许
5	2014-04-10 04:38:54	Medium	SMTP	10.1.3.109	user999@123.com	test spam shopping	None	关键字过滤	关键字总分大于等于阈值(100)，已知的最高分关键字为(shopping)。		标记
6	2014-04-10 04:38:31	Medium	SMTP	10.1.3.109	user999@123.com	test spam violence violence	None	关键字过滤	关键字总分大于等于阈值(100)，已知的最高分关键字为(violence)。		标记
7	2014-04-10 04:33:09	Medium	SMTP	10.1.3.109	user999@123.com	test spam sex	None	关键字过滤	关键字总分大于等于阈值(100)，已知的最高分关键字为(sex)。		标记
8	2014-04-09 07:10:20	Medium	SMTP	20.1.1.100	user666@123.com	None	None	IP允许列表	命中IP允许列表。		阻断

3. 如发现误报，可点击监控页面的超链接修改 AS 相关设置。

7.3 监控 IPS 功能

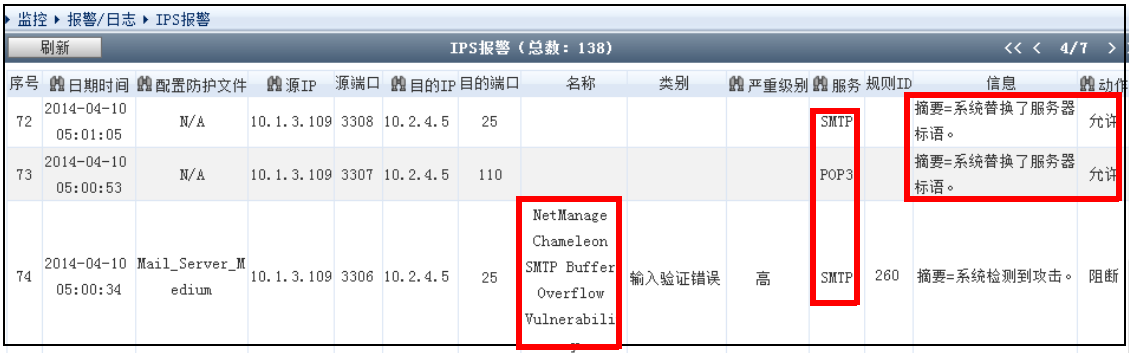
1. 选择**监控 > 报警 / 日志 >IPS 报警**，查看 IPS 监控信息。
2. HTTP 协议异常检测报警：

监控 ▸ 报警/日志 ▸ IPS报警

刷新　　IPS报警（总数：135）　　<< < 7/7 > >>

序号	日期时间	配置防护文件	源IP	源端口	目的IP	目的端口	服务	规则ID	信息	动作
127	2014-04-09 05:20:26	N/A	20.1.1.100	1658	10.1.3.109	8089	HTTP		URL=null 摘要=检测到非标准端口异常。	允许
128	2014-04-09 03:56:50	N/A	20.1.1.100	2293	10.1.3.109	8080	HTTP		URL=null 摘要=检测到非标准端口异常。	允许

3. 邮件协议 （SMTP&POP3）异常检测和服务器防护报警：



4. FTP 服务器防护报警：

5. DNS 服务器防护报警：

10.4. 配置参数说明

本节列出以下 UTM 功能的配置参数：

- 10.4.1. 概要信息
- 10.4.2. 出口控制
- 10.4.3. 客户端防护
- 10.4.4. 服务器防护
- 10.4.5. 防病毒
- 10.4.6. 反垃圾邮件
- 10.4.7.IPS
- 10.4.8. 通知消息

10.4.1. 概要信息

UTM 概要信息页面显示所有安全域的 UTM 信息。

表 173 UTM 概要信息页面参数

列名称	描述
安全域	配置 UTM 信息的安全域。
出口控制	在网络出口上控制出口流量，包括： • **应用控制**：控制用户访问 Internet 使用的应用。 • **URL 过滤**：过滤 URL 请求，阻断高危或可以网站流量。 • **DNS 控制**：阻断到未授权 DNS 域名的请求。 • **页面过滤**：过滤网页内容。
防护	用于防护指定安全域内的客户端或服务器。

10.4.2. 出口控制

出口控制用于在出口安全域上对用户流量进行安全检查。本节包含以下内容：

- 10.4.2.1. （出口控制）策略
- 10.4.2.2. 应用控制
- 10.4.2.3.URL 过滤
- 10.4.2.4.DNS 域名黑名单
- 10.4.2.5. 页面过滤

10.4.2.1. （出口控制）策略

出口控制策略包括应用控制策略、 URL 过滤策略、 DNS 域名黑名单 （开关）和页面过滤 （开关）。

10.4.2.1.1. 应用控制策略

应用控制策略定义了哪些应用将进行安全检测。管理员可以在指定的安全域上开启或关闭应用控制功能。

应用控制策略的匹配流程如下：

1. 根据源安全域、源 IP 地址、源用户查找优先级最高 （序号最小）的应用控制策略。如果未匹配到任何应用控制策略，则不再对用户访问进行应用控制。
2. 匹配策略的防护配置中指定的应用条目：
   a. 如果匹配到应用控制条目，则应用及其所属会话将按照该条目指定的动作进行处理；
   b. 如果未匹配到应用控制条目，则根据防护配置中指定的未知应用缺省处理动作进行处理。

提示：当应用不在应用知识库中 （不被 NISG 识别）时，则应用及其所属会话将被放行。

表 174 应用控制策略参数

参数	说明
开 / 关	在指定的安全域上启用或禁用应用控制功能。
序号	应用控制策略的优先级，序号越小，优先级越高。取值范围为 1-80000。 如果新建策略指定的序号已经存在，则新建策略将被插入已有策略的前面；如果新建策略未指定序号，则系统自动将其添加到策略列表的最后。
名称	应用控制策略的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?,"'\<>&#
源安全域	数据包发起的安全域，缺省为**任意**。
源 IP	添加类型包括： • **任意** （缺省） • **任意 IPv4 地址** • **任意 IPv6 地址** • **使用下表**：用户自定义 IP 地址，最多支持 4096 个 IP 地址或 IP 地址段。
源用户	添加类型包括： • **任意** （缺省） • **任意认证用户** • **使用下表**：可以选择包括未在 NISG 上创建的、在外部认证服务器上认证的用户。 每条策略最多支持 4096 个源用户。
防护配置	显示策略引用的防护配置名称。
日志	缺省启用日志功能。
启用	缺省启用应用控制策略。

提示：要查看应用控制的监控信息，请选择**监控 > 报警 / 日志 > 应用控制报警**。

10.4.2.1.2. URL 过滤策略

URL 过滤策略定义哪些 URL 允许访问、哪些 URL 禁止访问。管理员可以在指定的安全域上开启或关闭 URL 过滤功能。

URL 过滤策略的匹配流程如下：

1. NISG 根据源安全域、源 IP 地址、源用户查找优先级最高（序号最小）的 URL 过滤策略。如果未匹配到任何 URL 过滤策略，则不再对用户访问进行 URL 过滤。
2. 匹配 URL 过滤防护配置中的如下内容 （优先级从高到低）：
   a. 如果匹配到白名单条目，则用户访问将被放行；
   b. 如果匹配到黑名单条目，则用户访问将被阻断；
   c. 如果匹配到 URL 分类，则根据分类动作进行处理。
   d. 如果未匹配到任何 URL 分类，则分局未知 URL 分类缺省动作处理。

表 175 URL 过滤策略参数

参数	说明
开 / 关	在指定的安全域上开启或关闭 URL 过滤功能。
序号	URL 过滤策略的优先级，序号越小，优先级越高。取值范围为 1-80000。 如果新建策略指定的序号已经存在，则新建策略将被插入已有策略的前面；如果新建策略未指定序号，则系统自动将其添加到策略列表的最后。
名称	URL 过滤策略的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?,"'\<>&#
源安全域	数据包发起的安全域，缺省为**任意**。
源 IP	数据包发起的 IP 地址： • **任意** （缺省） • **任意 IPv4 地址** • **任意 IPv6 地址** • **使用下表**：用户自定义 IP 地址，最多支持 4096 个 IP 地址或 IP 地址段。
源用户	数据包发起的用户： • **任意** （缺省） • **任意认证用户** • **使用下表**：可以选择包括未在 NISG 上创建的、在外部认证服务器上认证的用户。 每条策略最多支持 4096 个源用户。
防护配置	显示引用的防护配置名称。
日志	缺省启用日志功能。
启用	缺省启用 URL 过滤策略。

提示：要查看 URL 过滤的监控信息，请选择**监控 > 报警 / 日志 >URL 过滤报警**。

10.4.2.2. 应用控制

应用控制控制出口应用流量。本节包含以下内容：

- 10.4.2.2.1. （应用控制）防护配置
- 10.4.2.2.2. 自定义应用
- 10.4.2.2.3. 应用知识库
- 10.4.2.2.4. （应用知识库）更新

提示：要查看应用控制的监控信息，请选择**监控 > 报警 / 日志 > 应用控制报警**。

10.4.2.2.1. （应用控制）防护配置

应用控制防护配置定义了 NISG 要进行控制的应用及每个应用的处理动作。所有虚拟系统最多支持 1024 个应用控制防护配置，每个防护配置最多支持 4096 个应用或应用分类。

表 176 应用控制防护配置参数

参数	说明
名称	应用控制防护配置的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?,"'\<>&#
引用	点击 查看引用防护配置的应用控制策略。 一个应用控制防护配置可以被多条策略引用，被应用控制策略引用的应用控制防护配置不能被删除。
描述	应用控制防护配置的描述信息。长度 0~255 字节， UTF-8 字符。不能包含以下字符：?"′ \<>&
不在下表中的应用的缺省处理动作	包括**阻断**和**放行**，缺省为**阻断**。
应用列表	添加要控制的应用，最多添加 256 个条目。 • **序号**：应用规则的匹配顺序，序号越小，越先匹配。如果新建防护配置的序号已经存在，则新建防护配置将被插入已有防护配置的前面；如果新建防护配置未指定序号，则系统自动将其添加到防护配置列表的最后。 • **类型**：包括指定应用和指定应用的过滤条件。可通过指定应用过滤条件批量添加应用，也可以通过指定应用名称添加单个应用。 • **应用名称**：应用的名称或分类。 • **动作**：对匹配到应用列表的应用的处理动作，包括**阻断**和**放行**，缺省为**阻断**。

10.4.2.2.2. 自定义应用

在应用控制防护配置中，管理员可以添加要控制的应用。添加的应用缺省按照 RFC 标准进行匹配。针对特定的应用，管理员可以添加自定义匹配条件进行应用控制。通过添加自定义应用，可以提高应用数据的转发速率。自定义应用的优先级高于 NISG 的协议识别，当两者存在冲突时以自定义应用为准。

自定义应用通过指定目的 IP 地址、传输层协议和目的端口来进行特殊的应用控制。一条自定义应用只能指定一个应用协议，如 DNS、 SIP 等。在自定义应用中，各应用之间的目的 IP 地址、传输层协议和目的端口不能同时相同。自定义应用列表最多添加 10240 个 IP+Port 对。

表 177 自定义应用参数

参数	说明
应用	进行自定义匹配的应用，可以是应用知识库中的任意应用。
应用协议	应用使用的协议，如 DNS、 FINGER、 FTP、 H.323、 HTTP、 IMAP、 MS-RPC、 MSSQL、 MYSQL、 NETBIOS、 NNTP、 ORACLE、 POP2、 POP3、 RTSP、 SIP、 SMB、 SMTP、 SNMP、 SSL、 SUN-RPC、 TELNET、 TFTP、 Tuxedo、 WINS 和 X11。
目的 IP	自定义应用数据包的目的 IP 地址。
传输协议	自定义应用使用的传输层协议，包括 TCP 和 UDP，缺省为 TCP。
目的端口	自定义应用数据包的目的端口号，取值范围为 1~65535。

10.4.2.2.3. 应用知识库

应用知识库中列出了 NISG 能够识别的所有 RFC 标准应用，包括应用的名称、分类、子分类、所用技术以及风险等级。过滤条件默认都为 Any，点击**查找**按钮查看所有应用。

表 178 应用知识库参数

参数	说明
分类	应用的分类，如交际类应用、商务类应用、多媒体类应用、网络构建类应用和通用互联网类应用。 Any 表示任意分类。
子分类	应用分类对应的子分类，如 Erp-Crm、 IP 协议、互联网实用类、内容共享、办公软件、加密隧道、即时通讯、图片视频、存储备份、数据库、文件共享、游戏、电子邮件、社交网络、管理软件、网站动态交互类、网络代理、网络会议、网络服务、网络电话、认证服务、路由协议、软件更新、远程控制、通用商务和音频。 Any 表示任意子分类。
技术	应用使用的技术，如基于浏览器类、客户端 - 服务器类、点对点类和网络协议类。 Any 表示任意技术。
风险	应用的风险等级，由低到高分为 5 种级别，如 、 、 、 和 。 Any 表示任意级别。
清空过滤条件	重置过滤条件并清空查询结果。
查找	输入应用的名称，点击**查找**，查询应用。
查找结果	显示匹配到过滤条件的应用。 将鼠标指向应用名称可以查看该应用的描述信息。

10.4.2.2.4. （应用知识库）更新

应用知识库规则支持手动和自动两种更新方式。规则升级包上载后立即生效，不需要重启。应用知识库更新不提供升级回退的功能。

应用知识库更新限制条件如下：

- License

  应用控制功能和应用知识库更新受 APPUP License 的限制。

- 虚拟系统

  NISG 只允许在根系统 （root）中进行应用知识库的更新操作，所有虚拟系统共享应用知识库更新后的结果。

表 179 应用知识库更新历史参数

参数	说明
规则库	应用知识库名称，固定为 Application-Control。
规则版本	应用知识库的版本。
引擎版本	应用知识库所对应的引擎版本。
上次更新时间	当前应用知识库上次更新时间。
显示 / 导出更新历史记录	点击查看或导出应用知识库的更新历史记录。 NISG 最大支持 50 条记录。

表 180 应用知识库更新模式参数

参数	说明
更新服务器地址	更新服务器的 URL 地址，可以为 IPv4/v6 地址或者域名。缺省为 nts.neusoft.com/autoupdate。
更新模式 （自动）	自动更新模式。
时间表	NISG 自动下载并安装升级包的定时更新时间。 当选择每天、每周或每日固定时间点自动升级时，系统在该时间点不会立即升级，而是在该时间点后两个小时内任意时间升级。
立即更新	当更新服务器地址和更新内容配置成功后，点击**立即更新**， NISG 立即从指定的更新服务器上获取升级包并执行安装。
手动上载升级包	上传本地的应用知识库更新包。

10.4.2.3. URL 过滤

UTM URL 过滤功能控制用户对 URL 的访问。本节包含以下内容：

- 10.4.2.3.1. （URL 过滤）常规设置
- 10.4.2.3.2. （URL 过滤）防护配置
- 10.4.2.3.3.URL 黑白名单
- 10.4.2.3.4. （URL 分类）更新

提示：要查看 URL 过滤的监控信息，请选择**监控 > 报警 / 日志 >URL 过滤报警**。

10.4.2.3.1. （URL 过滤）常规设置

表 181 URL 过滤常规设置参数

参数	说明
当 URL 过滤引擎扫描失败时	包括允许和阻断。
URL 分类查询	管理员和审计员可以输入要查询的 URL，点击**查找**按钮，查看 URL 分类。

10.4.2.3.2. （URL 过滤）防护配置

URL 过滤防护配置指定以下内容 （优先级从高到低）：

1. 一个白名单
2. 一个黑名单
3. URL 分类，包括：
   a. 指定 URL 分类的动作；
   b. 未知分类 URL 的缺省动作 （允许 / 阻断）。

所有虚拟系统最多可添加 1024 个 URL 过滤防护配置。

表 182 URL 过滤防护配置参数

参数	说明
名称	URL 过滤防护配置的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?,"'\ <>&#
引用	点击 查看引用 URL 过滤防护配置的策略。 一个 URL 过滤防护配置可以被多个 URL 过滤策略引用，且被引用的防护配置不能被删除。
描述	URL 过滤防护配置的描述信息。长度 0~255 字节， UTF-8 字符。不能包含以下字符：? "'\<>&
URL 白名单	勾选并选择 URL 白名单。
URL 黑名单	勾选并选择 URL 黑名单。
URL 分类	开启 URL 分类过滤功能。 • **未知分类 URL 的缺省处理动作**：包括**允许**和**阻断**，缺省为**允许**。 • **URL 分类列表**：开启或关闭指定的 URL 分类以及指定 URL 分类的处理动作。 URL 如果与被启用的 URL 分类匹配， NISG 则按照相应处理动作处理其请求；被禁用的 URL 分类，NISG 将直接放行。

10.4.2.3.3. URL 黑白名单

当一个 URL 请求到达 NISG 时，首先进行白名单的匹配，再进行黑名单的匹配。如果黑白名单存在冲突，则以白名单为准优先处理。 URL 黑白名单被 URL 过滤防护配置引用。

每个虚拟系统最多可添加 8 个 URL 黑名单和 8 个 URL 白名单。所有 URL 黑名单最多可添加 8000 个 URL 条目，所有 URL 白名单最多可添加 8000 个 URL 条目。

当 HTTP 会话请求被 URL 过滤阻断时，系统会自动向客户端发送一个通知消息作为 HTTP 服务器端的回应。关于通知消息的详细信息，请参见 10.4.8. 通知消息。

表 183 URL 黑白名单参数

参数	说明
名称	URL 黑名单或者白名单的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?, "'\ < > & #
类型	URL 黑白名单对应的类型，包括黑名单和白名单。
条目数	URL 黑白名单包含的 URL 条目数。
引用	点击 查看引用 URL 黑白名单的防护配置。一个 URL 黑白名单可以被多个防护配置引用。
描述	URL 黑白名单的描述信息。长度 0~255 字节， UTF-8 字符。不能包含以下字符：? " ′ \ < > &
URL 列表	向新建 URL 黑白名单中添加 URL 条目。 • **URL**：可以为 IP 地址或域名，支持通配符，取值范围为 2 ～ 255 字节。 • **描述**：长度 0~255 字节， UTF-8 字符。不能包含以下字符：? " ′ \ < > & • **启用**：启用 / 禁用 URL 条目。
导入	导入 URL 黑白名单。 重名的黑白名单不允许导入。当导入列表与已有列表之间存在重复条目时系统会提示是否继续添加；导入的列表本身存在重复条目时只添加一个条目。 导入文件的要求如下： • **文件类型**：文本文件。 • **文件格式**：每行一个 URL 地址。 • **文件扩展名**：.txt。

10.4.2.3.4. （URL 分类）更新

URL 分类支持手动和自动两种更新方式。规则升级包上载后立即生效，不需要重启。URL 分类更新不提供升级回退的功能。

URL 分类更新限制如下：

- License

  URL 分类更新受 UFOL License 的限制。

- 虚拟系统

  NISG 只允许在根系统 （root）中进行 URL 过滤规则更新操作，所有虚拟系统共享 URL 过滤规则更新后的结果。

表 184 URL 过滤规则更新历史参数

参数	说明
规则库	URL 过滤规则库名称，固定为 URL Filtering。
规则版本	URL 过滤规则库的版本。
引擎版本	URL 分类所对应的引擎版本。
上次更新时间	当前 URL 分类上次更新时间。
显示 / 导出更新历史记录	用于查看或导出 URL 分类的更新历史记录。 NISG 最大支持 50 条记录。

表 185 URL 过滤规则更新模式参数

参数	说明
更新服务器地址	URL 分类更新服务器的 URL 地址，可以为 IPv4/v6 地址或者域名。缺省为 nts.neusoft.com/urlrule。
更新模式 （自动）	自动更新模式。
时间表	NISG 自动下载并安装升级包的定时更新时间。 当选择每天、每周或每日固定时间点自动升级时，系统在该时间点不会立即升级，而是在该时间点后两个小时内任意时间升级。
立即更新	当更新服务器地址和更新内容配置成功后，点击**立即更新**， NISG 立即从指定的更新服务器上获取升级包并执行安装。
手动上载升级包	上传本地的 URL 过滤规则更新包。

10.4.2.4. DNS 域名黑名单

UTM 在网络出口安全域上对用户的 DNS 请求进行限制，阻断匹配黑名单的域名解析请求。需要在出口控制策略中为安全域开启 DNS 域名黑名单功能， DNS 域名黑名单的相应配置才会生效。

表 186 DNS 域名黑名单参数

参数	说明
产生日志	启用日志功能。
域名黑名单	配置项包括： • **域名**：到该域名的 DNS 请求将被丢弃。最多可添加 2048 个域名条目。 • **模糊匹配**：阻断域名部分匹配黑名单的 DNS 请求，缺省为禁用。 • **启用**：启用 / 禁用域名黑名单条目，缺省为启用。

提示：要查看 DNS 域名黑名单的监控信息，请选择**监控 > 报警 / 日志 >IPS 报警**。

10.4.2.5. 页面过滤

UTM 对用户访问的 Web 页面 （HTTP 服务器响应页面）上的文字内容进行检测，用于过滤包含特殊关键字的 Web 页面。如果含有管理员定义的关键字并且达到管理员自定义的分数阈值，则按照用户指定的动作进行处理。需要在出口控制策略中为安全域开启页面过滤功能，页面过滤的相应配置才会生效。

表 187 页面过滤参数

参数	说明
分数阈值	取值范围为 100 ～ 1000 之间的整数，缺省为 1000。当检测到的关键字的分数总合超过分数阈值时，则按照管理员配置的动作进行处理。
当 Web 页面上的关键字总分超过分数阈值时	包括**允许**和**阻断**，缺省为**阻断**。
产生日志	启用日志功能。
关键字过滤	关键字过滤规则列表，最大条目数 4096。 • **关键字**：要在 Web 页面的内容中过滤的字符串，允许输入 UTF-8 字符，不区分大小写，取值范围为 2 ～ 32 字节。最多可添加 4096 个关键字。 • **分值**：对 Web 页面的内容进行关键字检测时，每检查到一次与关键字相符的字符串所加的分值。取值范围为 1 ～ 100。 • **描述**：关键字的描述信息。长度 0~255 字节， UTF-8 字符。不能包含以下字符：? " ' \ < > & • **启用**：启用关键字过滤条目。

提示：要查看页面过滤的监控信息，请选择**监控 > 报警 / 日志 >IPS 报警**。

10.4.3. 客户端防护

本节包含以下内容：

- 10.4.3.1. （客户端防护）策略
- 10.4.3.2. （客户端防护）信任服务器列表
- 10.4.3.3. （客户端防护）信任邮件地址列表
- 10.4.3.4.DNS 缓存中毒防御

10.4.3.1. （客户端防护）策略

NISG 根据数据包的源 IP 地址和源用户查找优先级最高 （序号最小）的客户端防护策略。如果匹配，则按照策略设置进行处理；如果未匹配任何策略，则不进行客户端防护（IPS、防病毒、反垃圾邮件、协议异常检测和 DNS 缓存中毒防御）。

每安全域最多可添加 1024 条客户端防护策略。

表 188 客户端防护策略参数

参数	说明
开 / 关	为选择的安全域开启或关闭客户端防护。
序号	策略的优先级，序号越小，优先级越高，取值范围为 1-1024。 如果新建策略指定的序号已经存在，则新建策略将被插入已有策略的前面；如果新建策略未指定序号，则系统自动将其添加到策略列表的最后。
名称	策略的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?,"'\<>&#
源 IP （客户端 IP 地址）	安全域内被保护客户端的 IP 地址。添加类型包括： • **任意** （缺省） • **任意 IPv4 地址** • **任意 IPv6 地址** • **使用下表**：用户自定义 IP 地址，最多支持 4096 个 IP 地址或 IP 地址段。同一条客户端防护策略的客户端 IP 地址列表中不同同时添加 IPv4 地址和 IPv6 地址。
源用户	安全域内被保护的客户端： • **任意** （缺省） • **任意认证用户** • **使用下表**：可以选择包括未在 NISG 上创建的、在外部认证服务器上认证的用户。 每条策略最多支持 4096 个源用户。
IPS	缺省为禁用。设置 IPS 检测级别，包括低、中、高和自定义。 IPS 检测内容包括攻击签名检测和协议限制。详细信息请参见 10.4.7.IPS。
受保护应用	受客户端防护策略保护的应用，包括： • **Mail （POP3 和 IMAP）** • **FTP （FTP 下载）** • **Web （HTTP 下载）** • **DNS （DNS 缓存中毒防御）**
防病毒	开启或关闭基于 POP3 协议、IMAP 协议、FTP 下载和 HTTP 下载流量的防病毒检测功能，缺省为关闭。设置防病毒检测级别，包括低、中、高和自定义。关于详细信息，请参见 10.4.5. 防病毒。
反垃圾邮件	开启或关闭基于 POP3 协议流量的反垃圾邮件检测功能，缺省为关闭。设置反垃圾邮件检测级别，包括低、中、高和自定义。关于详细信息，请参见 10.4.6. 反垃圾邮件。

表 188 客户端防护策略参数 (*续*)

参数	说明
日志	缺省启用日志功能。
启用	缺省启用客户端防护策略。
最大受保护邮件	基于 POP3 或 IMAP 协议的邮件大小限制。 取值范围为 1~10MB，缺省为 10MB。如果邮件大小超出此限制，将不再进行后续的反病毒和防垃圾邮件检测。只有当防病毒或反垃圾邮件功能被启用，且邮件与阻止列表和允许列表都不匹配时，邮件大小限制的配置才生效。
协议异常检测	用于检测不符合 RFC 规定的异常流量。 检测 POP3 和 IMAP 流量异常： • **检测应答格式异常** • **检测应答长度异常** • **检测 MIME 格式和长度异常** 检测 HTTP 下载流量中以下内容的格式和长度异常： • **HTTP 版本** • **原因短语** • **状态码** • **首部** 检测 DNS 流量： • **格式和长度异常**
DNS 缓存中毒防御	开启或关闭 DNS 缓存中毒防御功能。 详细信息请参见 10.4.3.4.DNS 缓存中毒防御。

10.4.3.2. （客户端防护）信任服务器列表

信任服务器列表定义了指定安全域内受 NISG 信任的服务器。信任服务器列表在客户端防护策略之前进行匹配。 NISG 根据数据包的源安全域、服务器 IP 地址或域名以及服务器类型与信任服务器列表进行匹配。如果匹配到信任服务器条目，则后续数据包不再与客户端防护策略进行匹配，直接放行。

管理员可以为每个安全域配置一个信任服务器列表，每个信任服务器列表最多包含 32 个信任服务器条目。信任服务器列表默认为空。

表 189 信任服务器列表参数

参数	说明
开 / 关	在指定的安全域内启用或禁用信任客户端列表功能。
名称	信任服务器策略的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?,"'\<>&#
安全域	信任服务器所在的安全域。
IP 地址 / 域名 （服务器 IP 地址）	信任服务器的 IP 地址。添加类型包括： • **任意** （任意） • **任意 IPv4 地址** • **任意 IPv6 地址** • **使用下表**：用户自定 IP 地址或域名，最多支持 4096 个 IP 或 IP 地址段。
服务器类型	添加类型包括： • **任意** （任意） • **使用下表**：包括 Web 服务器、FTP 服务器、邮件服务器、DNS 服务器和其他类型服务器。

10.4.3.3. （客户端防护）信任邮件地址列表

信任邮件地址列表在客户端防护策略之后匹配，但是在反垃圾邮件检测之前进行。指定安全域内被保护的邮件客户端收到的所有邮件中，收件人或发件人在信任邮件地址列表中的邮件将不进行客户端防护。客户端防护中的信任邮件地址列表仅对 POP3 和 IMAP 流量进行检测。

每个安全域只能添加一个信任邮件地址列表，每个信任邮件地址列表最多可添加 128 条信任邮件地址。信任邮件地址列表默认为空。

表 190 信任邮件地址列表 （客户端保护）参数

参数	说明
开 / 关	在指定的安全域内启用或禁用信任邮件地址列表功能，缺省为关闭。
邮件地址	受信任的邮件地址或域名。允许配置 “(null)” 表示匿名发件人。

10.4.3.4. DNS 缓存中毒防御

DNS 缓存中毒防御功能用于防御客户端 DNS 缓存区中毒。管理员可以配置全局 DNS 缓存中毒防御功能，并在客户端防护策略中开启或关闭该功能。

表 191 DNS 缓存中毒防御参数

参数	说明
产生日志	启用日志功能。管理员另外需要在相应的客户端防护策略中开启日志和 DNS 缓存中毒防御功能，系统才能产生相应的日志。
启用 DNS 请求不规则化防护	改变 DNS 请求的 ID 号，使其不存在规律，防止攻击者利用 DNS 请求 ID 规律进行攻击。缺省为启用。
检测常不匹配的应答	缺省为启用。 • **最大不匹配应答数**：取值范围为 1 ～ 65535 次，缺省为 50 次。在限定时间 （**间隔**）内，产生超过一定数量的错误应答，可被看做发生了攻击。 • **间隔**：设置检测不匹配应答的间隔时间 （即计数周期），取值范围为 1 ～ 60 秒，缺省为 5 秒。

提示：要查看 DNS 缓存中毒防御功能的监控信息，请选择**监控 > 报警 / 日志 >IPS 报警**。

10.4.4. 服务器防护

本节介绍：

- 10.4.4.1. （服务器防护）策略
- 10.4.4.2. （服务器防护）信任客户端列表
- 10.4.4.3. （服务器防护）信任邮件地址列表
- 10.4.4.4.Web 防护
- 10.4.4.5. 邮件防护

10.4.4.1. （服务器防护）策略

NISG 根据服务器 IP 地址和服务器类型，查找与数据包匹配的服务器防护策略。如果匹配到策略，则按照匹配策略中规定的动作进行处理。如果没有匹配的策略，则不进行服务器防护。每个安全域最多配置 128 条服务器防护策略。

表 192 服务器防护策略参数

参数	说明
开 / 关	为指定安全域开启或关闭服务器防护功能。
序号	服务器防护策略的匹配优先级，序号越小，优先级越高。取值范围为 1-1024。 如果新建策略指定的序号已经存在，则新建策略将被插入已有策略的前面；如果新建策略未指定序号，则系统自动将其添加到策略列表的最后。
名称	服务器防护策略的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?,"'\<>&#
服务器 IP	受保护服务器的 IP 地址或 IP 地址范围，最多可添加 4096 个 IP 地址或 IP 地址段。
服务器类型	受保护服务器的类型，包括 Web、 Mail、 FTP、 Telnet、 DNS 和 Other。
IPS	启用或禁用 IPS 检测功能，缺省为禁用。设置 IPS 检测级别，包括低、中、高和自定义。为 Web、 Mail、 FTP、 Telnet、 DNS 和 Other 类型服务器防护策略配置 IPS 检测级别。关于详细信息，请参见 10.4.7.IPS。
防病毒	开启或关闭 FTP 上载和 SMTP 流量的防病毒检测功能，缺省为关闭。设置防病毒检测级别，包括低、中、高和自定义。关于详细信息，请参见 10.4.5. 防病毒。
反垃圾邮件	开启或关闭 SMTP 协议流量的反垃圾邮件检测功能，缺省为关闭。设置反垃圾邮件检测级别，包括低、中、高和自定义。关于详细信息，请参见 10.4.6. 反垃圾邮件。
防护	为 web 服务器防护策略启用 web 防护或为邮件服务器防护策略启用邮件防护。 关于详细信息，请参见 10.4.4.4.Web 防护和 10.4.4.5. 邮件防护。
启用	启用服务器防护策略。
日志	启用日志功能。

服务器防护策略为不同类型的服务器提供不同的防护功能：

表 193 服务器防护策略高级配置参数

类型	IPS	AV	AS	防护	针对特定服务器的配置
Web	是	--	--	**10.4.4.4. Web 防护**：全局配置，在策略中开启。	• **协议异常检测**：检测不符合 RFC 规定的 HTTP 上载流量。
Mail	是	是	是	**10.4.4.5. 邮件防护**：全局配置，在策略中开启。	• **最大受保护邮件**：基于 SMTP 协议邮件的大小限制。取值范围为 1~10 MB，缺省为 10 MB。如果邮件大小超出此限制，将不再进行后续的反病毒和防垃圾邮件检测。只有当防病毒或反垃圾邮件功能被启用，且邮件与阻止列表和允许列表都不匹配时，邮件大小限制的配置才生效。 • **协议异常检测**：检测不符合 RFC 规定的 SMTP、POP3、 IMAP 流量。
FTP 上载	是	是	--		--
Telnet	是	--	--		• **命令过滤**：对来自 ANSI、 Xterm、 VT100 和 VT52 等终端的 Telnet 流量进行检测。启用该功能后， NISG 将字符重组成串，然后与管理员自定义命令进行匹配。 • **用户自定义命令阻断列表**：最多可以配置 512 个自定义命令。每个命令由字母、数字、下划线组成，取值范围为 1 ～ 64 字节。
DNS	是	--	--		• **外部请求限制**：如果启用该功能，来自列表中安全域的外部 DNS 请求将被丢弃。对于来自这些受限安全域的 DNS 请求中，如果想允许对特定域名或 IP 地址的 DNS 请求，可以启用**授权域**功能并添加允许请求的 IP 地址或域名。 • **协议异常检测**：检测不符合 RFC 规定的 DNS 流量。
其他	是	--	--	--	--

10.4.4.2. （服务器防护）信任客户端列表

管理员可以为指定的安全域配置信任客户端列表，定义哪些客户端受保护。信任客户端列表在服务器防护策略之前匹配。此安全域被保护的服务器中，所有源自信任客户端发起的流量都不进行服务器防护安全检测，包括 IPS、防病毒和反垃圾邮件。

管理员可以为每个安全域配置一个信任客户端列表，最多包含 32 个信任客户端条目。信任客户端列表默认为空。

表 194 信任客户端列表参数

参数	说明
开 / 关	在指定的安全域内启用或禁用信任客户端列表。
名称	信任客户端策略的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?,"'\<>&#
安全域	信任客户端所在的安全域。
IP 地址（客户端 IP 地址）	列表中每个条目只能包含 1 个 IP 地址或 IP 地址段。 信任客户端 IP 地址列表添加类型： • **任意**（任意） • **任意 IPv4 地址** • **任意 IPv6 地址** • **使用下表**：用户指定 IP 地址。
源用户	信任源用户列表添加类型： • **任意**（任意） • **任意认证用户** • **使用下表**：可以选择包含不在 NISG 上创建的、在外部认证服务器上认证的用户。 每个信任列客户端表最多支持 4096 个源用户。

10.4.4.3. （服务器防护）信任邮件地址列表

管理员可以为指定的安全域配置信任邮件地址列表。信任邮件地址列表在服务器防护策略之后进行匹配，但是在反垃圾邮件检测之前。此安全域被保护的邮件服务器中，收件人或发件人与信任邮件地址列表匹配的邮件都不进行服务器防护安全检测，包括 IPS 的攻击签名检测和 MIME 剥离、防病毒和反垃圾邮件。服务防护中的信任邮件地址列表仅对 SMTP 流量生效。

每个安全域只能添加一个信任邮件地址列表，每个信任邮件地址列表最多可添加 128 条信任邮件地址。信任邮件地址列表默认为空。

表 195 （服务器防护）信任邮件地址列表参数

参数	说明
开 / 关	在指定的安全域内启用或禁用信任邮件地址。
邮件地址	信任发件人 / 收件人的邮件地址或域名。允许配置 “(null)” 表示匿名发件人。

10.4.4.4. Web 防护

Web 防护为系统全局配置，管理员可以在针对每安全域配置的每条服务器防护策略中开启或关闭 Web 防护。 Web 防护包括：

- 10.4.4.4.1. 信息泄露防护
- 10.4.4.4.2. 注入攻击防御

10.4.4.4.1. 信息泄露防护

NISG 分别针对于服务器端与客户端进行信息泄漏检测：

- **首部置换**：替换 HTTP 首部中包含的敏感信息（服务器名称或版本号等），以保护服务器。
- **隐藏错误信息**：隐藏 Web 服务器相关的错误信息，避免服务器内部信息泄露。
- **目录列表检测**：阻断 HTTP 传输中具有目录列表特征的信息，以防止信息泄漏或非法访问。该特性分为高、中、低三个级别：

表 196 目录列表检测级别

级别	检查内容	以下情况丢弃应答
低	只检查可疑的应答（包含以斜杠和反斜杠结尾的 URL）	被要求的目录出现在 HTML 页面的标题中； HTML 页面有父目录的链接。
中	检查所有 HTTP 应答	检查条件与低级相同
高	检查所有 HTTP 应答	HTTP 页面上有父目录的链接，且关键字为 “Parent Directory”

表 197 （Web 服务器）信息泄露防护参数

参数	说明
产生日志	启用 / 禁用日志功能。 管理员另外需要在相应的服务器防护策略中开启日志和 Web 防护功能，系统才能产生相应的日志。
首部置换	管理员最多可以添加 32 个首部置换条目。 • **首部**：1-32 字节长度，不可以输入控制字符及以下特殊字符：(、)、 <、 >、 @、 ,、 ;、 :、 \、 "、 /、 [、]、 ?、 =、 {、 }、 SP、 HT。 • **首部值**：要检测的首部值。支持正则表达式，长度为 1-32 字节。 • **动作**：当 NISG 检测到匹配的首部名和首部值时的替换动作，包括**删除**和**替换**，缺省为**替换**。替换值 1-32 字节，不可以输入 CRLF、 SP、 HT。 • **启用**：缺省为不启用。
隐藏错误信息	隐藏错误信息。
目录列表检测	缺省为禁用。 • **严重级别**：包括高、中和低，缺省为低。 • **动作**：查找到与当前级别限制匹配的目录列表信息时的处理动作，包括**允许**和**阻断**，缺省为**阻断**。

10.4.4.4.2. 注入攻击防御

NISG 可以防御以下几种注入攻击：

- **跨站脚本攻击**：指攻击者在具有信任关系的 Web 服务器和客户端之间，通过在 URL 中注入恶意的脚本，来获取包含用户的身份信息、资格证书的 Cookie 或者欺骗用户提供资格证书给攻击者。典型的攻击就是在 HTTP 请求中嵌入恶意的脚本，让用户不知不觉地将该请求发送到信任的服务器上。
- **LDAP 注入**：指攻击者在用户提交给 Web 应用的 HTTP 请求中，通过在 Form 和 URL 中注入非法的 LDAP 查询，来获取 LDAP 目录中存储的数据信息，导致用户信息泄露或者被添加、修改、甚至删除。 NISG 支持对 LDAP 注入攻击进行检测，检测用户提交给 Web 应用的 HTTP 请求，判断在 Form 和 URL 中是否包含非法的 LDAP 查询，再按照管理员设置的动作进行处理。 LDAP 注入分为过滤注入和 DN 注入。
  - **过滤注入**（Filter Injection，系统预定义）：被检测的内容如果包含 &、竖杠、感叹号、左括号或右括号的组合，即为检测到非法的 LDAP 查询内容。过滤注入由系统自动执行，无需用户设置。
  - **DN 注入**（DN Injection）：被检测的内容如果包含相对识别名称 （Relative Distinguished Name， RDN）字段的内容 （共七种：?xxx=， &xxx=， |xxx=， !xxx=， (xxx=，)xxx=， xxx=），即为检测到非法的 LDAP 查询内容。
- **SQL 注入**：指攻击者以 URL 或 Form 输入形式变相地到数据库中执行 SQL 命令。如果攻击成功，可能让数据库执行不希望执行的命令，导致信息泄露、改变数据库内容、甚至破坏数据库。
- **命令注入**：攻击者以 URL 或 Form 输入形式在 Web 服务器上执行系统命令。如果执行成功，攻击者可能以管理员的身份进入到 Web 服务器，造成巨大损失。

NISG 针对每种注入攻击提供三个级别的防御：

表 198 注入攻击防御级别

攻击类型	级别	检查位置	阻断含有以下内容的 HTTP 请求
跨站脚本攻击	低	• URL （path+query） • Form	脚本命令
	中	• URL （path+query） • Form	HTML 标签 （即 “<” 和 “>” 字符）
	高	• URL （path+query） • Form	HTML 标签或 HTML 标签的其他显示方式 （如：&lt，&gt， &#60， &#62）
LDAP 注入攻击	低	• URL （path） • Form	过滤注入定义的关键字
	中	• URL （path） • Form	过滤注入定义的关键字和 DN 注入定义的关键字
	高	• URL （path+query） • Form	过滤注入定义的关键字和 DN 注入定义的关键字
SQL 注入攻击	低	• URL （path） • Form	Distinct SQL 命令
	中	• URL （path） • Form	Non-Distinct SQL 命令
		• URL （path+query） • Form	Distinct SQL 命令
	高	• URL （path+query） • Form	Distinct SQL 命令或 Non-Distinct SQL 命令

表 198 注入攻击防御级别 (*续*)

攻击类型	级别	检查位置	阻断含有以下内容的 HTTP 请求
命令注入攻击	低	• URL （path） • Form	Distinct Shell 命令
	中	• URL （path） • Form	Non-Distinct Shell 命令
		• URL （path+query） • Form	Distinct Shell 命令
	高	• URL （path+query） • Form	Distinct Shell 命令或 Non-Distinct Shell 命令

表 199 （Web 服务器）注入攻击防御参数

参数	说明
产生日志	启用日志。管理员另外需要在相应的服务器防护策略中开启日志和 Web 防护功能，系统才能产生相应的日志。
跨站脚本攻击防御	管理员最多可以添加 64 条脚本命令。 • **严重级别**：包括高、中和低三种，缺省为低。 • **脚本命令**：NISG 缺省进行跨站脚本攻击防御的命令和管理员自定义的脚本命令， 1-32 字节，允许输入字母、数字以及除了空格和问号以外的特殊字符。 • **阻断**：缺省为不阻断。
LDAP 注入攻击防御	管理员最多可以添加 32 个识别名条目。 • **严重级别**：包括高、中和低三种，缺省为中。 • **识别名**：进行 LDAP 注入检测的关键字的名称，长度为 1 ～ 32 字节，允许输入字母、数字以及除了空格和问号以外的特殊字符。 • **阻断**：缺省为不阻断。
SQL 注入攻击防御	管理员最多可以添加 256 条 SQL 命令。 • **严重级别**：包括高、中和低三种，缺省为中。 • **类型**：包括 Distinct SQL 命令和 Non-Distinct SQL 命令。 • **SQL 命令**：进行 SQL 注入检测的命令，长度为 1 ～ 120 字节，允许输入字母、数字以及除了空格和问号以外的特殊字符。 • **阻断**：缺省为不阻断。
命令注入攻击防御	管理员最多可以添加 512 条 Shell 命令令。 • **严重级别**：包括高、中和低三种，缺省为中。 • **类型**：包括 Distinct Shell 命令和 Non-Distinct Shell 命令。进行命令注入检测的命令，长度为 1 ～ 120 字节，允许输入字母、数字以及除了空格和问号以外的特殊字符。 • **Shell 命令**：进行命令注入检测的命令，长度为 1 ～ 120 字节，允许输入字母、数字以及除了空格和问号以外的特殊字符。 • **阻断**：缺省为不阻断。

10.4.4.5. 邮件防护

服务器的部分应答信息可能会泄露服务器的配置信息，从而可能被攻击者利用。 NISG 信息泄漏功能可以将 SMTP、 POP3 和 IMAP 服务器的响应信息替换为管理员设置的信息，有效地防止服务器信息外露。

管理员可以全局配置邮件防护功能，然后在服务器防护策略中开启或关闭信息泄露防护功能。

表 200 （邮件服务器）信息泄露防护参数

参数	说明
产生日志	缺省为启用。管理员另外需要在相应的服务器防护策略中开启日志和邮件防护功能，系统才能产生相应的日志。
将 SMTP 服务器标题信息替换为	替换信息允许输入 UTF-8 所有字符，长度为 0 ～ 256 字节。
将 POP3 服务器标题信息替换为	替换信息允许输入 UTF-8 所有字符，长度为 0 ～ 256 字节。
将 IMAP 服务器标题信息替换为	替换信息允许输入 UTF-8 所有字符，长度为 0 ～ 256 字节。

10.4.5. 防病毒

NISG 的防病毒功能主要基于文件类型，对 NISG 策略允许的数据流进行病毒扫描。如果检测到病毒，则根据管理员配置的处理动作进行处理 （包括阻断或放行），并产生报警日志。 NISG 通过提供实时的防病毒规则升级功能。

当管理员启用防病毒功能时， NISG 默认对如下内容进行病毒扫描：

- 基于应用层协议 （包括 HTTP、 SMTP、 FTP、 POP3 和 IMAP）的数据流；
- 网络中传输的特定类型的文件；
- 网络中传输的压缩文件。

NISG 对文件的处理动作包括：

- 放行：指将文件正常转发，不对其做任何处理。
- 阻断：对于不同协议，其含义不同：
  - FTP 协议：阻断数据连接；
  - HTTP 协议：阻断 HTTP 会话；
  - Mail 协议（SMTP， POP3， IMAP）：从邮件中剥离有问题的附件，并提示客户端指定的提示信息。
- 扫描：进行病毒扫描。

提示：有关防病毒的监控信息，请选择**监控 > 报警 / 日志 > 防病毒报警**查看。

本节内容如下：

- 10.4.5.1. （AV）常规设置
- 10.4.5.2. 信任 URL
- 10.4.5.3. 信任 Web 服务器
- 10.4.5.4. 信任客户端
- 10.4.5.5. （防病毒）防护配置
- 10.4.5.6. （防病毒规则）更新

10.4.5.1. （AV）常规设置

当管理员在客户端防护策略或服务器防护策略中开启防病毒功能后，常规设置即生效。本节包含以下内容：

- 10.4.5.1.1. 启发式扫描
- 10.4.5.1.2. 压缩文件扫描
- 10.4.5.1.3. 扫描设置

10.4.5.1.1. 启发式扫描

启发式扫描能够检测潜在的威胁。 NISG 支持两种启发式扫描：针对钓鱼 （Phishing）网站进行的病毒检测以及基于算法进行的病毒检测。

表 201 启发式扫描参数

参数	说明
启用启发式扫描	勾选则表示启用启发式扫描，默认为禁用启发式扫描。
当引擎检测到病毒时	当启发式扫描发现病毒时， NISG 采取的处理动作，包括阻断文件和放行文件，默认为阻断文件。

10.4.5.1.2. 压缩文件扫描

表 202 压缩文件扫描参数

参数	说明
最大嵌套级别	一个嵌套压缩文档中的最大嵌套层数限制，取值范围为 1 ～ 20，缺省为 20。
压缩文件包含的最大文件数	一个压缩文档中的最大文件数目限制，取值范围为 1 ～ 15000 个，缺省为 10000。
当压缩文件超限时	处理动作包括**阻断文件**和**不经扫描放行文件**，缺省为**阻断文件**。

10.4.5.1.3. 扫描设置

NISG 默认对基于应用层协议（包括 HTTP， FTP， SMTP， POP3 和 IMAP）的数据流进行病毒扫描。管理员可以为 HTTP、 FTP、 SMTP、 POP3 及 IMAP 开启滴流 （持续下载）功能。当基于协议的内容接收完成后，防病毒引擎将对其进行病毒扫描。为了避免 NISG 缓存数据进行病毒扫描时数据传输阻塞引起连接超时， NISG 每隔一段时间将一部分已下载的未扫描数据传给客户端。

表 203 防病毒扫描设置参数

参数	说明
滴流	缺省为为 HTTP、 FTP、 SMTP、 POP3 及 IMAP 开启滴流 （持续下载）功能。可设置： • 时间间隔：向客户端传送数据的时间间隔。取值范围为 1 ～ 900 秒，缺省为 10 秒。 • 数据大小：NISG 每次向客户端发送的数据大小。取值范围为 1 ～ 10240 字节，缺省为 1 字节。
当引擎检测到病毒时	包括**阻断文件**和**放行文件**，缺省为**阻断文件**。
当引擎过载或扫描失败时	包括**阻断所有文件**和**不经扫描放行所有文件**，缺省为**不经扫描放行所有文件**。
当引擎初始化失败时	包括**阻断所有文件**和**不经扫描放行所有文件**，缺省为**不经扫描放行所有文件**。

10.4.5.2. 信任 URL

如果 HTTP 会话的 URL 与信任 URL 列表中的条目匹配，则 NISG 将不对其进行病毒扫描；反之，则继续进行防病毒扫描。每个信任 URL 列表最多支持 512 个 URL 条目。

表 204 信任 URL 列表参数

参数	说明
URL	不进行防病毒扫描的 URL 地址。允许输入 IPv4/v6 地址或域名。
启用 / 禁用	启用或禁用信任 URL 条目。
导入 / 导出	导入 / 导出信任 URL 列表文本文件。文本文件中每行一个 URL 地址及其状态 （enable/disable），如：www.test.com enable。导入的信任 URL 条目依次添加到信任 URL 列表中，完全重复的条目跳过不添加。

10.4.5.3. 信任 Web 服务器

如果 HTTP 会话的目的 IP 地址与信任 Web 服务器列表中的条目匹配，则 NISG 将不对其进行病毒扫描；反之，则继续进行防病毒扫描。每个信任 Web 服务器列表最多支持 512 个条目。

表 205 信任 Web 服务器列表参数

参数	说明
IP 地址	允许不进行防病毒扫描的服务器 IP 地址，添加类型包括 IPv4 地址 / 掩码和 IPv6 地址 / 前缀。
启用 / 禁用	启用或禁用信任服务端条目。
导入 / 导出	导入 / 导出信任 Web 服务器列表文本文件。文本文件中每行一个 IP 地址 / 掩码 （或前缀）及其状态 （enable/disable），如：192.168.1.64/27 enable。导入的信任 Web 服务器条目依次添加到信任 Web 服务器列表中，完全重复的条目跳过不添加。

10.4.5.4. 信任客户端

如果 HTTP 会话的源 IP 地址与信任客户端列表中的条目匹配，则 NISG 将不对其进行病毒扫描；反之，则继续进行防病毒扫描。每个信任客户端列表最多支持 512 个条目。

表 206 信任客户端列表参数

参数	说明
IP 地址	允许不进行防病毒扫描的客户端 IP 地址，添加类型包括 IPv4 地址 / 掩码和 IPv6 地址 / 前缀。
启用 / 禁用	启用或禁用信任客户端条目。
导入 / 导出	导入 / 导出信任客户端列表文本文件。文本文件中每行一个 IP 地址 / 掩码 （或前缀）及其状态 （enable/disable），如：192.168.1.64/27 enable。导入的信任客户端条目依次添加到信任客户端列表中，完全重复的条目跳过不添加。

10.4.5.5. （防病毒）防护配置

NISG 提供 3 个默认防病毒防护配置，名称分别是 Low、 Medium 和 High。默认的防病毒防护配置只能查看，不能删除或编辑。关于缺省防护配置的信息，请参见 10.5.1. 缺省防病毒防护配置。

防病毒防护配置只能在根系统中创建。系统最多支持 32 个防病毒防护配置。

表 207 防病毒防护配置参数

参数	说明
名称	防病毒防护配置的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?,"'\<>&# 缺省防护配置的名称代表了其防护级别。
引用	点击 查看引用防病毒防护配置的客户端防护策略或服务器防护策略。 一个防病毒防护配置可以被多条客户端或服务器防护策略引用，且正在被引用的防护配置不可以删除。
描述	防病毒防护配置的描述信息。长度 0~255 字节， UTF-8 字符。不能包含以下字符：? "'\<>&
最大扫描文件	可进行防病毒扫描的最大文件的大小。 • 1G 机型：默认 1 MB。取值范围为 1-5 MB。 • 2G 机型：默认 5 MB。取值范围为 1-10 MB。
当文件超过限定大小时	当文件（如果为压缩文件，则是解压后文件大小）超过可扫描的最大文件值时，NISG 采取的处理动作，包括**不经扫描放行文件**和**阻断文件**，缺省为**不经扫描放行文件**。
文件类型	NISG 病毒扫描功能可识别的文件类型。
动作	对特定类型文件采取的处理动作，包括**放行**、**扫描**和**阻断**。
启用文件类型特征识别	基于文件的特征来判断文件类型。特征识别的优先级比扩展名识别的优先级高。如果开启特征识别， NISG 优先选择特征识别结果作为处理文件的依据。
当文件类型不能识别时	当文件类型未被识别时的处理动作，包括**扫描**、**放行**和**阻断**。

10.4.5.6. （防病毒规则）更新

防病毒规则支持手动和自动两种更新方式。规则升级包上载后立即生效，不需要重启。防病毒规则更新不提供升级回退的功能。

防病毒规则更新功能限制如下：

- License

  防病毒规则更新受 AVUP License 的限制。

- 虚拟系统

  NISG 只允许在根系统 （root）中进行防病毒规则更新操作，所有虚拟系统共享防病毒规则更新后的结果。

表 208 防病毒规则库参数

参数	说明
规则库	防病毒规则库名称，固定为 Anti-Virus。
规则版本	最新的防病毒规则版本。
引擎版本	防病毒规则库所对应的引擎版本。
上次更新时间	当前防病毒规则库上次更新时间。
显示 / 导出更新历史记录	用于查看或导出防病毒规则库的更新历史记录。 NISG 最大支持 50 条记录。

表 209 防病毒规则更新模式参数

参数	说明
更新服务器地址	更新服务器的 URL 地址，可以为 IPv4/v6 地址或者域名。缺省为 nts.neusoft.com/virusrule。
更新模式 （自动）	防病毒规则自动更新的模式。
时间表	NISG 自动下载并安装升级包的定时更新时间。 当选择每天、每周或每日固定时间点自动升级时，系统在该时间点不会立即升级，而是在该时间点后两个小时内任意时间升级。
立即更新	当更新服务器地址和更新内容配置成功后，点击**立即更新**， NISG 立即从指定的更新服务器上获取升级包并执行安装。
手动上载升级包	上传本地的防病毒规则更新包。

10.4.6. 反垃圾邮件

NISG 反垃圾邮件功能功能能够有效阻断和过滤垃圾邮件。 NISG 只检测匹配到启用反垃圾邮件检测的客户端或服务器防护策略的流量。当管理员在客户端或服务器防护策略中开启反垃圾邮件检测功能后，反垃圾邮件设置即生效。

提示：有关反垃圾邮件的监控信息，请选择**监控 > 报警 / 日志 > 反垃圾邮件报警**。

本节包含以下内容：

- 10.4.6.1.（反垃圾有邮件）常规设置
- 10.4.6.2. 允许列表
- 10.4.6.3. 阻断列表
- 10.4.6.4. 关键字列表
- 10.4.6.5.（反垃圾邮件）防护配置
- 10.4.6.6.（反垃圾邮件规则）更新

10.4.6.1. （反垃圾有邮件）常规设置

当管理员在客户端防护策略或服务器防护策略中开启反垃圾邮件功能后，常规设置即生效。本节包含以下内容：

- 10.4.6.1.1. 规则设置
- 10.4.6.1.2. 扫描设置

10.4.6.1.1. 规则设置

当到达 NISG 的邮件匹配到相应的规则时，系统会根据规则对应的分数 （该分数为系统默认提供，管理员不能手动设置）为邮件进行分数累计。当累计分数达到管理员设置的分数阈值时，系统将根据管理员设置的动作对该邮件进行处理。关于分数阈值及其处理动作的设置请参见 10.4.6.5. （反垃圾邮件）防护配置。

管理员可以启用或禁用规则集，但是不可以编辑规则集。这套规则集适用于 SMTP 和 POP3，对系统性能几乎没有影响。详细信息，请参见 10.5.3. 反垃圾邮件规则集。

表 210 规则设置参数

参数	说明
启用 DNS 规则	缺省为禁用。 如果开启 DNS 规则， NISG 将根据管理员的配置对邮件内容进行 DNS 规则过滤。
规则设置	启用或禁用反垃圾邮件规则，缺省为启用所有反垃圾邮件规则。

10.4.6.1.2. 扫描设置

表 211 扫描设置参数

参数	说明
当引擎超时时	处理动作为**阻断所有邮件**和**不经扫描允许所有邮件通过**，缺省为**不经扫描允许所有邮件通过**。
当引擎过载或扫描失败时	处理动作为**阻断所有邮件**和**不经扫描允许所有邮件通过**，缺省为**不经扫描允许所有邮件通过**。

10.4.6.2. 允许列表

NISG 的反垃圾邮件功能，首先进行允许列表的匹配，再进行阻断列表的匹配。如果匹配允许列表（IP 允许列表、发件人允许列表或者收件人允许列表）中的条目，则不再进行后续的所有与反垃圾邮件相关的检测，直接转发邮件，或执行其他检测，如防病毒检测。每个虚拟系统包含一个 IP 允许列表、一个发件人允许列表和一个收件人允许列表。本节包含以下内容：

- 10.4.6.2.1.IP 允许列表
- 10.4.6.2.2. 发件人允许列表
- 10.4.6.2.3. 收件人允许列表

10.4.6.2.1. IP 允许列表

IP 允许列表检测适用于 SMTP。

表 212 IP 允许列表参数

参数	说明
IP 地址	SMTP 连接的源 IP 地址，允许输入 IPv4 地址或 IPv6 地址。 IP 允许列表最多支持 512 个 IP 地址条目。
类型	添加的允许 IP 地址类型，包括 IPv4 和 IPv6。
启用 / 禁用	启用 / 禁用 IP 允许列表条目，缺省为启用。
导入 / 导出	导入 / 导出 IP 允许列表文本文件。文本文件中每行一个 IP 地址及其状态 （enable/disable），如：10.1.1.1 enable。导入的 IP 地址条目依次添加到 IP 允许列表中，完全重复的条目跳过不添加。

10.4.6.2.2. 发件人允许列表

发件人允许列表检测适用于 SMTP 和 POP3。

表 213 发件人允许列表参数

参数	说明
邮件地址	发件人邮件地址或域名。 发件人允许列表最多支持 512 个邮件地址或域名条目。允许配置 “(null)” 表示匿名发件人地址。
启用 / 禁用	启用 / 禁用发件人允许列表条目。
导入 / 导出	导入 / 导出发件人允许列表文本文件。文本文件中每行一个邮件地址 （或域名）及其状态 （enable/disable），如：user1@test.com enable。导入的邮件地址条目依次添加到发件人允许列表中，完全重复的条目跳过不添加。

10.4.6.2.3. 收件人允许列表

收件人允许列表检测适用于 SMTP 和 POP3。

表 214 收件人允许列表参数

参数	说明
邮件地址	收件人邮件地址或域名。收件人允许列表最多支持 512 个邮件地址或域名条目。
启用 / 禁用	启用 / 禁用收件人允许列表条目。
导入 / 导出	导入 / 导出收件人允许列表文本文件。文本文件中每行一个邮件地址 （或域名）及其状态 （enable/disable），如：user1@test.com enable。导入的邮件地址条目依次添加到收件人允许列表中，完全重复的条目跳过不添加。

10.4.6.3. 阻断列表

NISG 的反垃圾邮件功能，首先进行允许列表的匹配，再进行阻断列表的匹配。如果没有匹配允许列表中的条目，则继续进行阻断列表的匹配。如果匹配阻断列表中的条目，则直接阻断连接。每个虚拟系统包含一个 IP 阻断列表、一个发件人阻断列表和一个收件人阻断列表。

本节包含以下内容：

- 10.4.6.3.1.IP 阻断列表
- 10.4.6.3.2. 发件人阻断列表
- 10.4.6.3.3. 收件人阻断列表

10.4.6.3.1. IP 阻断列表

IP 阻断列表检测适用于 SMTP 协议。

表 215 IP 阻断列表参数

参数	说明
IP 地址	SMTP 连接的源 IP 地址，允许输入 IPv4 地址和 IPv6 地址。 IP 阻断列表最多支持 512 个 IP 地址条目。
类型	添加的阻断 IP 地址类型，包括 IPv4 和 IPv6。
启用 / 禁用	启用 / 禁用 IP 阻断列表条目。
导入 / 导出	导入 / 导出 IP 阻断列表文本文件。文本文件中每行一个 IP 地址及其状态 （enable/disable），如：10.1.1.1 enable。导入的 IP 地址条目依次添加到 IP 阻断列表中，完全重复的条目跳过不添加。

10.4.6.3.2. 发件人阻断列表

发件人阻断列表检测适用于 SMTP 和 POP3。

表 216 发件人阻断列表参数

参数	说明
邮件地址	发件人邮件地址或域名。发件人阻断列表最多支持 512 个邮件地址或域名条目。允许配置 “(null)” 表示匿名发件人地址。
启用 / 禁用	启用 / 禁用发件人阻断列表条目。
导入 / 导出	导入 / 导出发件人阻断列表文本文件。文本文件中每行一个邮件地址 （或域名）及其状态 （enable/disable），如：user1@test.com enable。导入的邮件地址条目依次添加到发件人阻断列表中，完全重复的条目跳过不添加。

10.4.6.3.3. 收件人阻断列表

收件人阻断列表检测适用于 SMTP 和 POP3。

表 217 收件人阻断列表参数

参数	说明
邮件地址	收件人邮件地址或域名。收件人阻断列表最多支持 512 个邮件地址或域名条目。
启用 / 禁用	启用 / 禁用收件人阻断列表条目。
导入 / 导出	导入 / 导出收件人阻断列表文本文件。文本文件中每行一个邮件地址 （或域名）及其状态 （enable/disable），如：user1@test.com enable。导入的邮件地址条目依次添加到收件人阻断列表中，完全重复的条目跳过不添加。

10.4.6.4. 关键字列表

关键字列表对邮件的主题和正文进行关键字检测，如果含有管理员自定义的关键字，并且达到管理员自定义的分数阈值，则按照垃圾邮件进行处理；否则直接转发邮件，或执行其他检测，如防病毒检测。关键字列表检测适用于 SMTP 和 POP3。

表 218 关键字列表参数

参数	说明
分数阈值	分数阈值为管理员自定义的所有关键字总和的最大分值。取值范围为 100 ～ 1000，缺省为 100。 当检测到的关键字的分值总和达到分数阈值时，则按照垃圾邮件进行处理。
当邮件中的垃圾邮件关键字总分超过设定的阈值时	处理动作包括阻断邮件、允许邮件通过和标记邮件。缺省的处理动作为标记邮件。 如果动作为阻断邮件： • 对于 SMTP 协议，直接阻断当前连接。 • 对于 POP3 协议，阻断邮件，替换邮件主题为阻断通知消息且正文为空，并向服务器发送删除该邮件的操作。
关键字列表	添加要扫描的关键字： **关键字**：邮件的标题和正文中要过滤的字符串。关键字允许输入 UTF-8 所有字符，不区分大小写，长度为 2 ～ 32 字节。最多可添加 256 个关键字条目。 **位置**：包括主题和正文。 **分值**：1 ～ 100。对邮件的主题和正文进行关键字检测时，每检查到一次与关键字相符的字符串时即增加该分值。 **启用**：启用 / 禁用关键字列表条目。
导入 / 导出	导入 / 导出关键字列表文本文件。文本文件中每行一个关键字、位置、分值及其状态（enable/disable），如：test Subject,Body 100 enable。导入的垃圾邮件关键字条目依次添加到关键字列表中，完全重复的条目跳过不添加。

10.4.6.5. （反垃圾邮件）防护配置

反垃圾邮件防护配置定义了垃圾邮件分数阈值以及检测到垃圾邮件时 NISG 采取的动作。 NISG 提供 3 个默认反垃圾邮件防护配置，名称分别是 Low、 Medium 和 High。默认的反垃圾邮件防护配置只能查看，不能删除或编辑。关于详细信息，请参见 10.5.2. 缺省反垃圾邮件防护配置。

反垃圾邮件防护配置只能在根系统中创建。系统最多支持 32 个反垃圾邮件防护配置，包括三个缺省防护配置。

表 219 反垃圾邮件防护配置参数

参数	说明
名称	反垃圾邮件防护配置的名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?, "'\<>&#
引用	点击 查看引用反垃圾邮件防护配置的客户端防护策略或服务器防护策略。 一个反垃圾邮件防护配置可以被多条策略引用，正在被引用的防护配置不可以删除。
描述	反垃圾邮件防护配置的描述信息。长度 0~255 字节， UTF-8 字符。不能包含以下字符：? " ′ \<>&
分值	各级别垃圾邮件检测对应的分数阈值。分数的取值范围为 1 ～ 30 的整数，缺省为 5。 当邮件匹配管理员设置的规则时，系统会自动累计各规则的分数，如果分数总和大于等于相应级别的分数阈值，那么系统将根据该级别对应的动作对邮件进行处理。
动作	NISG 检测到垃圾邮件时的处理动作，包括如下三种： • **标记**：在邮件主题中添加管理员定义的标签后转发邮件。缺省为标记。 • **允许**：转发邮件。 • **阻断**：阻断连接。 如果是 SMTP 协议，则直接阻断当前连接。 如果是 POP3 协议，那么 NISG 将丢弃当前邮件，从 POP3 服务器上删除该垃圾邮件，并且阻断当前连接。
主题标签	当邮件分数累计达到各级别对应的分数阈值时，如果处理动作为标签，那么系统转发该邮件时，会在该邮件的主题中添加标签。邮件标题最大长度为 16 字节，标签允许输入 UTF-8 所有字符。缺省标签为 “[SPAM]”。

10.4.6.6. （反垃圾邮件规则）更新

反垃圾邮件规则支持手动和自动两种更新方式。反垃圾邮件规则升级包上载后立即生效，不需要重启。反垃圾邮件规则更新不提供升级回退的功能。

反垃圾邮件规则更新功能限制如下：

- License

  反垃圾邮件规则更新受 ASOL License 限制。

- 虚拟系统

  NISG 只允许在根系统 （root）中进行反垃圾邮件规则更新操作，所有虚拟系统共享反垃圾邮件规则更新后的结果。

表 220 反垃圾邮件规则库参数

参数	说明
规则库	反垃圾邮件规则库名称，固定为 Anti-Spam。
规则版本	最新的反垃圾邮件规则库版本。
引擎版本	反垃圾邮件规则库所对应的引擎版本。
上次更新时间	当前反垃圾邮件规则库上次更新时间。
显示 / 导出更新历史记录	用于查看或导出反垃圾邮件规则库的更新历史记录。 NISG 最大支持 50 条记录。

表 221 反垃圾邮件规则更新模式参数

参数	说明
更新服务器地址	更新服务器的 URL 地址，可以为 IPv4/v6 地址或者域名。缺省为 nts.neusoft.com/antispamrule。
更新模式	反垃圾邮件规则自动更新的模式，包括自动安装更新和从不检测更新。缺省为自动安装更新。
时间表	NISG 自动下载并安装升级包的定时更新时间。 当选择每天、每周或每日固定时间点自动升级时，系统在该时间点不会立即升级，而是在该时间点后两个小时内任意时间升级。
立即更新	当更新服务器地址和更新内容配置成功后，点击**立即更新**， NISG 立即从指定的更新服务器上获取升级包并执行安装。
手动上载升级包	上传本地的反垃圾邮件规则更新包。

10.4.7. IPS

NISG 提供针对客户端流量和服务器流量的 IPS 检测，包括攻击签名检测以及对各应用层协议的协议限制。

提示：有关 IPS 的监控信息，请选择**监控 > 报警 / 日志 >IPS 报警**。

本节包含以下内容：

- 10.4.7.1. （IPS）防护配置
- 10.4.7.2. 协议限制
- 10.4.7.3. （攻击签名规则）更新

10.4.7.1. （IPS）防护配置

IPS 防护配置是攻击签名规则的集合，管理员可以根据需要配置不同的防护配置。管理员还可以在 IPS 防护配置中开启或关闭协议限制功能。配置成功后，管理员可以在客户端防护策略和服务器防护策略中引用不同的 IPS 防护配置。 IPS 防护配置分为客户端和服务器两类：客户端 IPS 防护配置只能被客户端防护策略引用；服务器 IPS 防护配置只能被服务器防护策略引用。

NISG 提供 21 个缺省 IPS 防护配置。缺省的 IPS 防护配置只能查看，不能删除或编辑。管理员还可以添加自定义 IPS 防护配置。 IPS 防护配置只能在根系统中创建。系统最多支持 63 个 IPS 防护配置，包括 21 个缺省 IPS 防护配置。

NISG 提供基于协议分析的攻击签名检测。攻击签名检测是一种根据具体攻击特征进行攻击检测的攻击防御技术。一种攻击往往有诸多抽象的特征，攻击签名规则是指同一种攻击所包含的特征 （签名）的集合。 NISG 根据规则识别出特定类型的攻击，并设置处理动作，包括允许和阻断。详细信息，请参见 10.5.5. 攻击签名规则。

表 222 IPS 防护配置参数

参数	说明
名称	IPS 防护配置的名称。 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?,"'\<>&# 缺省 IPS 防护配置分别以 _Low， _Medium 和 _High 命名，分别表示了低、中、高三个级别的 IPS 防护。 • **低：**仅防御严重级别为高的攻击。 • **中：**防御级别为高和中的攻击。 • **高：**防御所有攻击。
类型	IPS 防护配置的类型，包括客户端和服务器。 • 如果选择客户端类型，则只能配置目标为客户端或双向的攻击签名规则。 • 如果选择服务器类型，则只能配置目标为服务器或双向的攻击签名规则。
引用	点击 查看引用 IPS 防护配置的客户端或服务器防护策略。 一个 IPS 防护配置可以被多个客户端或服务器防护策略引用，被引用的防护配置不能被删除。
描述	IPS 防护配置的描述信息。长度 0~255 字节， UTF-8 字符。不能以下字符：? " ' \<>&
服务器类型	当 IPS 防护配置的类型为服务器时，可以进一步配置服务器的类型，包括 Web、 Mail、 FTP、 Telnet、 DNS 和 Other。

表 222 IPS 防护配置参数 (*续*)

参数	说明
协议限制	用于启用或禁用 IPS 防护配置的协议限制功能： • 针对客户端：开启或关闭 POP3、 IMAP、 SMTP 和 DNS 的协议限制功能。 • 针对服务器：开启或关闭 HTTP、 POP3、 IMAP、 SMTP 和 DNS 的协议限制功能。
攻击签名规则列表	为新建 IPS 防护配置设置攻击签名规则。 鼠标指向攻击签名规则列表表头时，会出现 ▼ 图标，点击该图标可以编辑要显示的参数。
允许 / 阻断	设置攻击签名规则的动作，包括允许和阻断。 • 如果一条规则被启用且动作设为允许， NISG 将放行匹配该规则的流量。 • 如果一条规则被启用且动作设为阻断， NISG 将阻断匹配该规则的流量。
启用 / 禁用	启用和禁用攻击签名规则。

10.4.7.2. 协议限制

协议限制为应用级协议的访问控制。协议本身的一些漏洞会被攻击者利用，具有潜在风险。 NISG 分别为客户端防护和服务器防护提供了协议限制功能。管理员可以全局配置协议限制并在 IPS 防护配置中开启或关闭协议限制功能。一旦修改了协议限制的全局配置并保存，启用了协议限制功能的 IPS 防护配置也将随之更新。

NISG 提供以下协议限制：

- 10.4.7.2.1.HTTP 协议限制
- 10.4.7.2.2.SMTP 协议限制
- 10.4.7.2.3.POP3 协议限制
- 10.4.7.2.4.IMAP 协议限制
- 10.4.7.2.5.DNS 协议限制

10.4.7.2.1. HTTP 协议限制

HTTP 协议限制功能只能在 Web 服务器类型的 IPS 防护配置中开启。

表 223 HTTP 协议限制参数

参数	说明
级别	包括高、中、低和自定义四个级别，缺省级别为自定义。
产生日志	启用日志功能。管理员另外需要在相应的服务器防护策略中开启日志功能。
最大首部数	• **取值**：1 ～ 1024。 • **动作**：当首部数超出限制时的处理动作，包括允许和阻断。
最大 URL 长度	• **取值**：1 ～ 2048 字节。 • **动作**：当长度超出限制时的处理动作，包括允许和阻断。
最大请求正文长度	• **取值**：1 ～ 65535 字节。 • **动作**：当长度超出限制时的处理动作，包括允许和阻断。
最大首部长度	• **取值**：1 ～ 2048 字节。 • **动作**：当长度超出限制时的处理动作，包括允许和阻断。
首部长度限制	• **首部名称**：最多添加 32 个首部。 • **最大长度**：1 ～ 2048 字节。该项设置的首部长度需要小于通用的最大首部长度值。 • **启用**：当首部长度超出限制时，阻断连接。
请求方式阻断列表	阻断特定请求方式（已选命令）的 HTTP 流量。
阻断非 ASCII 码首部	如果在首部中检测到非 ASCII 码字节，则阻断连接。
阻断 Form 字段的非 ASCII 码字符	如果在 Form 字段中检测到非 ASCII 码字符，则阻断连接。

10.4.7.2.2. SMTP 协议限制

表 224 服务器防护中的 SMTP 协议限制参数

参数	说明
级别	包括高、中、低和自定义四个级别，缺省级别为中。
产生日志	启用日志功能。管理员另外需要在相应的服务器防护策略中开启日志功能。
最大命令长度	• **取值**：1 ～ 1024 字节。 • **动作**：当长度超出限制时的处理动作，包括允许、阻断和拒绝。
最大参数长度	• **取值**：1 ～ 512 字节。 • **动作**：当长度超出限制时的处理动作，包括允许、阻断和拒绝。
最大 NOOP 命令数	• **取值**：1 ～ 128。 • **动作**：当单次会话中命令次数超出限制时的处理动作，包括允许和阻断。NOOP 命令不执行任何操作，但是连续出现该命令可能为网络攻击。
最大命令数	• **取值**：1 ～ 256。 • **动作**：当单次会话中命令次数超出限制时的处理动作，包括允许和阻断。
最大未知命令数	• **取值**：1 ～ 128 之间的整数。 • **动作**：当单次会话中命令次数超出限制时的处理动作，包括允许和阻断。
阻断未知命令	阻断未知命令。管理员自定义命令不属于未知命令。
自定义 SMTP 命令列表	添加用户自定义命令，最大条目数 32。 命令中不允许包含空格与制表符，长度为 4 ～ 8 字节。
命令阻断列表	阻断已选 SMTP 命令。
转发时添加 Received 头字段	转发时添加 Received 头字段。
剥离带有多个 Content-Type 头字段的 MIME 字段	剥离带有多个 Content-Type 头字段的 MIME 字段。
剥离带有多个 Encoding 头字段的 MIME 字段	剥离带有多个 Encoding 头字段的 MIME 字段。
剥离带有未知 Encoding 头字段的 MIME 字段	剥离带有未知 Encoding 头字段的 MIME 字段。
剥离所有邮件附件	剥离所有邮件附件。
剥离所有分片邮件	剥离所有分片邮件。
阻断收件人没有域名的邮件	阻断收件人没有域名的邮件。

表 225 客户端防护中的 SMTP 协议限制参数

参数	说明
产生日志	启用日志功能。管理员另外需要在相应的客户端防护策略中开启日志功能。
最大应答长度	• **取值**：1 ～ 2048 字节。 • **动作**：当长度超出限制时的处理动作，包括允许和阻断。

10.4.7.2.3. POP3 协议限制

表 226 服务器防护中的 POP3 协议限制参数

参数	说明
级别	包括高、中、低和自定义四个级别，缺省级别为中。
产生日志	启用日志功能。管理员另外需要在相应的服务器防护策略中开启日志功能。
最大命令长度	• **取值**：1 ～ 1024 字节。 • **动作**：当命令长度超出限制时的处理动作，包括允许、阻断和拒绝。
最大参数长度	• **取值**：1 ～ 512 字节。 • **动作**：当参数长度超出限制时的处理动作，包括允许、阻断和拒绝。
最大 NOOP 命令数	• **取值**：1 ～ 128。 • **动作**：当单次会话中 NOOP 命令次数超出限制时的处理动作，包括允许和阻断。 NOOP 命令不执行任何操作，连续出现该命令可能为网络攻击。
最大命令数	• **取值**：1 ～ 256。 • **动作**：当单次会话中命令次数超出限制时的处理动作，包括允许和阻断。
最大未知命令数	• **取值**：1 ～ 128。 • **动作**：当单次会话中未知命令次数超出限制时的处理动作，包括允许和阻断。
阻断未知命令	阻断未知命令。管理员自定义命令不属于未知命令。
自定义 POP3 命令列表	添加用户自定义命令，最大条目数 32。 命令中不允许包含空格与制表符，长度为 4 ～ 8 字节。
命令阻断列表	阻断的已选 POP3 命令。

表 227 客户端中的 POP3 协议限制参数

参数	说明
产生日志	启用日志功能。管理员另外需要在相应的客户端防护策略中开启日志功能。
最大应答长度	• **取值**：1 ～ 2048 字节。 • **动作**：当应答长度超出限制时的处理动作，包括允许和阻断。

10.4.7.2.4. IMAP 协议限制

表 228 服务器防护中的 IMAP 协议限制参数

参数	说明
级别	包括高、中、低和自定义四个级别，缺省级别为中。
产生日志	启用日志功能。管理员另外需要在相应的服务器防护策略中开启日志功能。
最大命令长度	• **取值**：1 ～ 2048 字节。 • **动作**：当命令长度超出限制时的处理动作，包括允许、阻断和拒绝。
最大参数长度	• **取值**：1 ～ 1024 字节。 • **动作**：当参数长度超出限制时的处理动作，包括允许、阻断和拒绝。
最大 Tag 长度	• **取值**：1 ～ 512 字节。 • **动作**：当 Tag 长度超出限制时的处理动作，包括允许、阻断和拒绝。
最大 NOOP 命令数	• **取值**：1 ～ 128。 • **动作**：当单次会话中 NOOP 命令次数超出限制时的处理动作，包括允许和阻断。NOOP 命令不执行任何操作，连续出现该命令可能为网络攻击。
最大命令数	• **取值**：1 ～ 256。 • **动作**：当单次会话中命令次数超出限制时的处理动作，包括允许和阻断。
最大未知命令数	• **取值**：1 ～ 128。 • **动作**：当单次会话中未知命令次数超出限制时的处理动作，包括允许和缺省阻断。
阻断未知命令	阻断未知命令。管理员自定义命令不属于未知命令。
自定义 IMAP 命令列表	添加用户自定义命令，最大条目数 32。 命令中不允许包含空格与制表符，长度为 4 ～ 16 字节。
命令阻断列表	阻断已选 IMAP 命令。

表 229 客户端防护中的 IMAP 协议限制参数

参数	说明
产生日志	启用日志功能。管理员另外需要在相应的客户端防护策略中开启日志功能。
最大应答长度	• **取值**：1 ～ 4096 字节。 • **动作**：当应答长度超出限制时的处理动作，包括允许和阻断。

10.4.7.2.5. DNS 协议限制

表 230 服务器防护中的 DNS 协议限制参数

参数	说明
产生日志	启用日志功能。管理员另外需要在相应的服务器防护策略中开启日志功能。
除以下授权 IP 地址外，阻断 DNS 区域传输	添加允许 DNS 区域传输的授权 IP。来自列表中 IP 之外的 DNS 请求将被丢弃。最多添加 128 个 IP 地址条目。

表 231 客户端防护中的 DNS 协议限制参数

参数	说明
产生日志	启用日志功能，缺省启用。管理员另外需要在相应的客户端防护策略中开启日志功能。
UDP 资源记录数限制	限制资源记录数。启用该功能后，管理员可以为**最大回答记录数**、**最大授权记录数**和**最大附加记录数**配置如下内容： • **取值**：1 ～ 10，缺省为 4。 • **动作**：包括允许和阻断，缺省为允许。

10.4.7.3. （攻击签名规则）更新

NISG 通过加载攻击签名规则升级包更新攻击签名规则。攻击签名规则升级包上载后立即生效，不需要重启系统。攻击签名规则更新不支持升级回退。

攻击签名规则更新功能限制如下：

- License

  攻击签名规则更新需要 IPSUP License 的许可。

- 虚拟系统

  NISG 只允许在根系统 （root）中进行攻击签名规则更新操作，所有虚拟系统共享攻击签名规则更新后的结果。

表 232 攻击签名规则库参数

参数	说明
规则库	攻击签名规则库名称，默认包括 HTTP、 DNS、 FTP、 IMAP、 ORACLE、 OTHERS、 POP3、 SIP、 SMTP、 TELNET、 TFTP 和 BACKDOOR。
规则版本	最新的攻击签名规则库版本。
引擎版本	攻击签名规则库所对应的引擎版本。
上次更新时间	当前攻击签名规则库上次更新时间。
显示 / 导出更新历史记录	用于查看或导出攻击签名规则库的更新历史记录。 NISG 最大支持 50 条记录。

表 233 攻击签名规则更新模式参数

参数	说明
更新服务器地址	更新服务器的 URL 地址，可以为 IPv4/v6 地址或者域名。缺省为 nts.neusoft.com/autoupdate。
更新模式 （自动）	攻击签名规则自动更新的模式，包括自动安装更新和从不检测更新。缺省为自动安装更新。
时间表	NISG 自动下载并安装升级包的定时更新时间。 当选择每天、每周或每日固定时间点自动升级时，系统在该时间点不会立即升级，而是在该时间点后两个小时内任意时间升级。
立即更新	当更新服务器地址和更新内容配置成功后，点击**立即更新**， NISG 立即从指定的更新服务器上获取升级包并执行安装。
手动上载升级包	上传本地的攻击签名规则更新包。

10.4.8. 通知消息

通知消息用于替换被防病毒、 URL 过滤、协议限制、反垃圾邮件或攻击签名检测功能阻断的内容。 NISG 的通知消息分为两种：

- **用户自定义通知消息**：可通过 WebUI 进行配置。
- **系统预定义通知消息**：系统预定义，不可编辑。

用户自定义通知消息

表 234 缺省通知消息

发送时机	长度（UTF-8）	缺省消息
被 URL 分类阻断时	1-8192	<< The URL is blocked due to URL Category. URL: #URL# Category: #CATEGORYNAME#>>
被 URL 黑名单阻断时	1-8192	<< The URL is blocked due to URL Blacklist. URL: #URL#>>
HTTP 下载文件被病毒感染时	1-8192	<< High security alert!!! You are not permitted to download the file because it is infected with the virus "#VIRUS#". URL: #URL#>>
邮件附件被病毒感染时	1-512	<< Dangerous attachment has been stripped. The file "#FILENAME#" has been stripped because of a virus. It was infected with the "#VIRUS#" virus. >>
邮件附件被剥离时 （协议限制）	1-512	<< The attachment of this e-mail has been stripped. >>
邮件字段被剥离时 （协议限制）	1-512	<< One or more MIME parts of this e-mail have been stripped. >>

系统预定义通知消息

系统通知消息又分为：

- 防病毒检测替换附件的通知消息

  NISG 扫描出邮件附件含有病毒且处理动作为阻断时，将使用一个名为 attchment.txt 的通知消息文件替换邮件附件。替换文件中的通知消息内容如下表所示。

表 235 附件被扫描出病毒而被阻断时的系统通知消息

功能名称	文件 （attachment.txt）中包含的通知消息
当文件超过限定大小时	#FILENAME# oversizes the maximum file size (#Maximum_File_Size#).
当文件类型被识别时	File type is recognized. The type of #FILENAME# is #File_Type#. #File_Type# file is blocked.
当文件类型不能识别时	File type is unrecognized. The type of #FILENAME# is Unknown. Unknown file is blocked.
当压缩文件包含的文件数超过最大限制时	The number of files within the archive file exceeds the limit (#Maximum_Files#). #FILENAME# is blocked.
当压缩文件的嵌套级别超过最大限制时	The nesting levels of the archive file exceeds the limit (#Maximum_Nesting#). #FILENAME# is blocked.
当引擎过载或扫描失败时	The AV engine is overloaded or the scan failed. #FILENAME# is blocked.
当引擎超时时	The AV engine times out. #FILENAME# is blocked.
当引擎初始化失败时	Failed to initialize the AV engine. #FILENAME# is blocked.

- 反垃圾邮件通知消息

  对于客户端流量 （POP3），当 UTM 检测到垃圾邮件并且动作为阻断时，阻断邮件，替换邮件主题为阻断通知消息：

  The Mail is blocked due to Anti-Spam rules.

- 攻击签名检测通知消息

  当检测到客户端访问的网站存在威胁时， NISG 将发送一个预定义通知消息给客户端。同时， NISG 将阻断连接，并将 Web 服务器的 URL 保存到缓存中，缓存超时时间为 600 秒。 URL 缓存的最大条目数为 100 条。到达最大条目数时，新的 URL 条目将替换时间最久的缓存条目。

  当 URL 被攻击签名检测阻断时， NISG 发送给客户端的系统通知消息如下所示：

  <HTML><BODY><h2>High security alert!!!</h2> The URL you requested was found at risk(Attack Signatures Name=#Attack_Signatures_Name#,CVE=#CVE#). URL=http://#URL# <BODY></HTML>.

10.5. UTM 缺省设置

- 10.5.1. 缺省防病毒防护配置
- 10.5.2. 缺省反垃圾邮件防护配置
- 10.5.3. 反垃圾邮件规则集
- 10.5.4. 缺省 IPS 防护配置
- 10.5.5. 攻击签名规则
- 10.5.6.HTTP 协议限制缺省设置
- 10.5.7.SMTP 协议限制缺省设置
- 10.5.8.POP3 协议限制缺省设置
- 10.5.9.IMAP 协议限制缺省设置
- 10.5.10.DNS 协议限制缺省设置
- 10.5.11. （Web 防护）信息泄露防护
- 10.5.12. （Web 防护）注入攻击防御

10.5.1. 缺省防病毒防护配置

表 236 缺省防病毒防护配置

参数	低	Medium	High
描述	仅对易被感染的可执行二进制文件类型进行病毒检测	仅对易被感染的文件类型进行病毒检测，如 exe、zip、tar 等	对所有文件类型进行病毒检测
最大扫描文件	1 MB	• 1G 机型：1 MB • 2G 机型：5 MB	• 1G 机型：5 MB • 2G 机型：10 MB
当文件超过限定大小时	不经扫描，直接放行文件	不经扫描，直接放行文件	不经扫描，直接放行文件
7z	Pass	Scan	Scan
Z	Pass	Scan	Scan
ace	Pass	Scan	Scan
afx	Pass	Scan	Scan
arc	Pass	Scan	Scan
apk	Scan	Scan	Scan
arj	Pass	Scan	Scan
avi	Pass	Pass	Scan
bat	Scan	Scan	Scan
bh	Pass	Scan	Scan
bmp	Pass	Pass	Scan
bz2	Pass	Scan	Scan
cab	Pass	Scan	Scan
chm	Pass	Scan	Scan
class	Pass	Pass	Scan
csf	Pass	Pass	Scan
dat	Pass	Pass	Scan
dll	Scan	Scan	Scan
dmf	Pass	Scan	Scan
emf	Pass	Scan	Scan
eps	Pass	Scan	Scan
exe	Scan	Scan	Scan
flash	Scan	Scan	Scan
gif	Pass	Pass	Scan
gzip	Pass	Scan	Scan
hlp	Pass	Scan	Scan
html	Pass	Pass	Scan
ico	Pass	Scan	Scan

表 236 缺省防病毒防护配置 (*续*)

参数	低	Medium	High
jp2	Pass	Pass	Scan
jpg	Pass	Pass	Scan
js	Scan	Scan	Scan
lnk	Pass	Scan	Scan
lzh	Pass	Scan	Scan
lzo	Pass	Scan	Scan
m4a	Pass	Pass	Scan
mp2	Pass	Pass	Scan
mp3	Pass	Pass	Scan
mpa	Pass	Pass	Scan
mpeg	Pass	Scan	Scan
mpg	Pass	Scan	Scan
office	Pass	Scan	Scan
ogg	Pass	Scan	Scan
pcx	Pass	Pass	Scan
pdf	Scan	Scan	Scan
pdg	Pass	Scan	Scan
perl	Pass	Scan	Scan
php	Pass	Pass	Scan
png	Pass	Pass	Scan
postscript	Pass	Scan	Scan
psd	Pass	Scan	Scan
qt	Pass	Scan	Scan
rar	Pass	Scan	Scan
reg	Scan	Scan	Scan
rm	Pass	Pass	Scan
rpm	Pass	Pass	Scan
rtf	Pass	Scan	Scan
sct	Pass	Scan	Scan
shar	Pass	Scan	Scan
sig	Pass	Scan	Scan
sqx	Pass	Scan	Scan
tar	Pass	Scan	Scan
tif	Pass	Pass	Scan
wma	Pass	Pass	Scan
wmf	Pass	Scan	Scan

表 236 缺省防病毒防护配置 (*续*)

参数	低	Medium	High
xml	Pass	Pass	Scan
zip	Pass	Scan	Scan
zoo	Pass	Scan	Scan
nbh	Scan	Scan	Scan
img	Scan	Scan	Scan
apt	Scan	Scan	Scan
mtz	Scan	Scan	Scan
amt	Scan	Scan	Scan
启用文件类型特征识别	禁用	启用	启用
当文件类型不能识别时	放行	扫描	扫描

10.5.2. 缺省反垃圾邮件防护配置

表 237 缺省反垃圾邮件防护配置

参数	低	Medium	High
描述	邮件分数大于等于 10	邮件分数大于等于 5	邮件分数大于等于 3
分值	10	5	3
动作	Tag	Tag	Tag
主题标签	[SPAM]	[SPAM]	[SPAM]

10.5.3. 反垃圾邮件规则集

表 238 反垃圾邮件规则集

规则集名称	说明
advance_fee	对邮件中是否出现金融欺诈相关关键字进行检测。
body_tests	对邮件 body 部分进行相关检测。
compensate	根据邮件头部信息检测结果，确定是否对邮件的分值进行补偿 （减分）。该规则集被称为 “ 补偿规则集 ”，命中该规则集中规则的邮件会得到负数分值，这意味着这封邮件被认为是一封比较好的邮件。
dnsbl_tests	从邮件的 “Received:” 首部中提取 IP 地址，进行 DNSBL （DNS Blacklists）检测。
drugs	对邮件中是否出现药品相关关键字进行检测。
dynrdns	对邮件中包含的中继服务器信息进行检测，包括 IP 地址和域名。
fake_helo_tests	对邮件中可能出现的伪造 HELO 域名进行检测。
freemail	对邮件中出现的免费邮箱域名进行检测。如果一封邮件的 “from-address” 是一个免费邮箱的域名，同时， “Reply-to” 或者邮件体中是另一个免费邮箱的域名，那么这封邮件是垃圾邮件的可能性会比较大。
freemail_domains	定义了一些免费邮箱的域名，该规则与 freemail 规则同时被启用后，才能起到检测作用。
head_tests	对邮件头部的大部分测试规则，包括对 From 和 To 首部中出现的黑白名单地址的检测。
html_tests	对邮件中出现的 HTML 格式信息进行检测。
imageinfo	对邮件中的图像信息进行检测。
meta_tests	对邮件进行复合规则检测。
net_tests	对邮件头部中 Host 首部的域名进行 DNS 检测。
phrases	对邮件中出现的常用短语进行检测，例如：dear friend、 million dollars。
ratware	对邮件是否由垃圾邮件工具生成进行检测。
uri_tests	对邮件中出现的 URI 进行检测。
vbounce	对邮件是否为退信通知邮件进行检测。

表 238 反垃圾邮件规则集 (*续*)

规则集名称	说明
bayes	对邮件进行 Bayes 过滤器相关的检测。 Bayes 是一种基于统计的自学习算法。 NISG 可以根据扫描的垃圾邮件进行自学习，利用该算法判断后续邮件是垃圾邮件的概率。
dkim	对邮件进行 DKIM （Domain Keys Identified Mail）检测。 DKIM 即邮件域名密钥验证技术。 DKIM 的工作原理：一个组织通过 DNS 公开一个公钥。这个组织在发送邮件时，用私钥产生一个签名，添加到邮件的头部。接收方收到邮件，通过 DNS 取得公钥，进而验证这封邮件是否合法。
adsp_override_dkim	定义了一些 DKIM 默认检测策略，该规则与 dkim 规则同时被启用后，才能起到检测作用。
hashcash	该规则集定义了 Hashcash 相关的检测规则。 有 Hashcash 功能的客户端会在发送邮件时计算 Hash 值，并在邮件的头部添加类似如下的信息。 From: Someone <test@test.invalid> To: Adam Back <adam@cypherspace.org> Subject: test hashcash Date: Thu, 26 Jun 2003 11:59:59 +0000 X-Hashcash: 0:030626:adam@cypherspace.org:6470e06d773e05a8
replace	对邮件中出现的一些易被混淆的关键字进行检测，例如 credit、 Credit 和 CREDIT。
spf	对邮件进行 SPF 相关检测。 SPF （Sender Policy Framework），是一种防止发件人地址伪造的技术。
whitelist_spf	定义了一些 SPF 检测白名单。该规则与 spf 规则同时被启用后，才能起到检测作用。
textcat	对邮件语言进行检测。如果邮件使用的不是引擎所设置的语言，则会给邮件加上相应的分数。
uribl	通过分析 URL 的消息文本和 HTML，从中提取域名，在 DNS 的 NS 记录中查询，解析所使用的主机名，并为这些解析得到的 IP 地址查询各种 DNS 黑名单。
awl	该规则提供了自动白名单检测功能，根据跟踪发件人所发邮件的平均分，对该发件人发来邮件的分数进行调整。
whitelist	为知名地址和公司创建缺省白名单，如 Amazon.com。
whitelist_dkim	为 DKIM 检测提供缺省白名单。
active	对一些比较活跃的规则进行检测，例如：对邮件头部、邮件内容、 dnsbl 等进行检测。
update	更新的反垃圾邮件规则。

10.5.4. 缺省 IPS 防护配置

表 239 缺省 IPS 防护配置

名称	说明	协议限制	攻击签名 （启用的规则）	动作
Client_Low	**攻击目标**：客户端 **严重级别**：High	全部禁用	**严重级别**：High	全部阻断
Client_Medium	**攻击目标**：客户端 **严重级别**：High/Medium	全部禁用	**严重级别**：High/Medium	全部阻断
Client_High	**攻击目标**：客户端 **严重级别**：任意	全部禁用	**严重级别**：任意	全部阻断
Web_Server_Low	**攻击目标**：Web 服务器 **严重级别**：High	禁用	**服务**：HTTP **严重级别**：High	全部阻断
Web_Server_Medium	**攻击目标**：Web 服务器 **严重级别**：High/Medium	禁用	**服务**：HTTP **严重级别**：High/Medium	全部阻断
Web_Server_High	**攻击目标**：Web 服务器 **严重级别**：任意	禁用	**服务**：HTTP **严重级别**：任意	全部阻断
Mail_Server_Low	**攻击目标**：Mail 服务器 **严重级别**：High	禁用	**服务**：POP3/IMAP/SMTP **严重级别**：High	全部阻断
Mail_Server_Medium	**攻击目标**：Mail 服务器 **严重级别**：High/Medium	禁用	**服务**：POP3/IMAP/SMTP **严重级别**：High/Medium	全部阻断
Mail_Server_High	**攻击目标**：Mail 服务器 **严重级别**：任意	禁用	**服务**：POP3/IMAP/SMTP **严重级别**：任意	全部阻断
FTP_Server_Low	**攻击目标**：FTP 服务器 **严重级别**：High	禁用	**服务**：FTP **严重级别**：High	全部阻断
FTP_Server_Medium	**攻击目标**：FTP 服务器 **严重级别**：High/Medium	禁用	**服务**：FTP **严重级别**：High/Medium	全部阻断
FTP_Server_High	**攻击目标**：FTP 服务器 **严重级别**：任意	禁用	**服务**：FTP **严重级别**：任意	全部阻断
DNS_Server_Low	**攻击目标**：DNS 服务器 **严重级别**：High	禁用	**服务**：DNS **严重级别**：High	全部阻断
DNS_Server_Medium	**攻击目标**：DNS 服务器 **严重级别**：High/Medium	禁用	**服务**：DNS **严重级别**：High/Medium	全部阻断
DNS_Server_High	**攻击目标**：DNS 服务器 **严重级别**：任意	禁用	**服务**：DNS **严重级别**：任意	全部阻断

表 239 缺省 IPS 防护配置 (*续*)

名称	说明	协议限制	攻击签名 （启用的规则）	动作
Telnet_Server_Low	**攻击目标**：Telnet 服务器 **严重级别**：High	禁用	**服务**：Telnet **严重级别**：High	全部阻断
Telnet_Server_ Medium	**攻击目标**：Telnet 服务器 **严重级别**：High/Medium	禁用	**服务**：Telnet **严重级别**：High/Medium	全部阻断
Telnet_Server_ High	**攻击目标**：Telnet 服务器 **严重级别**：任意	禁用	**服务**：Telnet **严重级别**：任意	全部阻断
Other_Server_Low	**攻击目标**：Other 服务器 **严重级别**：High	禁用	**服务**：Others **严重级别**：High	全部阻断
Other_Server_Medium	**攻击目标**：Other 服务器 **严重级别**：High/Medium	禁用	**服务**：Others **严重级别**：High/Medium	全部阻断
Other_Server_High	**攻击目标**：Other 服务器 **严重级别**：任意	禁用	**服务**：Others **严重级别**：任意	全部阻断

10.5.5. 攻击签名规则

表 240 攻击签名规则

参数	说明
ID	规则的标识，该属性不可编辑。
名称	规则的名称，该属性不可编辑。 IPS 防护配置分别以 _Low， _Medium 和 _High 命名，分别表示了低、中、高三个级别的 IPS 防护。
服务	规则对应的协议，该属性不可编辑。
严重级别	不同严重级别的攻击发生时，按照相应的安全等级记录日志，以便管理员在进行审计配置时，可以决定哪些级别的事件以哪种方式 （SysLog、 Mail、 SNMP Trap、 Local Log）进行审计。该属性不可编辑。 严重级别与安全等级的对应关系为：High 对应 Critical， Medium 对应 Error， Low 对应 Warning， Info 对应 Notification。
类别	规则的类别，如 BACKDOOR/TROJAN、 BUFFER OVERFLOW、 CODE INJECTION、 DESIGN ERROR、 INPUT INVALIDATE FAILED、 MALWARE 和 UNKOWN 等，该属性不可编辑。
目标	攻击的目标，包括客户端、服务器和 Both 攻击三种，该属性不可编辑。
OS&APP	规则对应的操作系统和应用程序，该属性不可编辑。
CVE	公共漏洞和暴露 （Common Vulnerabilities&Exposures， CVE）编号，该属性不可编辑。
Bugtraq	Bugtraq 编号，该属性不可编辑。
描述	规则的描述信息，包含简单的原理介绍，该属性不可编辑。
启用	规则的状态，启用和禁用。
动作	规则的处理动作，包括允许和阻断。 • **允许**：放行匹配到当前规则签名的数据包。 • **阻断**：阻断匹配到当前规则签名的数据包。

10.5.6. HTTP 协议限制缺省设置

表 241 HTTP 协议限制的默认配置

参数	低	中	高	自定义
产生日志	启用	启用	启用	启用
最大首部数	500，阻断	300，阻断	100，阻断	300，允许
最大 URL 长度	2000 字节，阻断	1500 字节，阻断	1000 字节，阻断	2048 字节，允许
最大请求正文长度	禁用	禁用	50000 字节，阻断	禁用
最大首部长度	1500 字节，阻断	1000 字节，阻断	600 字节，阻断	2048 字节，允许
首部长度限制	启用，空列表	启用，空列表	启用，空列表	启用，空列表
请求方式阻断列表	启用，空列表	启用，阻断以下请求方式：PURGE, PROPFIND, PROPPATCH, MKCOL, COPY, MOVE, LOCK, UNLOCK, BMOVE, BDELETE, BPROPFIND, BPROPPATCH, BCOPY, SEARCH, SUBSCRIBE, UNSUBSCRIBE, POLL, REPORT, PATCH, VERSION-CONTROL, CHECKOUT, UNCHECKOUT, CHECKIN, UPDATE, LABEL, MKWORKSPACE, MKACTIVITY, BASELINE-CONTROL, MERGE	启用，阻断以下请求方式：PUT, CONNECT, TRACE, PURGE, OPTIONS, DELETE, PROPFIND, PROPPATCH, MKCOL, COPY, MOVE, LOCK, UNLOCK, BMOVE, BDELETE, BPROPFIND, BPROPPATCH, BCOPY, SEARCH, SUBSCRIBE, UNSUBSCRIBE, POLL, REPORT, PATCH, VERSION-CONTROL, CHECKOUT, UNCHECKOUT, CHECKIN, UPDATE, LABEL, MKWORKSPACE, MKACTIVITY, BASELINE-CONTROL, MERGE	启用，阻断以下请求方式：PURGE, PROPFIND, PROPPATCH, MKCOL, COPY, MOVE, LOCK, UNLOCK, BMOVE, BDELETE, BPROPFIND, BPROPPATCH, BCOPY, SEARCH, SUBSCRIBE, UNSUBSCRIBE, POLL, REPORT, PATCH, VERSION-CONTROL, CHECKOUT, UNCHECKOUT, CHECKIN, UPDATE, LABEL, MKWORKSPACE, MKACTIVITY, BASELINE-CONTROL, MERGE
阻断非 ASCII 码首部	禁用	禁用	启用	禁用
阻断 Form 字段的非 ASCII 码字符	禁用	禁用	启用	禁用

10.5.7. SMTP 协议限制缺省设置

表 242 SMTP 协议限制的默认配置

类型	参数	低	中 / 自定义	高
服务器防护	产生日志	启用	启用	启用
	最大命令长度	512 字节，拒绝	256 字节，拒绝	128 字节，阻断
	最大参数长度	512 字节，拒绝	256 字节，拒绝	128 字节，阻断
	最大 NOOP 命令数	禁用	10，阻断	5，阻断
	最大命令数	禁用	禁用	20，阻断
	最大未知命令数	20，阻断	10，阻断	5，阻断
	阻断未知命令	禁用	禁用	启用
	自定义 SMTP 命令列表	启用，空列表	启用，空列表	启用，空列表
	命令阻断列表	禁用	启用，阻断命令：NOOP	启用，阻断命令：VRFY, EXPN, NOOP
	转发时添加 Received 头字段	禁用	启用	启用
	剥离带有多个 Content-Type 头字段的 MIME 字段	启用	启用	启用
	剥离带有多个 Encoding 头字段的 MIME 字段	启用	启用	启用
	剥离带有未知 Encoding 头字段的 MIME 字段	禁用	禁用	启用
	剥离所有邮件附件	禁用	禁用	启用
	剥离所有分片邮件	禁用	禁用	启用
	阻断收件人没有域名的邮件	启用	启用	启用
客户端防护	产生日志	启用	启用	启用
	最大应答长度	禁用	512 字节，阻断	512 字节，阻断

10.5.8. POP3 协议限制缺省设置

表 243 POP3 协议限制的默认配置

类型	参数	低	中 / 自定义	高
服务器防护	产生日志	启用	启用	启用
	最大命令长度	512 字节，拒绝	255 字节，拒绝	128 字节，阻断
	最大参数长度	128 字节，拒绝	40 字节，拒绝	16 字节，阻断
	最大 NOOP 命令数	禁用	10，阻断	5，阻断
	最大命令数	禁用	禁用	20，阻断
	最大未知命令数	20，阻断	10，阻断	5，阻断
	阻断未知命令	禁用	禁用	启用
	自定义 POP3 命令列表	启用，空	启用，空	启用，空
	命令阻断列表	禁用	启用，阻断命令：NOOP	启用，阻断命令：NOOP
客户端防护	产生日志	启用	启用	启用
	最大应答长度	禁用	512 字节，阻断	128 字节，阻断

10.5.9. IMAP 协议限制缺省设置

表 244 IMAP 协议限制的默认配置

类型	参数	低	中 / 自定义	高
服务器防护	产生日志	启用	启用	启用
	最大命令长度	1024 字节，允许	512 字节，拒绝	256 字节，阻断
	最大参数长度	512 字节，允许	256 字节，拒绝	128 字节，阻断
	最大 Tag 长度	禁用	128 字节，拒绝	64 字节，阻断
	最大 NOOP 命令数	禁用	20，阻断	5，阻断
	最大命令数	禁用	禁用	20，阻断
	最大未知命令数	20，阻断	10，阻断	5，阻断
	阻断未知命令	禁用	启用	启用
	自定义 IMAP 命令列表	启用，空	启用，空	启用，空
	命令阻断列表	禁用	禁用	禁用
客户端防护	产生日志	启用	启用	启用
	最大应答长度	2048 字节，允许	1024 字节，阻断	512 字节，阻断

10.5.10. DNS 协议限制缺省设置

表 245 DNS 协议限制缺省设置

类型	参数	缺省值
服务器防护	产生日志	启用
	授权 IP 地址列表	启用 （空）
客户端防护	产生日志	启用
	UDP 资源记录数限制	启用
	最大回答记录数	启用， 4，允许
	最大授权记录数	启用， 4，允许
	最大附加记录数	启用， 4，允许

10.5.11. （Web 防护）信息泄露防护

表 246 （Web 防护）信息泄露防护

产生日志	禁用			
首部置换	禁用			
首部置换列表	**启用**	**首部**	**首部值**	**动作**
	true	Server	.*IIS.*	sustitute with "IIS"
	true	Server	.*Apache.*	sustitute with "Apache"
隐藏错误信息	启用			
隐藏错误信息列表	**隐藏**	**错误码**	**描述**	
	FALSE	400	Bad Request	
	FALSE	401	Unauthorized	
	FALSE	402	Payment Required	
	FALSE	403	Forbidden	
	FALSE	404	Not Found	
	FALSE	405	Method Not Allowed	
	FALSE	406	Not Acceptable	
	FALSE	407	Proxy Authentication Required	
	FALSE	408	Request Timeout	
	FALSE	409	Conflict	
	FALSE	410	Gone	
	FALSE	411	Length Required	
	FALSE	412	Precondition Failed	
	TRUE	413	Request Entity Too Large	
	TRUE	414	Request-URI Too Long	
	TRUE	415	Unsupported Media Type	
	TRUE	416	Requested Range Not Satisfiable	

表 246 （Web 防护）信息泄露防护 (*续*)

	TRUE	417	Expectation Failed
	FALSE	422	Unprocessable Entity
	FALSE	423	Locked
	FALSE	424	Method Failure
	FALSE	425	Insufficient Space on Resource
	TRUE	500	Internal Server Error
	TRUE	501	Not Implemented
	TRUE	502	Bad Gateway
	TRUE	503	Service Unavailable
	FALSE	504	Gateway Timeout
	FALSE	505	HTTP Version Not Supported
目录列表检测	禁用		

10.5.12. （Web 防护）注入攻击防御

表 247 （Web 防护）注入攻击防御缺省设置

参数	缺省值
产生日志	启用
跨站脚本攻击防御	启用
安全级别	低
脚本命令列表	阻断 （不勾选）： .cookie, ActiveXobject, CopyFile, CreateObject, CreateTextRange, DeleteFile, DriveType, FileExist, GetFile, GetFolder, GetParentFolder, GetSpecialFolder, ONBlur, ONabort, ONchange, ONfocus, ONload, ONmouseout, applet, copyparentfolder, javascript, livescript, mocha, object, onClick, onDragDrop, onKeyPress, onKeyUp, onMouseDown, onMouseMove, onkeyDown
LDAP 注入攻击防御	禁用
安全级别	中
识别名列表： cn, dc, l, o, ou, st, street, uid	阻断 （不勾选）
SQL 注入攻击防御	启用
安全级别	中
SQL 命令列表	阻断 （不勾选）
命令注入攻击防御	启用
安全级别	中
Shell 命令列表	阻断 （不勾选）

11 虚拟专用网

本章介绍了 NISG 的虚拟专用网 (Virtual Private Network， VPN) 功能，章节结构如下所示：

- 11.1 概述，描述 NISG 的 VPN 类型及特点。
- 11.2 基本配置，介绍基本配置步骤及配置中的注意事项。
- 11.3 范例，详细介绍 VPN 功能在实际环境中的应用。
- 11.4 配置参数说明，详细解释 VPN 相关的各项配置参数。

11.1 概述

下表概要介绍了 NISG 支持的 5 种 VPN 类型。

表 248 NISG 的 VPN 类型

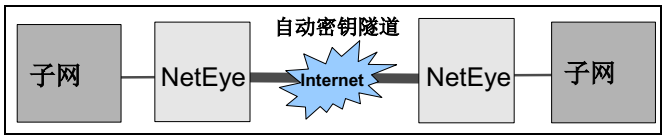
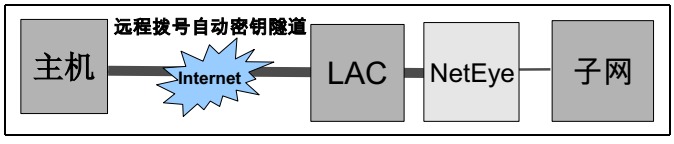
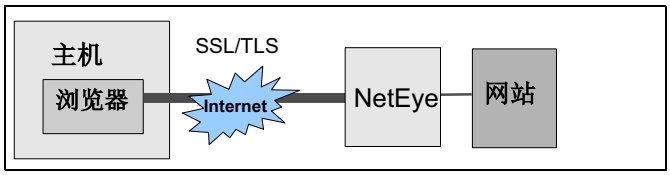
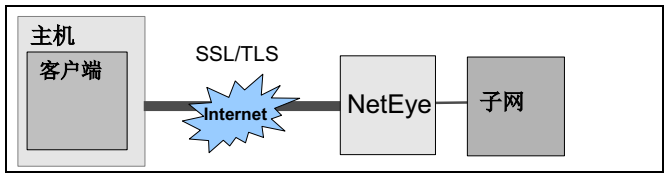
VPN 场景 （NISG= 网关设备）	描述 （+= 优点， -= 缺点）
	• **VPN 类型**：11.1.1 网段到网段 IPSec 手动密钥隧道 • **特点**：手动配置安全联盟 （SA) 安全参数、手动生成密钥和进行交换、 IP 封装、 ESP/AH。 • **优点**：配置简单。 • **缺点**：难以管理和扩大规模。没有对端或用户的验证过程。
	• **VPN 类型**：11.1.2 网段到网段自动密钥隧道 • **特点**：SA 安全参数自动协商、自动密钥生成和交换、对端认证 （证书或预共享密钥）、 ESP/AH。 • **优点**：使用方便、可扩展。 • **缺点**：配置复杂，需要更多的计算能力。
	• **VPN 类型**：11.1.3. 远程访问 IPSec VPN • **特点**：L2TP/Xauth、 SA 安全参数自动协商、自动密钥生成和交换、对端认证 （证书或预共享密钥）、ESP/AH、用户认证。 • **优点**：可移动性、对用户进行认证。 • **缺点**：需要在客户端主机上进行相关配置。

表 248 NISG 的 **VPN** 类型 (*续*)

	• **VPN 类型**：11.1.4. SSL VPN Web 入口页面访问 • **特点**：自动密钥协商、自动密钥生成和交换、客户端通过证书对 SSL VPN 服务器进行认证、用户通过用户名和密码进行身份认证。 • **优点**：配置最少。 • **缺点**：仅限于 HTTP/HTTPS、 FTP、及 SMTP 网站的访问。
	• **VPN 类型**：11.1.5 SSL VPN 隧道访问 • **特点**：自动密钥协商、自动密钥生成 / 交换。客户端通过证书对 SSL VPN 服务器进行认证。用户则通过用户名和密码进行身份认证。 • **优点**：可以访问受保护的子网。 • **缺点**：需要安装 SSL VPN 客户端。

本章还介绍了 NAT 和 HA 环境下 VPN 的配置和应用。

- 11.1.6 NAT 环境下网段到网段 IPSec VPN (隧道模式）
- 11.1.7 高可用环境下的 VPN

11.1.1 网段到网段 IPSec 手动密钥隧道

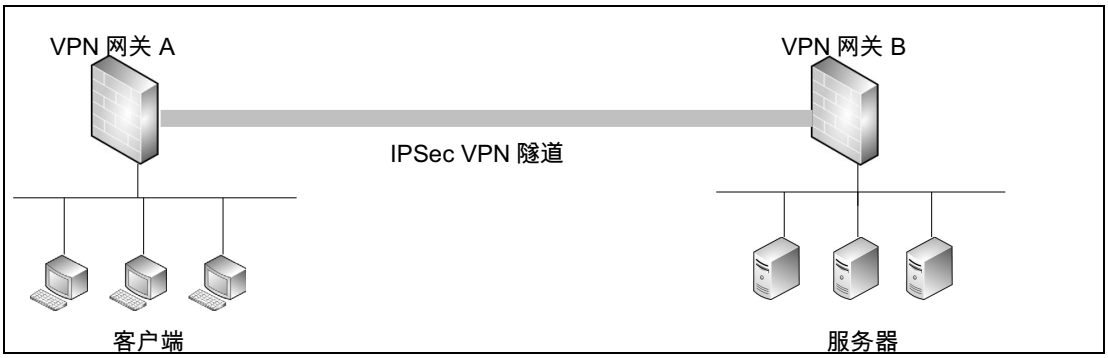
- 11.1.1.1 需求
- 11.1.1.2 实现
- 11.1.1.3 IPSec SA 的安全协议与工作模式

11.1.1.1 需求

当您有如下需求时，可以创建一条手动密钥隧道：

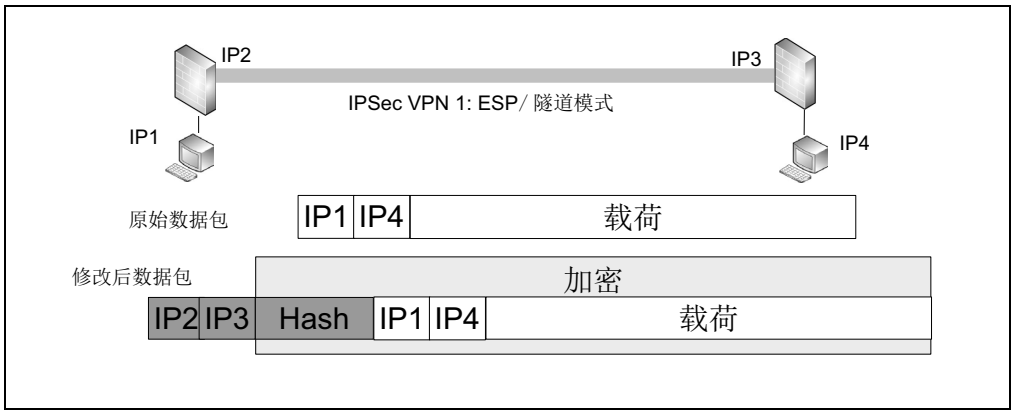
- 在 VPN 网关 A 和 B 之间建立一条隧道。
- 不需要在客户端或者服务器上进行配置和安装。

简单配置和安装是最优先考虑的问题，不需要考虑扩展性问题。



11.1.1.2 实现

IPSec VPN 通过修改数据包来达到保护的目的 （隧道模式）。



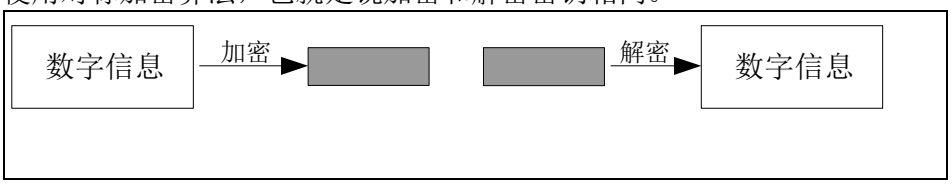
下面的 IPSec 安全机制是通过修改原始数据包实现的。

- 11.1.1.2.1 数据机密性 （ESP 模式加密）
- 11.1.1.2.2 对端机密性 （隧道模式，有局限性）
- 11.1.1.2.3 数据完整性 / 认证 （Hash 签名）
- 11.1.1.2.4 抗重放

IPSec VPN 手动密钥隧道不需要对端认证，因为只有真实对端才会知道所有的加密参数和密钥，所以默认对端是真实可靠的。

11.1.1.2.1 数据机密性 （ESP 模式加密）

使用对称加密算法，也就是说加密和解密密钥相同。

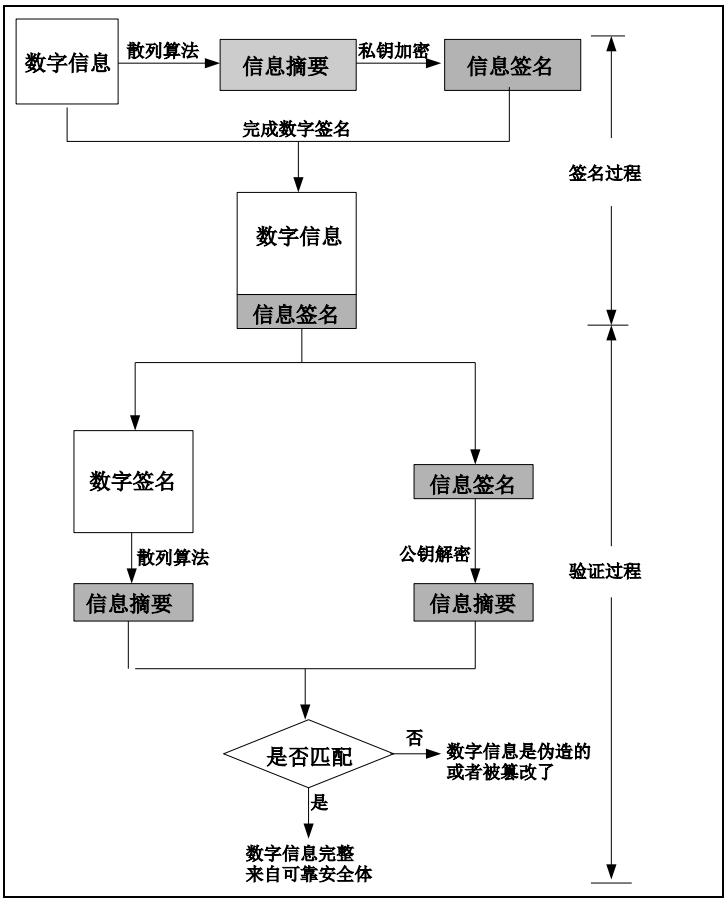


11.1.1.2.2 对端机密性 （隧道模式，有局限性）

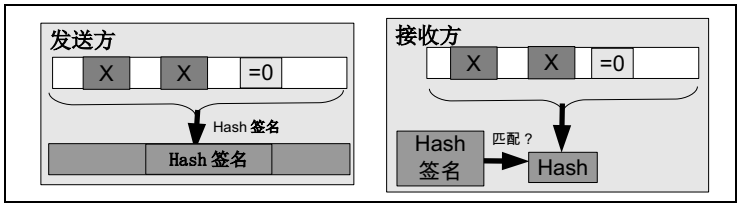
IP1 和 IP4 被封装在修改后的数据包中，所以源 / 目的 IP 地址是受保护的。然而 IP2 和 IP3 却没有被隐藏，因此机密性是有局限性的。

11.1.1.2.3 数据完整性 / 认证 （Hash 签名）

下图显示了如何对数据包进行 Hash 签名。



下图显示了 Hash 算法如何只对原始数据包的一部分进行签名。



11.1.1.2.4 抗重放

攻击者有可能截获 ISAKMP 报文重复发送，攻击 IKE 的一方，使其忙于接受重复的报文而拒绝新报文。IPSec 数据包专门使用一个序列号，在每个 IPSec 头内，都包含一个独一无二且单调递增的序列号。 IKE 协议通过检测每个 ISAKMP 报文是否重复来抵御这种攻击，保护 IKE 协商过程。

11.1.1.3 IPSec SA 的安全协议与工作模式

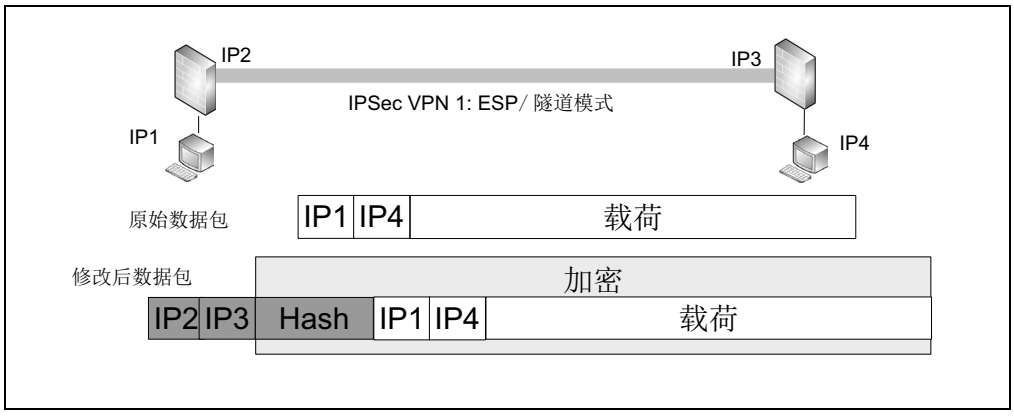
IPSec 使用鉴别首部协议 （AH) 和封装安全载荷协议 (ESP) 提供认证和加密机制。工作模式可以分为传输模式和隧道模式。

- 11.1.1.3.1 ESP/ 隧道模式
- 11.1.1.3.2 AH/ 隧道模式
- 11.1.1.3.3 ESP/ 传输模式
- 11.1.1.3.4 AH/ 传输模式

11.1.1.3.1 ESP/ 隧道模式

隧道模式中， NISG 相当于网关设备而不是终端，可以提供：

- 数据源认证
- 终端设备机密性 （ESP 加密）
- 数据完整性 （Hash)
- 数据机密性 （加密）

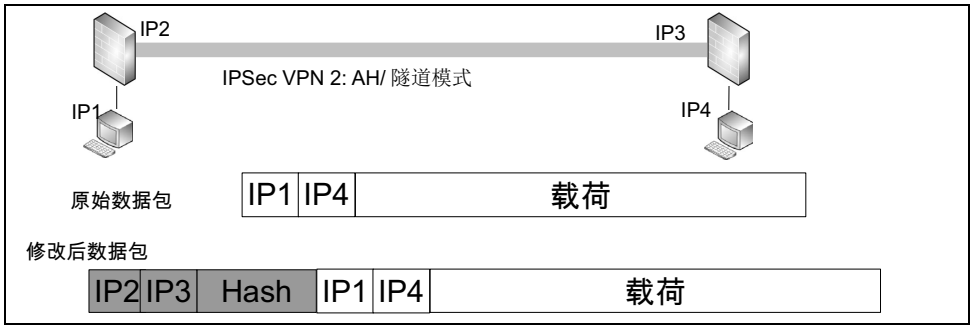


11.1.1.3.2 AH/ 隧道模式

隧道模式中， NISG 相当于网关设备而不是终端 , 可以提供：

- 数据源认证
- 数据完整性验证

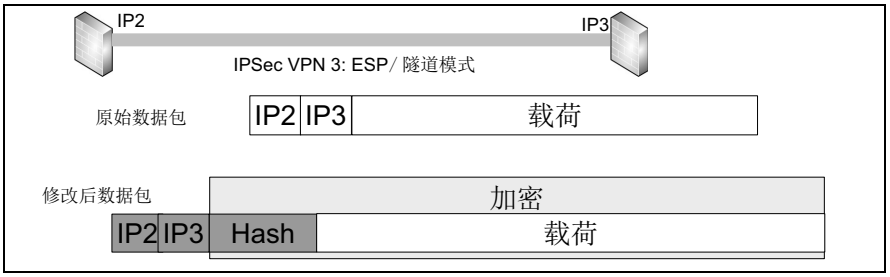
终端设备 IP 地址无加密。



11.1.1.3.3 ESP/ 传输模式

传输模式中， NISG 是终端设备，可以提供：

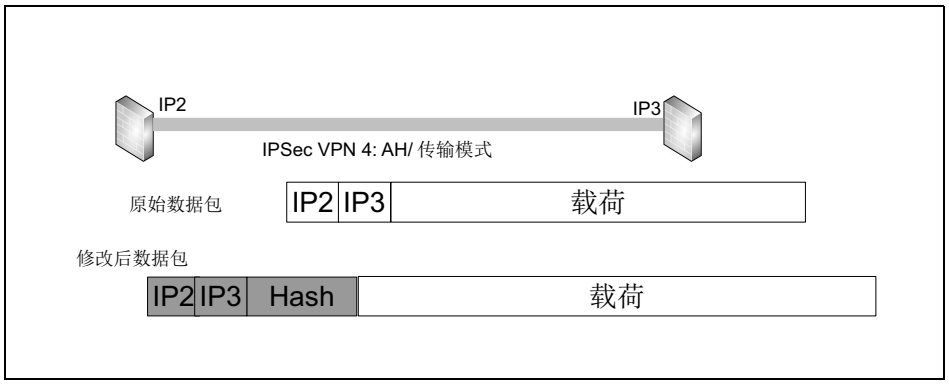
- 数据源认证
- 数据完整性验证
- 数据机密性 (加密）



11.1.1.3.4 AH/ 传输模式

传输模式中， NISG 是终端设备，作用如下：

- 数据源认证
- 数据完整性验证
- 无加密，用于传输非机密性数据或者不能加密的数据。

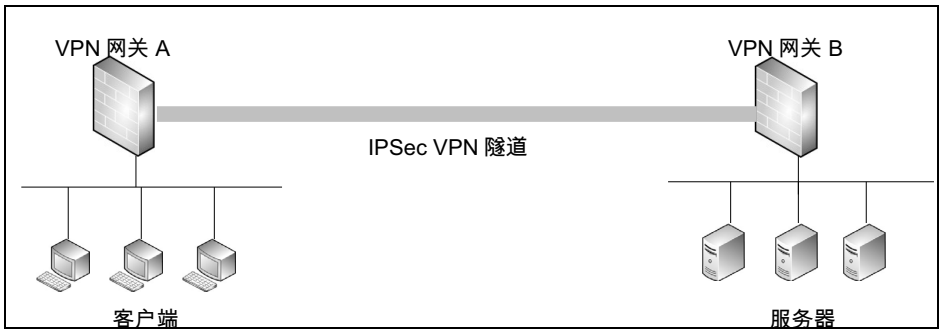


11.1.2 网段到网段自动密钥隧道

- 11.1.2.1 需求
- 11.1.2.2 实现

11.1.2.1 需求

需求场景与手动密钥隧道部分的需求基本上是一样的，请参见 11.1.1.1 需求。



与手动密钥隧道相同的需求包括：

- 数据机密性
- 对端机密性
- 数据完整性
- 抗重放

自动密钥隧道的其他需求包括：

- **自动密钥交换：**同时维护和跟踪所有的密钥是有风险的，而且需要花费大量的时间。自动密钥隧道交换，配置虽然相对复杂，但是从长远意义上看却能节省大量时间，而且安全性更高。
- **自动协商 SA 安全参数：**避免了事先定义复杂的安全协议 （AH/ESP）参数。
- **对端认证：**使用证书或者预共享密钥认证。

11.1.2.2 实现

- 11.1.2.2.1 阶段一主模式
- 11.1.2.2.2 阶段一激进模式
- 11.1.2.2.3 阶段二快速模式 （建立子安全联盟）

11.1.2.2.1 阶段一主模式

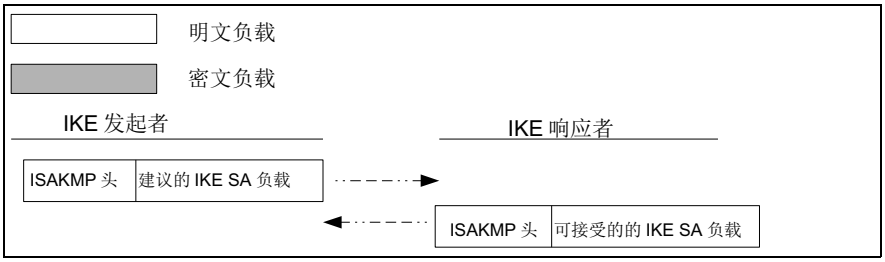
在主模式下，IKE SA 发起者和响应者进行三次交换，相互发送 6 条信息完成第一阶段。在 WebUI 上指定主模式。

- 11.1.2.2.1.1 阶段一：自动确定 IKE SA （IKE_SA_INIT)
- 11.1.2.2.1.2 阶段一：密钥交换
- 11.1.2.2.1.3 阶段一：验证 IKE 发起者 ID/ 验证信息 （IKE_AUTH)

11.1.2.2.1.1 阶段一：自动确定 IKE SA （IKE_SA_INIT)

IKE 发起方提出一组或多组由所支持的各种算法组成的提议集，发起方和接收方需要协商如下内容：

IKE 策略 （SA 安全参数)，加密 （3DES 或 AES)， Hash 算法 （MD5 或 SHA-1)， DH 组 （1,2,5）。

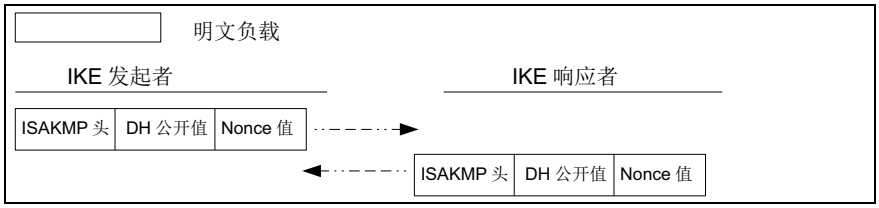


隧道两端可以自动协商提议集，也可以在 NISG 的 WebUI 下指定，最多可以自定义 4 个提议集。

在 WebUI 上设置预共享密钥或者证书认证方式。

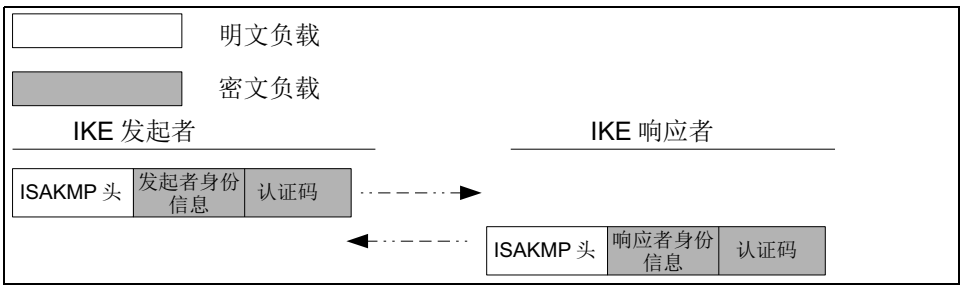
11.1.2.2.1.2 阶段一：密钥交换

两端交换 DH 公开值来生成密钥。



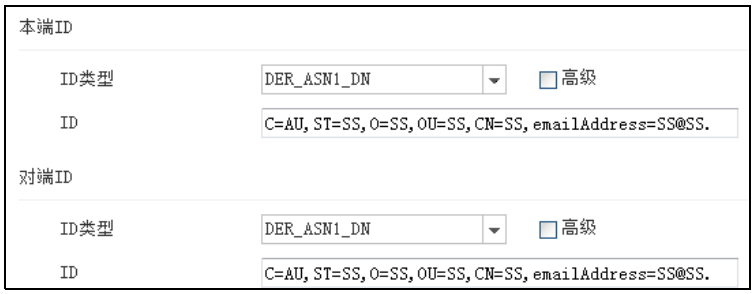
11.1.2.2.1.3 阶段一：验证 IKE 发起者 ID/ 验证信息 （IKE_AUTH)

密钥可以被用来创建安全通道。



建立安全通道后，发送信息：

- 身份信息。请选择 **VPN** > **IPSec VPN** > **自动密钥隧道** > **高级设置**，通过 WebUI 设置身份信息。



- 认证码 （加密之前的交换信息）。每一方先将自己的身份信息使用协商好的认证方式 （预共享密钥或者证书）生成身份信息认证码。将此认证码和身份信息发送给对方，用户向对方证实身份。

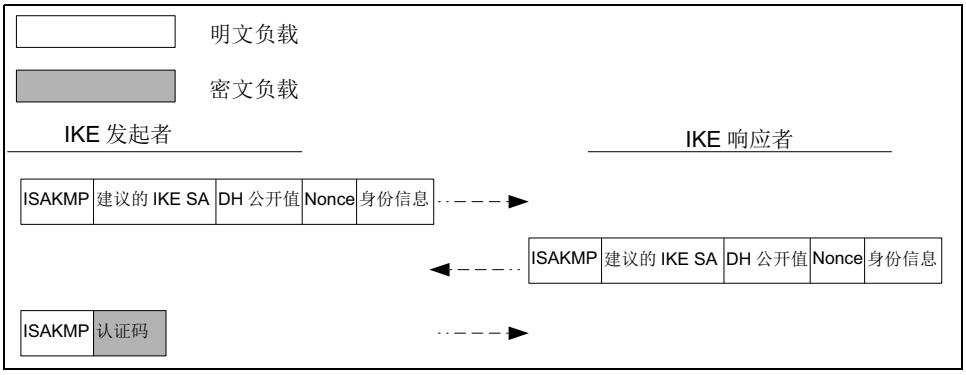
WebUI 中，选择 **VPN** > **IPSec VPN** > **自动密钥隧道**设置认证方式。如果认证方式设置为证书认证，则隧道的一端必须要上载另一端的 CA 证书。

11.1.2.2.2 阶段一激进模式

激进模式通过三条消息完成 IKE 阶段一的信息交换。

- 前两条消息完成 IKE SA、 DH 公开值、 Nonce 值、身份信息等交换。
- 最后一条消息是发起者的认证码，用于响应者验证发起者是 IKE 协商的参与者。

激进模式加速了信息交换，但是不能对双方的身份信息进行保护。



WebUI 中，请选择 **VPN** > **IPSec VPN** > **自动密钥隧道** > **高级设置**设置激进模式。

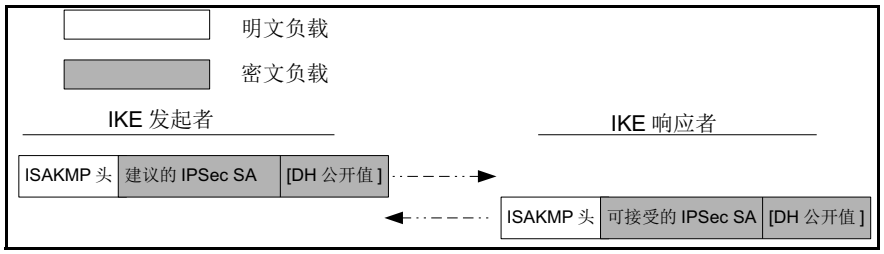
11.1.2.2.3 阶段二快速模式 （建立子安全联盟）

阶段二的信息交换受 IKE SA 保护，也就是说阶段一生成的密钥用于加密阶段二的所有交换信息。

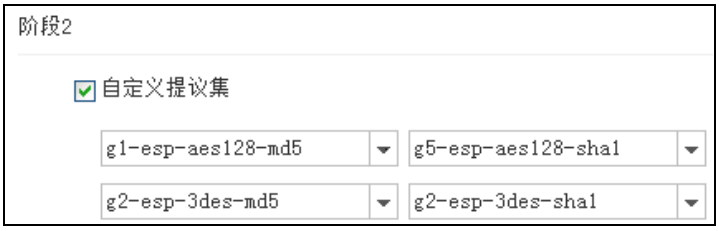
快速模式下前两条消息交换完成 IPSec SA 策略协商和密钥材料生成，交换的信息如下：

- IPSec SA 参数，包括安全协议（AH 或 ESP)、DH 组（如果执行完美向前保护）、加密算法和 Hash 算法。
- DH 公开值，发起者和响应者的身份信息 （ID）（如果执行完美向前保护）。

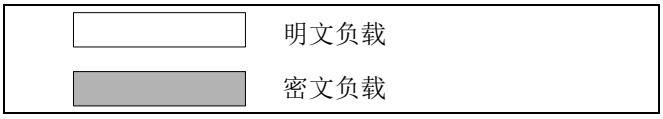
1. 协商建立的 SA 以及公开值是加密的。



请选择 **VPN** > **IPSec VPN** > **自动密钥隧道** > **高级设置**自定义提议集。



2. 最后交换的认证码，用于证明发起者一直参与阶段二的交换过程，它确保了 IKE 过程的完整性。



11.1.3. 远程访问 IPSec VPN

- 11.1.3.1. 需求
- 11.1.3.2. 解决方案

11.1.3.1. 需求

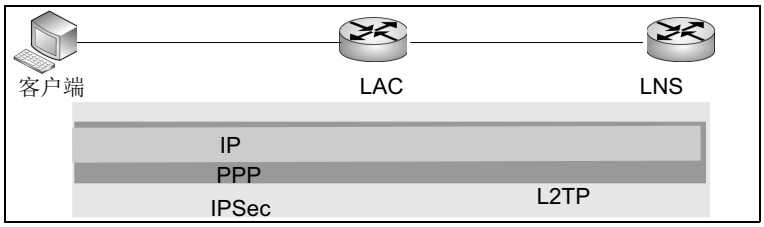
远程访问 VPN 主要被移动办公人员用来访问企业的服务器资源。

远程访问 VPN 的需求与网段到网段 VPN 的需求不同，主要是因为：

- 远程访问用户无固定 IP 地址
- 用户必须使用账号登录
- 如果使用证书认证，必须要创建证书并且在客户端导入
- 使用 Xauth 或者 L2TP 认证

11.1.3.2. 解决方案

客户端与 LNS 间的隧道：客户端发起到 LAC 的 PPP 会话连接。 LAC 与 LNS 协商一条 L2TP 通道，将客户端的 PPP 会话转发至 LNS。客户端与 LNS 协商一条 IPSec VPN 隧道来加密客户端的 PPP 会话。



解决方案可以提供如下安全机制：

- 对端机密性，客户端 IP 已知，但是是变化的
- 对端认证：证书认证或预共享密钥认证
- 用户认证 :
  - IPSec VPN
  - 本地 / 外部认证
  - Xauth/L2TP
- 载荷加密：ESP
- 载荷完整性：HMAC/SHA-1

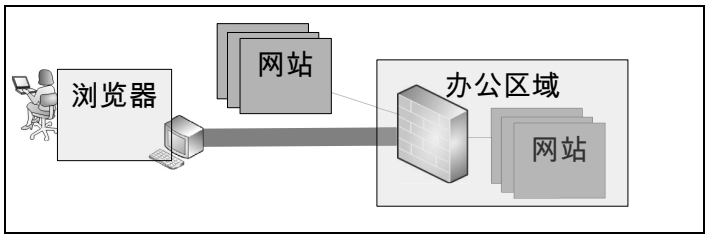
11.1.4. SSL VPN Web 入口页面访问

- 11.1.4.1. 需求
- 11.1.4.2. 解决方案
- 11.1.4.3. 实现

11.1.4.1. 需求

用户需求：

- 非办公区域通过安全连接访问内网资源 （收发公司的邮件、登录人力资源系统、申请休假等）和外网资源。 NISG 对远程用户访问的外网进行限制并且提供安全机制阻止网站恶意传播非法内容
- 不需要安装客户端软件或者在客户端 PC 上进行任何配置。
- 授权用户可以添加允许访问的网站。

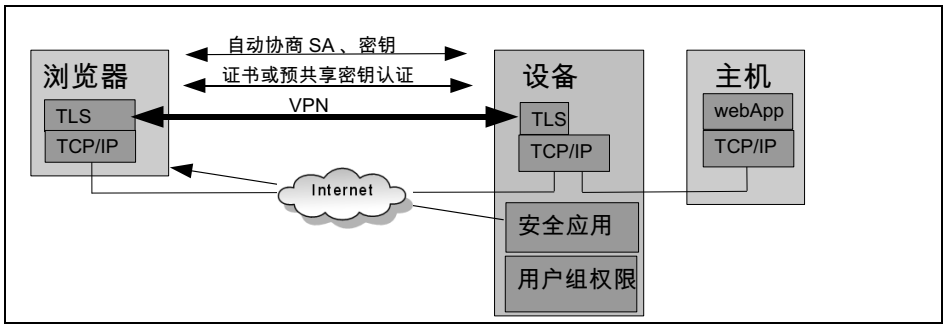


安全需求：

- 自动密钥交换
- 加密大量数据
- MAC 算法
- 证书认证 （进行对端认证）
- 用户认证 （用户名和密码）

11.1.4.2. 解决方案

下图显示了基本的解决方案。



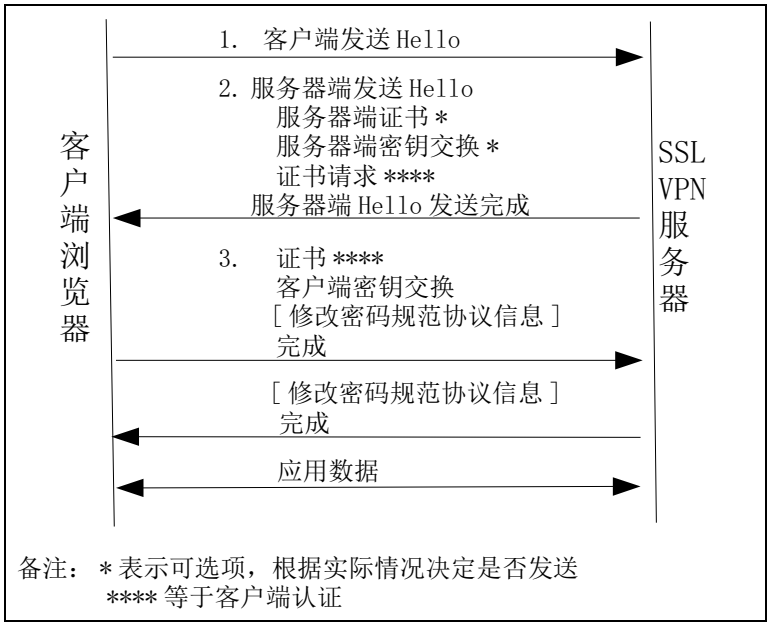
通过浏览器登录后，用户会进入如下页面：

以上配置的的安全机制包括：

- 无对端机密性
- 对端认证：通过服务器和 SSL VPN 客户端的内置证书认证
- 用户认证：通过用户名和密码在本地认证或通过外部服务器认证
- 对载荷加密
- 对载荷进行完整性校验

11.1.4.3. 实现

SSL VPN 的实现与 11.1.2.2.1 阶段一主模式非常相似，包含 3 个主要部分。客户端与服务器端的整个握手过程如下：



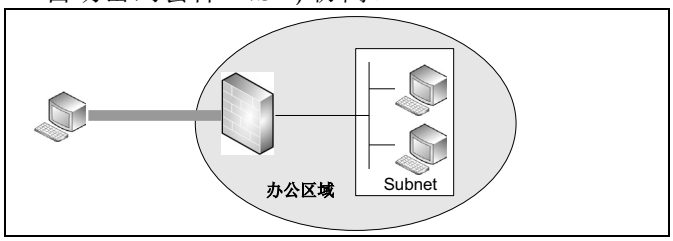
11.1.5 SSL VPN 隧道访问

- 11.1.5.1 需求
- 11.1.5.2 解决方案
- 11.1.5.3 实现

11.1.5.1 需求

用户需求：

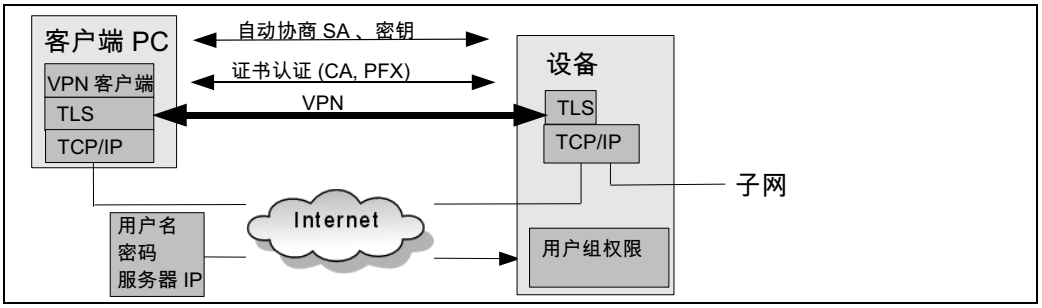
- 非办公区域通过安全连接访问内网资源。
- 无需通过浏览器访问，可以安装 VPN 客户端。
- 配置简单，避免类似 IPSec VPN 的复杂配置。
- 自动密码套件 （SA) 协商。



安全需求：

- 密钥交换
- 加密大量数据 （包括密钥长度）
- MAC 算法
- 证书 （对端认证）
- 用户认证 （用户名 / 密码）

11.1.5.2 解决方案



以上配置的安全机制包括：

- 无对端机密性
- 对端认证：通过服务器和 SSL VPN 客户端的内置证书认证
- 用户认证：通过用户名和密码在本地认证或通过外部服务器认证
- 对载荷加密
- 对载荷进行完整性校验

11.1.5.3 实现

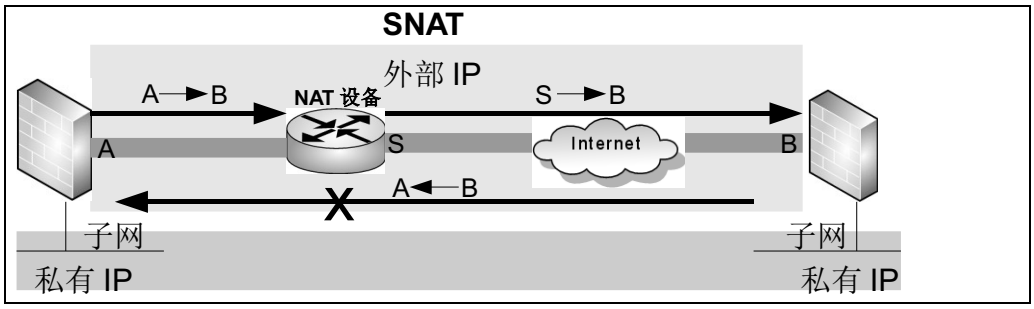
用户通过使用客户端软件进行 SSL VPN 访问而不是浏览器，但是在密码组 （ciphersuite) 确定，密钥和证书交换方面与 SSL VPN 入口页面访问是相同的，请参见 11.1.4.3. 实现。

11.1.6 NAT 环境下网段到网段 IPSec VPN (隧道模式）

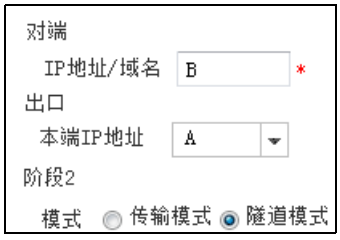
- 11.1.6.1 IPSec VPN +SNAT
- 11.1.6.2 DNAT
- 11.1.6.3 MIP

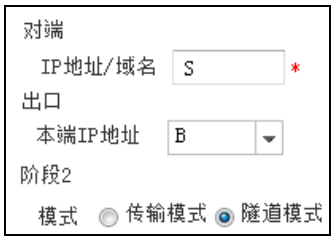
11.1.6.1 IPSec VPN +SNAT

下图为 SNAT 环境下的网关到网关 IPSec VPN 隧道。网关 A 可以主动发起隧道协商，而网关 B 因为 SNAT 策略的存在不能主动发起协商。



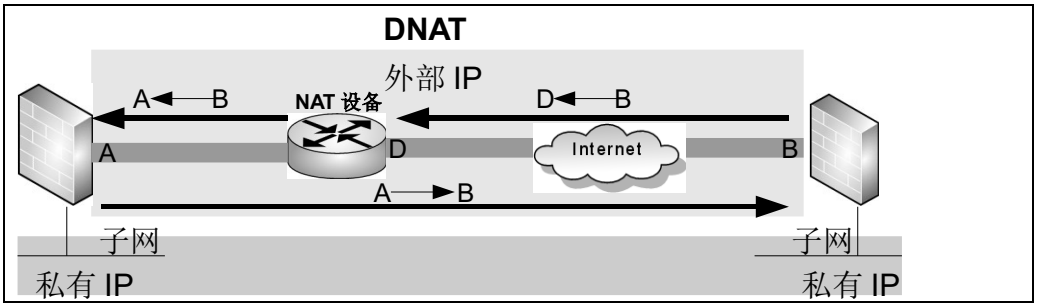
当配置了 SNAT 策略的情况下，自动密钥隧道两端需要进行如下配置 (请选择 **VPN** > **IPSec VPN** > **自动密钥隧道**）：



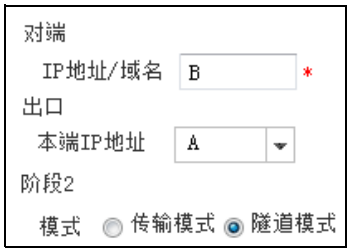


11.1.6.2 DNAT

下图为 DNAT 环境下网关到网关的 IPSec VPN 隧道。网关 A 和网关 B 都可以主动发起隧道协商。 VPN 网关 A 发起的包不受 NAT 设备保护。



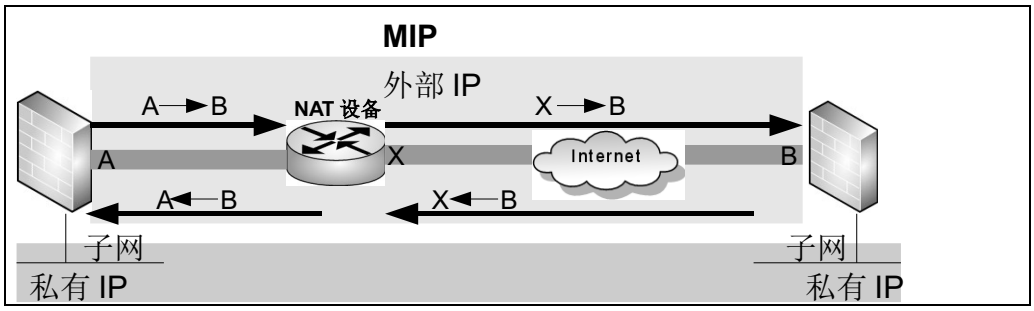
当配置了 DNAT 的情况下，自动密钥隧道两端需要进行如下配置：



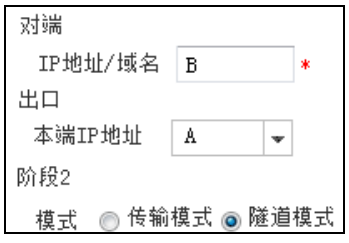
11.1.6.3 MIP

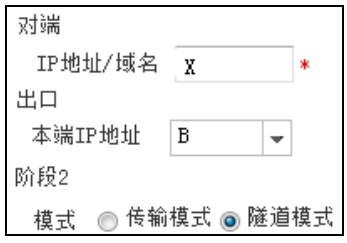
在配置了 MIP 的情况下，隧道任意一端都可以发起隧道协商，且 VPN 网关 A 的 IP 地址是受保护的。下图显示了 NAT 环境下隧道两端的源和目的 IP 地址。

- 初始数据包的源 （A, X) 和目的 （B）地址。
- 初始数据包的源 （B）和目的 （X, A) IP 地址。



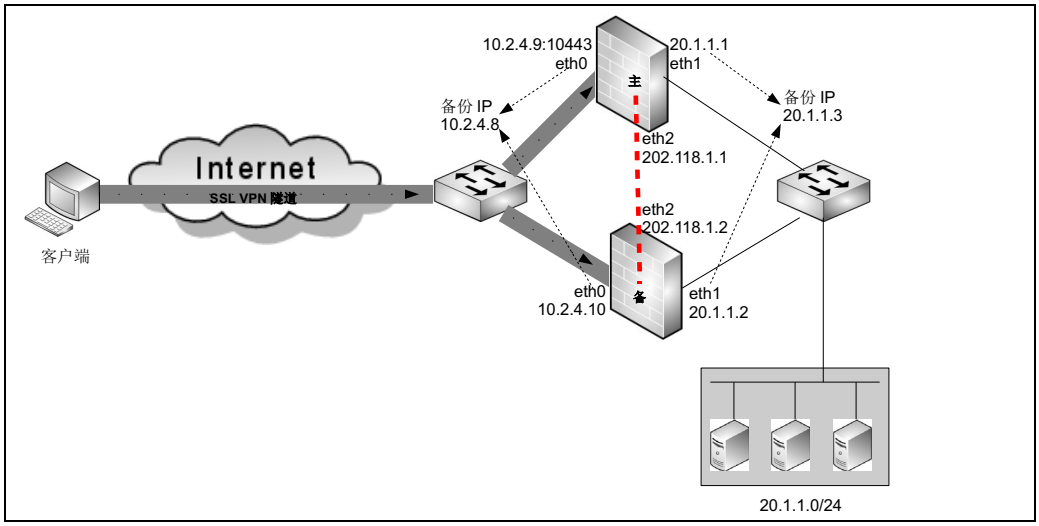
当配置了 MIP 的情况下，自动密钥隧道两端需要进行如下配置：





11.1.7 高可用环境下的 VPN

与常规 HA 环境相同，通常需要将虚拟路由器的备份 IP 指定为 SSL VPN 服务器 IP。



在 SSL VPN 隧道页面以及 SSL 客户端上指定虚拟路由器的备份 IP。

11.2 基本配置

本节描述了 NISG VPN 的基本配置步骤。在用户的实际应用场景中，并不会用到所有这些配置信息。

- 11.2.1 网段到网段手动密钥隧道 （范例 1）
- 11.2.2 网段到网段 IPSec 自动密钥隧道 （范例 2）
- 11.2.3 远程访问 IPSec 自动密钥隧道 （范例 3）
- 11.2.4 SSL VPN Web 入口页面访问 （范例 4）
- 11.2.5 SSL VPN 隧道 （范例 5）

11.2.1 网段到网段手动密钥隧道 （范例 1）

- 11.2.1.1 事先准备
- 11.2.1.2 配置步骤

11.2.1.1 事先准备

VPN 隧道的两端必须根据要求配置 SA 参数 （ 1.2 创建手动密钥隧道 (联动创建隧道接口）)，可能包括：

- ESP 加密算法 / 密钥
- ESP 认证算法 / 密钥
- ESP 本端 / 对端 SPI
- AH 认证算法 / 密钥
- AH 本端 / 对端 SPI

11.2.1.2 配置步骤

1. 创建隧道。请选择 **VPN** > **手动密钥隧道**在本端和对端设备上分别创建一条 VPN 隧道（请参见 1.2 创建手动密钥隧道 (联动创建隧道接口）)。
2. 选择**防火墙** > **访问策略**或者**网络** > **路由**在访问策略或者路由中引用隧道，将匹配的数据包引入到 VPN 隧道。（请参见 1.3 引用隧道）。
3. 隧道生效。配置完成后，隧道就生效了。（请参见 1.4 监控 VPN 信息）。

11.2.2 网段到网段 IPSec 自动密钥隧道 （范例 2）

- 11.2.2.1 事先准备
- 11.2.2.2 配置步骤

11.2.2.1 事先准备

本端和对端可能需要配置如下信息：

- 启用 NAT 穿越 （在隧道两端之间存在 NAT 设备的情况下）

- 对端静态 / 动态 IP 地址，是否启用永久隧道。
- 本端出口和 IP 地址
- 对端认证方式：预共享密钥认证和证书认证。如果是证书认证的话，需要上载本地证书和对端的 CA 证书。
- 本端和对端受保护的子网

高级设置 （通常情况下使用默认值即可）

- 阶段一自定义提议集、协商模式 （主模式或者激进模式）、 SA 的生存时间
- 阶段二自定义提议集、抗重放攻击、工作模式 （传输或者隧道模式）、 SA 生存时间
- 失效对等体检测 （DPD)
- 本端或对端 ID 类型 （例如 IPV4_ADDR)

11.2.2.2 配置步骤

1. 导入证书。（ 2.2.2 使用证书认证）请选择**系统** > **证书** > **CA 证书 / 本地证书**导入 CA 证书或本地证书。
2. 创建自动密钥隧道。请选择 **VPN** > **自动密钥隧道**创建自动密钥隧道（ 2.2 创建自动密钥隧道 （联动创建隧道接口））。
3. 选择**防火墙** > **访问策略**或者**网络** > **路由**在路由或者访问策略中引用隧道（请参见 1.3 引用隧道）。
4. 隧道生效。当配置完成后，隧道就生效了。请参见 2.4 监控信息。

11.2.3 远程访问 IPSec 自动密钥隧道 （范例 3）

- 11.2.3.1 事先准备
- 11.2.3.2 配置步骤

11.2.3.1 事先准备

本端和对端可能需要配置如下信息：

VPN 网关：

- 启用 NAT 穿越 （在隧道两端之间存在 NAT 设备的情况下）
- 对端类型、本端出口和 IP 地址
- 对端认证：预共享密钥或者证书。如果是证书认证的话，需要在 NISG 上导入对端的 CA 证书以及本端的本地证书。
- 本端和对端的子网 IP。
- 高级设置 （通常情况下会使用默认设置）：
  - 阶段一自定义提议集、协商模式 （主模式或者激进模式）、 SA 的生存时间
  - 阶段二自定义提议集、抗重放攻击、传输或者隧道模式、 SA 的生存时间
  - 失效对等体检测 （DPD)
  - 本端或对端 ID 类型 （例如 IPV4_ADDR)

用户：

- 用户名、特定超时时间、多点登录、密码、分配 IP（无、静态 IP 地址、IP 地址池）、DNS/WINS IP 地址。
- 用户认证：本地或外部认证、客户端类型 (L2TP 或者 Xauth)、WebAuth 认证（主动或者被动）。

VPN 客户端：

如果使用证书认证，导入对端 CA 和本端的本地证书。

11.2.3.2 配置步骤

1. 创建并导入证书或者设置预共享密钥。
2. 进行客户端配置，请参见 3.2 Windows 客户端配置。
3. 请选择**系统** > **认证** > **用户**，创建一个新的用户。请参见 3.3 创建 IPSec VPN 用户。
4. 请选择 **VPN** > **自动密钥隧道**创建自动密钥隧道。请参见范例 3.4 创建自动密钥隧道（联动创建隧道接口）。
5. 在客户端拨号连接 VPN。请参见 3.5 拨号连接。

11.2.4 SSL VPN Web 入口页面访问 （范例 4）

- 11.2.4.1 事先准备
- 11.2.4.2 配置步骤

11.2.4.1 事先准备

SSL VPN 网关可能需要配置如下信息：

- 用户：
  - 用户名、特定超时时间、多点登录、密码、分配 IP （无、静态 IP 地址、 IP 地址池）、 DNS/WINS IP 地址。
  - 用户认证：本地或外部认证、客户端类型 (L2TP 或者 Xauth)、WebAuth（主动或者被动）。
- SSL VPN 网关 :
  - 用户组
  - IP 地址池
  - 应用 : URLs
  - 页面模板：Web 页面设计、内容、图标等。
  - 页面服务：服务绑定接口和 IP 地址、用户组、入口页面、会话超时时间、登录失败上限；启用登录时需要验证码、验证用户证书、保存用户配置、允许用户修改密码； SSL VPN 证书、支持的 SSL 版本、算法等级；开启客户端安全要求；访问允许列表；用户组访问授权列表和用户默认权限。

11.2.4.2 配置步骤

- 创建和导入 SSL 证书，有关该步骤的详细信息，请参见 4.3 导入 CA/ 本地证书。
- 创建SSL VPN用户/用户组/IP地址池。请选择**系统**> **认证**>**用户**进入用户页面。请选择**VPN** > **SSL VPN** > **用户组**创建 SSL VPN 用户组。请参见 4.2 创建 IP 地址池， SSL VPN 用户， SSL VPN 用户组。
- 请选择**VPN** > **SSL VPN** > **SSL VPN Web入口页面** > **应用/页面模板**进入应用和页面模板页面添加应用和创建页面模板。参见 4.4 创建 SSL VPN 应用， SSL VPN 页面模板。
- 创建 SSL VPN 页面服务。请参见 4.5 创建 SSL VPN 页面服务。
- 隧道生效。客户端 PC 发起访问，按照提示安装插件，访问应用链接，也可以自定义应用。4.6 使用 SSL VPN 进行访问。

11.2.5 SSL VPN 隧道 （范例 5）

- 11.2.5.1 事先准备
- 11.2.5.2 配置步骤

11.2.5.1 事先准备

SSL VPN 的用户信息请参见 SSL VPN 入口页面访问的 11.2.4.1 事先准备。

SSL VPN 隧道的独有配置包括：

- 出口接口和 IP 地址
- 授权子网列表

11.2.5.2 配置步骤

1. 安装和配置 SSL VPN 客户端。SSL VPN 用户需要通过安装 SSL VPN 客户端软件来访问 SSL VPN 隧道。有关 SSL VPN 客户端的详细信息，请参见*东软 NISG SSL VPN Android 客户端用户使用指南*和*东软 NISG SSL VPN Windows 客户端用户使用指南*。请参见 5.2 安装 SSL VPN 客户端软件 / 添加 SSL VPN 连接 。
2. 配置 IP 地址池、用户和用户组。请参 4.2 创建 IP 地址池，SSL VPN 用户，SSL VPN 用户组。
3. 创建 SSL VPN 隧道。请选择 **VPN** > **SSL VPN** > **SSL VPN 隧道** > **隧道**进入**隧道**页面创建新的隧道。请参见 5.4 创建 SSL VPN 隧道。
4. 隧道生效。在 SSL VPN 客户端点击**连接**，成功连接后，用户就可以通过 SSL VPN 隧道进行访问了。请参见 5.5 连接到 SSL VPN 服务器。

11.3 范例

本节分步骤详细介绍了 VPN 范例的配置：

- 范例 1. 网段到网段的手动密钥隧道。该范例描述了如何在两个网站之间创建一条手动密钥隧道。之所以把这个范例放到第一个是因为所涉及的配置简单而且所有的配置都是手动进行的。
- 范例 2. 基于路由的网段到网段自动 IKE。该范例介绍了通过自动密钥生成和安全管理来创建一条隧道。尽管自动密钥隧道相对手动密钥隧道复杂很多，但是在实际应用中却比手动密钥隧道更安全、应用更广泛。
- 范例 3. 远程访问 VPN 隧道。该范例演示了如何在 Windows 客户端和 NISG 设备之间创建一条 IPSec VPN 隧道。
- 范例 4. 通过 SSL VPN Web 入口页面访问。该范例描述了如何为远程用户创建一条 Web-Only 型 SSL VPN 隧道，只允许授权用户访问受保护的内网资源。
- 范例 5. 通过 SSL VPN 隧道访问。该范例描述了如何在 VPN 客户端和 NISG 设备之间创建一条 SSL VPN 隧道。

NAT

- 范例 6. NAT 穿越（IPSec VPN)。该范例描述了在 IPSec VPN 环境中存在 NAT 设备的情况下如何配置 VPN 隧道两端。

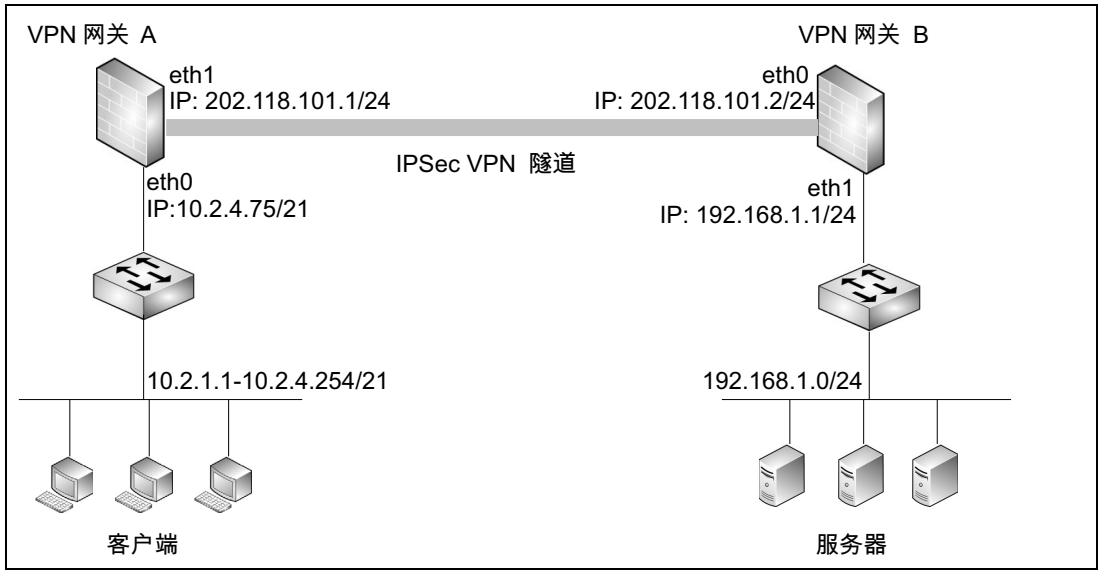
HA

- 范例 7. HA 自动同步 （SSL VPN)。该范例描述了 HA 环境下 VPN 隧道的配置。
- 范例 8. IPSec VPN 隧道组。该范例描述了如何配置隧道组来保证隧道两端不会因隧道的中断而影响通信。

范例 1. 网段到网段的手动密钥隧道

如图 47 所示，在 VPN 网关 A 和 VPN 网关 B 之间建立一条手动密钥隧道来保护位于 VPN 网关 A 内部子网和 VPN 网关 B 子网间的通信安全。

图 47 VPN 网关 A 和 VPN 网关 B 使用手动密钥隧道连接



安全需求：

- 通信数据加密
- 隐藏内网 IP 地址
- 配置和维护简单

配置步骤

- 1.1 配置接口 IP 地址 / 缺省路由 / 缺省策略
- 1.2 创建手动密钥隧道 (联动创建隧道接口）
- 1.3 引用隧道
- 1.4 监控 VPN 信息

1.1 配置接口 IP 地址 / 缺省路由 / 缺省策略

1.1.1 配置接口 IP 地址

VPN 网关 A:

1. 请选择**网络** > **接口**，进入**接口**页面对 eth0 和 eth1 进行配置。
   - eth0: 接口状态 = 开，模式 = 三层， MTU=1500，获取 IP 地址方式 = 静态 IP, IP 地址列表主 IP=10.2.4.75/21.
   - eth1: 接口状态 = 开，模式 = 三层， MTU=1500，获取 IP 地址方式 = 静态 IP, IP 地址列表主 IP=202.118.101.1/24.
2. 点击**确定**。

VPN 网关 B:

用同样的方法为 VPN 网关 B 配置 IP 地址 .

- eth0: 开，三层， MTU=1500，静态 IP, IP 地址列表主 IP=202.118.101.2/24。
- eth1: 开，三层， MTU=1500, 静态 IP, IP 地址列表主 IP=192.168.1.1/24。

CLI

VPN 网关 A:

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet 0
NetEye@root-system-if-eth0] working-type layer3-interface
NetEye@root-system-if-eth0] ip address 10.2.4.75 255.255.248.0
NetEye@root-system-if-eth0] exit
NetEye@root-system] interface ethernet 1
NetEye@root-system-if-eth1] working-type layer3-interface
NetEye@root-system-if-eth1] ip address 202.118.101.1 255.255.255.0
NetEye@root-system-if-eth1] end
NetEye@root> save config
```

VPN 网关 B:

除了以下两条，其他的命令与 VPN 网关 A 一致。

```
NetEye@root-system-if-eth0] ip address 202.118.101.2 255.255.248.0
NetEye@root-system-if-eth1] ip address 192.168.1.1 255.255.255.0
```

1.1.2 添加缺省路由

VPN 网关 A:

1. 请选择**网络** > **路由** > **缺省路由**，进入**缺省路由**页面添加一条缺省路由。

   类型 =IPv4 地址，目的 IPv4 地址 =0.0.0.0，掩码长度 =0， Metric=1, 出口接口 / 网关 = 常规，接口 =eth1, 网关 =202.118.101.2。

2. 点击**确定**。

VPN 网关 B:

以同样的方法在 VPN 网关 B 上添加一条缺省路由：

IPv4 地址，目的 IPv4 地址 =0.0.0.0，掩码长度 =0， Metric=1, 出口接口 / 网关 = 常规，接口 =eth0, 网关 =202.118.101.1。

CLI

VPN 网关 A:

```
NetEye@root-system] route 0.0.0.0 0.0.0.0 interface eth1 gateway
202.118.101.2
NetEye@root-system] exit
NetEye@root> save config
```

VPN 网关 B:

```
NetEye@root-system] route 0.0.0.0 0.0.0.0 interface eth0 gateway
202.118.101.1
NetEye@root-system] exit
NetEye@root> save config
```

1.1.3 配置访问策略

VPN 网关 A:

1. 请选择**防火墙** > **访问策略**，进入**访问策略**页面。
   - 序号 =1，名称 =atob, 启用 = 勾选
   - 源安全域 =Any, 源 IP= 使用下表，源 IP 地址列表 =IPv4 地址范围 =10.2.1.1-10.2.4.254。
   - 源用户 =Any。
   - 目的安全域 =Any, 目的 IP 地址 = 使用下表，目的 IP 地址列表 =IPv4 地址范围 =192.168.1.1-192.168.1.254。
   - 服务 = 任意，动作 = 允许。

VPN 网关 B:

请选择**防火墙** > **缺省策略配置**，配置域间缺省策略的动作为**允许**。

CLI

VPN 网关 A:

```
NetEye@root-system] policy access atob any 10.2.1.1-10.2.4.254 any
192.168.1.1-192.168.1.254 any any permit enable
NetEye@root-system] exit
NetEye@root> save config
```

VPN 网关 B:

```
NetEye@root-system] policy default inter-zone access permit
```

提示：如果在步骤 1.3 引用隧道中需要创建访问策略引用手动密钥隧道接口，则不需要在 1.1.3 配置访问策略中为 VPN 网关 A 设置访问策略。

1.2 创建手动密钥隧道 (联动创建隧道接口）

VPN 网关 A:

1. 请选择 **VPN** > **手动密钥隧道**，进入**手动密钥隧道**页面。
2. 点击**新建**，创建一条手动密钥隧道，进行如下配置：

3. 点击**确定**。

VPN 网关 B:

4. 请选择 **VPN > 手动密钥隧道**，进入**手动密钥隧道**页面。
5. 点击**新建**，创建一条手动密钥隧道，进行如下配置：

6. 点击**确定**。
7. 点击 。

提示：ESP 和 AH 必须至少配置一项；本端和对端的加密算法和认证算法必须相同；本端和对端的 SPI 值正好相反。

CLI

VPN 网关 A:

```
NetEye@root-system-vpn] tunnel atob manual gateway remote-ip
202.118.101.2 local-ip 202.118.101.1 esp 10011001 1eeeffff auth
hmac-md5 key 6c6a79b4357c6c6a6c6a79b4357c6c6a encrypt aes128 key
6c6a79b4357c6c6a6c6a79b4357c6c6a mode tunnel enable
NetEye@root-system-vpn] end
NetEye@root> save config
```

VPN 网关 B:

```
NetEye@root-system-vpn] tunnel btoa manual gateway remote-ip
202.118.101.1 local-ip 202.118.101.2 esp 1eeeffff 10011001 auth
hmac-md5 key 6c6a79b4357c6c6a6c6a79b4357c6c6a encrypt aes128 key
6c6a79b4357c6c6a6c6a79b4357c6c6a mode tunnel enable
```

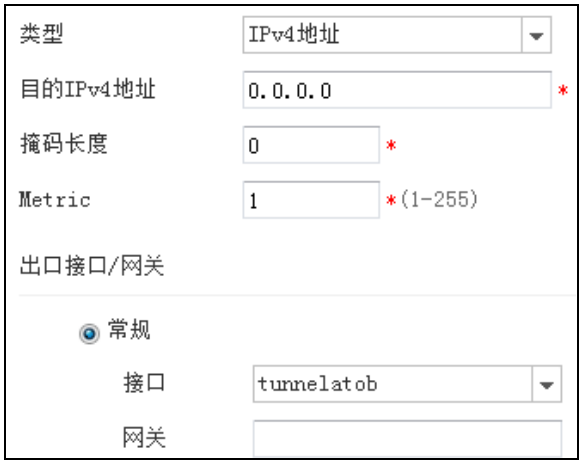
1.3 引用隧道

对于 VPN 网关 A 转发的数据包，可以通过路由或访问策略将匹配的数据包引入手动密钥隧道：

- 1.3.1 路由
- 1.3.2 访问策略

1.3.1 路由

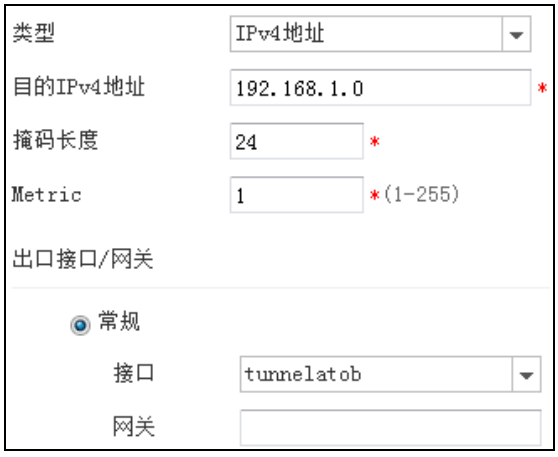
- 请选择**网络** > **路由** > **缺省路由**，点击**新建**添加缺省路由引用隧道：



CLI

```
NetEye@@root-system] route default interface tunnelatob 1
```

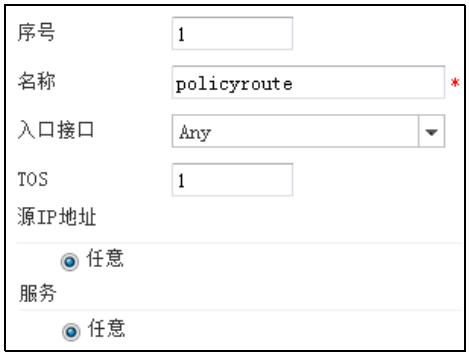
- 请选择**网络** > **路由** > **缺省路由**，点击**新建**添加静态路由引用隧道：

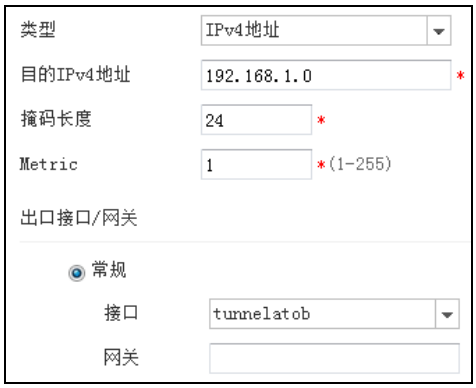


CLI

```
NetEye@@root-system] route 192.168.1.0 255.255.255.0 interface
tunnelatob
```

- 请选择**网络** > **路由** > **策略路由**配置策略路由，在策略路由的路由表中添加路由引用隧道。





CLI

```
NetEye@@root-system] policy route policyroute number 1
NetEye@@root-system-routepolicy-policyroute] route 192.168.1.0
255.255.255.0 interface tunnelatob
NetEye@@root-system-routepolicy-policyroute] exit
NetEye@@root-system] policy route policyroute enable
```

1.3.2 访问策略

1. 请选择**防火墙** > **访问策略**，进入**访问策略**页面。

2. 点击**确定**。
3. 点击 。

CLI

```
NetEye@root-system] policy access atob any 10.2.1.1-10.2.4.254 any
192.168.1.1-192.168.1.254 any any permit enable
NetEye@root-system] policy access atob tunnel atob
NetEye@root-system] exit
NetEye@root> save config
```

1.4 监控 VPN 信息

VPN 网关 A/B:

选择**监控** > **IPSec VPN 隧道** > **手动密钥隧道**，进入手动密钥隧道监控页面，查看 VPN 隧道的监控信息。

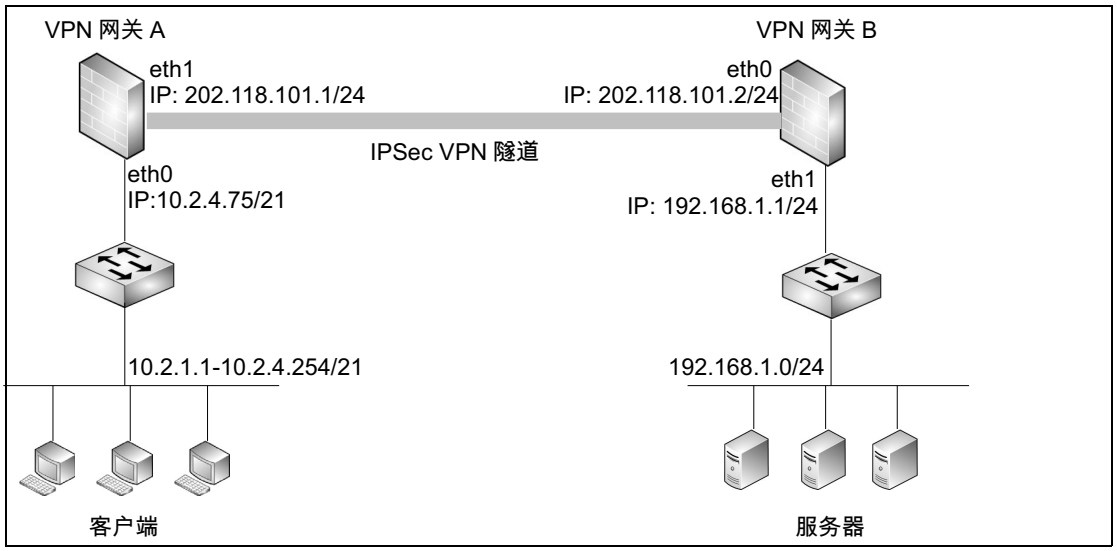
基本信息	
名称	atob
本端IP地址	202.118.101.1
对端IP地址	202.118.101.2
模式	隧道模式
ESP	true
Auth ALG	hmac-md5
ENC ALG	aes128
本端SPI	10011001
对端SPI	1eeeffff
AH	false

基本信息	
名称	btoa
本端IP地址	202.118.101.2
对端IP地址	202.118.101.1
模式	隧道模式
ESP	true
Auth ALG	hmac-md5
ENC ALG	aes128
本端SPI	1eeeffff
对端SPI	10011001
AH	false

范例 2. 基于路由的网段到网段自动 IKE

如图 48 所示，在 VPN 网关 A 和 B 之间建立一条自动密钥隧道，当位于 VPN 网关 A 内部的子网发起对 VPN 网关 B 内部的服务器的访问时，数据包将会被转发至 VPN 隧道，从而保证了通信安全。

图 48 VPN 网关 A 和 VPN 网关 B 使用 IPSec VPN 自动密钥隧道连接



安全需求：

- 自动 SA 协商
- 自动密钥协商
- 使用预共享密钥或者证书认证

配置步骤

- 2.1 配置接口 IP 地址 / 缺省路由 / 访问策略
- 2.2 创建自动密钥隧道 （联动创建隧道接口）
- 2.3 引用隧道
- 2.4 监控信息

2.1 配置接口 IP 地址 / 缺省路由 / 访问策略

2.1.1 配置接口 IP 地址

VPN 网关 A:

1. 请选择**网络** > **接口**，进入**接口**页面对 eth0 和 eth1 进行配置。
   - eth0: 接口状态 = 开，模式 = 三层， MTU=1500，获取 IP 地址方式 = 静态 IP, IP 地址列表主 IP=10.2.4.75/21。
   - eth1: 接口状态 = 开，模式 = 三层， MTU=1500，获取 IP 地址方式 = 静态 IP, IP 地址列表主 IP=202.118.101.1/24。
2. 点击**确定**。

VPN 网关 B:

用同样的方法为 VPN 网关 B 配置 IP 地址。

- eth0: 开，三层， MTU=1500，静态 IP, IP 地址列表主 IP=202.118.101.2/24。
- eth1: 开，三层， MTU=1500, 静态 IP, IP 地址列表主 IP=192.168.1.1/24。

CLI

VPN 网关 A:

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet 0
NetEye@root-system-if-eth0] working-type layer3-interface
NetEye@root-system-if-eth0] ip address 10.2.4.75 255.255.248.0
NetEye@root-system-if-eth0] exit
NetEye@root-system] interface ethernet 1
NetEye@root-system-if-eth1] working-type layer3-interface
NetEye@root-system-if-eth1] ip address 202.118.101.1 255.255.255.0
NetEye@root-system-if-eth1] exit
NetEye@root> save config
```

VPN 网关 B:

除了以下两条，其他的命令与 VPN 网关 A 一致。

```
NetEye@root-system-if-eth0] ip address 202.118.101.2 255.255.248.0
NetEye@root-system-if-eth1] ip address 192.168.1.1 255.255.255.0
```

2.1.2 添加缺省路由

VPN 网关 A:

1. 请选择**网络** > **路由** > **缺省路由**，进入**缺省路由**页面添加一条缺省路由。

   类型 =IPv4 地址，目的 IPv4 地址 =0.0.0.0，掩码长度 =0， Metric=1,
   出口接口 / 网关 = 常规，接口 =eth1, 网关 =202.118.101.2。

2. 点击**确定**。

VPN 网关 B:

以同样的方法在 VPN 网关 B 上添加一条缺省路由：

IPv4 地址，目的 IPv4 地址 =0.0.0.0，掩码长度 =0， Metric=1, 出口接口 / 网关 = 常规，接口 =eth0, 网关 =202.118.101.1。

CLI

VPN 网关 A:

```
NetEye@root-system] route 0.0.0.0 0.0.0.0 interface eth1 gateway
202.118.101.2
NetEye@root-system] exit
NetEye@root> save config
```

VPN 网关 B:

```
NetEye@root-system] route 0.0.0.0 0.0.0.0 interface eth0 gateway
202.118.101.1
NetEye@root-system] exit
NetEye@root> save config
```

2.1.3 创建访问策略

VPN 网关 A:

1. 请选择**防火墙** > **访问策略**，进入**访问策略**页面。
   - 序号 =1，名称 =atob，启用 = 勾选
   - 源安全域 =Any, 源 IP= 使用下表，源 IP 地址列表 =IPv4 地址范围 =10.2.1.1-10.2.4.254。
   - 源用户 =Any。
   - 目的安全域 =Any，目的 IP 地址 = 使用下表，目的 IP 地址列表 =IPv4 地址范围 =192.168.1.1-192.168.1.254。
   - 服务 = 任意，动作 = 允许。

VPN 网关 B:

请选择**防火墙** > **缺省策略设置**，配置域间缺省策略的动作为**允许**。不需要自定义访问策略。

CLI

VPN 网关 A:

```
NetEye@root-system] policy access atob any 10.2.1.1-10.2.4.254 any
192.168.1.1-192.168.1.254 any any permit enable
NetEye@root-system] exit
NetEye@root> save config
```

VPN 网关 B:

```
NetEye@root-system] policy default inter-zone access permit
```

提示：如果在步骤 2.3 引用隧道中需要创建访问策略引用自动密钥隧道接口，则不需要在 2.1.3 创建访问策略中为 VPN 网关 A 设置访问策略。

2.2 创建自动密钥隧道 （联动创建隧道接口）

- 2.2.1 使用预共享密钥认证
- 2.2.2 使用证书认证

2.2.1 使用预共享密钥认证

VPN 网关 A：

1. 请选择 **VPN** > **IPSec VPN** > **自动密钥隧道**创建一条新的隧道。

2. 设置本端和对端子网。本端子网 =10.2.0.0/21，对端子网 =192.168.1.0/24。

VPN 网关 B：

1. 请选择请选择 **VPN** > **IPSec VPN** > **自动密钥隧道**创建一条新的隧道。

2. 设置本端和对端子网。本端子网 =192.168.1.0/24，对端子网 =10.2.0.0/21。

CLI

VPN 网关 A：

```
NetEye@root-system] vpn
NetEye@root-system-vpn] tunnel atob gateway 202.118.101.2 interface
eth1 202.118.101.1 preshared-key 123456 local-subnet 10.2.0.0
255.255.248.0 remote-subnet 192.168.1.0 255.255.255.0 enable
```

VPN 网关 B：

```
NetEye@root-system] vpn
NetEye@root-system-vpn] tunnel btoa gateway 202.118.101.1 interface
eth0 202.118.101.2 preshared-key 123456 local-subnet 192.168.1.0
255.255.255.0 remote-subnet 10.2.0.0 255.255.248.0 enable
```

2.2.2 使用证书认证

- 2.2.2.1 生成或导入证书
- 2.2.2.2 创建证书认证的自动密钥隧道

2.2.2.1 生成或导入证书

如果无可用的 CA 和本地证书，可以向证书颁发机构 （CA）申请证书。有关证书申请和生成的详细信息，请参见 3.23.3 范例：自动生成证书。

如果已存在可用的 CA 和本地证书，请按照以下步骤导入证书。

VPN 网关 A:

1. 请选择**系统** > **证书** > **CA 证书**，进入 **CA 证书**页面。
2. 点击**导入**，导入 CA 证书。

3. 点击**确定**。
4. 请选择**系统** > **证书** > **本地证书**，进入**本地证书**页面。

5. 点击**导入**。

6. 点击**确定**。

VPN 网关 B:

以同样的方法为 VPN 网关 B 导入 CA 和本地证书。

提示：对端需要导入本端的 CA 证书，本端需要导入对端的 CA 证书，两端的 CA 证书可以相同；对端和本端导入各自的本地证书。

CLI

VPN 网关 A:

```
NetEye@root-system] import certificate ca from x/zmodem ca
NetEye@root-system] import certificate local from x/zmodem local1
NetEye@root-system] exit
NetEye@root> save config
```

VPN 网关 B:

```
NetEye@root-system] import certificate ca from x/zmodem ca
NetEye@root-system] import certificate local from x/zmodem local2
NetEye@root-system] exit
NetEye@root> save config
```

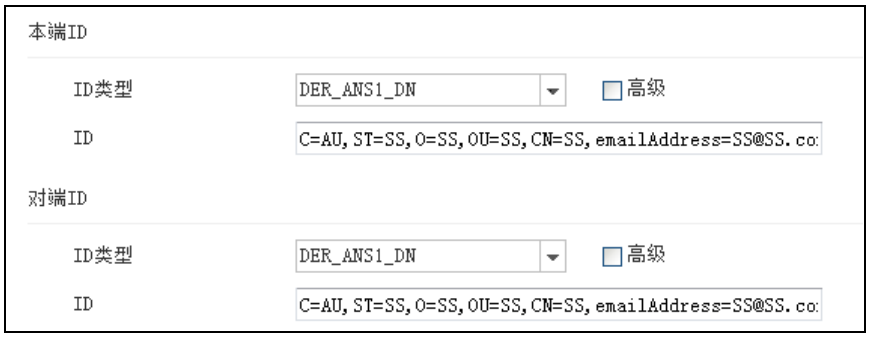
2.2.2.2 创建证书认证的自动密钥隧道

VPN 网关 A:

1. 请选择 **VPN** > **自动密钥隧道**，进入**自动密钥隧道**页面。

2. 点击**新建**，进行如下配置：

3. 点击高级设置，设置本端和对端 ID， ID 值为本端和对端本地证书的主题信息。



4. 点击**确定**。
5. 点击 。

VPN 网关 B:

对 VPN 网关 B 进行同样的配置，除下列内容外：

1. 名称 =btoa, 对端 IP 地址 / 域名 =202.118.101.1，出口 =eth0, 本端 IP 地址 =202.118.101.2，本地证书 =local2。
2. 配置 VPN 网关 B 的本端和对端 ID 如下：
   - 本端 ID:

   ID 类型 =DER_ANS1_DN,
   ID=C=AU,ST=SS,O=SS,OU=SS,CN=SS,emailAddress=SS@SS.com。

   - 对端 ID:

   ID 类型 =DER_ANS1_DN,
   ID=C=AU,ST=SS,O=SS,OU=SS,CN=SS,emailAddress=SS@SS.com。

CLI

VPN 网关 A:

```
NetEye@root-system-vpn] tunnel atob gateway 202.118.101.2 interface
eth1 202.118.101.1 certificate local1 ca enable
NetEye@root-system-vpn] tunnel atob ike local-id asn1-dn
ID=C=AU,ST=SS,O=SS,OU=SS,CN=SS,emailAddress=SS@SS.com
NetEye@root-system-vpn] tunnel atob ike peer-id asn1-dn
ID=C=AU,ST=SS,O=SS,OU=SS,CN=SS,emailAddress=SS@SS.com
NetEye@root-system-vpn] end
NetEye@root> save config
```

VPN 网关 B:

```
NetEye@root-system-vpn] tunnel btoa gateway 202.118.101.1 interface
eth0 202.118.101.2 certificate local2 ca enable
NetEye@root-system-vpn]tunnel btoa ike local-id asn1-dn
ID=C=AU,ST=SS,O=SS,OU=SS,CN=SS,emailAddress=SS@SS.com
NetEye@root-system-vpn]tunnel btoa ike peer-id asn1-dn
ID=C=AU,ST=SS,O=SS,OU=SS,CN=SS,emailAddress=SS@SS.com
NetEye@root-system-vpn] end
NetEye@root> save config
```

2.3 引用隧道

请参见范例 1 手动密钥隧道的 1.3 引用隧道。

2.4 监控信息

当隧道协商成功后，可以查看 VPN 隧道的监控信息。

VPN 网关 A/B:

请选择**监控** > **IPSec VPN 隧道** > **自动密钥隧道**，查看 VPN 隧道信息。

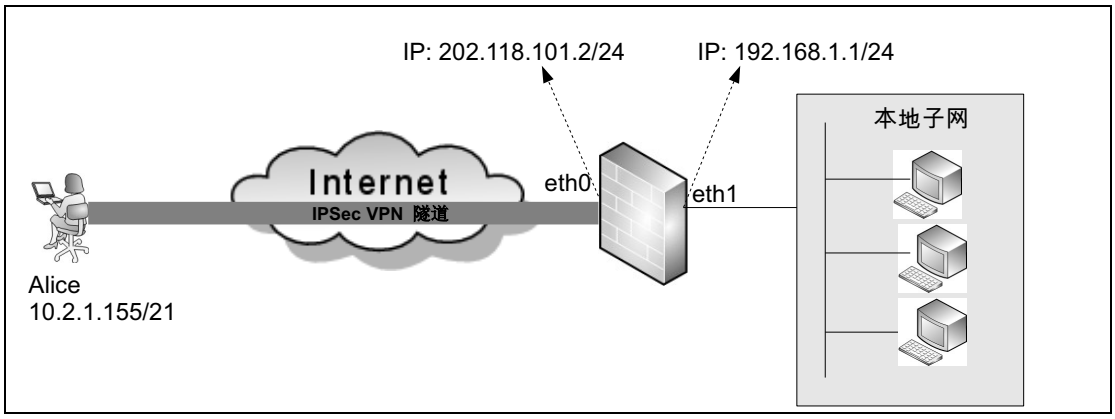
基本信息	
名称	atob
对端类型	静态IP地址
对端信息	202.118.101.2
拨号IP地址	202.118.101.2
出口	eth1
本端IP地址	202.118.101.1
认证模式	证书

基本信息	
名称	btoa
对端类型	静态IP地址
对端信息	202.118.101.1
拨号IP地址	202.118.101.1
出口	eth0
本端IP地址	202.118.101.2
认证模式	证书

范例 3. 远程访问 VPN 隧道

如图 49 所示，远程用户 Alice 使用 Windows 操作系统，通过 Internet 拨号进入公司内网，要与 VPN 网关后的子网 192.168.1.0/24 进行通信。

图 49 远程访问 VPN



安全需求：

- L2TP/Xauth 拨号连接 VPN
- 自动 SA 协商
- IKE 自动密钥协商
- 使用预共享密钥或者证书认证

配置步骤：

- 3.1 配置接口 IP 地址和缺省访问策略
- 3.2 Windows 客户端配置
- 3.3 创建 IPSec VPN 用户
- 3.4 创建自动密钥隧道 （联动创建隧道接口）
- 3.5 拨号连接
- 3.6 查看 VPN 监控信息

3.1 配置接口 IP 地址和缺省访问策略

3.1.1 配置接口 IP 地址

1. 请选择**网络** > **接口** , 进入**接口**页面对 eth0 和 eth1 进行配置。
   - eth0: 接口状态 = 开，模式 = 三层， MTU=1500，获取 IP 地址方式 = 静态 IP, IP 地址列表主 IP=202.118.101.2/24。
   - eth1: 接口状态 = 开，模式 = 三层， MTU=1500，获取 IP 地址方式 = 静态 IP, IP 地址列表主 IP=192.168.1.1/24。
2. 点击**确定**。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet 0
NetEye@root-system-if-eth0] working-type layer3-interface
NetEye@root-system-if-eth0] ip address 202.118.101.2 255.255.255.0
NetEye@root-system-if-eth0] exit
NetEye@root-system] interface ethernet 1
NetEye@root-system-if-eth1] working-type layer3-interface
NetEye@root-system-if-eth1] ip address 192.168.1.1 255.255.255.0
NetEye@root-system-if-eth1] end
NetEye@root> save config
```

3.1.2 配置缺省访问策略

1. 请选择**防火墙** > **缺省策略设置**，设置域间缺省策略的动作为**允许**。

2. 点击**确定**。

CLI

```
NetEye@root-system] policy default inter-zone access permit
NetEye@root-system] exit
NetEye@root> save config
```

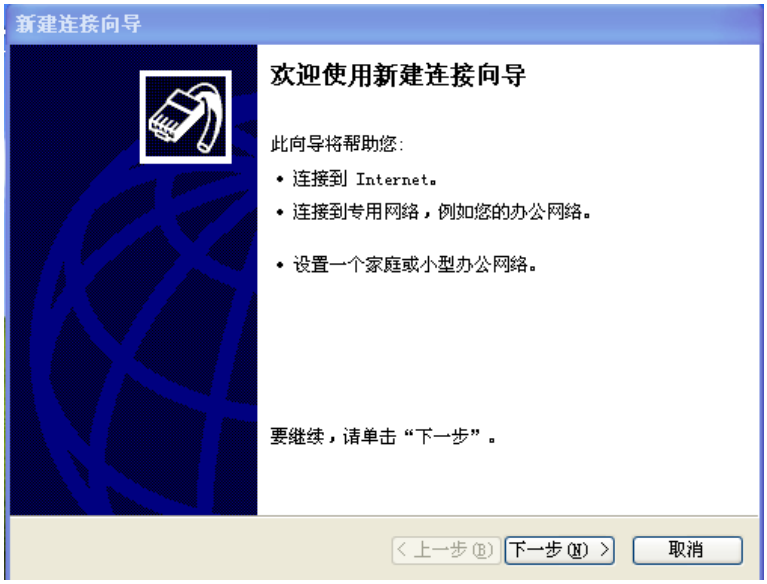
3.2 Windows 客户端配置

IPSec VPN 远程访问用户可以使用 Wiondows 内置客户端连接到 VPN 网关，也可以安装 VPN 客户端软件进行访问。

- 3.2.1 Windows 内置客户端配置
- 3.2.2 东软 NISG VPN 客户端软件安装和配置
- 3.2.3 TheGreenBow IPSec VPN 客户端配置

3.2.1 Windows 内置客户端配置

1. 请选择**开始** > **所有程序** > **附件** > **通讯** > **网络连接**。
2. 在**网络任务**里选择**创建一个新的连接**，出现如下对话框。

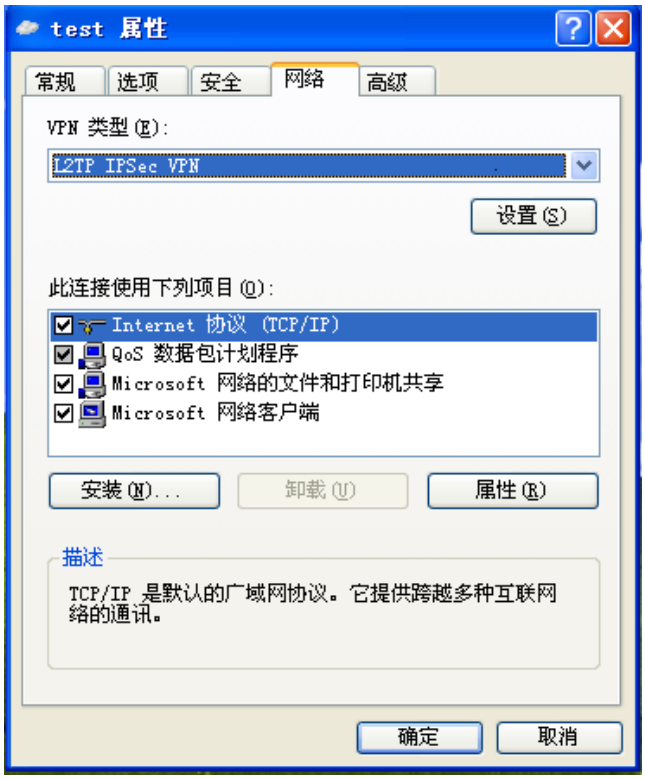


3. 点击**下一步**。
4. 选择**连接到我的工作场所的网络**，点击**下一步**，进入下一步操作。
5. 选择**虚拟专用网络连接**，点击**下一步**，进入下一步操作。
6. 输入公司名 test，点击**下一步**，进入下一步操作。
7. 输入 VPN 连接的名称，点击**下一步**，进入下一步操作。
8. 选择**不拔初始连接**，点击**下一步**，进入下一步操作。
9. 输入隧道的外出接口地址 202.118.101.2，点击**下一步**，进入下一步操作。

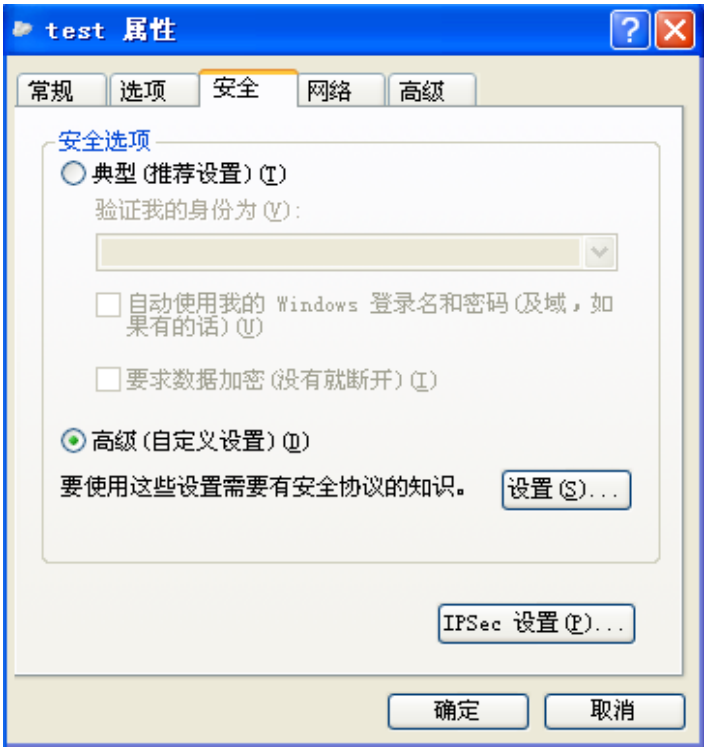
10. 点击**完成**，完成创建连接。

11. 在弹出的连接对话框上，点击**属性**，进行更多配置。

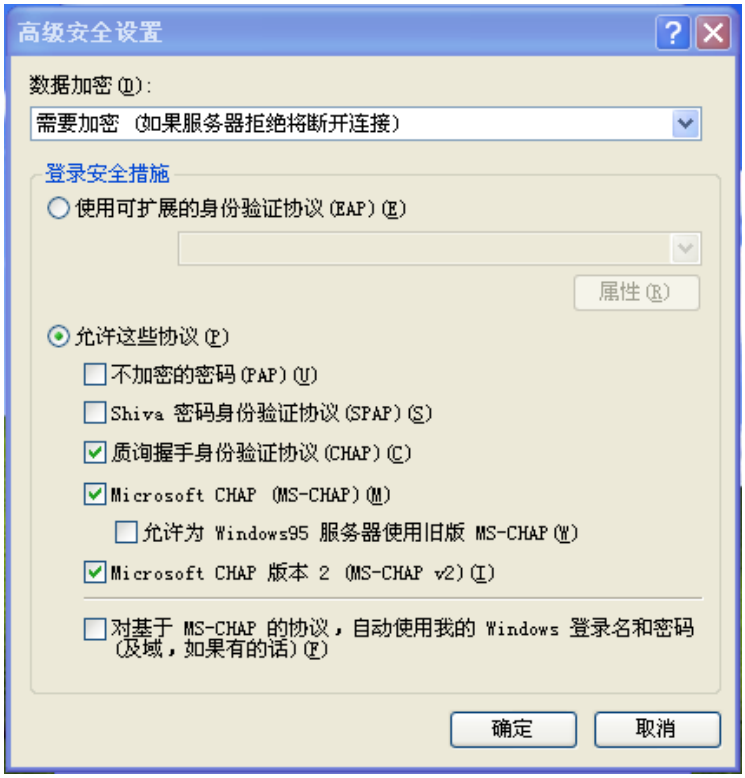
12. 选择**网络**页面，在 **VPN 类型**下拉框中选择 **L2TP IPSec VPN**。点击**确定**，返回连接对话框。



13. 选择**安全**页面，进行安全设置。



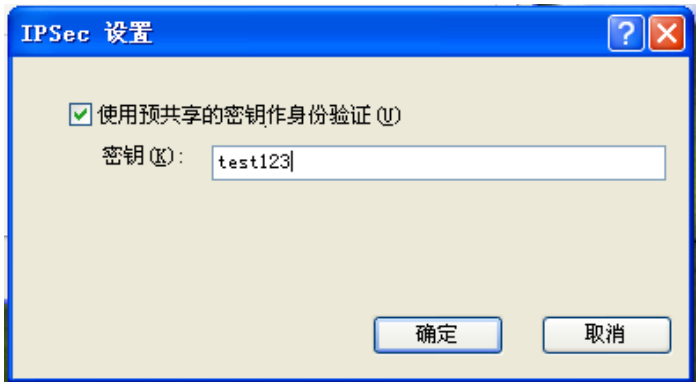
14. 选择**高级 （自定义设置）**，点击**设置。**



15. 在**允许这些协议**下，勾选**质询握手身份验证协议 (CHAP)**，点击**确定**，完成设置。

16. 配置预共享密钥认证或者证书认证

- **设置预共享密钥认证**。点击 **IPSec 设置 ...**，勾选**使用预共享的密钥作身份认证**，设置预共享密钥为 test123，点击**确定**完成。

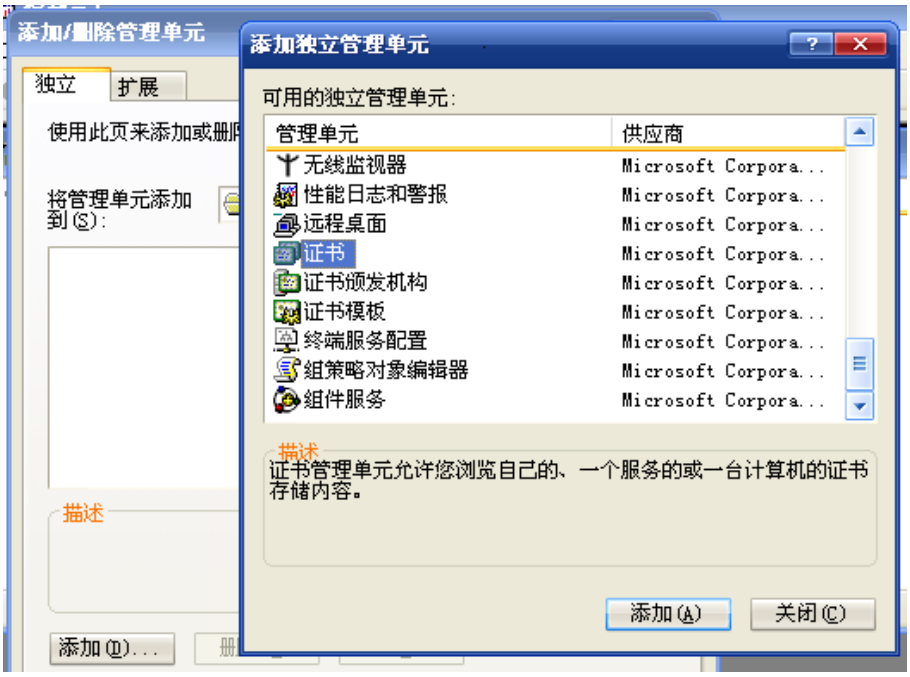


提示：当使用证书认证时，需要取消勾选**使用预共享的密钥作身份验证**。

- **设置证书认证 （导入证书）**

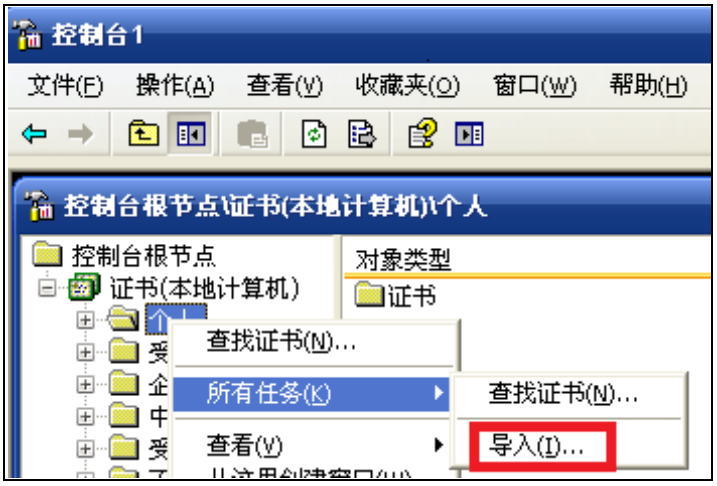
  a. 点击**开始** > **运行**，输入 **mmc** 命令。

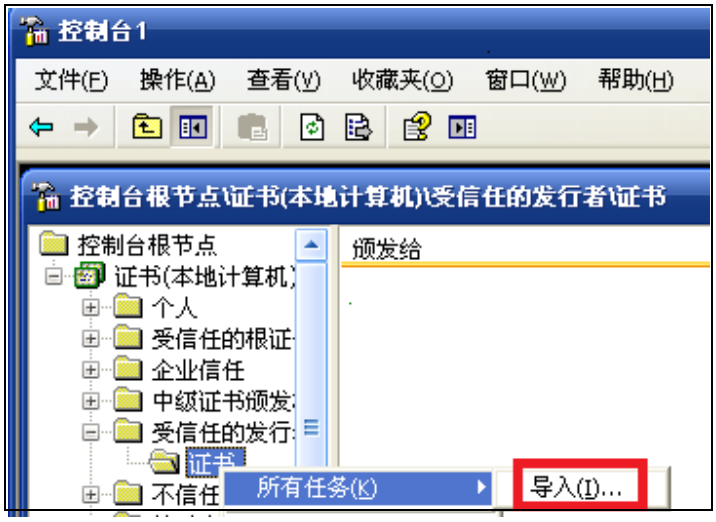
  b. 选择**文件** > **添加 / 删除管理单元**，添加证书。



  c. 选择**计算机账户** > **本地计算机** （运行这个控制台的计算机），添加证书完成。

d. 在控制台根节点下，展开证书节点，导入个人证书和 CA 证书。



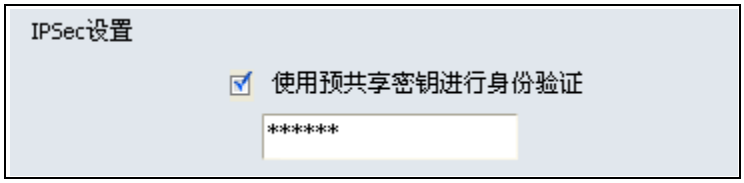


3.2.2 东软 NISG VPN 客户端软件安装和配置

1. 在 Windows 操作系统下安装 IPSec VPN 客户端软件。
2. 点击**创建**，在弹出的**新建 VPN 连接**窗口中创建 VPN 连接。

3. 点击**安全选项**选项卡，设置安全选项信息。

- 如果使用预共享密钥认证，请勾选使用**预共享密钥进行身份验证**复选框。



- 如果使用证书认证，则需要取消勾选**使用预共享密钥进行身份验证**复选框。在证书选项卡中导入 CA 和本地证书。

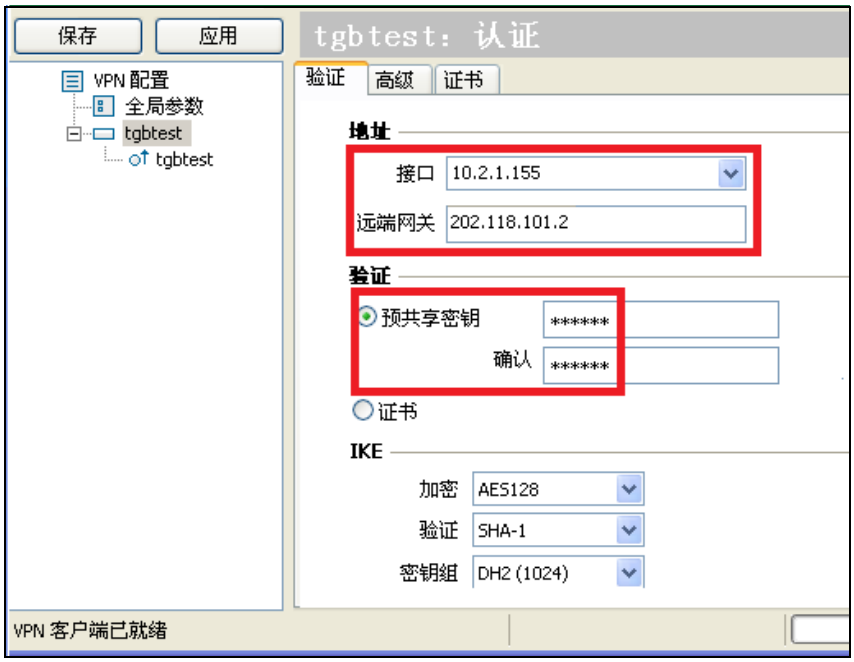
有关 VPN 客户端安装和配置的详细信息，请参见*东软 NISG VPN 客户端用户使用指南*。

3.2.3 TheGreenBow IPSec VPN 客户端配置

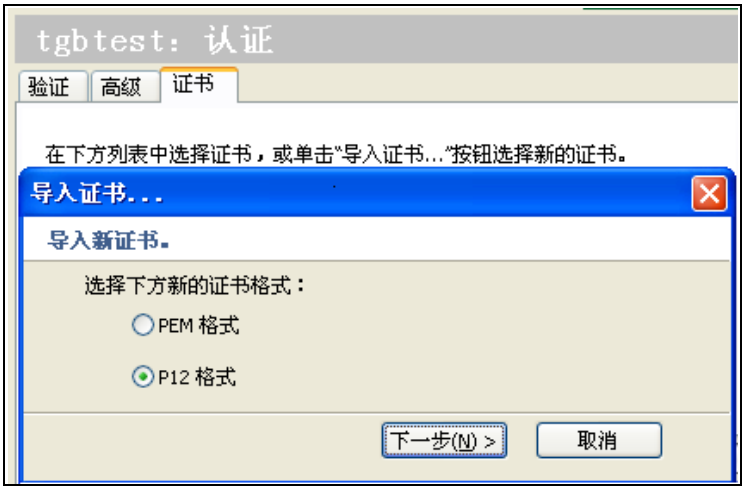
Xauth 认证用户可以安装和配置 TheGreenBow IPSec VPN 客户端软件连接到 IPSec VPN 网关。配置如下：

第一阶段：

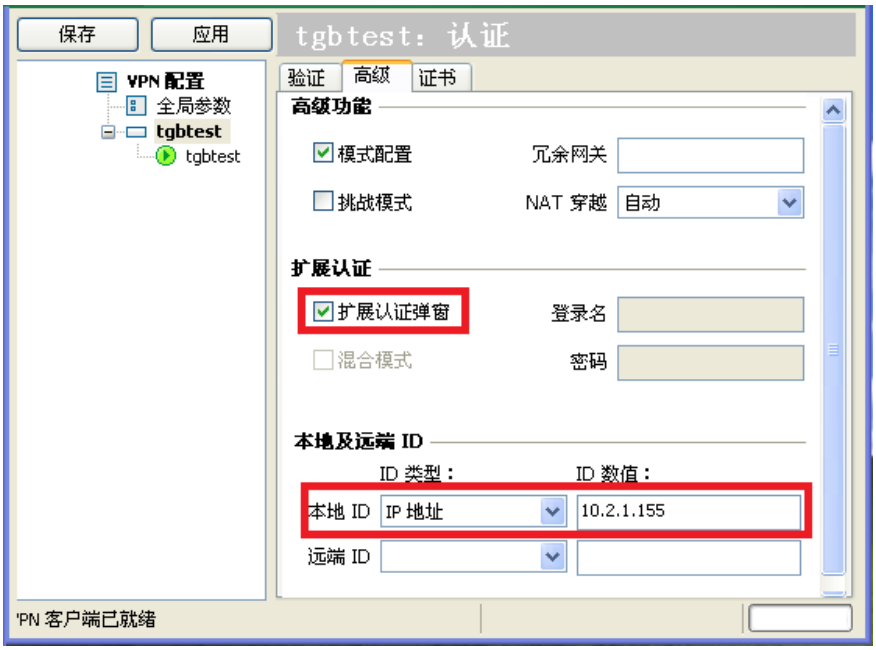
1. 进入**验证**页面，进行如下配置：



- 如果选择证书认证，则需要在证书页面导入 CA 和本地证书（选择 P12 格式选择本地证书，选择 PEM 格式导入 CA 证书）。

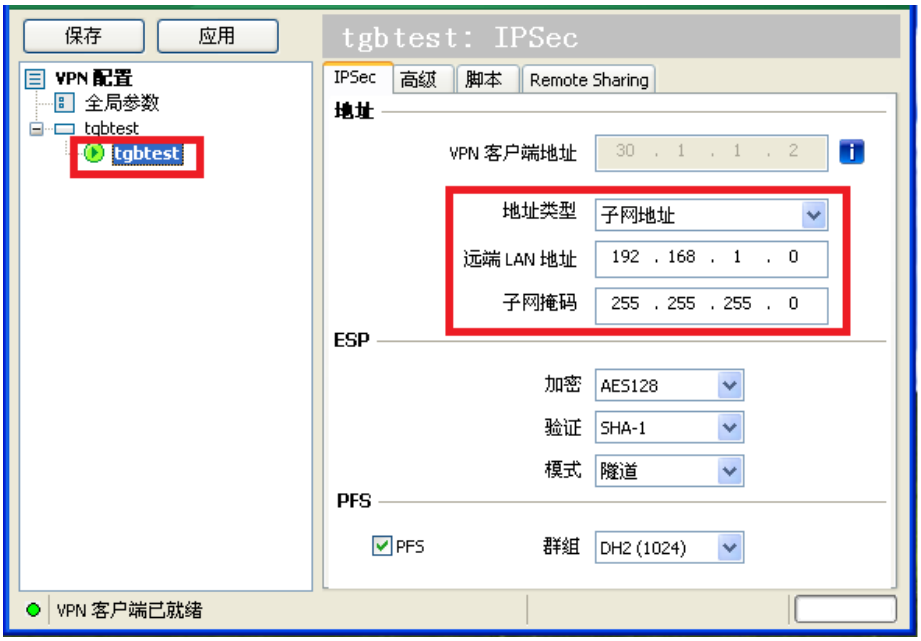


2. 进入**高级**页面，进行如下配置：

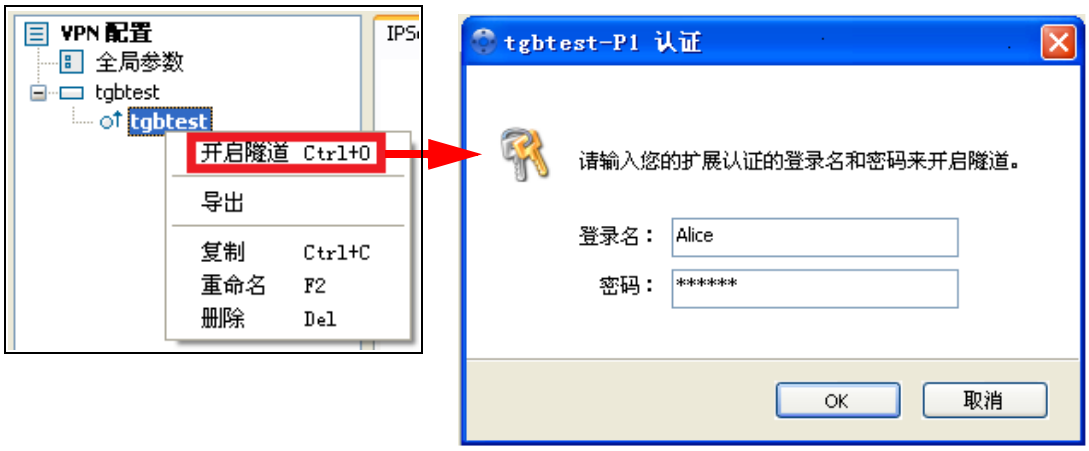


第二阶段：

3. 进入 **IPSec** 页面，进行如下配置：



4. 点击**开启隧道**，在弹出的登录页面中输入用户名和密码进行 VPN 连接。



3.3 创建 IPSec VPN 用户

1. 请选择**系统** > **认证** > **网络用户**，进入**网络用户**页面。
2. 点击**新建**，进行如下配置：

3. 点击**确定**。

提示：1. 当给用户分配静态 IP 地址或者 IP 地址池时，不建议使用 VPN 网关后的子网 IP。
2. 当远程客户端为 Xauth 用户时，请在 **IPSec VPN 配置**区域选择 **Xauth**。

- 如果认证方式设置为**证书认证**，则用户的 ID 类型要进行如下设置：

CLI

- 预共享密钥认证用户

```
NetEye@root-system] user authuser Alice authtype local password
alice123 enable
NetEye@root-system] user authuser Alice ipsecvpn ike-id ipv4-address
10.2.1.155 type l2tp
NetEye@root-system] user authuser Alice assigned-ip 30.1.1.10
NetEye@root-system] exit
NetEye@root> save config
```

- 证书认证命令

```
NISG@root-system] user authuser Alice ipsecvpn ike-id asn1-dn
C=cn,ST=liaoning,O=test,OU=nsd,CN=Alice,emailAddress=Alice@test.com
type l2tp
```

提示：如果客户端与 VPN 网关之间存在 NAT 设备、或者用户通过 PPPoE 拨号连接的场景下，且用户的 ID 类型不能设置为 IPV4_ADDR。在此种场景下，当 VPN 的认证方式为预共享密钥认证时， ID 类型需设置为 FQDN、 USER_FQDN 或 KEY_ID （Windows 的 VPN 客户端需设置为 FQDN）； 当 VPN 的认证方式为证书认证时， ID 类型需设置为 DER_ANS1_DN。

3.4 创建自动密钥隧道 （联动创建隧道接口）

- 3.4.1 使用预共享密钥认证
- 3.4.2 使用证书认证

3.4.1 使用预共享密钥认证

1. 请选择 **VPN** > **自动密钥隧道**，进入**自动密钥隧道**页面。

2. 点击**新建**，进行如下配置：

3. 点击**确定**。
4. 点击 。

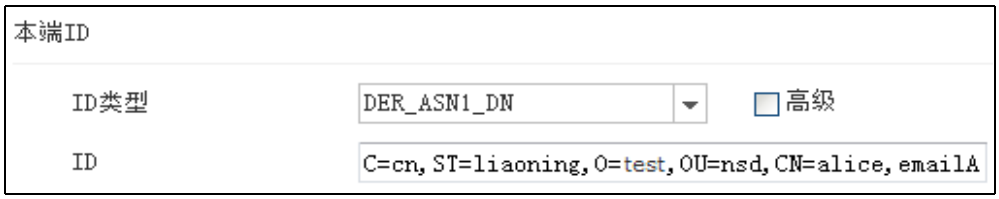
CLI

```
NetEye@root-system] vpn
NetEye@root-system-vpn] tunnel ctog dialup-user user Alice interface
eth0 202.118.101.2 preshared-key test123 enable
NetEye@root-system-vpn] exit
NetEye@root> save config
```

3.4.2 使用证书认证

1. 请选择 **VPN** > **IPSec VPN** > **自动密钥隧道**，进入**自动密钥隧道**页面创建一条自动密钥隧道，请参见 3.4.1 使用预共享密钥认证。设置认证方式为证书认证。

2. 点击**高级设置**，设置本端 ID 如下：



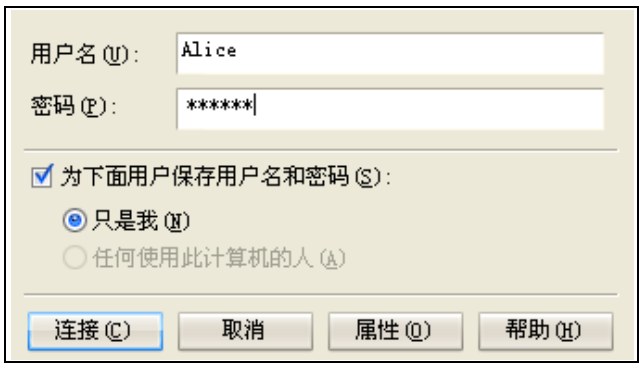
CLI

```
NetEye@root-system] vpn
NetEye@root-system-vpn] tunnel ctog dialup-user user Alice interface eth0 202.118.101.2 certificate local ca enable
NetEye@root-system-vpn] tunnel ctog ike local-id asn1-dn C=cn,ST=liaoning,O=test,OU=nsd,CN=alice,emailAddress=Alice@test.com
NetEye@root-system-vpn] end
NetEye@root> save config
```

3.5 拨号连接

- VPN 内置客户端登录：

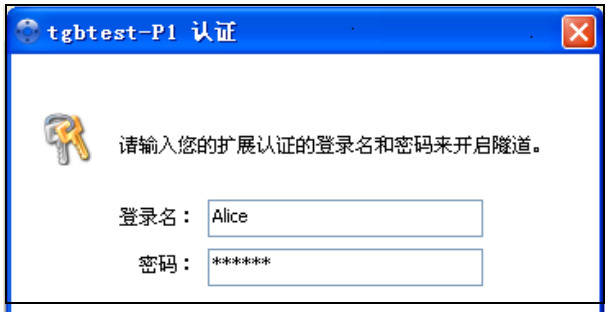
  输入用户名 Alice 及其对应的密码 alice123，点击**连接**，登录到 VPN 网关。



- 东软 NISG VPN 客户端软件登录：

选中 ctog 连接，点击**连接**。

- Xauth 用户通过 TheGreenBow 客户端软件登录。



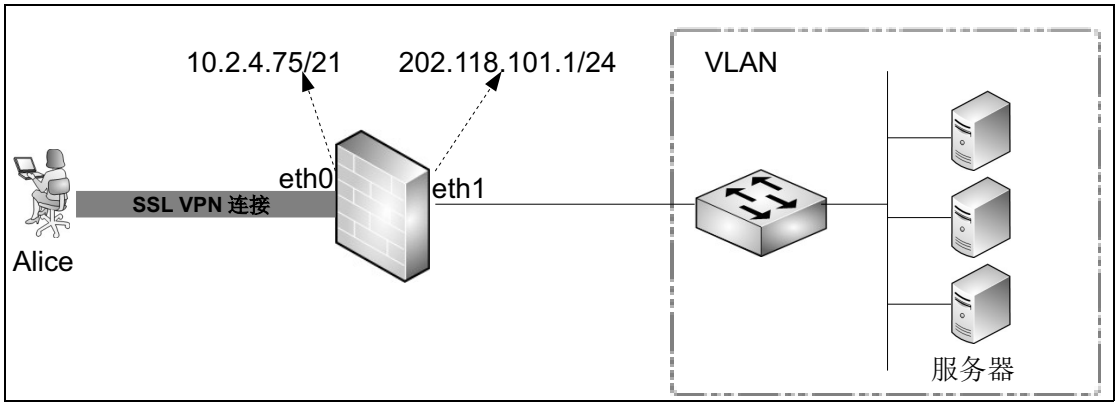
3.6 查看 VPN 监控信息

选择**监控 > IPSec VPN 隧道 > 自动密钥隧道**，进入 **自动密钥隧道**页面，查看 L2TP 用户和 Xauth 用户拨号连接 VPN 隧道的监控信息。

范例 4. 通过 SSL VPN Web 入口页面访问

如图 50 所示，远程用户 Alice 使用 SSL VPN 入口页面对 VPN 网关保护的子网中的服务器资源进行访问。

图 50 SSL VPN 入口页面访问



本范例包含如下配置信息：

- 4.1 配置接口 IP 地址
- 4.2 创建 IP 地址池， SSL VPN 用户， SSL VPN 用户组
- 4.3 导入 CA/ 本地证书
- 4.4 创建 SSL VPN 应用， SSL VPN 页面模板
- 4.5 创建 SSL VPN 页面服务
- 4.6 使用 SSL VPN 进行访问

4.1 配置接口 IP 地址

1. 请选择**网络** > **接口**，进入**接口**页面对 eth0 和 eth1 进行配置。
   - eth0: 接口状态 = 开，模式 = 三层， MTU=1500，获取 IP 地址方式 = 静态 IP, IP 地址列表主 IP=10.2.4.75/21。
   - eth1: 接口状态 = 开，模式 = 三层， MTU=1500，获取 IP 地址方式 = 静态 IP, IP 地址列表主 IP=202.118.101.1/24。
2. 点击**确定**。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet 0
NetEye@root-system-if-eth0] working-type layer3-interface
NetEye@root-system-if-eth0] ip address 10.2.4.75 255.255.248.0
NetEye@root-system-if-eth0] exit
NetEye@root-system] interface ethernet 1
NetEye@root-system-if-eth1] working-type layer3-interface
NetEye@root-system-if-eth1] ip address 202.118.101.1 255.255.255.0
NetEye@root-system-if-eth1] end
NetEye@root> save config
```

4.2 创建 IP 地址池， SSL VPN 用户， SSL VPN 用户组

4.2.1 创建 IP 地址池

1. 请选择 **VPN** > **IP 地址池**，为远程用户进行 SSL VPN 连接创建一个新的 IP 地址池。

2. 点击**确定**。

CLI

```
NetEye@root-system] ippool pool1 192.168.1.2-192.168.1.100
NetEye@root-system] exit
NetEye@root> save config
```

4.2.2 创建 SSL VPN 用户

1. 请选择**系统** > **认证** > **网络用户**，进入**网络用户**页面。
2. 点击**新建**，创建一个新的用户。

3. 点击**确定**。

CLI

```
NetEye@root-system] user authuser Alice authtype local password abcdef enable
NetEye@root-system] user authuser Alice sslvpn
NetEye@root-system] user authuser Alice assigned-ip pool1
NetEye@root-system] exit
NetEye@root> save config
```

4.2.3 创建 SSL VPN 用户组

1. 请选择 **VPN** > **SSL VPN** > **用户组**，进入**用户组**页面。
2. 点击**新建**，创建一个新的用户组并为其分配用户 Alice。

3. 点击**确定**。

CLI

```
NetEye@root-system] sslvpn
NetEye@root-system-sslvpn] group group1 user Alice
NetEye@root-system-sslvpn] group group1 external no
NetEye@root-system-sslvpn] end
NetEye@root> save config
```

4.3 导入 CA/ 本地证书

1. 请选择**系统** > **证书** > **CA 证书** > **导入**，导入 CA 证书。

2. 请选择**系统** > **证书** > **本地证书** > **导入**，导入本地证书。

CLI

```
NetEye@root-system] import certificate ca from x/zmodem ca
NetEye@root-system] import certificate local from x/zmodem local
NetEye@root-system] exit
NetEye@root> save config
```

4.4 创建 SSL VPN 应用， SSL VPN 页面模板

4.4.1 创建 SSL VPN 应用

1. 请选择 **VPN** > **SSL VPN** > **SSL VPN Web 入口页面** > **应用**，进入**应用**页面。
2. 点击**新建**，添加新的应用。

3. 点击**确定**。

CLI

```
NetEye@root-system] sslvpn
NetEye@root-system-sslvpn] application Application1 type http url
www.test.com
NetEye@root-system-sslvpn] application Application2 type https url
202.118.1.100:4043
NetEye@root-system-sslvpn] end
NetEye@root> save config
```

4.4.2 创建 SSL VPN 页面模板

1. 请选择 **VPN** > **SSL VPN** > **SSL VPN Web 入口页面** > **页面模板**，进入**页面模板**页面。
2. 点击**新建**，创建一个新的页面模板。

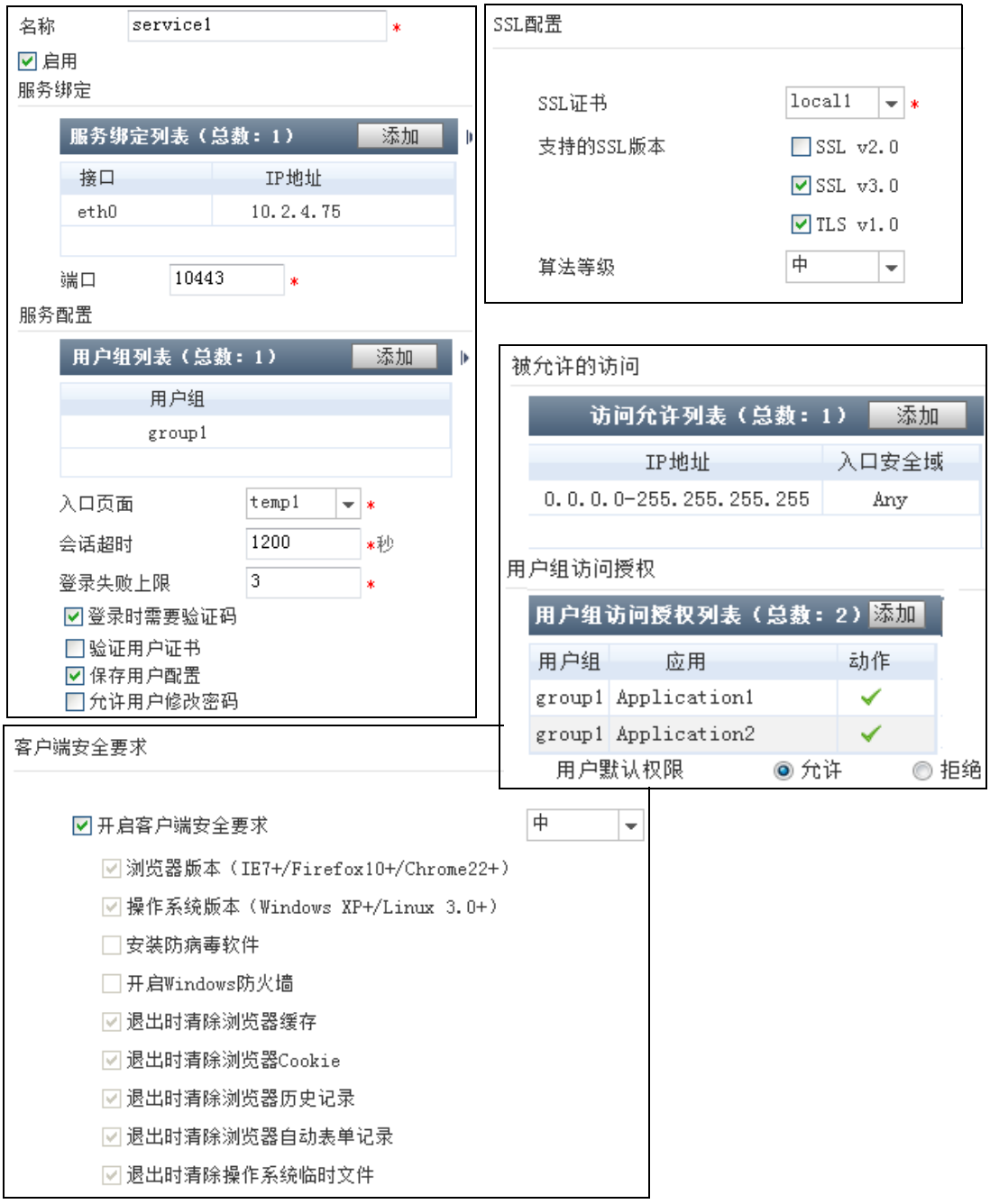
3. 点击**确定**。

CLI

```
NetEye@root-system] sslvpn
NetEye@root-system-sslvpn] portal-template temp1
NetEye@root-system-sslvpn] portal-template temp1 applist Application1
NetEye@root-system-sslvpn] portal-template temp1 applist Application2
NetEye@root-system-sslvpn] portal-template temp1 title Welcome
NetEye@root-system-sslvpn] portal-template temp1 language Chinese
NetEye@root-system-sslvpn] portal-template temp1 themecolor #FFCC99
NetEye@root-system-sslvpn] portal-template temp1 customapp HTTP enable
NetEye@root-system-sslvpn] portal-template temp1 customapp HTTPS
enable
NetEye@root-system-sslvpn] end
NetEye@root> save config
```

4.5 创建 SSL VPN 页面服务

1. 请选择 **VPN > SSL VPN > SSL VPN Web 入口页面 > 页面服务**，进入**页面服务**页面。
2. 点击**新建**，创建新的页面服务。



3. 点击**确定**。
4. 点击 。

CLI

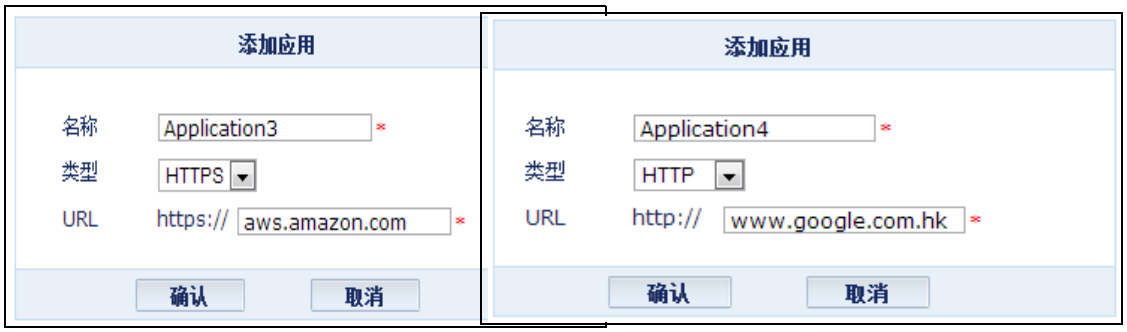
```
NetEye@root-system] sslvpn
NetEye@root-system-sslvpn] portal-service service1 interface eth0 ip
10.2.4.75 port 10443 portal temp1 certificate local group1
NetEye@root-system-sslvpn] portal-service service1 privilege group
group1 application Application1 permit
NetEye@root-system-sslvpn] portal-service service1 privilege group
group1 application Application2 permit
NetEye@root-system-sslvpn] portal-service service1 privilege default-
group-privilege permit
NetEye@root-system-sslvpn] portal-service service1 enable
NetEye@root-system-sslvpn] end
NetEye@root> save config
```

4.6 使用 SSL VPN 进行访问

1. 打开浏览器 , 输入 https://10.2.4.75:10443, 登录到 SSL VPN Web 入口页面。输入用户名 Alice, 密码 test12, 及验证码。

2. 点击应用对应的超链接，可对各应用进行访问。

3. 点击**添加**，添加新的应用。

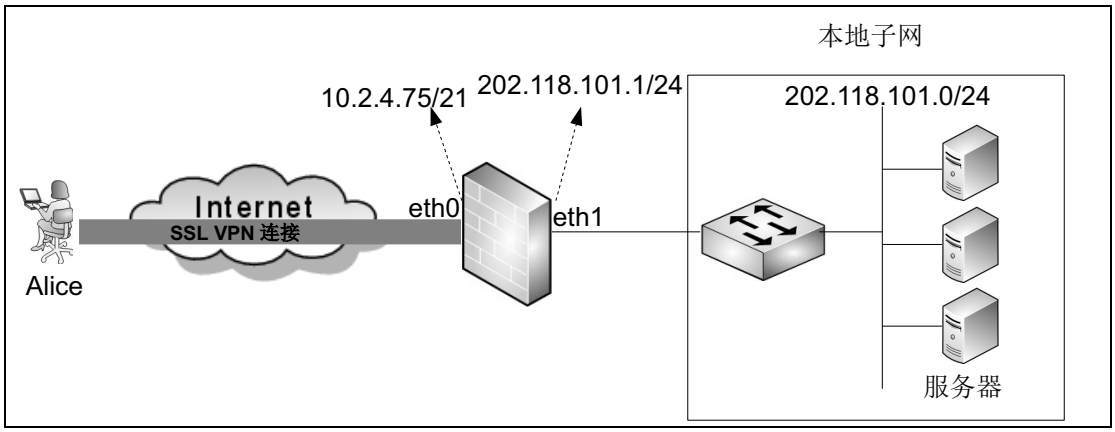


4. 可以查看 Web 入口页面的应用列表。自定义应用可以删除。

范例 5. 通过 SSL VPN 隧道访问

如图 51 所示，为远程用户 Alice 配置 SSL VPN 隧道来访问受保护的服务器资源。

图 51 SSL VPN 隧道访问



本范例包含如下配置步骤：

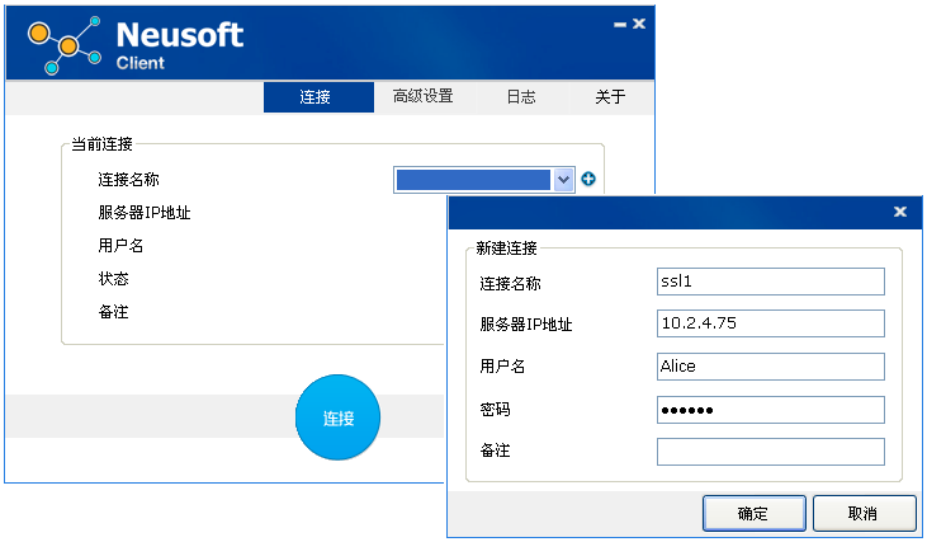
- 5.1 配置接口 IP 地址
- 5.2 安装 SSL VPN 客户端软件 / 添加 SSL VPN 连接
- 5.3 创建 IP 地址池 /VPN 用户 /VPN 用户组
- 5.4 创建 SSL VPN 隧道
- 5.5 连接到 SSL VPN 服务器
- 5.6 监控 SSL VPN 隧道信息

5.1 配置接口 IP 地址

该步骤与 SSL VPN Web 入口页面范例中的 4.1 配置接口 IP 地址相同。

5.2 安装 SSL VPN 客户端软件 / 添加 SSL VPN 连接

在客户端安装 SSL VPN 客户端软件。关于 SSL VPN 客户端软件具体的安装步骤，请参见*东软 NISG SSL VPN Android 客户端用户使用指南*和*东软 NISG SSL VPN Windows 客户端用户使用指南*。添加一条 SSL VPN 连接，配置如下：



5.3 创建 IP 地址池 /VPN 用户 /VPN 用户组

此步骤与 SSL VPN Web 入口页面范例中的 4.2 创建 IP 地址池， SSL VPN 用户， SSL VPN 用户组相同。

5.4 创建 SSL VPN 隧道

1. 请选择 **VPN** > **SSL VPN** > **SSL VPN 隧道** > **隧道**，进入**隧道**页面。
2. 点击**新建**，创建一条新的 SSL VPN 隧道。

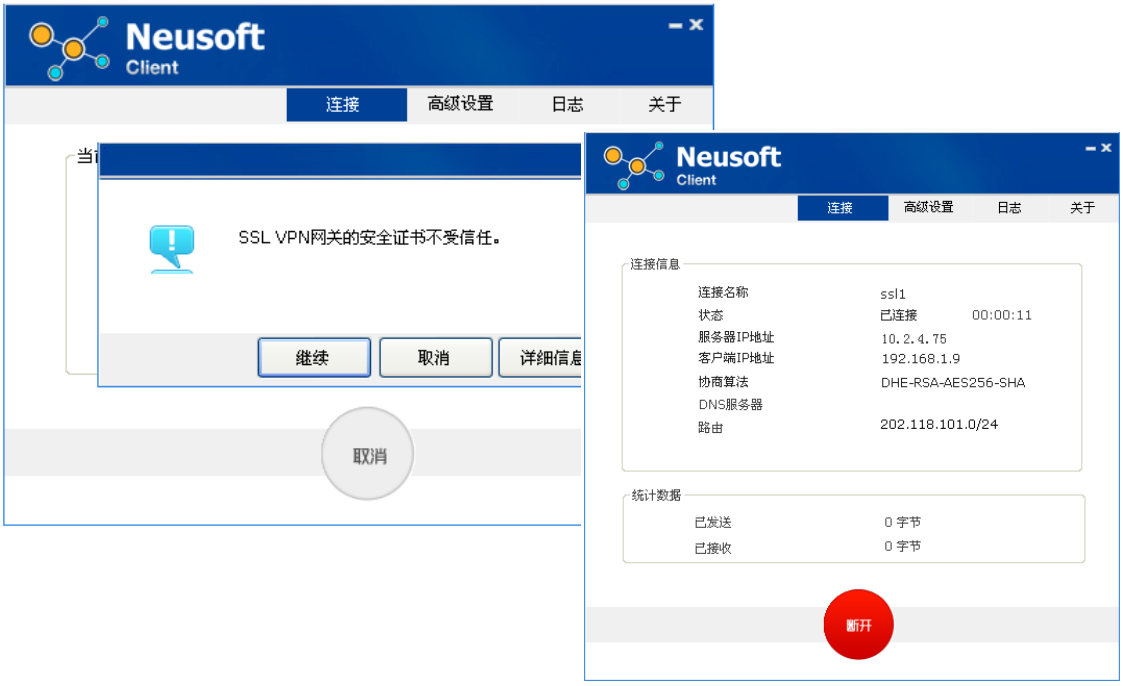
3. 点击**确定**。
4. 点击 。

CLI

```
NetEye@root-system] sslvpn
NetEye@root-system-sslvpn] tunnel tunnel1 interface eth0 10.2.4.75
group group1 allowed-subnet 202.118.101.0 255.255.255.0 enable
NetEye@root-system-sslvpn] end
NetEye@root> save config
```

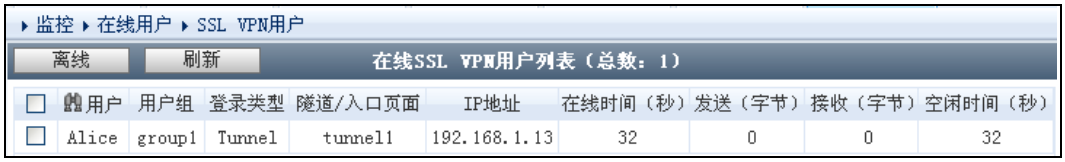
5.5 连接到 SSL VPN 服务器

点击**连接**和**继续**， Alice 会成功连接到 SSL VPN 服务器。



5.6 监控 SSL VPN 隧道信息

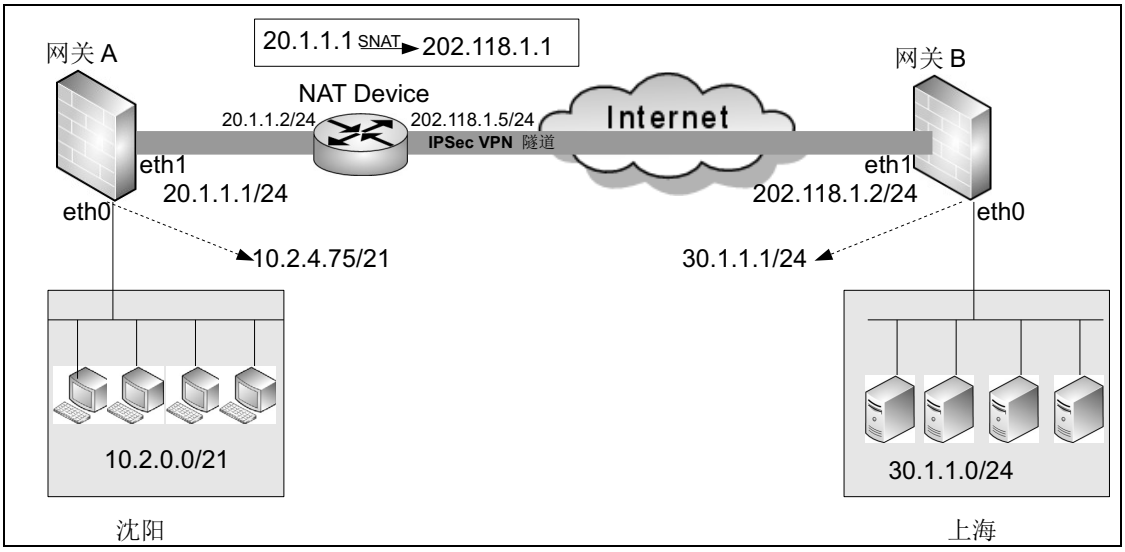
当 Alice 成功连接到 SSL VPN 服务器之后，可以选择**监控** > **在线用户** > **SSL VPN 用户**，查看 Alice 的在线信息。



范例 6. NAT 穿越 （IPSec VPN)

如图 52 所示，沈阳分公司需要远程访问上海总部的内网服务器资源。为了保证数据在互联网上安全传输，在沈阳分公司和上海总部之间建立了一条 IPSec VPN 隧道。另外，在沈阳分公司的出口上部署了一台 NAT 设备来隐藏沈阳分公司的 VPN 网关地址。

图 52 基于 SNAT 的 IPSec VPN



解决方案：

在 VPN 网关 A 的前端部署一台 NAT （SNAT) 设备，在 NISG 的 VPN 中启用 NAT 穿越。

该范例包含以下配置：

- 6.1 配置接口 IP 地址 / 缺省路由
- 6.2 创建自动密钥隧道
- 6.3 创建访问策略
- 6.4 监控 VPN 信息

提示：当存在 DNAT 或 MIP 策略的情况下， VPN 隧道两端的配置与 SNAT 环境下的配置相同。

6.1 配置接口 IP 地址 / 缺省路由

6.1.1 配置接口 IP 地址

网关 A:

1. 请选择**网络** > **接口**，对接口 eth0 和 eth1 进行配置：
   - eth0: 接口状态 = 开，模式 = 三层，MTU=1500，获取 IP 地址方式 = 静态 IP，IP 地址列表，主 =10.2.4.75/21。
   - eth1: 接口状态 = 开 , 模式 = 三层 , MTU=1500，获取 IP 地址方式 = 静态 IP，IP 地址列表，主 =20.1.1.1/24。
2. 点击**确定**。

网关 B:

1. 请选择**网络** > **接口**，对接口 eth0 和 eth1 进行配置：
   - eth0: 接口状态 = 开，模式 = 三层，MTU=1500，获取 IP 地址方式 = 静态 IP，IP 地址列表，主 =30.1.1.1/24。
   - eth1: 接口状态 = 开 , 模式 = 三层 , MTU=1500，获取 IP 地址方式 = 静态 IP，IP 地址列表，主 =202.118.1.2/24。
2. 点击**确定**。

CLI

网关 A:

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet 0
NetEye@root-system-if-eth0] working-type layer3-interface
NetEye@root-system-if-eth0] ip address 10.2.4.75 255.255.248.0
NetEye@root-system-if-eth0] exit
NetEye@root-system] interface ethernet 1
NetEye@root-system-if-eth1] working-type layer3-interface
NetEye@root-system-if-eth1] ip address 20.1.1.1 255.255.255.0
NetEye@root-system-if-eth1] end
NetEye@root> save config
```

网关 B:

除以下两条命令，其他命令与网关 A 的命令相同。

```
NetEye@root-system-if-eth0] ip address 30.1.1.1 255.255.255.0
NetEye@root-system-if-eth1] ip address 202.118.1.2 255.255.255.0
```

6.1.2 配置缺省路由

网关 A:

1. 请选择**网络** > **路由** > **缺省路由**，进入**缺省路由**页面添加一条缺省路由。

   类型 =IPv4 地址，目的 IPv4 地址 =0.0.0.0，掩码长度 =0， Metric=1,
   出口接口 / 网关 = 常规，接口 =eth1, 网关 =20.1.1.2。
2. 点击**确定**。

网关 B:

以同样的方法在 VPN 网关 B 上添加一条缺省路由：

IPv4 地址，目的 IPv4 地址 =0.0.0.0，掩码长度 =0， Metric=1, 出口接口 / 网关 = 常规，接口 =eth1, 网关 =202.118.1.5。

CLI

网关 A:

```
NetEye@root-system] route 0.0.0.0 0.0.0.0 interface eth1 gateway
20.1.1.2
NetEye@root-system] exit
NetEye@root> save config
```

网关 B:

```
NetEye@root-system] route 0.0.0.0 0.0.0.0 interface eth1 gateway
202.118.1.5
NetEye@root-system] exit
NetEye@root> save config
```

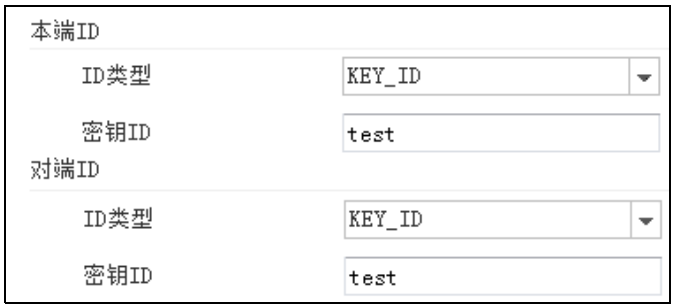
6.2 创建自动密钥隧道

网关 A：

1. 请选择**网络** > **IPSec VPN** > **自动密钥隧道**。点击**新建**创建一条隧道。

2. 设置本端和对端子网。本端子网 =10.2.0.0/21, 对端子网 =30.1.1.0/24。

3. 点击**高级设置**，配置本端和对端 ID。



4. 点击**确定**。

提示：当设置 ID 类型为 IPV4_ADDR 时，需要将本端密钥 ID 设置为 SNAT 转换后 IP，在本范例中为 202.118.1.1.

CLI

```
NetEye@root-system] vpn
NetEye@root-system-vpn] tunnel atb gateway 202.118.1.2 interface eth1
202.118.1.1 preshared-key 123 local-subnet 10.2.0.0 255.255.248.0
remote-subnet 30.1.1.0 255.255.255.0 enable
NetEye@root-system-vpn] tunnel atb ike local-id key-id test
NetEye@root-system-vpn] tunnel atb ike peer-id key-id test
NetEye@root-system-vpn] end
NetEye@root> save config
```

VPN 网关 B：

方案 A：设置对端类型为**静态 IP 地址**，该 IP 地址为 SNAT 转换后 IP。

1. 请选择 **VPN** > **IPSec VPN** > **自动密钥隧道**，创建一条新的隧道。

2. 设置本端和对端子网。本端子网 =30.1.1.0/24, 对端子网 =10.2.0.0/21。

3. **高级配置**区域：本端 ID 类型 =IKE_ID=test, 对端 ID 类型 =IKE_ID=test。
4. 点击**确定**。

CLI

```
NetEye@root-system] vpn
NetEye@root-system-vpn] tunnel bta gateway 202.118.1.1 interface eth1
202.118.1.2 preshared-key 123 local-subnet 30.1.1.0 255.255.255.0
remote-subnet 10.2.0.0 255.255.248.0 enable
NetEye@root-system-vpn] tunnel bta ike local-id key-id test
NetEye@root-system-vpn] tunnel bta ike peer-id key-id test
NetEye@root-system-vpn] end
NetEye@root> save config
```

方案 B：设置对端类型为**动态 IP 地址**。

名称 =bta, 启用 = 勾选，启用 NAT 穿越 Keepalive 间隔 =20 秒，

对端 IP 地址 / 域名 = 动态 IP 地址，出口 =eth1, 本端 IP 地址 =202.118.1.2，认证方式 = 预共享密钥，密钥 =test12, 本端子网 =30.1.1.0/24, 对端子网 =10.2.0.0/21。

提示：当设置对端类型为动态 IP 时，不需要进入 VPN 网关 A 和网关 B 的自动密钥隧道的**高级配置**区域，设置本端和对端 ID。

CLI

```
NetEye@root-system] vpn
NetEye@root-system-vpn] tunnel bta gateway any interface eth1
202.118.1.2 preshared-key test12 local-subnet 30.1.1.0 255.255.255.0
remote-subnet 10.2.0.0 255.255.248.0 enable
NetEye@root-system-vpn] end
NetEye@root> save config
```

6.3 创建访问策略

网关 A:

1. 请选择**防火墙** > **访问策略**，创建一条新的访问策略。

2. 其他参数使用默认配置。点击**确定**。
3. 点击 。

网关 B:

请选择**防火墙** > **缺省策略配置**，配置域间缺省策略的动作为**允许**。

CLI

网关 A:

```
NetEye@root-system] policy access policy1 any 10.2.4.1-10.2.4.100 any
any any any permit enable 1
NetEye@root-system] policy access policy1 tunnel atb
NetEye@root-system] exit
NetEye@root> save config
```

网关 B:

```
NetEye@root-system] policy default inter-zone access permit
NetEye@root-system] exit
NetEye@root> save config
```

提示：除访问策略外，还可以通过路由将匹配的数据包引入 VPN 隧道。有关 IPSec VPN 中路由引用隧道的详细信息，请参见 1.3 引用隧道。

6.4 监控 VPN 信息

请选择**监控** > **IPSec VPN 隧道** > **自动密钥隧道**，查看**自动密钥隧道**信息。

网关 A/B:

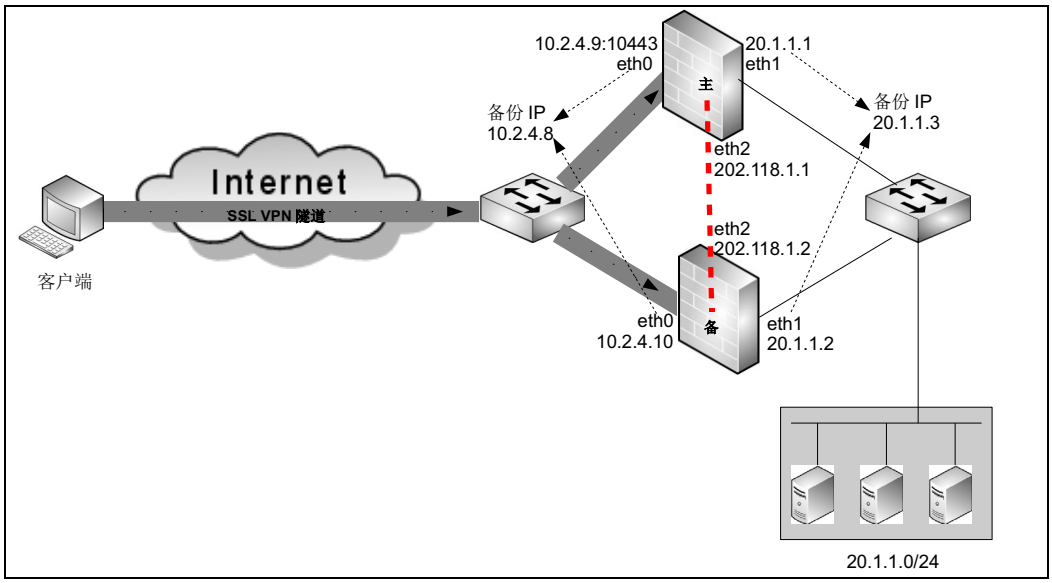
基本信息	
名称	atb
对端类型	静态IP地址
对端信息	202.118.1.2
拨号IP地址	202.118.1.2
出口	eth1
本端IP地址	20.1.1.1
认证模式	预共享密钥

基本信息	
名称	bta
对端类型	静态IP地址
对端信息	202.118.1.1
拨号IP地址	202.118.1.1
出口	eth1
本端IP地址	202.118.1.2
认证模式	预共享密钥

范例 7. HA 自动同步 （SSL VPN)

该范例描述了如何在隧道型 SSL VPN 环境中应用高可用性。如图 53 所示，主设备使用 IP 地址 10.2.4.8:10443 提供 SSL VPN 隧道服务 , 当发生故障时，备份设备会接管它的工作。

图 53 隧道型 SSL VPN 环境下的高可用性



该范例包含如下配置：

- 主备设备的配置：
  - 7.1 配置接口 IP 地址
  - 7.2 配置虚拟路由器探测组
  - 7.3 配置虚拟路由器
  - 7.4 配置集群
- 主设备的配置：
  - 7.5 创建 IP 地址池
  - 7.6 创建 SSL VPN 用户
  - 7.7 创建 SSL VPN 用户组
  - 7.8 创建 SSL VPN 隧道

  这些配置会自动同步到备份设备中。
- 客户端配置：
  - 7.9 安装 SSL VPN 客户端
  - 7.10 创建客户端连接
  - 7.11 连接到 SSL VPN 服务器

7.1 配置接口 IP 地址

主设备：

1. 请选择**网络** > **接口**，对 eth0、 eth1 和 eth2 进行编辑。

- eth0: 接口状态 = 开，模式 = 三层， MTU=1500，获取 IP 地址方式 = 静态 IP （主）=10.2.4.9/21。
- eth1: 接口状态 = 开，模式 = 三层， MTU=1500，获取 IP 地址方式 = 静态 IP （主）=20.1.1.1/24。
- eth2: 接口状态 = 开，模式 = 二层。

2. 点击**确定**。

提示：以太网接口 eth2 作为二层接口，其 IP 地址只能在集群中设置。有关设置 eth2 的 IP 地址的详细信息，请参见 7.4 配置集群。

备份设备：

1. 请选择**网络** > **接口**，对 eth0、 eth1 和 eth2 进行编辑。

- eth0: 接口状态 = 开，模式 = 三层， MTU=1500，获取 IP 地址方式 = 静态 IP （主）=10.2.4.10/21。
- eth1: 接口状态 = 开，模式 = 三层， MTU=1500，获取 IP 地址方式 = 静态 IP （主）=20.1.1.2/24。
- eth2: 接口状态 = 开，模式 = 二层。

CLI

主设备：

```
NetEye@root-system] interface ethernet eth0
NetEye@root-system-if-eth0] ip address 10.2.4.9 255.255.248.0
NetEye@root-system-if-eth0] exit
NetEye@root-system] interface ethernet eth1
NetEye@root-system-if-eth1] working-type layer3-interface
NetEye@root-system-if-eth1] ip address 20.1.1.1 255.255.255.0
```

```
NetEye@root-system-if-eth1] exit
NetEye@root-system] interface ethernet eth2
NetEye@root-system-if-eth2] working-type layer2-interface
NetEye@root-system-if-eth2] end
NetEye@root> save config
```

备份设备：

```
NetEye@root-system] interface ethernet eth0
NetEye@root-system-if-eth0] ip address 10.2.4.10 255.255.248.0
NetEye@root-system-if-eth0] exit
NetEye@root-system] interface ethernet eth1
NetEye@root-system-if-eth1] working-type layer3-interface
NetEye@root-system-if-eth1] ip address 20.1.1.2 255.255.255.0
NetEye@root-system-if-eth1] exit
NetEye@root-system] interface ethernet eth2
NetEye@root-system-if-eth2] working-type layer2-interface
NetEye@root-system-if-eth2] end
NetEye@root> save config
```

7.2 配置虚拟路由器探测组

主设备：

1. 请选择**系统** > **高可用性** > **虚拟路由器探测组**。
2. 点击**新建**，进行如下配置：

3. 点击**确定**。

备份设备：

执行相同的步骤在备份设备上创建一个虚拟路由器探测组。

CLI

主设备：

```
NetEye@root-system] detection group 1
NetEye@root-system-dg1] priority 120
NetEye@root-system-dg1] interval 1
NetEye@root-system-dg1] ip-track type ping interface any ip 20.1.1.4 interval 3 threshold 3 weight 30
NetEye@root-system-dg1] end
NetEye@root> save config
```

备份设备：

```
NetEye@root-system] detection group 1
NetEye@root-system-dg1] priority 100
NetEye@root-system-dg1] interval 1
NetEye@root-system-dg1] ip-track type ping interface any ip 20.1.1.4 interval 3 threshold 3 weight 30
NetEye@root-system-dg1] end
NetEye@root> save config
```

7.3 配置虚拟路由器

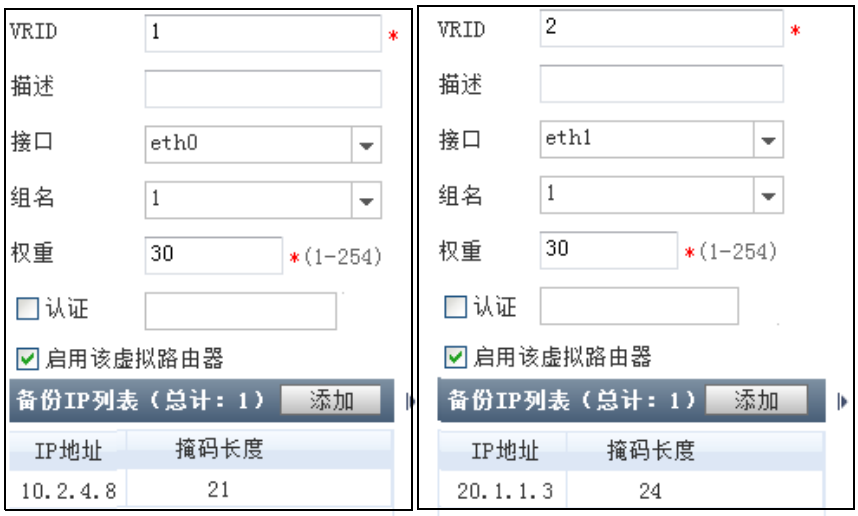
主设备：

1. 请选择**系统** > **高可用性** > **虚拟路由器**，创建ID号分别为1和2的虚拟路由器并分配到7.2 配置虚拟路由器探测组创建的虚拟路由器探测组中。
2. 点击**新建**，进行如下配置：

3. 点击**确定**。
4. 点击 。

备份设备：

1. 请选择**系统** > **高可用性** > **虚拟路由器**，创建ID号分别为1和2的虚拟路由器并分配到7.2 配置虚拟路由器探测组创建的虚拟路由器探测组中。
2. 点击**新建**，进行如下配置：



3. 点击**确定**。
4. 点击 。

CLI

主设备：

```
NetEye@root-system] virtual router 1
NetEye@root-system-vr1] election interface eth0
NetEye@root-system-vr1] backup ip address 10.2.4.8 mask 255.255.248.0
NetEye@root-system-vr1] virtual-router enable
NetEye@root-system-vr1] exit
NetEye@root-system] virtual router 2
NetEye@root-system-vr2] election interface eth1
NetEye@root-system-vr2] backup ip address 20.1.1.3 mask 255.255.255.0
NetEye@root-system-vr2] virtual-router enable
NetEye@root-system-vr2] exit
NetEye@root-system] detection group 1
NetEye@root-system-dg1] hold virtual-router 1 weight 30
NetEye@root-system-dg1] hold virtual-router 2 weight 30
NetEye@root-system-dg1] end
NetEye@root> save config
```

备份设备：

备份设备的CLI配置与主设备相同。

7.4 配置集群

当在主备两台设备分别配置集群并且启用自动同步功能之后，两台设备上的配置信息和运行信息都会自动同步到对端。

请选择**系统** > **高可用性** > **集群** , 进入集群页面进行配置。

主设备：

CLI

```
NetEye@root-system] cluster
NetEye@root-system-cluster] clusterid 1
NetEye@root-system-cluster] local interface eth2
NetEye@root-system-cluster] local ip address 202.118.1.1 mask
255.255.255.0
NetEye@root-system-cluster] peer ip address 202.118.101.2
NetEye@root-system-cluster] rti sync enable
NetEye@root-system-cluster] time syn enable
NetEye@root-system-cluster] time boot on
NetEye@root-system-cluster] config sync auto enable
NetEye@root-system-cluster] end
NetEye@root> save config
```

备份设备：

CLI

```
NetEye@root-system] cluster
NetEye@root-system-cluster] clusterid 1
NetEye@root-system-cluster] local interface eth2
NetEye@root-system-cluster] local ip address 202.118.1.2 mask
255.255.255.0
NetEye@root-system-cluster] peer ip address 202.118.101.1
NetEye@root-system-cluster] rti sync enable
NetEye@root-system-cluster] time syn enable
NetEye@root-system-cluster] time boot on
NetEye@root-system-cluster] config sync auto enable
NetEye@root-system-cluster] end
NetEye@root> save config
```

7.5 创建 IP 地址池

主设备：

1. 请选择 **VPN** > **IP 地址池**，进入 **IP 地址池**页面。
2. 点击**新建**，为远程用户进行 SSL VPN 连接创建一个新的地址池。

3. 点击**确定**。

CLI

```
NetEye@root-system] ippool ippool1 30.1.1.1-30.1.1.100
NetEye@root-system] exit
NetEye@root> save config
```

提示：1. 在集群中配置自动同步后，主设备中 IP 地址池的配置会自动同步到备份设备中。
2. IP 地址池包含的 IP 不能与 SSL VPN 服务器后的子网 IP 重合。

7.6 创建 SSL VPN 用户

主设备：

1. 请选择**系统** > **认证** > **网络用户**，进入**网络用户**页面。
2. 点击**新建**，创建一个新的 SSL VPN 用户。

3. 点击**确定**。

CLI

```
NetEye@root-system] user authuser Bob authtype local password 123456 enable
NetEye@root-system] user authuser Bob sslvpn multipoint enable
NetEye@root-system] user authuser Bob assigned-ip ippool1 dns1 10.1.3.121 wins1 10.1.3.119
NetEye@root-system] exit
NetEye@root> save config
```

提示：1. 由于 Windows 虚拟网卡驱动的限制，当 SSL VPN 用户需要通过 SSL VPN 隧道访问内网资源时，为其分配的 IP 地址（无论是静态 IP 地址或 IP 地址池）必须符合掩码 255.255.255.252。另外，为 SSL VPN 用户分配的 IP 地址不能是 VPN 网关后子网的 IP 地址。
2. 在集群中配置自动同步后，主设备中 SSL VPN 用户的配置会自动同步到备份设备中。

7.7 创建 SSL VPN 用户组

主设备：

1. 请选择 **VPN** > **SSL VPN** > **用户组**，进入**用户组**页面。
2. 点击**新建**，进行如下配置：

3. 点击**确定**。

CLI

```
NetEye@root-system] ssl vpn
NetEye@root-system-sslvpn] group group1
NetEye@root-system-sslvpn] group group1 user Bob
NetEye@root-system-sslvpn] end
NetEye@root> save config
```

提示：在集群中配置自动同步后，主设备中 SSL VPN 用户组的配置会自动同步到备份设备中。

7.8 创建 SSL VPN 隧道

主设备：

1. 请选择 **VPN** > **SSL VPN** > **SSL VPN 隧道** > **隧道**，进入**隧道**页面。
2. 点击**新建**，创建一条新的隧道。

3. 点击**确定**。
4. 点击 。

提示：1. 本地 IP 地址可以设置为 Any. 这种情况下，如果本地已存在到对端的 session，按照正常的转发流程匹配现有的 session 来选择协商 IP；否则，则优先使用浮动 IP 进行协商。
2. 在集群中配置自动同步后，主设备中 SSL VPN 隧道的配置会自动同步到备份设备中。

CLI

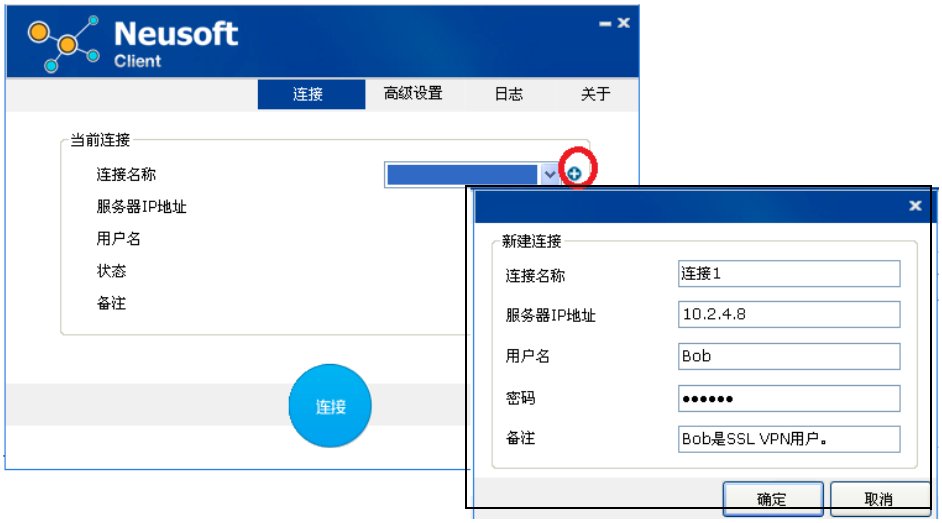
```
NetEye@root-system] sslvpn
NetEye@root-system-sslvpn] tunnel ssltunnel1 interface eth0 10.2.4.8
enable
NetEye@root-system-sslvpn] tunnel ssltunnel1 group group1
NetEye@root-system-sslvpn] tunnel ssltunnel1 allowed-subnet 20.1.1.0
NetEye@root-system-sslvpn] tunnel ssltunnel1 allowed-subnet 20.1.1.0
255.255.255.0
NetEye@root-system-sslvpn] end
NetEye@root> save config
```

7.9 安装 SSL VPN 客户端

在客户端安装 SSL VPN 客户端软件。有关 SSL VPN 客户端软件使用的详细信息，请参见*东软 NISG SSL VPN Windows 客户端用户使用指南*和*东软 NISG SSL VPN Android 客户端用户使用指南*。

7.10 创建客户端连接

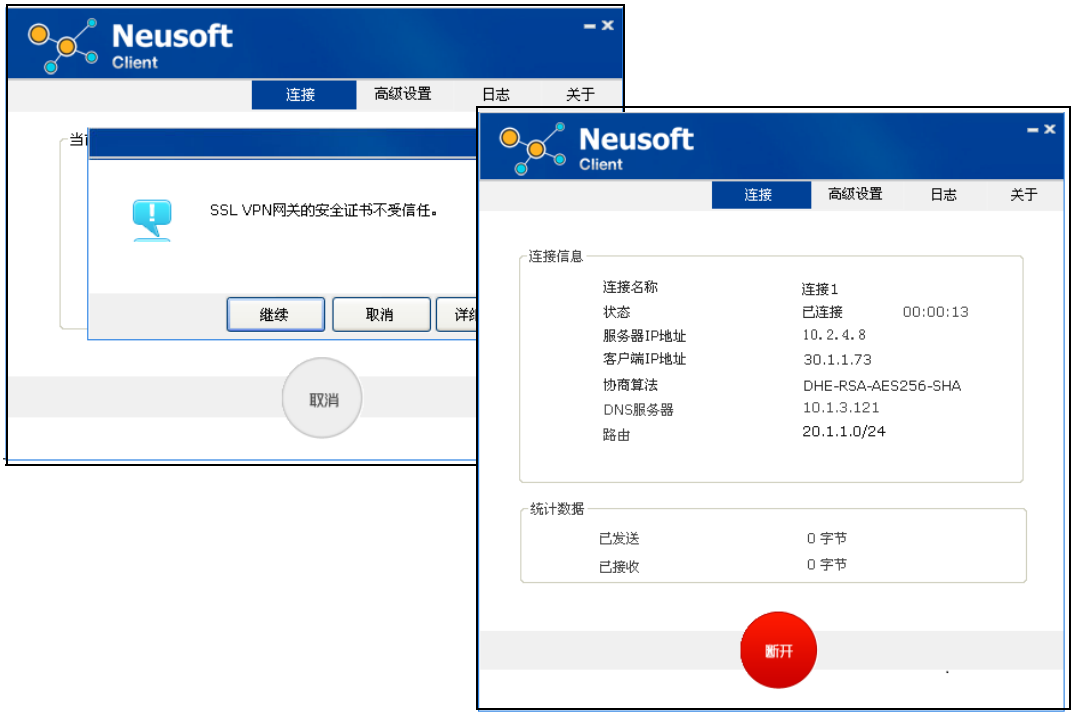
1. 添加一条 SSL VPN 连接，进行如下配置：



2. 点击**高级设置**选项卡，勾选**自动重连**复选框，保证当发生故障切换时， SSL VPN 可以立即重新连接。

7.11 连接到 SSL VPN 服务器

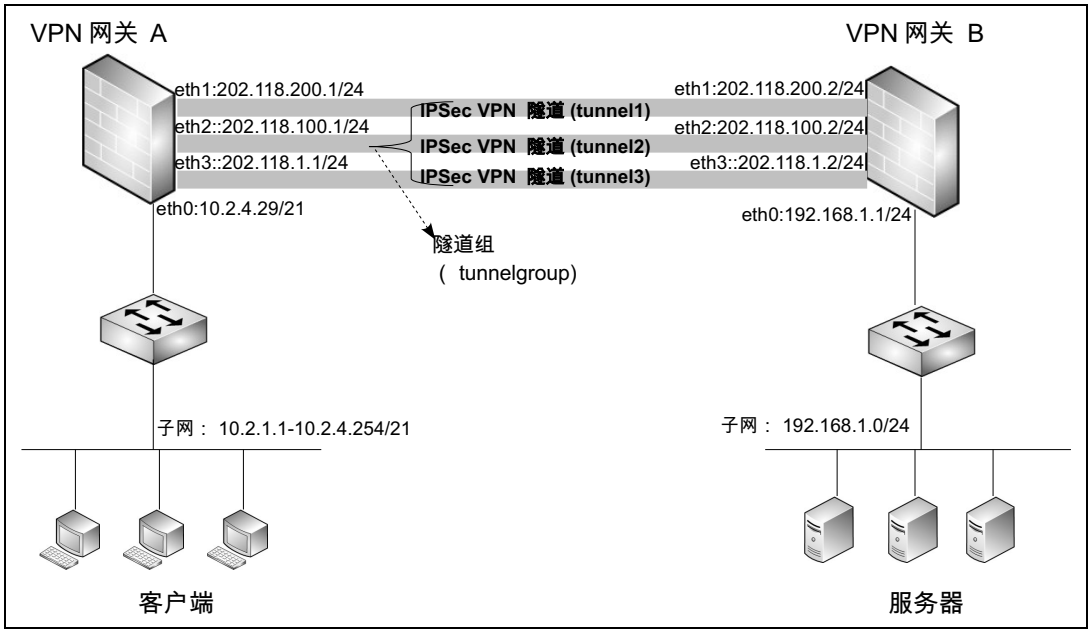
点击**连接**和**继续**。 SSL VPN 用户 Bob 可以成功连接到 SSL VPN 服务器，从而对内网资源进行访问。当主设备发生故障时，备份设备会立即接替其工作，从而使 Bob 的访问不受任何影响。



范例 8. IPSec VPN 隧道组

如图图 54 所示，为了防止正在工作的隧道断开而影响 VPN 网关 A 和 B 之间的通信，需要建立包含多条隧道的隧道组，当正在工作的隧道断开时，则选择当前优先级最高的可用隧道作为通信的隧道。

图 54 IPSec VPN 隧道组



该范例的配置步骤如下：

8.1 配置接口 IP 地址 / 缺省策略

8.2 创建自动密钥隧道

8.3 创建自动密钥隧道组

8.4 创建静态路由引用隧道组

8.5 监控信息

8.1 配置接口 IP 地址 / 缺省策略

有关配置接口 IP 地址、缺省策略的详细信息，请参见范例 2 中的 2.1 配置接口 IP 地址 / 缺省路由 / 访问策略。

8.2 创建自动密钥隧道

1. 请选择 **VPN > IPSec VPN > 自动密钥隧道**，点击**新建**创建一条自动密钥隧道。

CLI

VPN Gateway A:

```
NetEye@root-system] vpn
NetEye@root-system-vpn] tunnel tunnel1 gateway 202.118.200.2 interface
eth1 202.118.200.1 preshared-key 123456 enable
```

VPN Gateway B:

```
NetEye@root-system] vpn
NetEye@root-system-vpn] tunnel tunnel1 gateway 202.118.200.1 interface
eth1 202.118.200.2 preshared-key 123456 enable
```

2. 以同样的方式创建自动密钥隧道tunnel2和tunnel3。创建完成后，VPN网关A和B的自动密钥隧道列表显示如下：

VPN 网关 A:

新建 删除 启用 禁用 **自动密钥隧道列表（总数：3）**

	名称	VPN类型	对端类型	对端	出口	本端IP地址	认证方式	引用	启用
☐	tunnel1	网关到网关	静态IP地址	202.118.200.2	eth1	202.118.200.1	预共享密钥		✓
☐	tunnel2	网关到网关	静态IP地址	202.118.100.2	eth2	202.118.100.1	预共享密钥		✓
☐	tunnel3	网关到网关	静态IP地址	202.118.1.2	eth3	202.118.1.1	预共享密钥		✓

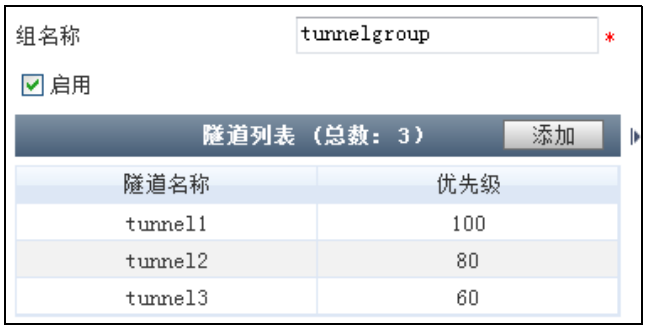
VPN 网关 B:

	名称	VPN类型	对端类型	对端	出口	本端IP地址	认证方式	引用	启用
☐	tunnel1	网关到网关	静态IP地址	202.118.200.1	eth1	202.118.200.2	预共享密钥		✓
☐	tunnel2	网关到网关	静态IP地址	202.118.100.1	eth2	202.118.100.2	预共享密钥		✓
☐	tunnel3	网关到网关	静态IP地址	202.118.1.1	eth3	202.118.1.2	预共享密钥		✓

8.3 创建自动密钥隧道组

请选择 **VPN** > **IPSec VPN** > **隧道组**，点击**新建**，创建一个新的隧道组将隧道 tunnel1、tunnel2、 tunnel3 包含进来。

VPN 网关 A/B:



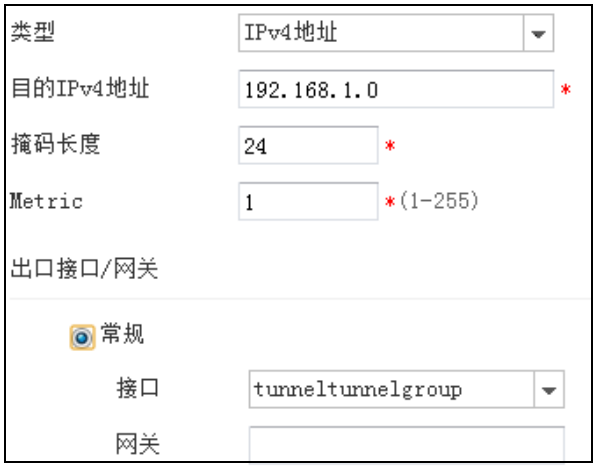
隧道名称	优先级
tunnel1	100
tunnel2	80
tunnel3	60

CLI

```
NetEye@root-system] vpn
NetEye@root-system-vpn] tunnelgroup tunnelgroup tunnel tunnel1
priority 100
NetEye@root-system-vpn] tunnelgroup tunnelgroup tunne2 tunnel1
priority 80
NetEye@root-system-vpn] tunnelgroup tunnelgroup tunne3 tunnel1
priority 60
NetEye@root-system-vpn] tunnelgroup tunnelgroup enable
```

8.4 创建静态路由引用隧道组

请选择**网络** > **路由** > **缺省路由**，点击**新建**，添加一条静态路由，将此路由的出口接口指定为隧道组接口。



CLI

```
NetEye@root-system] route 192.168.1.0 255.255.255.0 interface
tunneltunnelgroup
```

提示：隧道组创建时自动创建隧道组接口 tunneltunnelgroup。

8.5 监控信息

- 请选择**监控** > **IPSec VPN 隧道** > **自动密钥隧道**查看隧道的监控信息。

VPN 网关 A：

隧道类型 全部 自动密钥隧道列表（总数：3）

名称	状态	对端类型	对端	隧道添加时间	接收数据包数	发送数据包数	
tunnel1	开启	静态IP地址	202.118.200.2	2014-03-28 23:38:39	51	59	
tunnel2	开启	静态IP地址	202.118.100.2	2014-03-28 23:39:26	0	0	
tunnel3	开启	静态IP地址	202.118.1.2	2014-03-28 23:40:25	0	0	

VPN 网关 B：

监控 ▸ IPSec VPN隧道 ▸ 自动密钥隧道

隧道类型 全部 自动密钥隧道列表（总数：3）

名称	状态	对端类型	对端	隧道添加时间	接收数据包数	发送数据包数	
tunnel1	开启	静态IP地址	202.118.200.1	2014-03-29 00:39:49	1987	6396	
tunnel2	开启	静态IP地址	202.118.100.1	2014-03-29 00:40:35	0	0	
tunnel3	开启	静态IP地址	202.118.1.1	2014-03-29 00:41:13	0	0	

- 当 tunnel1 发生故障时， NISG 会根据优先级选择 tunnel2 来接替 tunnel1 继续工作。

VPN 网关 A:

隧道类型 全部 自动密钥隧道列表（总数：2）

名称	状态	对端类型	对端	隧道添加时间	接收数据包数	发送数据包数	
tunnel2	开启	静态IP地址	202.118.100.2	2014-03-28 23:39:26	6528	2165	
tunnel3	开启	静态IP地址	202.118.1.2	2014-03-28 23:40:25	0	0	

VPN 网关 B：

隧道类型 全部 自动密钥隧道列表（总数：2）

名称	状态	对端类型	对端	隧道添加时间	接收数据包数	发送数据包数	
tunnel2	开启	静态IP地址	202.118.100.1	2014-03-29 00:40:35	2148	6499	
tunnel3	开启	静态IP地址	202.118.1.1	2014-03-29 00:41:13	0	0	

11.4 配置参数说明

本节介绍了 IPSec VPN 和 SSL VPN 的相关参数。

- 11.4.1 IPSec VPN 相关参数
- 11.4.2 SSL VPN 相关参数
- 11.4.3 IP 地址池相关参数

11.4.1 IPSec VPN 相关参数

在 IPSec VPN 隧道的配置过程中，会涉及到如下参数配置：

- 11.4.1.1 IPSec VPN 用户组参数
- 11.4.1.2 自动密钥隧道参数
- 11.4.1.3 手动隧道参数
- 11.4.1.4 隧道组参数
- 11.4.1.5 常规设置

11.4.1.1 IPSec VPN 用户组参数

表 249 IPSec VPN 用户组参数

配置信息	说明
组名称	IPSec VPN 用户组名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #
包含的用户	组内包含的在 NISG 上创建的 IPSec VPN 用户。
引用隧道	与 IPSec VPN 用户组关联的隧道。
包括外部用户	表示该用户组是否包含外部 Xauth 或 L2TP 用户。

11.4.1.2 自动密钥隧道参数

表 250 自动密钥隧道参数

参数	描述
名称	IPSec VPN 隧道名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & # 不能与现有的手动 IPSec VPN 隧道，隧道组，和 SSL VPN 隧道重名。
启用	该 IPSec VPN 隧道是否处于启用状态。
启用 NAT 穿越	启用 NAT 穿越功能。在 Keepalive 间隔文本框中输入发送 NAT Keepalive 数据报文的时间间隔。取值范围为 1-3600 的整数，单位为秒，缺省为 20 秒。
对端类型	IPSec VPN 隧道对端类型，包含静态 IP 地址、动态 IP 地址、拨号用户和拨号用户组。 • 静态 IP 地址 — 对端的 IP 地址或域名 • 动态 IP 地址 — 表示对端使用非固定 IP 地址 • 拨号用户 — 对端的拨号用户名 • 拨号用户组 — 对端的拨号用户组名称
永久隧道	当对端类型为静态 IP 地址时，可以将隧道设置为永久隧道，在被启用后立即主动发起协商，直到协商成功为止。而非永久隧道仅当有流量经过隧道时才发起协商。
出口信息	在该区域可以选择设置出口接口和本地 IP 地址。 • 出口：IPSec VPN 隧道协商口。 • 本地 IP 地址：IPsec VPN 隧道协商口的 IP 地址。 IP 选择 any 时，表示包括该接口上的所有 IP 地址。
认证方式	在 IKE 交换过程中对对端进行身份认证时采用的认证方式，包括预共享密钥认证方式和证书认证方式。
密钥	使用预共享密钥作为认证方式时，用于识别隧道双方身份的密钥。长度 1-127 字节， UTF-8 字符。不能包含？和空格。
本地证书 /CA 证书	使用证书作为认证方式时，本地保存的所有本地证书和 CA 证书。 CA 证书选择 any 时，表示包括 NISG 上的所有 CA 证书。
本地子网	受保护的本端子网。不支持多播地址 224.0.0.0-255.255.255.255，不能以 0 开头，最多支持 32 个本地子网。
对端子网	受保护的对端子网。不支持多播地址 224.0.0.0-255.255.255.255，不能以 0 开头，最多支持 32 个本地子网。

表 250 自动密钥隧道参数 (*续*)

参数	描述
高级设置	
在阶段 1 中，通讯双方协商一条 IKE 隧道。	
自定义提议集	IKE 交换第一阶段使用的提议集包括： • g1-3des-md5, g1-3des-sha1, g1-aes128-md5, g1-aes128-sha1 • g2-3des-sha1, g2-3des-md5, g2-aes128-sha1, g2-aes128-md5, g2-aes192-md5, g2-aes192-sha1, g2-aes256-md5, g2-aes256-sha1 • g5-3des-md5, g5-3des-sha1, g5-aes256-md5, g5-aes256-sha1. 可以选择一到四个提议集。默认的提议集为：g2-3des-sha1、g2-3des-md5、g2-aes128-sha1 和 g2-aes128-md5。 每个提议集都提示了在阶段 1 中使用的算法，例如提议集 g1-aes128-md5： • g1— 使用 DH 组 1 用于密钥交换 • 3des— 使用的加密算法 • md5— 使用的 Hash 函数
模式	指定 IPSec VPN 隧道使用的隧道模式，包括主模式和激进模式。默认使用的交换模式是主模式。
生存时间	第一阶段协商生成的 IKE SA 的生存时间，超过设置的时间后，将重新生成 IKE SA。输入范围为 180-2147483647，默认为 86400，单位为秒。
在阶段 2 中，通讯双方协商 IPSec SA。	
自定义提议集	IKE 交换第二阶段使用的提议集包括： • nopfs-esp-3des-md5, nopfs-esp-3des-sha1, nopfs-esp-aes128-md5, nopfs-esp-aes128-sha1 • g1-esp-3des-sha1, g1-esp-aes128-md5 • g5-esp-3des-md5, g5-esp-3des-sha1, g5-esp-aes128-md5, g5-esp-aes128-sha1 • g2-ah-md5, g2-ah-sha1 • g2-esp-aes128-md5, g2-esp-aes128-sha1, g2-esp-3des-md5, g2-esp-3des-sha1, g2-esp-aes192-md5, g2-esp-aes192-sha1, g2-esp-aes256-md5, g2-esp-aes256-sha1 • g2-ah-md5-esp-3des, g2-ah-md5-esp-3des, g2-ah-sha1-esp-3des, g2-ah-md5-esp-aes128, g2-ah-sha1-esp-aes128 第二阶段的默认提议集为 g2-esp-aes128-md5，g2-esp-aes128-sha1，g2-esp-3des-md5， g2-esp-3des-sha1 。表示默认情况下是启用 PFS 并且使用 DH 组 2 的。四个自定义提议集必须类型相同，如果第一个自定义提议集以 g2 开头，则其他三个也必须以 g2 开头；如果第一个以 nopfs 开头，其他三个也必须以 nopfs 开头。 每个提议集都提示了在阶段 2 中使用的算法，例如 nopfs-esp-3des-md5： • nopfs— 未启用完美向前保护 • esp— 使用的封装协议 • 3des— 使用的加密算法 • md5— 使用的 Hash 函数
抗重放攻击	重放攻击防护，默认为启用。
模式	指定 IPSec VPN 隧道使用的隧道模式，包括传输模式和隧道模式。默认使用隧道模式。

表 250 自动密钥隧道参数 (*续*)

参数	描述
生存时间	第二阶段协商生成的 IPSec SA 的生存时间，超过生存时间后，将会重新生成 IPSec SA。输入范围为 180-2147483647，默认为 28800，单位为秒。
DPD	即隧道两端的 IPSec VPN 网关通过发送 keepalive 报文来探测对端的状态。 • DPD 发送周期输入范围为 1-3600 秒。 • DPD 重试次数输入范围为 2-32767。
本端标识	配置在 IKE 协商过程中对本端身份进行认证的认证标识。 在标识类型下拉框中选取一个选项作为本端的标识类型，包括：IPV4_ADDR、FQDN、 USER_FQDN、 DER_ASN1_DN 和 KEY_ID 五种类型。选取不同的类型，本端标识的输入格式会发生相应的变化，以下列出了五种类型本端标识的输入格式。 • IPV4_ADDR：在标识文本框内输入 IP 地址作为本端标识。 • FQDN：在标识文本框内输入完全合格域名作为本端标识。 • USER_FQDN：在标识文本框内输入邮件地址作为本端标识。 • DER_ASN1_DN：在标识文本框内输入固定的格式 （例如 C=country,ST=state,L=city,O=company,OU=department,CN=user, emailAddress=mail）或者勾选高级复选框，输入相关参数，其中国家代码使用 2 个字母表示，省份、城市、公司、部门和公共名长度 1-127 字节， UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & • KEY_ID：在密钥标识文本框内输入字符串作为本端标识，长度 1-1023 字节，UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & 使用证书认证时，标识类型只能选择 DER_ASN1_DN。
对端标识	配置在 IKE 协商过程中对对端身份进行认证的认证标识。 输入要求和本端标识相同。
VPN 类型	指示对端类型，包括网关到网关和拨号用户。
引用	指示该隧道是否被策略引用。
启用 / 禁用	用于启用或禁用 IPSecVPN 隧道。

11.4.1.3 手动隧道参数

表 251 手动密钥隧道配置信息

参数	描述
名称	IPSec VPN 隧道名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：?, " ' \ < > & #
	不能与现有的自动 IPSec VPN 隧道，隧道组，和 SSL VPN 隧道重名。
启用	设定所创建的隧道的状态。
模式	IPSec VPN 隧道的模式，包括隧道模式和传输模式。默认为隧道模式。
本端 IP 地址	创建 IPSec VPN 隧道时，本端 NISG 设备所使用接口的 IP 地址。不支持多播地址 224.0.0.0-255.255.255.255，不支持 192.168.255.254 以及 127.0.0.0/8 范围的 IP 地址。
对端 IP 地址	创建 IPSec VPN 隧道时，远端 NISG 设备所使用接口的 IP 地址。不支持多播地址 224.0.0.0-255.255.255.255，不支持 192.168.255.254 及 127.0.0.0/8 范围的 IP 地址。
ESP	
加密算法	用于对在 IPSec VPN 隧道中传输的 IP 数据包进行加密的加密算法，包括 AES-128， AES-192， AES-256， 3DES 和无。数字表示密钥的长度，密钥越长，被保护的数据包越安全，但用于解析密钥的时间也越长。
加密密钥	ESP 加密的密钥。不同的加密算法对应的加密密钥长度也不同： • AES-128— 密钥为 32 位十六进制数 • AES-192— 密钥为 48 位十六进制数 • AES-256— 密钥为 64 位十六进制数 • 3DES— 密钥为 48 位十六进制数
认证算法	IPSec VPN 隧道使用的认证算法，包括 HMAC-MD5， HMAC-SHA1 和无。
认证密钥	ESP 认证的密钥。不同的认证算法对应的认证密钥长度也不同： • HMAC-MD5— 密钥为 32 位十六进制数 • HMAC-SHA1— 密钥为 40 位十六进制数
本端 SPI	用于标识所建立的 SA 的本端 SPI，必填项，为 8 位十六进制数，范围为 00000100-2FFFFFFF。
远端 SPI	用于标识所建立的 SA 的远端 SPI，必填项，为 8 位十六进制数，范围为 00000100-2FFFFFFF。
AH	
认证算法	用于对通过 IPSec VPN 隧道传输的 IP 数据包进行认证的认证算法，包括 HMAC-MD5、HMAC-SHA1 和无。
认证密钥	AH 认证的密钥。不同的加密算法对应的认证密钥长度也不同： • HMAC-MD5— 密钥为 32 位十六进制数 • HMAC-SHA1— 密钥为 40 位十六进制数
本端 SPI	用于标识所建立的 SA 的本端 SPI，必填项，为 8 位十六进制数，范围为 00000100-2FFFFFFF。
对端 SPI	用于标识所建立的 SA 的本端 SPI，必填项，为 8 位十六进制数，范围为 00000100-2FFFFFFF。

提示：用户至少需要选择 AH 和 ESP 协议中的一个，也可以两个都选择。如果选择了 ESP 协议，则 ESP 的加密算法和认证算法至少需要选择一个，可以两个都选择。

11.4.1.4 隧道组参数

表 252 隧道组参数

参数	说明
组名称	隧道组名称，长度 1-63 字节，UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #。不能与自动隧道、手动隧道以及 SSL VPN 隧道重名。
隧道名称	隧道组中包含的网关到网关自动密钥隧道隧道，最多可包含 16 条。
优先级	隧道组中包含的隧道的优先级。为 0-255 之间的整数，数值越大，优先级越高。允许隧道优先级相同，此时系统会自动选择一条隧道。
隧道状态	VPN 隧道组包含的隧道的状态，包括 usable 和 unusable。
引用	当前的隧道组是否用作 VPN 隧道被路由或访问策略引用。
启用	该隧道组是否处于启用状态。

11.4.1.5 常规设置

NISG 可以通过使用硬件加速卡来提升 VPN 的性能。可以通过点击**是**和**否**来启用和禁用加速卡。

11.4.2 SSL VPN 相关参数

在 SSL VPN 的配置过程中，会涉及到如下参数的配置：

- 11.4.2.1 SSL VPN 用户组参数

SSL VPN Web 入口页面参数包括应用、页面模板和页面服务的配置参数。

- 11.4.2.2 SSL VPN Web 入口页面的应用参数
- 11.4.2.3 SSL VPN Web 入口页面的页面模板参数
- 11.4.2.4 SSL VPN Web 入口页面的页面服务参数

SSL VPN 隧道配置包括：

- 11.4.2.5 SSL VPN 隧道参数

11.4.2.1 SSL VPN 用户组参数

SSL VPN 用户必须被用户组包含才能使用 SSL VPN 服务。

表 253 SSL VPN 用户组参数

参数	说明
名称	SSL VPN 用户组名称。长度 1-63 字节，UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #
包含用户	用户组包含的 SSL VPN 用户。一个 SSL VPN 用户只能被一个 SSL VPN 用户组包含。
引用服务	引用该 SSL VPN 用户组的 SSL VPN 服务。
引用隧道	引用该 SSL VPN 用户组的 SSL VPN 隧道。
包括外部用户	用户组是否包含外部 SSL VPN 用户。 外部用户包括在 NISG 上创建，而密码保存在外部服务器上的用户，以及在外部服务器上创建，用户名和密码都保存在外部服务器上的用户。 如果用户组包含远程用户，那么所有的远程用户都属于该组。 默认为不包含。

提示：被 SSL VPN 服务引用的 SSL VPN 用户组可以被修改，但不能被删除。

11.4.2.2 SSL VPN Web 入口页面的应用参数

表 254 应用参数

参数	说明
名称	SSL VPN 应用名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & #
类型	SSL VPN 应用的类型，包括 HTTP 和 HTTPS。
URL	SSL VPN 应用的地址。

提示：被 SSL VPN 页面模板引用的 SSL VPN 应用不能被删除。

11.4.2.3 SSL VPN Web 入口页面的页面模板参数

表 255 页面模板参数

参数	说明
名称	SSL VPN 页面模板名称。长度 1-63 字节，UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & #
入口设置	• 标题 — 显示在入口页面上方的文字，长度 1-90 字节， UTF-8 字符。可以为空。 • 主题色 — 入口页面显示的主题颜色，包括页面的线框、上方颜色条、登录页面的边框和底色等。可以点击色块后进行选择，也可以在文本框中直接输入颜色编码。颜色编码的取值范围为 #000000-#FFFFFF。 • Logo— 显示在入口页面左上角和登录页面登录框上方的图片。 要求为 jpg、 gif、 png 或 bmp 格式的图片文件，图片规格为 15 （高） x80 （宽），单位为像素。文件大小不能超过 150KB。选择 Logo 图片后可以在预览区域查看实际显示效果。 上传长度为 0 的空文件时， Logo 显示为空白。 • 语言 — 入口页面的显示语言，包括英文和简体中文。 默认值为英文。
应用设置	• 类型 — 要添加至列表中的应用类型。 • 应用 — 要添加至列表中的应用名称。 • URL— 所添加应用对应的 URL 地址。 • 分割线 — 用于在入口页面上分开两种应用，便于查看的横线，分割线一端有文字描述。 应用和分割线会根据添加的顺序出现在入口页面上。可以点击应用右侧的 ⬆ 或 ⬇ 移动它们的排序。 一个 SSL VPN 页面模板中最多可以添加 32 个应用或分割线。
允许自定义应用	设置用户是否可以在入口页面自定义应用。

提示：被 SSL VPN 服务引用的 SSL VPN 页面模板不能被删除，但可以修改。

11.4.2.4 SSL VPN Web 入口页面的页面服务参数

表 256 页面服务参数

参数	说明
名称	SSL VPN 服务名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：? , " ' \ < > & #
用户组	被 SSL VPN 服务引用的用户组。用户组中的用户可以登录到此 SSL VPN 服务。
服务地址	提供此 SSL VPN 服务的 IP 地址和端口。
启用	用于启用该 SSL VPN 服务。
服务绑定	定义了 SSL VPN 对外提供服务的接口、 IP 地址和端口号，一个 SSL VPN 服务可以在 NISG 的多个 IP 地址和端口上提供服务。一个 Vsys 中最多可支持 4 个 SSL VPN 服务，每个 SSL VPN 服务可以绑定最多 4 个 IP 地址和端口对。 • 接口 — 表示除 loopback 接口、隧道接口和虚拟接口外的所有三层接口。 • IP 地址 — 表示所选的三层接口的 IP 地址。 Any 表示该接口上的所有 IP 地址。 • 端口 — 表示提供服务的端口号。
服务配置	• 用户组列表 — 服务包含的 SSL VPN 用户组，列表中的用户组内成员可以登录该服务。 • 入口页面 — 服务提供内容的入口页面，入口页面为用户登录 SSL VPN 后能够看到的页面。 • 会话超时 — 用户登录 SSL VPN 服务后不进行任何操作后自动登出时的时间，范围为 0-60000，默认值为 1200，单位为秒。超时时间设置为 0 时，用户登录后永不超时，但用户关闭浏览器后会自动登出。 • 登录失败上限 — 用户由于输入错误的用户名、密码或验证码导致的最大登录失败次数。上限为 0-10 的整数， 0 表示没有登录失败上限。达到失败次数上限后，该登录失败的 IP 地址会被系统锁定，即使用该 IP 地址的用户不能以任何方式登录 NISG。具体的锁定时间为第一次 5 分钟，，第二次 1 小时，第三次 24 小时。 24 小时过期后该 IP 地址的登录锁定次数清零。 • 登录需要验证码 — 指定用户登录该 SSL VPN 服务时是否需要验证码，为每次用户登录时需要输入的一组长度为 4 的字母字符串。默认为启用。 • 需要验证用户证书 — 勾选该选项表示启用客户端和服务器端的双向认证，否则只进行客户端对服务器的认证。当服务启用后，该选项不能修改。默认为不勾选。 • 保存用户配置 — 设置是否将用户自定义应用保存在系统上。但当 SSL VPN 服务所选择的页面模板不允许用户自定义应用时，此选项失去作用。此选项从开启到关闭时，将清空用户已经保存的全部设置。 • 允许用户修改密码 — 管理员勾选此复选框之后，用户可以修改 SSL VPN 入口页面的密码。新密码将在用户下次通过验证时生效。如果 SSL VPN 用户同时也是 WebAuth 或 VPN 用户，则 WebAuth 和 VPN 密码也会同时变化。用户进行认证时需要输入新密码。对于已经通过认证的用户则没有影响。默认为不勾选。

表 256 页面服务参数 (*续*)

参数	说明

SSL 配置	• SSL 证书 —SSL VPN 服务端的证书，只能选择本地证书类型。默认为添加时的证书，不能为空。
	• 支持的 SSL 版本 — 包括 SSL v2.0、 SSL v3.0 和 TLS v1.0。默认为 SSL v3.0 和 TLS v1.0。当三个选项全不勾选时，系统无法通过 SSL 进行连接，所有客户端均不能使用 SSL VPN 进行网络访问。
	• 算法级别 — 加密算法强度，包括高、中、低。级别越高，其安全性越高。
	  • 高 —ADH-AES256-SHA, DHE-RSA-AES256-SHA, DHE-DSS-AES256-SHA, AES256-SHA, ADH-AES128-SHA, DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA, AES128-SHA, ADH-DES-CBC3-SHA,EDH-RSA-DES-CBC3-SHA,EDH-DSS-DES-CBC3-SHA,DES-CBC3-SHA, 和 DES-CBC3-MD5
	  • 中 —ADH-RC4-MD5, IDEA-CBC-SHA, RC4-SHA, RC4-MD5, IDEA-CBC-MD5, RC2-CBC-MD5 和 RC4-MD5
	  • 低 —ADH-DES-CBC-SHA, EDH-RSA-DES-CBC-SHA, EDH-DSS-DES-CBC-SHA, DES-CBC-SHA, 和 DES-CBC-MD5

客户端安全要求	定义了登录到 SSL VPN 服务的用户使用的操作系统以及浏览器必须满足的安全性要求。 • 开启客户端安全要求 — 是否要求客户端浏览器安装安全性插件，并选择安全强度。包括高、中、低。默认为勾选此选项，强度为中。 • 浏览器版本 — 是否要求客户端必须使用要求的浏览器类型和版本。 • 操作系统版本 — 是否要求客户端必须使用要求的系统版本。 • 安装杀毒软件 — 是否要求客户端操作系统中安装杀毒软件。 • 开启防火墙 — 是否要求客户端操作系统中开启防火墙。 • 退出时清空浏览器缓存 — 是否在用户登出系统时清除浏览器缓存。只有访问当前服务产生的缓存文件会被清除。 • 退出时清除浏览器 cookie— 是否在用户登出系统时清除浏览器 cookie。只有访问当前服务产生的 cookie 会被清除。 • 退出时清除浏览器访问历史记录 — 是否在用户登出系统时清除浏览器访问历史记录。只有访问当前服务产生的历史记录会被清除。 • 退出时清除浏览器自动表单和密码记录 — 是否在用户登出系统时清除自动表单和密码记录。只有访问当前服务产生的自动表单和密码记录会被清除。 • 退出时清除浏览器操作系统临时文件 — 是否在用户登出系统时清除系统临时文件。只有访问当前服务产生的系统临时文件会被清除。
被允许的访问	可以访问 SSL VPN 服务的地址列表，由 IP 地址段或单个 IP 地址组成。 允许访问列表中， IP 地址段和安全域共同组成一个允许访问列表项。安全域可以从当前 Vsys 中选择，也可以设置为 Any，表示可以从来自设置 IP 地址段的任意安全域进行访问。 访问控制列表最多可以包含 32 个访问控制项。
用户组访问授权	• 用户组 — 可以使用或不能使用当前 SSL VPN 服务的 SSL VPN 用户组。 • 应用 — 该 SSL VPN 所属页面模板中包含的应用。 • 动作 — 表示对应的用户组对于应用的权限。 • 用户默认权限 — 当用户组和应用的组合不在用户组访问权限列表中时，按照默认用户组权限设定值进行处理。 用户组访问权限列表最多可以包含 65535 条记录。

11.4.2.5 SSL VPN 隧道参数

表 257 SSL VPN 隧道参数

参数	描述
名称	SSL VPN 隧道名称。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #
	SSL VPN 隧道名称创建后不能修改，不能与已经存在的 IPSec VPN 隧道和 IPSec VPN 隧道组名称相同。
用户组	允许连接此 SSL VPN 隧道的用户组。
出口接口	该 SSL VPN 隧道对外提供连接的服务接口。
本端 IP 地址	出口接口的 IP 地址。当指定为 Any 时，表示包含该接口上的所有 IP 地址。
授权子网	用户可以通过此 SSL VPN 隧道访问的网络范围，可以是除多播地址 224.0.0.0-255.255.255.255 以外的 IPv4 地址和 FF00/8-FFFF/8 以外的 IPv6 地址。 IPv4 地址的掩码范围为 0-32， IPv6 地址的前缀为 0-128。
启用	是否启用本 SSL VPN 隧道。

11.4.3 IP 地址池相关参数

IP 地址池被用来为 IPSec VPN 用户和 SSL VPN 用户分配 IP 地址。

表 258 IP 地址池参数

名称	说明
名称	IP 地址池的名称，创建后不可修改。长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #
IP 地址范围	IP 地址范围，也可以是单个 IP 地址 , 但不能是 192.168.255.254。
被用户引用	引用 IP 地址池的 IPSec VPN 或 SSL VPN 用户。

12 高可用性

本章介绍 NISG 如何通过使用 VRRP 协议、增强的 VRRP 选举协议以及集群功能来提供高可用性 （HA）服务。章节结构如下所示：

- 12.1 概述，介绍 HA 的基本概念和原理。
- 12.2 基本配置步骤，介绍基本配置步骤 （WebUI 操作和 CLI 命令）。
- 12.3 范例，提供详细步骤的范例。
- 12.4 配置参数说明，介绍配置参数的详细信息。

12.1 概述

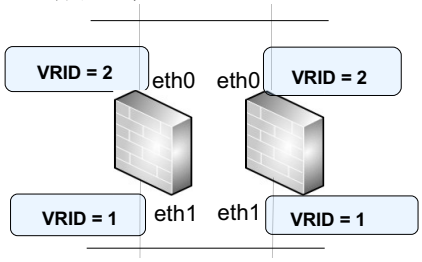
本节介绍：

- 12.1.1 标准 VRRP 和增强 VRRP, NISG 支持标准的 VRRP 虚拟路由器（VR）功能。同时提供虚拟路由器探测组 （VRDG）和集群，增强了 VR 功能。
- 12.1.2 标准的 VRRP 配置
- 12.1.3 增强的 VRRP （VRDG/ 集群）配置，介绍 VR、 VRDG 和集群的配置。
- 12.1.4 标准的 VRRP 运行原理
- 12.1.5 增强的（VRDG/ 集群）运行原理，介绍 VR、VRDG 和集群的运行（同步、IP 探测和选举）。

12.1.1 标准 VRRP 和增强 VRRP

标准 VRRP

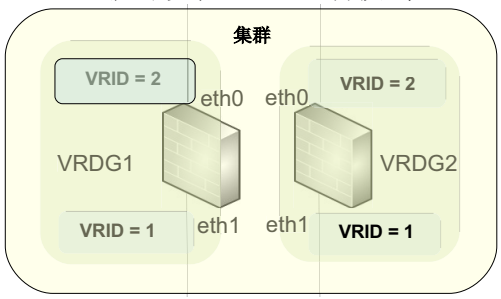
标准的 VRRP 使用虚拟路由器 （VR）的概念。在 NISG 中，需要成对创建 VR，每个设备各有一个 VR，它们处于同一网段，具有相同的 VRID。在下例中， VRID=2 的两个 VR 组成一对。



增强 VRRP

增强的 VRRP 包含如下组件：

- **虚拟路由器 （VR）对**。
- **虚拟路由器探测组 （VRDG）：**一个探测组包含数个位于同一设备但不同网段上的 VR。探测组可以成对创建，每个集群设备上各创建一个。 VRDG 在保持与 VRRP 协议的兼容性的同时，能够有效地使一组 VR 切换为备份状态。
- **集群**：指两个设备，通过专用的以太网接口或以太网通道互相同步数据，以实现无缝的 VR 故障切换 （如下图，当 device1 设备本身或 device1 的 VR1 接口发生故障，VR1 就可以从 device1 切换到 device2）。



12.1.2 标准的 VRRP 配置

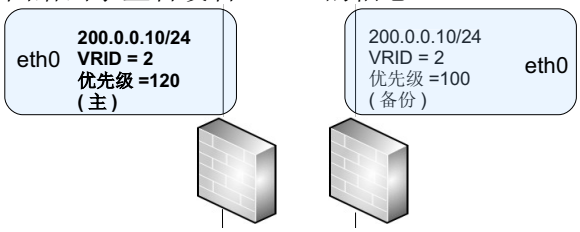
本节描述了下列功能的基本配置：

- 12.1.2.1 VR
- 12.1.2.2 VR 选举
- 12.1.2.3 VR 的 IP 探测

关于参数信息，参见 12.4.1 虚拟路由器。
关于配置步骤，参见 12.2.1 VRRP 基本配置。

12.1.2.1 VR

下图给出了主备设备上 VR 的信息。



VR 配置包括：

- **接口：**用于主备选举和数据通讯。可以是三层或三层共享以太网接口、三层或三层共享以太网通道，以及 VLAN 接口。
- **备份 IP 地址：**起到默认网关的作用，可以是子网中一个 IP 或不同网段上一组 IP 地址。

提示：如果备份 IP 被设置成接口的 IP 地址，此时接口为 IP 地址所有者，优先级永远是 255，即使接口故障， VR 也不发生故障切换。因此不要将 IP 地址所有者的地址设置为备份 IP。

- **VRID：**同一网段上的主备 VR 具有相同的 VRID。虚拟 MAC 地址（格式为 00-00-5E-00-01-[VRID]）由主 VR 使用，对 ARP 请求进行响应。

12.1.2.2 VR 选举

选举设置包括：

- **优先级：**用于决定 VR 选举的主备角色，具有较高优先级的设备成为主。
- **通告周期：**主设备发送通告报文的时间间隔。
- **抢占模式：**备份设备抢占低优先级的主设备。

关于 VR 的选举过程，参见 12.1.4.2 选举。
关于范例，参见 范例 2：主备选举。

12.1.2.3 VR 的 IP 探测

VR 的 IP 探测用于检测目的 IP 地址的可达性。通过修改主备 VR 的优先级，将接口处于良好运行状态的设备选举为主。 IP 探测设置包括：

a. 类型：ARP、 ICMP 或 TCP
b. 接口
c. 探测的 IP 地址
d. 探测端口 （只在 TCP Ping 时使用）
e. 发送探测报文的时间间隔 （秒）
f. 探测重试次数 （从最后一次收到回应起，发送的探测报文的次数限值）
g. 权重：IP 探测失败后，将从 VR 的优先级中减去该权重值

关于范例，参见 范例 4：IP 探测。

12.1.3 增强的 VRRP （VRDG/ 集群）配置

本节描述了下列功能的基本配置：

- 12.1.3.1 VR
- 12.1.3.2 VRDG
- 12.1.3.3 VRDG 选举
- 12.1.3.4 VRDG 的 IP 探测
- 12.1.3.5 集群

关于参数信息，参见 12.4.2 虚拟路由器探测组和 12.4.3 集群。

关于基本配置，参见 12.2.2 增强的 （VRDG/ 集群）。

关于范例描述，参见

- 范例 1：增强 （VRDG/ 集群）基本配置
- 范例 2：主备选举
- 范例 5：集群同步

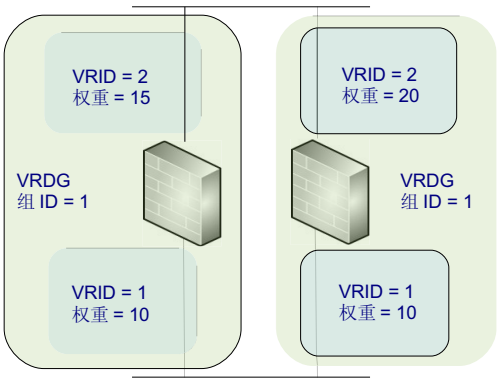
12.1.3.1 VR

与标准 VRRP 配置相同。不同在于 VR 的 IP 探测设置将被 VRDG 的设置所覆盖，因此无需设置。

12.1.3.2 VRDG

设备的 VRDG 具有：

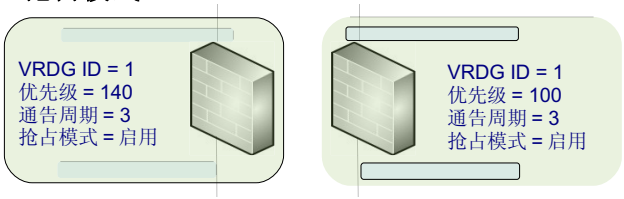
- **组 ID**：VR 所属的探测组标识。
- **成员 VR**：位于不同网段，但处于同一设备中。位于两台设备上的 VRDG 应具有相同的 VR 成员。
- **VR 权重**：当一个 VR 加入 VRDG 时，本身具有一个权重值（见下图）。当发生 VR 故障时，将从 VRDG 的优先级中减去其权重值。



12.1.3.3 VRDG 选举

实际是 VRDG 包含的 VR 内部进行的选举。以下 VRDG 设置会覆盖 VR 设置：

- **优先级**：VRDG 通过调整 VR 的优先级，以保证 VRDG 中的主 VR 全在同一个设备上。
- **通告周期**：VRDG 发送报文的时间间隔。
- **抢占模式**



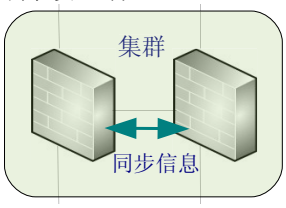
12.1.3.4 VRDG 的 IP 探测

VRDG 的 IP 探测与基本探测 （VR）相似。在检测到故障时，可以统一降低 VRDG 中所有 VR 的优先级 （数值相同）。

提示：当 VR 加入 VRDG 时，其 IP 探测设置将被清空。 VR 发生故障时，将从 VRDG 的优先级中减去 VR 的权重值。

12.1.3.5 集群

集群由两台 NISG 设备组成，承载 VR 的可同步的配置信息及运行信息。在 VR 发生故障切换后，承载新的主 VR 的设备将会获得原主设备的全部信息，以无缝方式实现 VR 的持续运行。



组成集群的两台 NISG 设备硬件型号和系统版本最好相同。

集群配置包括：

1. **链路**：专用的二层链路。两台设备间的同步接口为二层以太网接口或以太网通道。建议使用：
   - 二层以太网接口，同步配置信息。
   - 二层以太网通道 （增加带宽），同步运行信息。
   - 为了保证可靠、安全地通信，推荐将两台设备的 HA 接口直连。
2. **加密**：使用 DES 算法对同步数据包加密。当集群成员通过集线器、交换机等中间设备相连时，推荐使用加密功能。集群成员间应该具有相同的加密密码。
3. **认证**：对集群内的成员设备进行身份认证，集群成员间应该具有相同的认证密码。
4. **运行信息同步**：启用该功能，并可以选择性地设置 “ 自定义会话信息 ”。

5. **系统时间同步**：管理员可以在下列情形中执行系统时间同步
   a. 当设备启动时
   b. 到达每天某个特定时间点时
   c. 当系统时间手动修改或通过 NTP 同步改变时
   在 a) 和 b) 的情形中，可以将一台设备设置为时间同步基准。
6. **查看本地和对端设备信息的差异**：在进行配置同步前，点击此按钮，比较两台集群设备的配置差异。
7. **立即同步**：在启用自动同步配置功能前，推荐先进行手动同步，以保证集群成员的配置和拓扑结构基本一致。
8. 执行**手动（整体）同步**：同步所有配置信息，并覆盖现有的配置。
9. 启用**自动（增量）同步**：当配置信息有改动时，以自动方式进行同步，原有信息仍然保留。

12.1.4 标准的 VRRP 运行原理

- 12.1.4.1 状态
- 12.1.4.2 选举
- 12.1.4.3 IP 探测

12.1.4.1 状态

运行 VRRP 的 NISG 路由器具有以下三种状态：

- **Initialize**：表示 NISG 未参与选举。
- **Master**：NISG 通过选举切换为 Master 状态，此状态下可以转发数据包。
- **Backup**：NISG 通过选举切换到 Backup 状态，此状态下只监听主设备的 VRRP 组播报文，不参与数据转发。

12.1.4.2 选举

触发选举的时机

- 设备启动时。
- VR 优先级改变时。
  - 高优先级的设备成为主；
  - 如果两台设备优先级相同，选举接口上主 IP 地址较大的设备成为主。
- 原主设备从故障恢复时。故障恢复的前提条件：1）启用抢占模式； 2）两台设备的初始优先级不同。

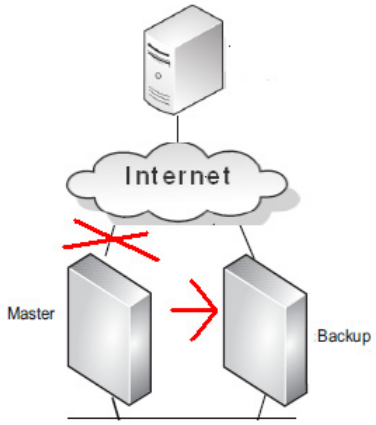
结果。除优先级外，选举结果还取决于：

- **抢占模式**。
  - **启用**：当备份设备从主设备收到优先级低于它的 VRRP 报文时，三倍通告周期加时滞时间后，备份设备将会抢占成为主。
  - **禁用**：只有主设备出现故障时，备份设备才会转变成为主。

- **通告间隔。**如果备份设备连续三个通告周期未收到主设备发来的 VRRP 报文，或收到优先级为 0 的报文，则认为主设备已经无法正常工作，时滞时间 （Skew time）后就会转变为主。

12.1.4.3 IP 探测

以下为 IP 探测示意图。



通过 IP 探测，监控到目的主机的路由。如果检测发现主设备的探测重试次数达到某一设定阈值，其优先级将会减去自身的权重，可能会触发新的选举。触发选举的条件：（1）启用抢占模式 （2）权重应大于两个 VR 的优先级之差。

在原主设备上仍然进行故障探测。当若原主设备恢复故障，它将恢复原始优先级，重新成为主设备。

关于范例，参见 范例 4：IP 探测。

12.1.5 增强的 （VRDG/ 集群）运行原理

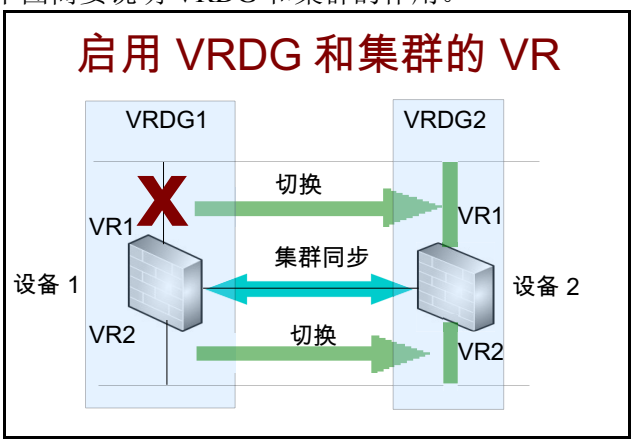
- 12.1.5.1 VRDG/ 集群运行
- 12.1.5.2 集群同步信息

12.1.5.1 VRDG/ 集群运行

NISG 提供虚拟路由器探测组的功能，通过将不同网段的多个虚拟路由器划分到同一个设备，可以确保所有的主虚拟路由器都在一个设备上。在出现故障时，可以实现设备级的整体切换。

集群提供同步功能，能够将主墙的设置实时同步到备墙上，保证信息的一致性。在故障切换时，能够实现信息的无缝迁移。

下图简要说明 VRDG 和集群的作用。



12.1.5.2 集群同步信息

同步数据包括：

- **系统时间**
- **系统配置。**有些配置信息不可同步，管理员需要进行手动配置。这些配置信息包括：
  - 主机名
  - 系统语言
  - 接口的配置 （Tunnel 接口除外）
  - Vsys 的配置

    当两台 NISG 设备分别存在名字相同的 Vsys 时，可以对 Vsys 内的配置信息和运行信息进行同步。
  - 虚拟网络的配置
  - STP 的配置
  - 管理用户的登录、退出、配置锁
  - 虚拟路由器的优先级、 IP 探测、选举接口和认证
  - 虚拟路由器探测组的优先级和 IP 探测
  - 集群配置

- License 的相关操作
- 标题信息 （Banner）的设置
- 重启、关闭、恢复出厂设置的操作
- 技术支持
- 系统的备份和恢复
- 系统升级的配置和操作
- 日志的复制和删除
- 设置存储介质
- 显示的相关操作
- 导出的相关操作
- 查询的相关操作
- NTP 手动校时

- **运行信息。**发生故障切换时，备份设备将接管主设备的所有工作，包括运行信息。

NISG 默认同步下列运行信息：

- UDP 会话 （53 端口除外）
- TCP 会话 （80 和 8080 端口除外）
- IPSec SAs
- NAT 资源
- ARP 表
- DHCP 地址分配信息
- WebAuth 用户认证状态
- VPN 用户连接状态
- VPN IP 地址池分配

12.2 基本配置步骤

本节描述了下列功能的基本配置：

- 12.2.1 VRRP 基本配置
- 12.2.2 增强的 （VRDG/ 集群）

12.2.1 VRRP 基本配置

- 12.2.1.1 Device1：配置 VR
- 12.2.1.2 Device2

关于参数信息，参见 12.4.1 虚拟路由器。

关于范例信息，参见 范例 2：主备选举和 范例 4：IP 探测。

12.2.1.1 Device1：配置 VR

1. 选择**系统** > **高可用性** > **虚拟路由器**。
2. 点击**新建**，配置选举接口和其他参数。

备份 IP 地址格式为 [1-223].[0-255].[0-255].[0-255]，不可以是 127.0.0.0-127.255.255.255 或 192.168.255.254。

3. （可选）在三层接口上配置 IP 探测，探测链路的可达性。

- 添加两条针对相同接口和相同 IP 地址的探测条目，后一个条目会覆盖前一个。
- 备份 IP 地址格式为 [1-223].[0-255].[0-255].[0-255]，不可以是 127.0.0.0-127.255.255.255 或 192.168.255.254。
- 最多能够配置 64 个 IP 探测条目。

12.2.1.2 Device2

配置与 Device1 相同。

表 259 VR 命令

virtual router *vr_id*	添加虚拟路由器或进入到虚拟路由器配置模式。
unset virtual router *vr_id*	删除当前指定的虚拟路由器。
election interface *interface_name*	设置虚拟路由器的选举接口。
unset election interface *interface_name*	删除虚拟路由器的选举接口。
priority *pri*	设置 VRRP 路由器在虚拟路由器中的优先级。
interval *interval_value*	设置主路由器向备份路由器发送报文的通告周期。
preempt {enable | disable}	启用或禁用抢占模式。
auth {enable password *auth_key* **| disable}**	启用或禁用同一虚拟路由器内 VRRP 路由器成员间的认证。
virtual-router {enable | disable}	启用或禁用虚拟路由器。
backup ip address *ipv4* **mask** *netmask*	添加虚拟路由器的备份 IP 地址。
unset backup ip address *ipv4*	删除虚拟路由器的备份 IP 地址。
ip-track	设置虚拟路由器的 IP 探测。
unset ip-track	删除虚拟路由器的 IP 探测。
show virtual-router {all | *vr_id***}**	显示虚拟路由器的配置信息。

12.2.2 增强的 （VRDG/ 集群）

- 12.2.2.1 Device1：配置 VR
- 12.2.2.2 Device1：配置 VRDG
- 12.2.2.3 Device1：配置集群
- 12.2.2.4 Device2

关于参数信息，参见 12.4.2 虚拟路由器探测组和 12.4.3 集群。

关于范例信息，参见 范例 1：增强 （VRDG/ 集群）基本配置，范例 3：负载分担 （主主模式）和 范例 5：集群同步。

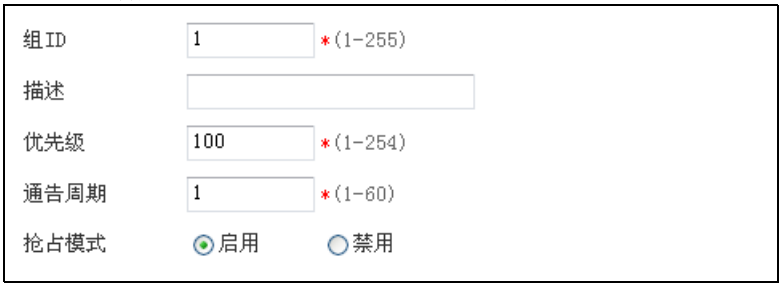
12.2.2.1 Device1：配置 VR

请参见 12.2.1.1 Device1：配置 VR。

提示：不必配置 VR 的 IP 探测，因为 VR 加入 VRDG 后，其 IP 探测设置将被清空。

12.2.2.2 Device1：配置 VRDG

1. 选择**系统 > 高可用性 > 虚拟路由器探测组**。
2. 点击**新建**。配置组 ID、优先级、通告间隔和抢占模式。



3. 添加虚拟路由器和权重。

4. （可选）在三层接口上配置 IP 探测，探测链路的可达性。

创建一个重复 ID 的虚拟路由器探测组，后创建的探测组将覆盖之前创建的探测组。

表 260 VRDG 命令

detection group *group_id*	创建 VRDG 或进入到 VRDG 配置模式。
unset detection group *group_id*	删除指定的 VRDG。
hold virtual-router weight	设置 VRDG 成员。
unset hold virtual-router *vr_id*	从 VRDG 中删除指定的虚拟路由器成员。
priority *pri*	设置 VRDG 的优先级。
interval *interval_value*	设置 VRDG 的通告周期。
preempt {enable | disable}	启用或禁用 VRDG 的抢占模式。
ip-track	设置虚拟路由器的 IP 探测。
unset ip-track	删除 VRDG 的 IP 探测。
show detection-group {all | *group_id*}	显示 VRDG 的配置信息。

12.2.2.3 Device1：配置集群

1. 选择**系统 > 高可用性 > 集群**。
2. 配置集群 ID、本端和对端 IP 地址、用于同步的二层以太网接口或以太网通道。

- 建议使用二层以太网接口同步配置信息，二层以太网通道同步运行信息。
- 本端和对端 IP 地址格式为 [1-223].[0-255].[0-255].[0-255]，不可以是 127.0.0.0-127.255.255.255 或 192.168.255.254.

3. 配置同步、加密和认证。

- **查看本地和对端设备信息的差异**：启用自动同步配置功能前，可以查看两台集群设备的配置差异。
- **立即同步**：在执行自动配置同步前，推荐先进行手动同步，以保证集群设备的拓扑结构基本一致。

- **将此时间设置应用到两端设备**：同一个集群内，只有一台设备可以设置为时间同步基准。
- **加密**：如果 Device1 和 Device2 直连，关闭加密功能。

12.2.2.4 Device2

配置与 Device1 相同。

表 261 集群命令

clusterid *cluster_id*	设置集群标识，将 NISG 设备加入到指定的集群中。
unset clusterid	将 NISG 设备从集群中删除。
local interface *interface_name*	设置集群设备本端的同步接口。
unset local interface	删除集群设备的本端同步接口。
local ip address *ipv4* **mask** *netmask*	设置集群设备本端同步接口的 IP 地址。
peer ip address *ipv4*	设置集群设备对端同步接口的 IP 地址。
config check	检验集群内设备配置信息的一致性。
config sync	手动同步配置信息到对端设备。
config sync auto {**enable** | **disable**}	启用或禁用自动同步配置信息功能。
rti sync {**enable** | **disable**}	启用或禁用自动同步运行信息功能。
rti session default	设置同步默认的会话信息。
rti session {**tcp** | **udp** | **other**}	添加要进行同步的自定义会话信息。
unset rti session {**tcp** | **udp** | **other**}	删除要进行同步的自定义会话信息。
time sync {**enable** | **disable**}	启用或禁用自动同步系统时间功能。
time boot {**on** | **off**}	设置当 NISG 启动时，是否立即同步系统时间。
time daily {*time_sync* | **off**}	设置每日同步系统时间。
time benchmark {**on** | **off**}	设置当前 NISG 为系统时间同步基准。
time modified {**on** | **off**}	设置 NISG 系统时间更改时，是否立即同步系统时间。
encrypt {**enable password** *enc_key* | **disable**}	启用或禁用同一集群内设备间的同步信息加密功能。
auth {**enable** | **disable**}	启用或禁用集群内设备间的认证。
show cluster	显示集群配置信息。

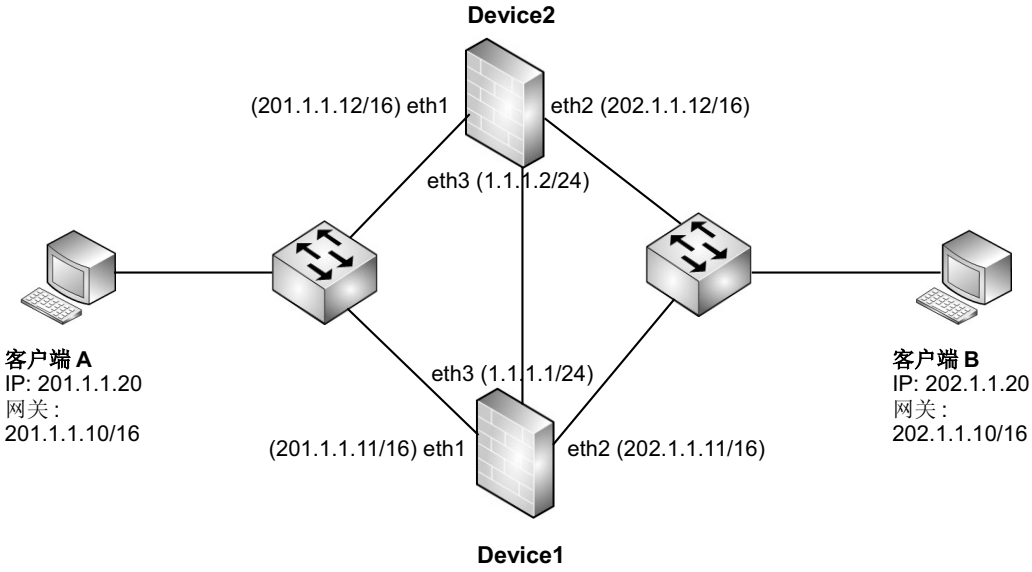
12.3 范例

- 范例 1：增强 （VRDG/ 集群）基本配置
- 范例 2：主备选举
- 范例 3：负载分担 （主主模式）
- 范例 4：IP 探测
- 范例 5：集群同步

范例 1：增强 （VRDG/ 集群）基本配置

处于主状态的设备发生异常时，处于备份状态的设备将变成主设备。本范例说明如何通过两个二层以太网接口连接 Device1 和 Devcie2，并启用配置同步、运行信息同步和系统时间同步功能。

图 55 主备模式



- 1.1 配置缺省策略和接口
- 1.2 配置 VR
- 1.3 配置 VRDG
- 1.4 配置集群

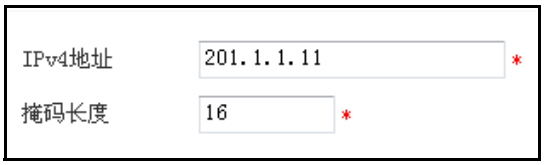
1.1 配置缺省策略和接口

Device1.

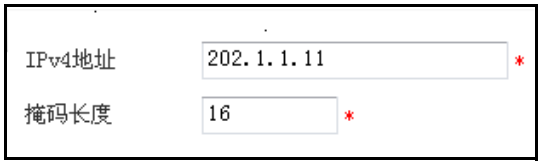
1. 选择**防火墙** > **缺省策略设置**。

2. 点击**确定**。
3. 选择**网络 > 接口**。
4. 在**接口列表中**点击 eth1 所对应的，进入到 eth1 的**编辑**页面。在 **IP 地址列表**中，点击**添加**。

提示：如果接口为二层工作模式，需要首先将其设置为三层工作模式，然后配置相应的 IP 地址。



5. 在**接口列表中**点击 eth2 所对应的，进入到 eth2 的**编辑**页面。在 **IP 地址列表**中，点击**添加**。



6. 点击**确定**。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy default inter-zone access permit
NetEye@root-system] interface ethernet 1
NetEye@root-system-if-eth1] ip address 201.1.1.11 255.255.0.0
NetEye@root-system] exit
NetEye@root-system] interface ethernet 2
NetEye@root-system-if-eth2] ip address 202.1.1.11 255.255.0.0
NetEye@root-system] exit
```

Device2.

7. 访问策略 = 允许
8. 在 **IP 地址列表**中，添加 eth1 201.1.1.12/16 和 eth2 202.1.1.12/16。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy default inter-zone access permit
NetEye@root-system] interface ethernet 1
NetEye@root-system-if-eth1] ip address 201.1.1.12 255.255.0.0
NetEye@root-system] exit
NetEye@root-system] interface ethernet 2
NetEye@root-system-if-eth2] ip address 202.1.1.12 255.255.0.0
NetEye@root-system] exit
```

1.2 配置 VR

Device1.

1. 选择**系统** > **高可用性** > **虚拟路由器**。
2. 点击**新建**，进行如下配置(单个VR的优先级、通告周期和抢占模式将被VRDG设置取代)。

3. 点击**确定**。

4. 点击**新建**，进行如下配置。

5. 点击**确定**。

CLI

```
NetEye@root-system] virtual router 1
NetEye@root-system-vr1] backup ip address 201.1.1.10 mask 255.255.0.0
NetEye@root-system-vr1] election interface eth1
NetEye@root-system-vr1] virtual-router enable
NetEye@root-system-vr1] exit
NetEye@root-system] virtual router 2
NetEye@root-system-vr2] backup ip address 202.1.1.10 mask 255.255.0.0
NetEye@root-system-vr2] election interface eth2
NetEye@root-system-vr2] virtual-router enable
NetEye@root-system-vr2] exit
```

Device2.

6. 创建新的 VR。VRID=1，eth1，优先级 =100，通告周期 =1，抢占模式 = 启用，VR= 启用，备份 IP=201.1.1.10/16。
7. 创建新的 VR。VRID=2，eth2，优先级 =100，通告周期 =1，抢占模式 = 启用，VR= 启用，备份 IP=202.1.1.10/16。

CLI

```
NetEye@root-system] virtual router 1
NetEye@root-system-vr1] backup ip address 201.1.1.10 mask 255.255.0.0
NetEye@root-system-vr1] election interface eth1
NetEye@root-system-vr1] virtual-router enable
NetEye@root-system-vr1] exit
NetEye@root-system] virtual router 2
NetEye@root-system-vr2] backup ip address 202.1.1.10 mask 255.255.0.0
NetEye@root-system-vr2] election interface eth2
NetEye@root-system-vr2] virtual-router enable
NetEye@root-system-vr2] exit
```

1.3 配置 VRDG

Device1.

1. 选择**系统** > **高可用性** > **虚拟路由器探测组**。
2. 点击**新建**，进行如下配置。将 Device1 上两个 VR 的权重均设置为 20。如果其中一个发生故障，将从探测组优先级中减去其权重，即 120-20=100，结果小于 110 （在步骤 4 中为 Device2 设置的优先级），可以发生故障切换。

3. 点击**确定**。

CLI

```
NetEye@root-system] detection group 1
NetEye@root-system-dg1] hold virtual-router 1 weight 20
NetEye@root-system-dg1] hold virtual-router 2 weight 20
NetEye@root-system-dg1] priority 120
NetEye@root-system-dg1] exit
```

Device2.

4. 创建新的 VRDG。组 ID=1，优先级 =110，通告周期 =1，抢占模式 = 启用，成员路由器为 VRID1 （权重 =20） +VRID2 （权重 =20）。

CLI

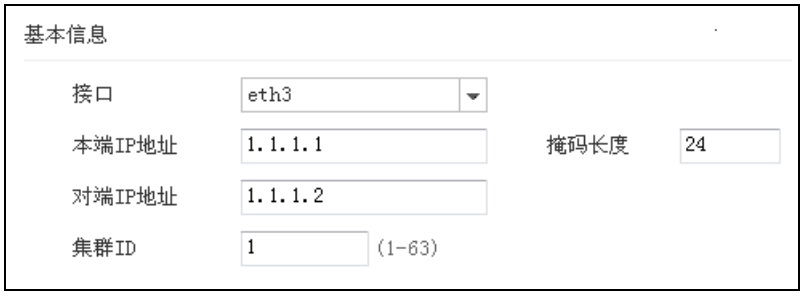
```
NetEye@root-system] detection group 1
NetEye@root-system-dg1] hold virtual-router 1 weight 20
NetEye@root-system-dg1] hold virtual-router 2 weight 20
NetEye@root-system-dg1] priority 110
NetEye@root-system-dg1] exit
```

1.4 配置集群

Device1.

HA 同步接口应该是二层以太网接口或以太网通道。在 Device1 上进行集群设置，其数据信息将同步到 Device2 上。

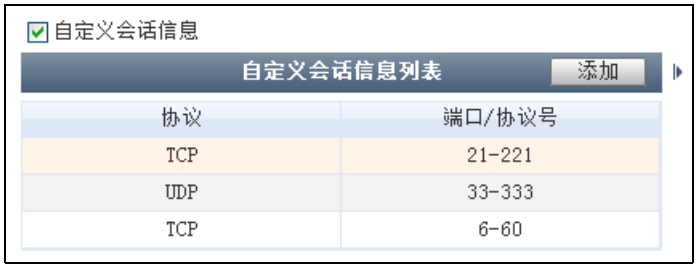
1. 选择**系统** > **高可用性** > **集群**，设置集群。



2. （可选）点击**查看本地和对端设备信息的差异**，可以检查对端设备，查看两端配置是否有差异。
3. 如果有差异，点击**立即同步**，Device1 的配置信息将同步到 Device2，保持配置一致。
4. 点击**自动同步配置信息**对应的**开启**按钮， Device1 上的实时配置变化将被同步到 Device2。当 Device2 也启用了该项功能，则任意一端的配置变化将导致两台设备彼此之间进行自动同步。

5. 点击**自动同步运行信息**对应的**开启**按钮，则 Device1 上的默认运行信息将被同步到 Device2 上。当 Device2 也开启了该项功能时，两端设备将互相同步默认运行信息。

6. 勾选**自定义会话信息**，可以通过指定协议类型和对应端口来自定义所要同步的会话。



7. 点击**自动同步系统时间**所对应的开启按钮。

8. 勾选**当设备启动时**，并勾选**将此时间设置应用到两端设备**（可选）。当 Device1 启动时，其系统时间将自动同步到 Device2。

提示：在一个集群中，只有一台设备可被设置为时间同步基准。

9. 点击**确定**。
10. 点击 。

CLI

```
NetEye@root-system] cluster
NetEye@root-system-cluster] clusterid 1
NetEye@root-system-cluster] local interface eth3
NetEye@root-system-cluster] local ip address 1.1.1.1 mask
255.255.255.0
NetEye@root-system-cluster] peer ip address 1.1.1.2
NetEye@root-system-cluster] config check
NetEye@root-system-cluster] config sync
NetEye@root-system-cluster] config sync auto enable
NetEye@root-system-cluster] rti sync enable
NetEye@root-system-cluster] rti session default
NetEye@root-system-cluster] rti session tcp 21-221
NetEye@root-system-cluster] rti session udp 33-333
NetEye@root-system-cluster] rti session other 6-60
NetEye@root-system-cluster] time sync enable
NetEye@root-system-cluster] time boot on
NetEye@root-system-cluster] time benchmark on
NetEye@root-system-cluster] end
NetEye@root> save config
```

Device2.

11. 创建集群。接口 =eth3，本端 IP=1.1.1.2/24，对端 IP=1.1.1.1，集群 ID=1。
12. 配置同步，开启**自动同步配置信息 / 运行信息 / 系统时间**。

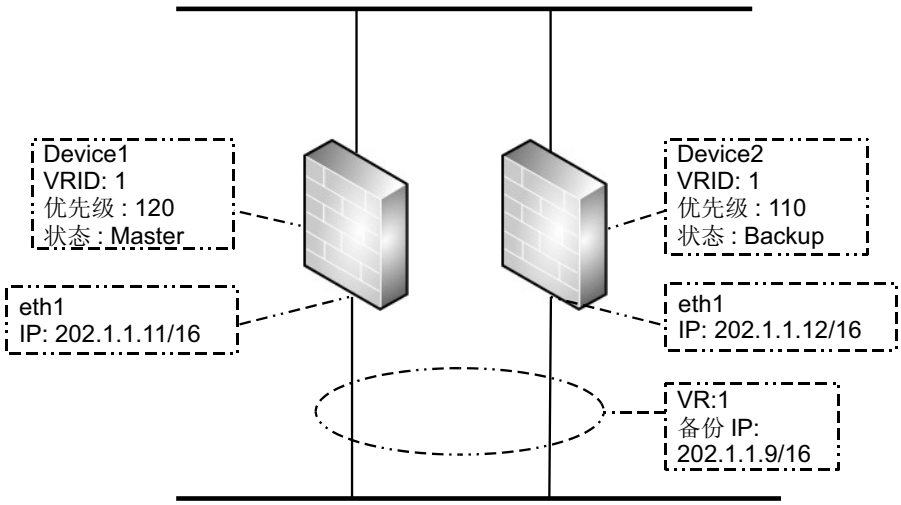
CLI

```
NetEye@root-system] cluster
NetEye@root-system-cluster] clusterid 1
NetEye@root-system-cluster] local interface eth3
NetEye@root-system-cluster] local ip address 1.1.1.2 mask
255.255.255.0
NetEye@root-system-cluster] peer ip address 1.1.1.1
NetEye@root-system-cluster] config sync auto enable
NetEye@root-system-cluster] rti sync enable
NetEye@root-system-cluster] time sync enable
NetEye@root-system-cluster] end
NetEye@root> save config
```

范例 2：主备选举

下例阐释虚拟路由器选举和主备设备角色确定的过程。

图 56 主备选举



- 2.1 配置缺省策略和接口
- 2.2 配置 VR
- 2.3 查看选举结果
- 2.4 故障切换
- 2.5 故障恢复

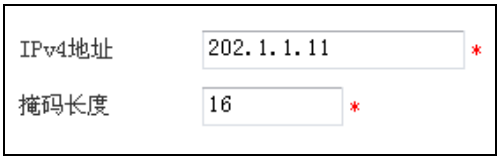
2.1 配置缺省策略和接口

Device1.

1. 选择**防火墙** > **缺省策略设置**。

2. 点击**确定**。
3. 选择**网络 > 接口**。
4. 在**接口列表中**点击 eth1 所对应的，进入到 eth1 的**编辑**页面。在 **IP 地址列表**中，点击**添加**。

提示：如果接口为二层工作模式，需要首先将其设置为三层工作模式，然后配置相应的 IP 地址。



5. 点击**确定**。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy default inter-zone access permit
NetEye@root-system] interface ethernet 1
NetEye@root-system-if-eth1] ip address 202.1.1.11 255.255.0.0
NetEye@root-system] exit
```

Device2.

6. 访问策略 = 允许
7. 在 **IP 地址列表**中，添加 eth1 202.1.1.12/16。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy default inter-zone access permit
NetEye@root-system] interface ethernet 1
NetEye@root-system-if-eth1] ip address 202.1.1.12 255.255.0.0
NetEye@root-system] exit
```

2.2 配置 VR

Device1.

1. 选择**系统** > **高可用性** > **虚拟路由器**。
2. 点击**新建**，进行如下配置 (通告周期和抢占模式采用默认值)。

3. 点击**确定**。
4. 点击 。

CLI

```
NetEye@root-system] virtual router 1
NetEye@root-system-vr1] priority 120
NetEye@root-system-vr1] backup ip address 202.1.1.9 mask 255.255.0.0
NetEye@root-system-vr1] election interface eth1
NetEye@root-system-vr1] virtual-router enable
NetEye@root-system-vr1] end
NetEye@root> save config
```

Device2.

5. 创建新的 VR。VRID=1，eth1，优先级 =110，通告周期 =1，抢占模式 = 启用，VR= 启用， 备份 IP=202.1.1.9/16。

CLI

```
NetEye@root-system] virtual router 1
NetEye@root-system-vr1] priority 110
NetEye@root-system-vr1] backup ip address 202.1.1.9 mask 255.255.0.0
NetEye@root-system-vr1] election interface eth1
NetEye@root-system-vr1] virtual-router enable
NetEye@root-system-vr1] end
```

2.3 查看选举结果

选举开始。

1. 选择**系统** > **高可用性** > **虚拟路由器**。
2. 查看 Device1 的状态。 Device1 具有更高的优先级，因此成为主设备。

```
NetEyc@root>show virtual-router all
VRID:           1
Enable:         on
Interface:      eth1
Interval:       1
Preempt:        Enable
Authentication: None
Backup ip:      202.1.1.9/16
State:          master
Detection Group:
Config Priority:        120
Election Priority:      120
Description:
```

3. 查看 Device2 的状态，为备份设备。

```
NetEyc@root>show virtual-router all
VRID:           1
Enable:         on
Interface:      eth1
Interval:       1
Preempt:        Enable
Authentication: None
Backup ip:      202.1.1.9/16
State:          backup
Detection Group:
Config Priority:        110
Election Priority:      110
Description:
```

如果优先级相同， Device2 将成为主设备，因为它的主 IP 地址 （202.1.1.12/16）大于 Device1 的主 IP （202.1.1.11/16）。关于主 IP 的更多信息，请参见 12.1.2.2 VR 选举。

2.4 故障切换

当 Device1 的 eth1 接口发生故障，将触发新的选举。

1. 选择**网络 > 接口**， eth1 接口显示为断开连接状态。

2. 选择**系统 > 高可用性 > 虚拟路由器**。
   在 WebUI 和 CLI 下查看主备状态， Device1 成为备份设备。

```
NetEyc@root>show virtual-router all
VRID:           1
Enable:         on
Interface:      eth1
Interval:       1
Preempt:        Enable
Authentication: None
Backup ip:      202.1.1.9/16
State:          backup
Detection Group:
Config Priority:        120
Election Priority:      120
Description:
```

3. Device2 成为主设备。

```
NetEye@root> show virtual-router all
VRID:           1
Enable:         on
Interface:      eth1
Interval:       1
Preempt:        Enable
Authentication: None
Backup ip:      202.1.1.9/16
State:          master
Detection Group:
Config Priority:        110
Election Priority:      110
Description:
```

初始配置的优先级（在 CLI 中显示为“配置优先级”）不发生变化。设备根据动态优先级（在 CLI 中显示为“选举优先级”）调整主备状态。

2.5 故障恢复

当 Device1 的 eth1 接口从故障恢复，将触发新的选举。查看设备的主备状态， Device1 恢复为主设备。 WebUI 和 CLI 显示与 2.3 查看选举结果相同。

提示：当两台设备初始优先级相同时，将不进行故障恢复。

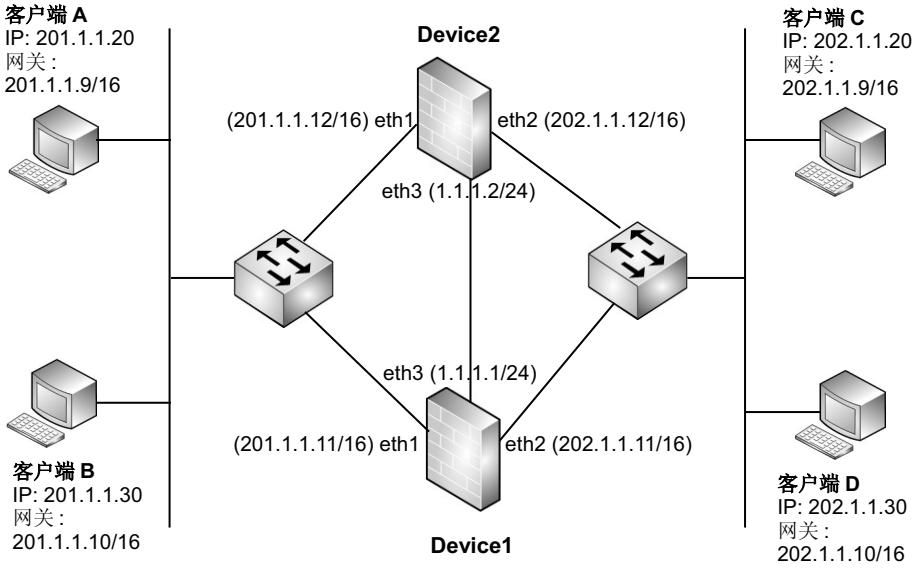
范例 3：负载分担 （主主模式）

在主主模式中，两台设备均为主设备，可同时处理数据流。在实现冗余功能的同时，也可实现流量的负载分担。

本范例需完成如下设置：

- 通过两个二层以太网接口连接 Device1 和 Device2 设备。
- 在两台设备上启用配置同步、运行信息同步和系统时间同步功能。
- 设置在设备每次启动时同步系统时间，并将 Device1 的时间设置为基准时间。
- 客户端 A 通过 Device1 访问客户端 C，客户端 B 通过 Device2 访问客户端 D。

图 57 主主模式



- 3.1 配置缺省策略和接口
- 3.2 配置 VR
- 3.3 配置 VRDG
- 3.4 配置集群

3.1 配置缺省策略和接口

Device1.

1. 访问策略 = 允许
2. 在 **IP 地址列表**中，添加 eth1 201.1.1.11/16 和 eth2 202.1.1.11/16。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy default inter-zone access permit
NetEye@root-system] interface ethernet 1
NetEye@root-system-if-eth1] ip address 201.1.1.11 255.255.0.0
NetEye@root-system] exit
NetEye@root-system] interface ethernet 2
NetEye@root-system-if-eth2] ip address 202.1.1.11 255.255.0.0
NetEye@root-system] exit
```

Device2.

3. 访问策略 **=** 允许
4. 在 **IP 地址列表**中，添加 eth1 201.1.1.12/16 和 eth2 202.1.1.12/16。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy default inter-zone access permit
NetEye@root-system] interface ethernet 1
NetEye@root-system-if-eth1] ip address 201.1.1.12 255.255.0.0
NetEye@root-system] exit
NetEye@root-system] interface ethernet 2
NetEye@root-system-if-eth2] ip address 202.1.1.12 255.255.0.0
NetEye@root-system] exit
```

3.2 配置 VR

Device1.

1. 创建新的 VR。VRID=1，eth1，优先级 =100，通告周期 =1，抢占模式 = 启用，VR= 启用，备份 IP=201.1.1.9/16。
2. 创建新的 VR。VRID=2，eth1，优先级 =100，通告周期 =1，抢占模式 = 启用，VR= 启用，备份 IP=201.1.1.10/16。
3. 创建新的 VR。VRID=3，eth2，优先级 =100，通告周期 =1，抢占模式 = 启用，VR= 启用，备份 IP=202.1.1.9/16。
4. 创建新的 VR。VRID=4，eth2，优先级 =100，通告周期 =1，抢占模式 = 启用，VR= 启用，备份 IP=202.1.1.10/16。

CLI

```
NetEye@root-system] virtual router 1
NetEye@root-system-vr1] backup ip address 201.1.1.9 mask 255.255.0.0
NetEye@root-system-vr1] election interface eth1
NetEye@root-system-vr1] virtual-router enable
NetEye@root-system-vr1] exit
NetEye@root-system] virtual router 2
NetEye@root-system-vr2] backup ip address 201.1.1.10 mask 255.255.0.0
NetEye@root-system-vr2] election interface eth1
NetEye@root-system-vr2] virtual-router enable
NetEye@root-system-vr2] exit
NetEye@root-system] virtual router 3
NetEye@root-system-vr3] backup ip address 202.1.1.9 mask 255.255.0.0
NetEye@root-system-vr3] election interface eth2
NetEye@root-system-vr3] virtual-router enable
NetEye@root-system-vr3] exit
NetEye@root-system] virtual router 4
NetEye@root-system-vr4] backup ip address 202.1.1.10 mask 255.255.0.0
NetEye@root-system-vr4] election interface eth2
NetEye@root-system-vr4] virtual-router enable
NetEye@root-system-vr4] exit
```

Device2.

配置与 Device1 完全相同。

5. 创建新的 VR。VRID=1，eth1，优先级 =100，通告周期 =1，抢占模式 = 启用，VR= 启用，备份 IP=201.1.1.9/16。
6. 创建新的 VR。VRID=2，eth1，优先级 =100，通告周期 =1，抢占模式 = 启用，VR= 启用，备份 IP=201.1.1.10/16。
7. 创建新的 VR。VRID=3，eth2，优先级 =100，通告周期 =1，抢占模式 = 启用，VR= 启用，备份 IP=202.1.1.9/16。
8. 创建新的 VR。VRID=4，eth2，优先级 =100，通告周期 =1，抢占模式 = 启用，VR= 启用，备份 IP=202.1.1.10/16。

CLI

```
NetEye@root-system] virtual router 1
NetEye@root-system-vr1] backup ip address 201.1.1.9 mask 255.255.0.0
NetEye@root-system-vr1] election interface eth1
NetEye@root-system-vr1] virtual-router enable
NetEye@root-system-vr1] exit
NetEye@root-system] virtual router 2
NetEye@root-system-vr2] backup ip address 201.1.1.10 mask 255.255.0.0
NetEye@root-system-vr2] election interface eth1
NetEye@root-system-vr2] virtual-router enable
NetEye@root-system-vr2] exit
NetEye@root-system] virtual router 3
NetEye@root-system-vr3] backup ip address 202.1.1.9 mask 255.255.0.0
NetEye@root-system-vr3] election interface eth2
NetEye@root-system-vr3] virtual-router enable
NetEye@root-system-vr3] exit
NetEye@root-system] virtual router 4
NetEye@root-system-vr4] backup ip address 202.1.1.10 mask 255.255.0.0
NetEye@root-system-vr4] election interface eth2
NetEye@root-system-vr4] virtual-router enable
NetEye@root-system-vr4] exit
```

3.3 配置 VRDG

Device1.

1. 创建新的 VRDG。组 ID=1，**优先级 =100**，通告周期 =1，抢占模式 = 启用，成员路由器为 VRID1 （权重 =10） +VRID3 （权重 =10）。
2. 创建新的 VRDG。组 ID=2，**优先级 =95**，通告周期 =1，抢占模式 = 启用，成员路由器为 VRID2 （权重 =10） +VRID4 （权重 =10）。

CLI

```
NetEye@root-system] detection group 1
NetEye@root-system-dg1] hold virtual-router 1 weight 10
NetEye@root-system-dg1] hold virtual-router 3 weight 10
NetEye@root-system-dg1] priority 100
NetEye@root-system-dg1] exit
NetEye@root-system] detection group 2
NetEye@root-system-dg2] hold virtual-router 2 weight 10
NetEye@root-system-dg2] hold virtual-router 4 weight 10
NetEye@root-system-dg2] priority 95
NetEye@root-system-dg2] exit
```

Device2.

3. 创建新的 VRDG。组 ID=1，**优先级 =95**，通告周期 =1，抢占模式 = 启用，成员路由器为 VRID1 （权重 =10） +VRID3 （权重 =10）。
4. 创建新的 VRDG。组 ID=2，**优先级 =100**，通告周期 =1，抢占模式 = 启用，成员路由器为 VRID2 （权重 =10） +VRID4 （权重 =10）。

CLI

```
NetEye@root-system] detection group 1
NetEye@root-system-dg1] hold virtual-router 1 weight 10
NetEye@root-system-dg1] hold virtual-router 3 weight 10
NetEye@root-system-dg1] priority 95
NetEye@root-system-dg1] exit
NetEye@root-system] detection group 2
NetEye@root-system-dg2] hold virtual-router 2 weight 10
NetEye@root-system-dg2] hold virtual-router 4 weight 10
NetEye@root-system-dg2] priority 100
NetEye@root-system-dg2] exit
```

3.4 配置集群

Device1.

1. 创建集群。接口 =eth3，本端 IP=1.1.1.1/24，对端 IP=1.1.1.2，集群 ID=1.
2. 配置同步。
   a. 点击**立即同步**。
   b. 开启**自动同步配置信息 / 运行信息**。
   c. 开启**自动同步系统时间**。
      - 勾选**当设备启动时**。
      - 勾选**将此时间设置应用到两端设备**。

CLI

```
NetEye@root-system] cluster
NetEye@root-system-cluster] clusterid 1
NetEye@root-system-cluster] local interface eth3
NetEye@root-system-cluster] local ip address 1.1.1.1 mask
255.255.255.0
NetEye@root-system-cluster] peer ip address 1.1.1.2
NetEye@root-system-cluster] config sync
NetEye@root-system-cluster] config sync auto enable
NetEye@root-system-cluster] rti sync enable
NetEye@root-system-cluster] time sync enable
NetEye@root-system-cluster] time boot on
NetEye@root-system-cluster] time benchmark on
NetEye@root-system-cluster] end
NetEye@root> save config
```

Device2.

3. 创建集群。接口 =eth3，本端 IP=1.1.1.2/24，对端 IP=1.1.1.1，集群 ID=1.
4. 配置同步。
   a. 开启**自动同步配置信息 / 运行信息 / 系统时间**。
   b. 勾选**当设备启动时**。

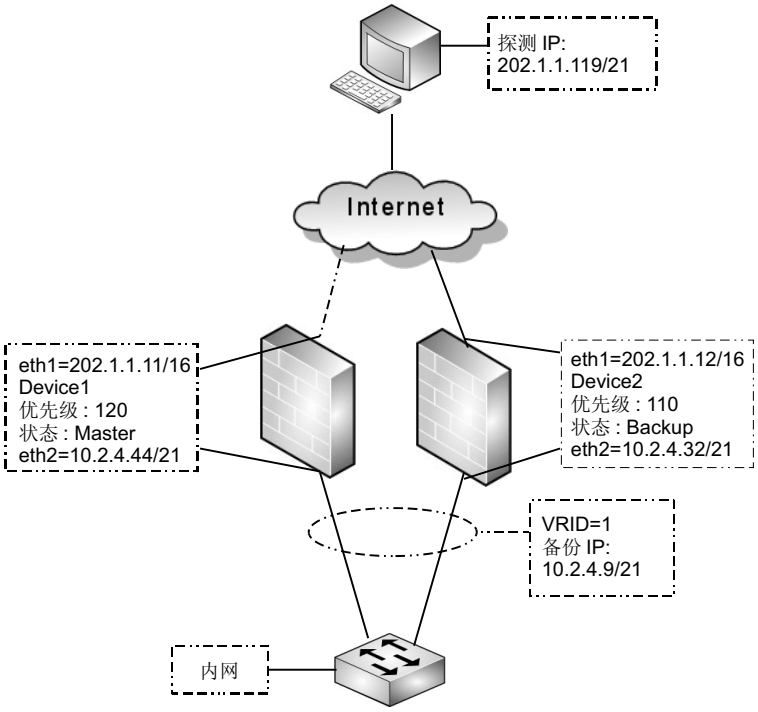
CLI

```
NetEye@root-system] cluster
NetEye@root-system-cluster] clusterid 1
NetEye@root-system-cluster] local interface eth3
NetEye@root-system-cluster] local ip address 1.1.1.2 mask
255.255.255.0
NetEye@root-system-cluster] peer ip address 1.1.1.1
NetEye@root-system-cluster] config sync auto enable
NetEye@root-system-cluster] rti sync enable
NetEye@root-system-cluster] time sync enable
NetEye@root-system-cluster] time boot on
NetEye@root-system-cluster] end
NetEye@root> save config
```

范例 4：IP 探测

IP 探测用于虚拟路由器探测外部链路是否可达，探测结果影响虚拟路由器的优先级，并可能触发切换。下列示例阐释了 VR 的 IP 探测如何用于检测外网链路的连通性。

图 58 IP 探测



在上述场景中，在两个内网接口 （eth2）上创建了一个虚拟路由器 （VRID=1），Device1 为主设备。当 Device1 到目的主机 (202.1.1.119) 之间的链路发生故障时，外网流量流经 Device2，而内网流量依旧被发送到 Device1，致使流量中断。

此时，在两台设备上配置 IP 探测，通过动态监视从 eth1 到指定 IP 地址 (202.1.1.119) 的链路状况，解决这个问题。

- Device1 每隔 4 秒发送 Ping 探测包，当 IP 探测连续失败的次数到达了 5 次，Device1 将从自身优先级中减去权重值 （15）， Device2 就会成为主设备。
- 若 Device1 的故障链路恢复正常，它将恢复原始优先级 （120），重新成为主设备。

本范例需完成如下设置：

- 4.1 配置缺省策略和接口
- 4.2 配置 VR 和 IP 探测
- 4.3 查看探测状态
- 4.4 探测故障 （Device1）
- 4.5 故障恢复

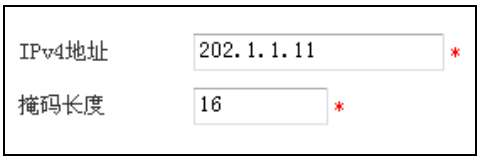
4.1 配置缺省策略和接口

Device1.

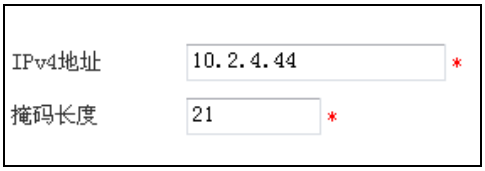
1. 选择**防火墙 > 缺省策略设置**。

2. 点击**确定**。
3. 选择**网络 > 接口**。
4. 在**接口列表**中点击 eth1 所对应的，进入到 eth1 的**编辑**页面。在 **IP 地址列表**中，点击**添加**。

提示：如果接口为二层工作模式，需要首先将其设置为三层工作模式，然后配置相应的 IP 地址。



5. 在**接口列表**中点击 eth2 所对应的，进入到 eth2 的**编辑**页面。在 **IP 地址列表**中，点击**添加**。



6. 点击**确定**。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy default inter-zone access permit
NetEye@root-system] interface ethernet 1
NetEye@root-system-if-eth1] ip address 202.1.1.11 255.255.0.0
NetEye@root-system] exit
NetEye@root-system] interface ethernet 2
NetEye@root-system-if-eth2] ip address 10.2.4.44 255.255.248.0
NetEye@root-system] exit
```

Device2.

7. 访问策略 = 允许
8. 在 **IP 地址列表**中，添加 eth1 202.1.1.12/16 和 eth2 10.2.4.32/21。

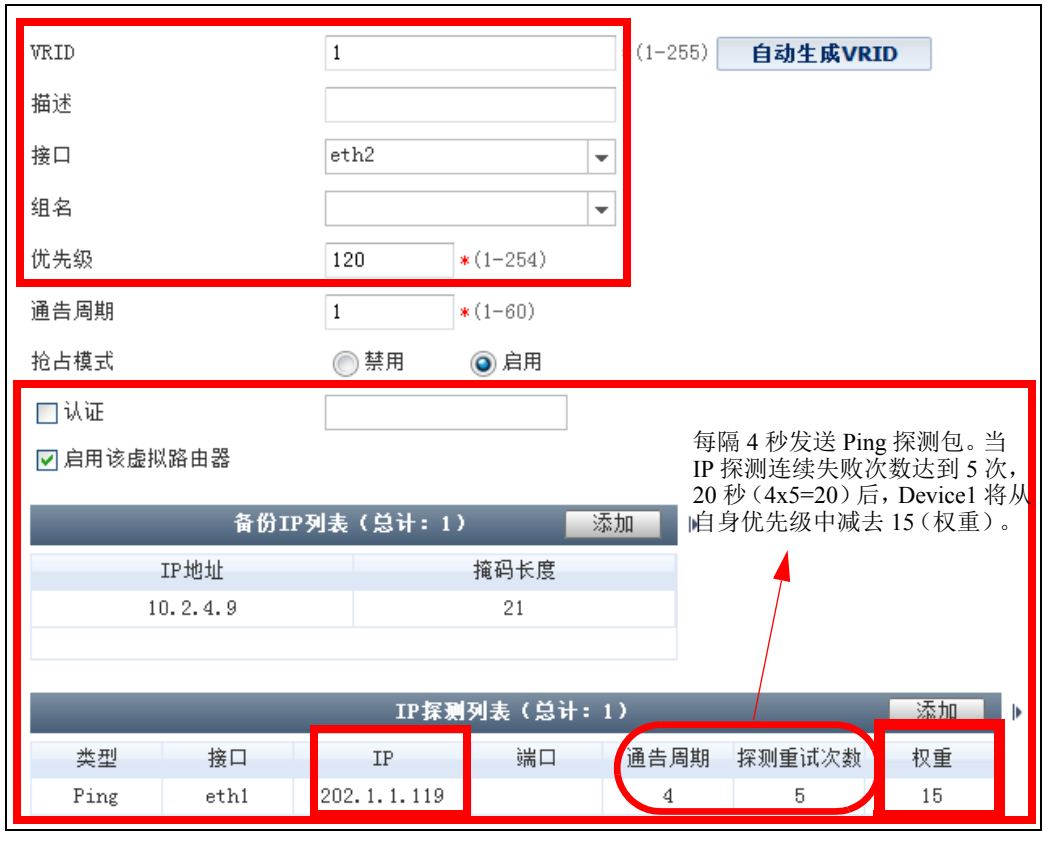
CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy default inter-zone access permit
NetEye@root-system] interface ethernet 1
NetEye@root-system-if-eth1] ip address 202.1.1.12 255.255.0.0
NetEye@root-system] exit
NetEye@root-system] interface ethernet 2
NetEye@root-system-if-eth2] ip address 10.2.4.32 255.255.248.0
NetEye@root-system] exit
```

4.2 配置 VR 和 IP 探测

Device1.

1. 选择**系统** > **高可用性** > **虚拟路由器**。
2. 点击**新建**，进行如下配置 (通告周期、抢占模式和认证采用默认值)。



- 在两台主备设备上配置的到某一目的的 IP 探测设置应该具有相同的 IP 地址。

- 为确保发生故障时进行切换，需要启用抢占模式，每个 VR 的权重值应该大于 VR 的优先级之差。

3. 点击**确定**。
4. 点击 。

CLI

```
NetEye@root-system] virtual router 1
NetEye@root-system] priority 120
NetEye@root-system-vr1] backup ip address 10.2.4.9 mask 255.255.248.0
NetEye@root-system-vr1] election interface eth2
NetEye@root-system-vr1] virtual-router enable
NetEye@root-system-vr1] ip-track type ping interface eth1 ip
202.1.1.119 interval 4 threshold 5 weight 15
NetEye@root-system-vr1] end
NetEye@root> save config
```

Device2.

5. 创建新的 VR。VRID=1，eth2，优先级 =110，通告周期 =1，抢占模式 = 启用，VR= 启用，备份 IP=10.2.4.9/21 ； IP 探测类型 =Ping，探测接口 =eth1，探测 IP=202.1.1.119，探测周期 =5，阈值 =6，权重 =20。

CLI

```
NetEye@root-system] virtual router 1
NetEye@root-system] priority 110
NetEye@root-system-vr1] backup ip address 10.2.4.9 mask 255.255.248.0
NetEye@root-system-vr1] election interface eth2
NetEye@root-system-vr1] virtual-router enable
NetEye@root-system-vr1] ip-track type ping interface eth1 ip
202.1.1.119 interval 5 threshold 6 weight 20
NetEye@root-system-vr1] end
```

4.3 查看探测状态

1. 选择**监控 > 高可用性 > 虚拟路由器**。
2. 查看主备状态， Device1 成为主设备。

4.4 探测故障 （Device1）

当 Device1 到 202.1.1.119 的 IP 探测在 20 秒内连续探测失败达到 5 次 （间隔为 4 秒，4x5=20），其 VR 优先级 （120）将减去探测权重 （15），优先级变为 105。 Device2 将转变为主设备。

1. 选择**监控 > 高可用性 > 虚拟路由器**。
2. 在 WebUI 和 CLI 下查看 Device1 的状态。

```
NetEye@root> show virtual-router 1
VRID:            1
Enable:          on
Interface:       eth2
Interval:        1
Preempt:         Enable
Authentication:  0
Backup ip:       10.2.4.9/21
State:           backup
Detection Group:
Config Priority:         120
Election Priority:       105
Description:

Type      Interface IP                Port      Interval  Threshold Weight
Ping      eth1      202.1.1.119       -         4         5         15
```

4.5 故障恢复

当 Device1 的 IP 探测从故障恢复时， VR 将在当前的选举优先级 （105）基础上加上探测权重 （15），从而恢复其原始的配置优先级 （120）。

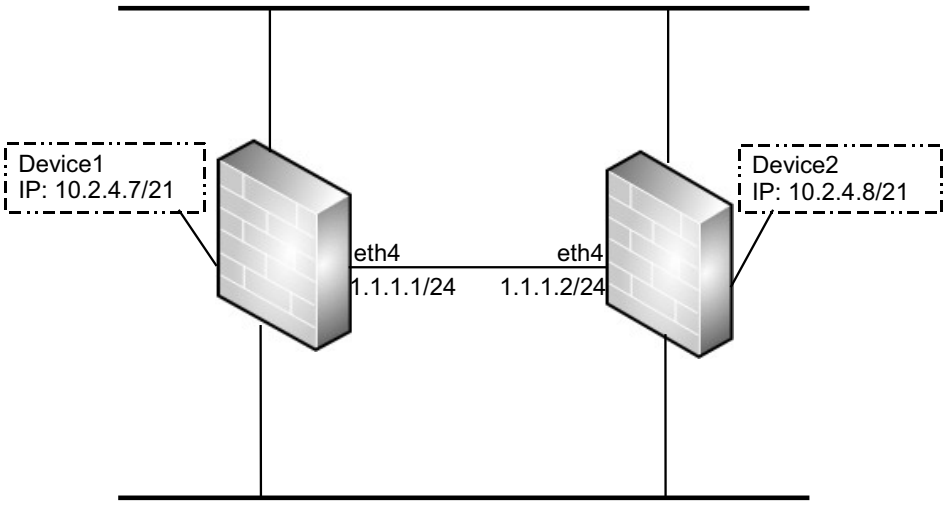
1. 选择**监控 > 高可用性 > 虚拟路由器**。
2. 查看状态， Device1 恢复为主设备。

范例 5：集群同步

NISG 提供集群同步的功能。对两台 NISG 设备执行同步，无需 VR 配置。

下图展示了集群同步的基本范例，无任何 VR 配置。

图 59 同步



提示：同一集群中的两台 NISG 设备最好具有相同的硬件型号和系统版本。

- Device1 配置了 DNS 信息。
  - DNS 主机：首选 DNS=192.2.2.22，备选 DNS1=202.2.2.234
  - DNS 代理：域名 =abc，接口 =any, 首选 DNS=192.123.23.23
  - 静态缓存：状态 = 启用，域名 =abc，接口 =any， IP 地址 =192.168.2.4
- 用户需要手动执行从 Device1 到 Device2 的整体同步，以保证两端设备配置一致。
- 修改任意一端设备上的配置时，会彼此进行同步。
- 将 Device1 设置为时间基准，当该设备启动时，其系统时间将同步到另外一端设备。

本范例需完成如下设置：

- 5.1 配置集群
- 5.2 查看本地和对端设备的差异
- 5.3 手动同步配置
- 5.4 自动同步配置
- 5.5 同步系统时间

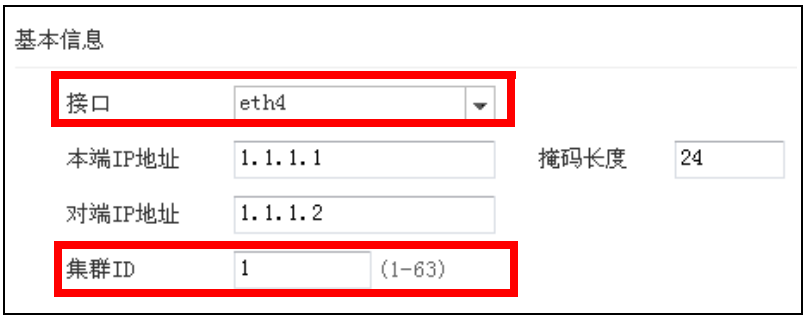
5.1 配置集群

- Device1. 缺省策略，集群
- Device2. 缺省策略，集群

Device1. 缺省策略，集群

1. 选择**防火墙 > 缺省策略设置**。

2. 点击**确定**。
3. 选择**系统 > 高可用性 > 集群**。
4. 配置如下信息。



   - 同步接口应该为二层以太网接口或以太网通道。建议使用二层以太网接口同步配置信息，二层以太网通道同步运行信息。
   - 本端和对端设备应该具有相同的集群 ID。

5. 点击**确定**。
6. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy default inter-zone access permit
NetEye@root-system] cluster
NetEye@root-system-cluster] clusterid 1
NetEye@root-system-cluster] local interface eth4
NetEye@root-system-cluster] local ip address 1.1.1.1 mask
255.255.255.0
NetEye@root-system-cluster] peer ip address 1.1.1.2
NetEye@root-system-cluster] end
NetEye@root> save config
```

Device2. 缺省策略，集群

配置同 Device1。

7. 访问策略 = 允许
8. 接口 =eth4，本端 IP 地址 =1.1.1.2/24，对端 IP 地址 =1.1.1.1/24，集群 ID=1。

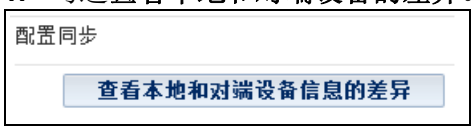
CLI

```
NetEye@root> configure mode override
NetEye@root-system] policy default inter-zone access permit
NetEye@root-system] cluster
NetEye@root-system-cluster] clusterid 1
NetEye@root-system-cluster] local interface eth4
NetEye@root-system-cluster] local ip address 1.1.1.2 mask
255.255.255.0
NetEye@root-system-cluster] peer ip address 1.1.1.1
NetEye@root-system-cluster] end
NetEye@root> save config
```

5.2 查看本地和对端设备的差异

在进行同步前，通过 Device1 查看两端设备的差异。

1. 勾选**查看本地和对端设备的差异**。



2. 查看差别。减号 （-）代表本地设备 （Device1），加号 （+）代表对端设备（Device2）。

CLI

在集群配置模式下，运行 **config check** 命令，查看设备差异。

```
 [dns]

-dns host 192.2.2.22 primary
-dns host 202.2.2.234 secondary

 [dns-proxy]

-dns server-select abc output-interface Any primary 192.123.23.23

 [dns-cache]

-dns cache abc 192.168.2.4 input-interface Any
-dns cache-state on
+dns cache-state off
```

5.3 手动同步配置

- Device1. 执行手动同步
- Device2. 查看同步

Device1. 执行手动同步

1. 选择**系统 > 高可用性 > 集群**。
2. 点击**立即同步**，将 Device1 上的配置同步到 Device2。

建议在进行自动同步前，执行整体的手动同步功能， Device1 的配置信息将覆盖 Device2 的配置。

3. 点击**确定**。

CLI

```
NetEye@root-system] cluster
NetEye@root-system-cluster] cluster 1
NetEye@root-system-cluster] config sync
```

Device2. 查看同步

4. 选择**网络 >DNS**，查看已经同步的 DNS 信息。

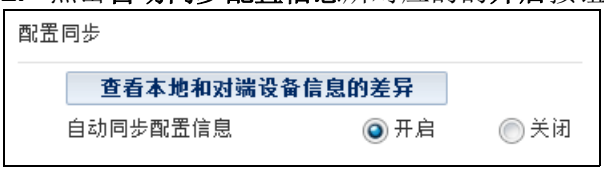
如果从 Device2 手动同步信息到 Device1， Device2 的配置将覆盖 Device1。由于 Device2 最初没有任何 DNS 设置， Device1 的 DNS 信息将被清除。

5.4 自动同步配置

- Device1. 执行自动同步
- Device2. 查看同步

Device1. 执行自动同步

1. 选择**系统 > 高可用性 > 集群**。
2. 点击**自动同步配置信息**所对应的的**开启**按钮。



   - Device1 将其设备上可同步的配置自动同步到 Device2 上，即使 Device2 禁用了自动同步功能。
   - 如果两端设备均开启了自动同步，则互相同步当前的可同步配置信息。

3. 点击**确定**。
4. 选择**网络 > 安全域**，配置安全域。

5. 点击**确定**。

CLI

```
NetEye@root-system] cluster
NetEye@root-system-cluster] cluster 1
NetEye@root-system-cluster] config sync auto enable
```

Device2. 查看同步

6. 选择**网络 > 安全域**，查看安全域信息。

由于接口配置 （隧道接口除外）不可同步，同步过来的 zone2 默认基于三层接口。更多不可同步的配置信息，参见 12.1.5.2 集群同步信息。

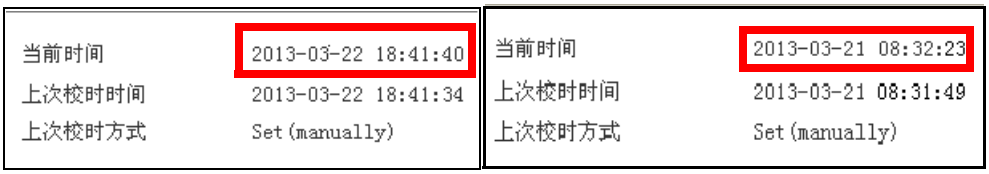
提示：在 CLI 下，使用 **show zone** 命令查看安全域。

5.5 同步系统时间

- Device1, Device2. 查看系统时间
- Device1. 同步时间到 Device2
- Device1, Device2. 查看同步

Device1, Device2. 查看系统时间

1. 选择**系统 > 维护 > 日期时间**。



提示：在 CLI 下，使用 **show system time** 命令查看系统时间。

Device1. 同步时间到 Device2

2. 选择**系统 > 高可用性 > 集群**。
3. 启用系统时间自动同步，将 Device1 设置为同步的基准时间。

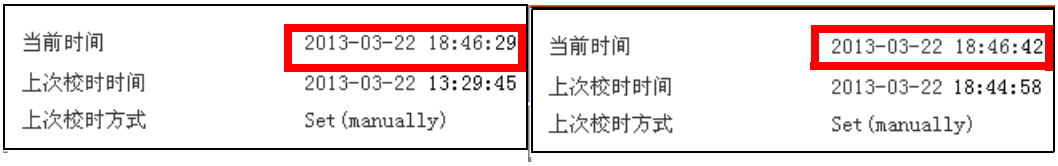
   - 当 Device1 启动时，它会将自身系统时间自动同步到 Device2 上，即使 Device2 上禁用了时间同步功能。 Device2 将进行时间同步。
   - 只能将一台设备设置为基准时间。
4. 点击**确定**。

CLI

```
NetEye@root-system] cluster
NetEye@root-system-cluster] cluster 1
NetEye@root-system-cluster] time sync enable
NetEye@root-system-cluster] time boot on
NetEye@root-system-cluster] time benchmark on
NetEye@root-system-cluster] end
NetEye@root> save config
```

5. 选择**系统 > 维护 > 日期时间**，查看两端设备的系统时间，可以看到它们的日期和时间基本一致。

Device1, Device2. 查看同步



12.4 配置参数说明

本节介绍以下配置参数信息：

- 12.4.1 虚拟路由器
- 12.4.2 虚拟路由器探测组
- 12.4.3 集群

12.4.1 虚拟路由器

管理员可以在根系统和 Vsys 中配置 VR。

- VR 退出探测组后，该 VR 的优先级、通告周期和抢占模式将恢复到原有的配置。
- 当 VR 未配置任何选举接口或备份 IP 时，它将一直处于 Backup 状态；加入到 VRDG 后，整个 VRDG 的优先级将减去该 VR 的权重。

表 262 VR 的配置信息

配置信息	说明
VRID	虚拟路由器的唯一标识，取值范围是 1 ～ 255 的整数。 管理员也可以点击旁边的**自动生成 VRID** 按钮，由系统自动生成一个唯一的 VRID 值。
描述	虚拟路由器的描述信息，为 0 ～ 255 字节 UTF-8 字符，不包含：?'\"<>&。
接口	指虚拟路由器的选举接口，包括三层和三层共享以太网接口、三层和三层共享以太网通道、VLAN 接口。其中，三层共享接口应用在 Vsys 中。
组名	指虚拟路由器所属的探测组的 ID。
优先级	虚拟路由器的优先级。取值范围是 1 ～ 254 的整数，缺省为 100。
通告周期	指虚拟路由器中的主设备发送报文的时间间隔。同一虚拟路由器中的 VRRP 路由器，其通告周期必须相同。 通告周期取值范围为 1 ～ 60，单位秒，缺省为 1 秒。
抢占模式	指拥有较高优先级的备份设备是否抢占当前低优先级的主设备而成为新的主设备。IP 地址所有者永远处于抢占模式。 该功能缺省为启用。
认证	指对虚拟路由器内成员之间 VRRP 报文和通讯数据采用简单的明文方式的认证。 认证信息为 1-8 字节 UTF-8 字符，不包含问号和空格。 两台成员设备之间需要配置相同的认证信息。 该功能缺省为禁用。
启用该虚拟路由器	当前 NISG 设备参与该虚拟路由器的选举过程。 该功能缺省为禁用。
备份 IP 地址	指虚拟路由器所备份的 IP 地址，可以是一个或多个。一个虚拟路由器最多支持 255 个备份 IP 地址。 正被 VPN 隧道引用的备份 IP 地址及其对应的虚拟路由器不可以被删除。

表 262 VR 的配置信息 (*续*)

配置信息	说明
IP 探测	探测某个 IP 地址是否可达。管理员需指定以下配置选项： • **类型**：探测探测，包括： **•ARP Ping**：向处于同一个局域网的主机发送 ARP 请求。 **•Ping**：向目的 IP 地址发送 ICMP 回送 （Echo）请求，并监听 ICMP 应答 （Reply）报文。 **•TCP Ping**：使用 TCP 协议探测 IP 地址。 • **接口**：指定用哪个接口发送探测报文进行 IP 探测。管理员可以选择： **•Any—** 表示通过查询路由决定探测所使用的接口。 • **指定接口 —** 任何三层或三层共享以太网接口、三层或三层共享以太网通道、 VLAN 接口。 **•IP 地址**：要探测的目的 IP 地址，即探测此 IP 地址是否可达。 • **探测端口**：使用 TCP Ping 方式需要指明探测端口，取值范围为 1 ～ 65535。 • **探测周期**：指定每隔多久发一个探测报文。取值范围为 1 ～ 30000 秒，缺省为 3 秒。 • **探测重试次数**：指定连续重试的次数。超过该值就认为发生了故障。取值范围为 1 ～ 999，缺省为 3。 • **权重**：当 IP 探测失败后，虚拟路由器的优先级将减去该权重。取值范围为 1 ～ 254 之间的整数，缺省为 5。
状态	指 NISG 设备在虚拟路由器中的状态。分为三种：Initialize、 Master、 Backup。

12.4.2 虚拟路由器探测组

管理员可以在根系统和 Vsys 中配置 VRDG。

表 263 VRDG 的配置信息

配置信息	说明
组 ID	标识虚拟路由器探测组。取值范围是 1 ～ 255 的整数。
描述	虚拟路由器探测组的描述信息，为 0 ～ 255 个字节的 UTF-8 字符。不包含：?'\"<>&。
优先级	探测组的优先级。取值范围是 1 ～ 254 的整数，缺省为 100。
通告周期	虚拟路由器探测组发送报文的时间间隔。取值范围为 1 ～ 60 秒，缺省为 1 秒。
抢占模式	表示高优先级的探测组是否抢占低优先级的探测组。该功能缺省为启用。
成员	指该探测组中所包含的虚拟路由器，一个虚拟路由器只能加入一个探测组。
权重	当 IP 探测失败后，探测组的优先级将减去该虚拟路由器权重。取值范围是 1 ～ 254 的整数，缺省为 5。
IP 探测	探测某个 IP 地址是否可达。虚拟路由器探测组的 IP 探测功能与虚拟路由器相同。 更多信息，请见表 262。
状态	探测组内虚拟路由器成员的状态，包括三种：Initialize、 Master、 Backup。

12.4.3 集群

管理员只能在根系统中配置集群。

表 264 集群的配置信息

配置信息	说明
接口	HA 接口，即同步数据使用的接口。可以是任何一个未被使用的二层以太网接口和二层以太网通道。
本端 IP 地址	本端同步接口的 IP 地址及相应的掩码长度。
对端 IP 地址	对端同步接口的 IP 地址。
集群 ID	标识所属的集群。 ID 范围：1 ～ 63。 集群成员必须具有相同的集群 ID。
配置同步	手动或自动同步配置信息，使集群内各成员配置保持一致。 在执行配置同步前，管理员可以点击**查看本地和对端设备信息的差异**按钮，查看两端配置信息的差异。 该功能默认禁用。
运行信息同步	自动同步运行信息，使集群内各成员运行信息保持一致。开启后，可以勾选**自定义会话信息**复选框，对要同步的会话信息进行自定义设置。 该功能默认禁用。
系统时间同步	同步系统时间，使集群内所有成员的时间保持一致。该功能默认禁用。
加密	对集群中的同步数据进行加密。两端设备都需要配置相同的加密密码。 密码为 1-255 字节的 UTF-8 字符，不包含问号和空格。 该功能默认禁用。
认证	验证集群中本端和对端设备的身份。两端设备都需要配置相同的认证密码。 密码为 1-255 字节的 UTF-8 字符，不包含问号和空格。 该功能默认禁用。

13 虚拟系统

本章介绍虚拟系统相关功能，内容包括：

- 13.1. 概述，描述虚拟系统和虚拟网络相关的概念和工作原理。
- 13.2. 基本配置步骤，描述 WebUI 配置步骤，用户场景不一定需要配置所有步骤。
- 13.3. 场景，描述实际应用场景和解决方案。
- 13.4. 范例，给出步骤描述详细的范例。
- 13.5. 配置参数说明，详细解释虚拟系统相关的配置参数。

13.1. 概述

NISG 初始是一个单独的系统，我们将它称为根系统。一台 NISG 设备可以被逻辑地划分成多个虚拟设备，每个虚拟设备拥有自己的管理员、审计员、策略、用户认证数据库等。这些虚拟设备即被称为虚拟系统 (Virtual System， Vsys)。一台 NISG 设备可以被划分成多个虚拟系统，虚拟系统最大数目由 License 决定。NISG 还支持虚拟网络 （Virtual Network），通过虚拟接口 （见 4.5 虚拟接口）连接多个虚拟系统。

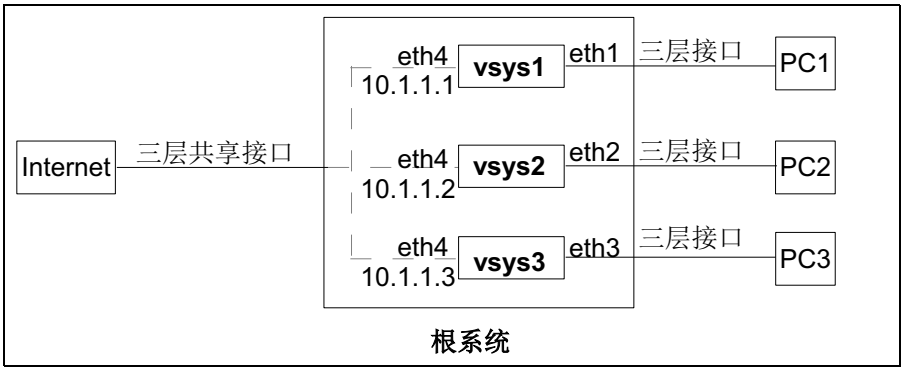
本节包含以下内容：

- 13.1.1. 虚拟系统 （Vsys）
- 13.1.2. 虚拟网络 （Vnet）

13.1.1. 虚拟系统 （Vsys）

下图演示了 Vsys 的基本用途。

图 60 Vsys



有以下需求时使用虚拟系统：

- 独立的管理员

  Vsys 管理员由根系统管理员创建和管理。Vsys 管理员不能改变虚拟系统的网络拓扑，也没有修改接口工作模式的权限。关于 Vsys 管理员的详细信息，请参见 3.13 管理用户。

- 独立的安全配置

  每个虚拟系统可以有自己的攻击防御、策略、 UTM 和其他安全配置， UTM 功能包括防病毒、反垃圾邮件、 IPS、 URL 过滤和应用控制。

- 最大资源限制

  NISG 的会话资源和规则资源 （包括 ARP 和 CAM 表）对于所有 Vsys 来说是共享的，规则资源指策略、路由、 NAT 规则和防护配置等。会话资源和规则资源将按照实际需要，由系统动态地分配给每个 Vsys，从而保证资源需求尽可能地得到满足。

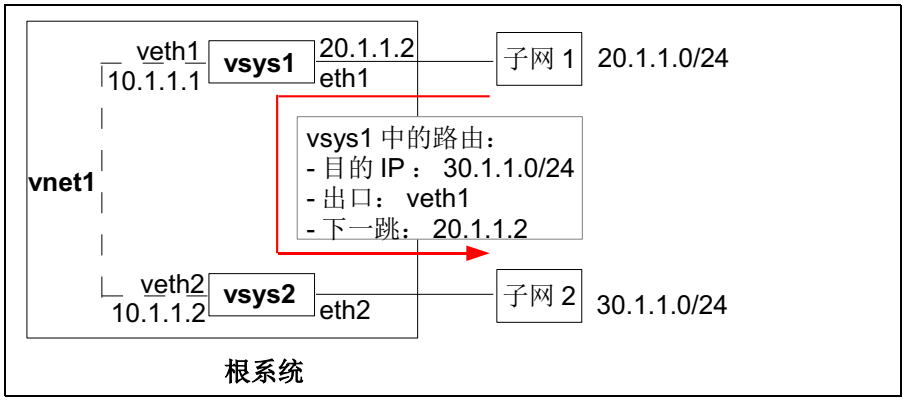
- 独立的管理 IP/ 接口

  管理 IP 是虚拟系统的一个三层接口 IP， Vsys 管理员可以通过管理 IP 来远程管理 NISG 虚拟系统。该管理 IP 可以与根系统或其他 Vsys 的管理 IP 相同 （三层共享接口充当管理接口的情况除外）。

13.1.2. 虚拟网络 （Vnet）

下图演示了虚拟网络的基本用途。

图 61 Vnet



- 虚拟接口
  - 二层虚拟接口可以划分到 VLAN 接口中，这些 VLAN 接口再划分到虚拟系统中。
  - 三层虚拟接口可以直接划分到虚拟系统中。
  - 一个虚拟接口只能被划分给一个虚拟系统。
- 虚拟网络

  通过虚拟接口相连的多个虚拟系统组成一个虚拟网络 （Virtual Network）。从一个虚拟接口上发出的数据包，会被该虚拟网络的其他虚拟接口收到。

13.2. 基本配置步骤

本节介绍虚拟系统的基本配置流程：

- 13.2.1. 创建三层接口
- 13.2.2. 创建虚拟系统 （资源限制 / 接口 / 管理 IP/UTM）
- 13.2.3. 创建虚拟系统管理员
- 13.2.4. 登录 / 切换虚拟系统
- 13.2.5. 管理虚拟系统
- 13.2.6. 创建虚拟网络

13.2.1. 创建三层接口

1. 选择**网络 > 接口**。

2. 将已有的二层接口设置为三层或三层共享接口，或创建新的三层或三层共享接口。

- 如果三层接口被划分到虚拟系统中：
  - 接口的MAC地址、MTU值以及IP地址等信息只能在虚拟系统中进行设置，在根系统下无法查看。
  - 三层接口所绑定的二层接口在虚拟系统下将无法修改，而只能在根系统下修改。
- 如果一个三层共享接口被划分到不同的虚拟系统，其 IP 地址不能相同，但可以是同一网段的 IP 地址。

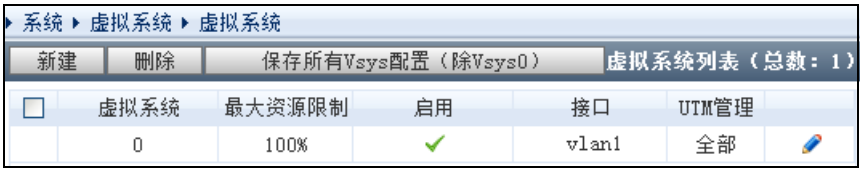
表 265 接口命令

interface ethernet	进入以太网接口配置模式。
working-type layer3-shared-interface	设置接口为三层共享工作模式。
channel	进入以太网通道配置模式。
hold ethernet	添加二层接口到以太网通道。

更多信息请参见*东软集成安全网关软件 V4.2 命令参考手册*中的**网络配置命令**章节。

13.2.2. 创建虚拟系统 （资源限制 / 接口 / 管理 IP/UTM）

1. 选择**系统 > 虚拟系统 > 虚拟系统**。



系统默认存在一个编号为 0 的虚拟系统，即根系统。默认情况下，根系统是启用状态，最大资源限制是 100%（表示根系统最多可占用 100% 的系统资源），包含所有三层接口， UTM 功能全部开启。

2. 创建虚拟系统，指定以下内容：

3. 点击**确定**。

表 266 虚拟系统命令

show vsys [*vsys_id* | **root**]	查看虚拟系统信息。
vsys *vsys_id* **resource-limit** *num*	创建虚拟系统。
unset vsys [*vsys_id*]	删除指定虚拟系统或所有虚拟系统。
vsys *vsys_id* **enable**	启用指定的虚拟系统。
vsys *vsys_id* **disable**	禁用指定的虚拟系统。
hold	添加以太网接口、以太网通道、 VLAN 接口、荣誉接口、虚拟接口和 PPPoE 接口到指定虚拟系统。
unset hold	将以太网接口、以太网通道、 VLAN 接口、荣誉接口、虚拟接口和 PPPoE 接口从指定虚拟系统中删除。
vsys *vsys_id* **resource-limit** *num*	修改虚拟系统资源限制。
manage-ip-address	为指定虚拟系统设置管理 IPv4 地址。
manage-ipv6-address	为指定虚拟系统设置管理 IPv6 地址。
save all-vsys-config	保存除根系统外的所有虚拟系统的配置信息。
switch vsys *vsys_name*	切换虚拟系统。

13.2.3. 创建虚拟系统管理员

根系统管理员可以创建虚拟系统并管理虚拟系统资源。

1. 点击**管理用户**超链接或选择**系统 > 认证 > 管理用户**。

2. 为虚拟系统创建虚拟系统管理员，点击**确定**：

3. 将虚拟系统划分给已有的根系统管理员或虚拟系统管理员。一个根系统管理员可以管理多个虚拟系统。

4. 点击**确定**。

表 267 虚拟系统管理员命令

user administrator *user_name* **vsys-administrator vsys**	为指定虚拟系统创建虚拟系统管理员。
unset user administrator *user_name*	删除虚拟系统管理员。
user administrator *user_name* **allowed-vsys** *vsys_name*	为指定根系统管理员或虚拟系统管理员添加虚拟系统管理权限。
unset user administrator *user_name* **allowed-vsys** *vsys_name*	删除指定根系统管理员或虚拟系统管理员的虚拟系统管理权限。

表 267 虚拟系统管理员命令 (*续*)

show user administrator [*user_name*]	显示当前虚拟系统的所有管理员信息。
show line	显示当前虚拟系统的所有在线管理员信息。

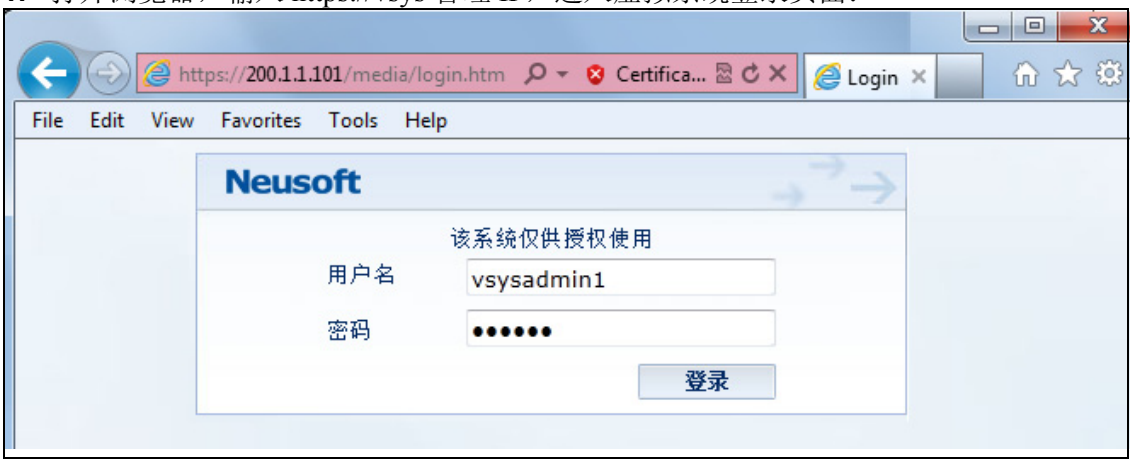
13.2.4. 登录 / 切换虚拟系统

以下步骤包括：

1. 通过管理 IP 登录虚拟系统
2. 通过 CLI 登录虚拟系统
3. 通过 WebUI 切换虚拟系统

通过管理 IP 登录虚拟系统：

1. 打开浏览器，输入 https://vsys 管理 IP，进入虚拟系统登录页面：



2. 输入用户名和密码登录虚拟系统：

通过 CLI 登录虚拟系统：

上面两个操作步骤没有对应的命令，但是如果虚拟系统已经划分给根系统管理员管理，根系统管理员可以通过命令行控制台进行以下操作达到相同目的：

a. 退出根系统。

b. 输入虚拟系统名称，按 Enter 键。

c. 输入用户名和密码登录虚拟系统。

通过 WebUI 切换虚拟系统：

1. 要切换虚拟系统，点**虚拟系统**查看页面底端的**切换虚拟系统**链接。

2. 点击对应的按钮。

提示：根系统管理员可以在根系统和授权虚拟系统之间进行切换。虚拟系统管理员只能在授权虚拟系统之间进行切换。

表 268 虚拟系统切换命令

switch vsys *vsys_name*	切换虚拟系统。

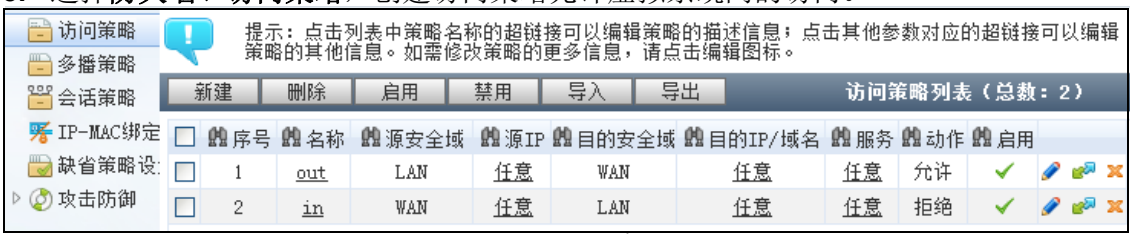
13.2.5. 管理虚拟系统

以下是管理虚拟系统最常见的步骤。

1. 选择**网络 > 接口**，并设置虚拟系统间通讯用的接口 IP 地址：

2. 选择**网络 > 安全域**，创建安全域。

3. 选择**防火墙 > 访问策略**，创建访问策略允许虚拟系统间的访问。



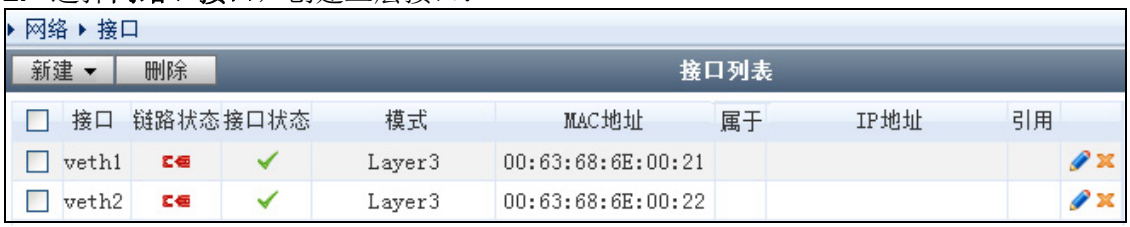
4. 自定义虚拟系统中的功能。更多信息请参见 13.5.3. 虚拟系统中可配置的功能。
   - 只能在根系统下进行的配置：
     - UTM 防病毒、反垃圾邮件和 IPS 的防护配置。
     - UTM 防病毒、反垃圾邮件、攻击签名、 URL 过滤规则和应用知识库升级。
   - 每 Vsys 配置：
     - URL 过滤和应用控制的防护配置。
     - 所有虚拟系统共享升级后规则库。
   - 虚拟系统中不提供缺省的 UTM 策略。

表 269 安全域和访问策略命令

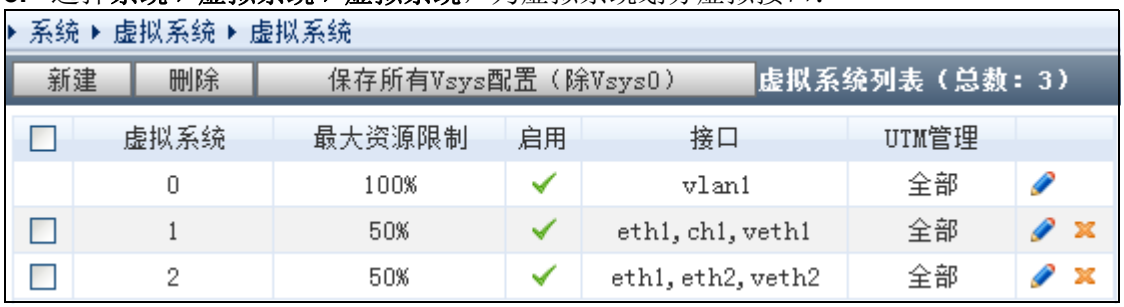
zone *zone_name*	创建安全域。
zone based-layer3	配置基于三层或三层共享接口的安全域。
policy access	添加访问策略。

13.2.6. 创建虚拟网络

1. 切换到根系统，选择工作模式后进行以下配置。关于工作模式的更多信息请参见 13.3. 场景。（虚拟网络只能在根系统下配置。）
2. 选择**网络 > 接口**，创建三层接口：



3. 选择**系统 > 虚拟系统 > 虚拟系统**，为虚拟系统划分虚拟接口：



4. 选择**系统 > 虚拟系统 > 虚拟网络**，创建虚拟网络，为虚拟网络划分虚拟接口和虚拟系统。

5. 登录虚拟系统创建访问策略，允许虚拟系统间通讯。参见 8.2.2 创建访问策略。
6. 对于工作在路由模式的虚拟系统，还需要创建缺省路由。参见 5.2.1 单播。

关于策略和路由的相关命令，请参见*东软集成安全网关软件 V4.2 命令参考手册*中的**策略命令**和**路由命令**章节。

表 270 虚拟网络命令

vnet *vnet_id*	创建虚拟网络。
unset vnet *vnet_id*	删除虚拟网络。
hold veth *veth_id*	划分虚拟接口到虚拟网络。
unhold veth *veth_id*	从虚拟网络中删除虚拟接口。
description [*string*]	为虚拟网络添加描述信息或修改、删除虚拟网络描述信息。
show vnet [*vnet_id* | **brief**]	查看虚拟网络信息。

13.3. 场景

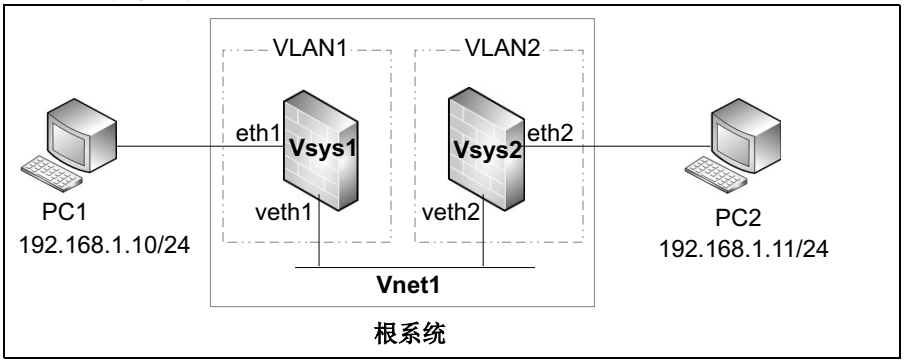
虚拟系统支持三种工作模式：

- 1. 透明模式
- 2. 路由模式
- 3. 混合模式

1. 透明模式

透明模式主要用于数据流的二层转发。

图 62 透明模式典型拓扑



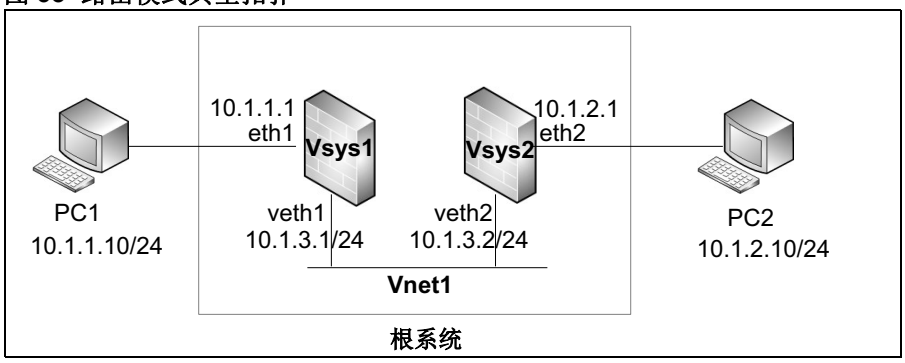
此范例的配置步骤包括：

1. 将 eth1 和 veth1 划入 VLAN1。
2. 将 VLAN1 划入 Vsys1。
3. 将 eth2 和 veth2 划入 VLAN2。
4. 将 VLAN2 划入 Vsys2。
5. 创建虚拟系统 Vnet1。
6. 将 veth1 和 Vsys1 划入 Vnet1。
7. 将 veth2 和 Vsys2 也划入 Vnet1。
8. 在 Vsys1 和 Vsys2 中分别配置访问策略，允许 PC 之间通讯。

2. 路由模式

路由模式是指虚拟设备可以让工作在不同网段之间的主机以三层路由的方式进行通信。虚拟设备处于路由工作模式时，各接口所连接的网络必须处于不同的网段，需要为虚拟设备的接口设置 IP 地址。

图 63 路由模式典型拓扑



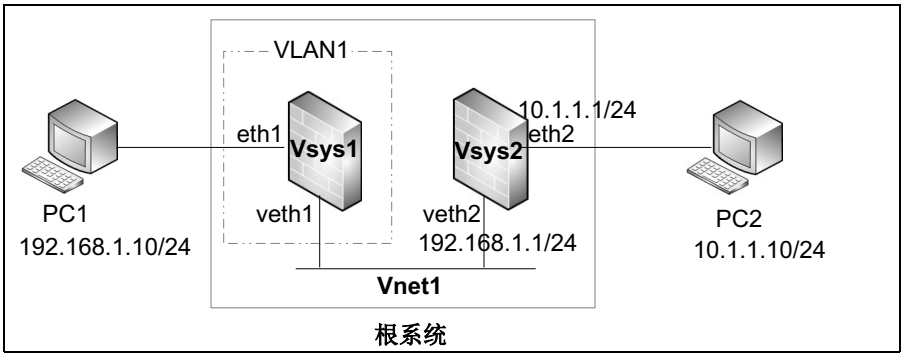
此范例的配置步骤包括：

1. 将 eth1 和 eth2 设置为三层工作模式，创建三层虚拟接口 veth1 和 veth2。
2. 创建虚拟系统 Vsys1，将 eth1 和 veth1 划入 Vsys1。
3. 创建虚拟系统 Vsys2，将 eth2 和 veth2 划入 Vsys2。
4. 在 Vsys1 中，配置 eth1 的 IP 地址为 10.1.1.1，配置 veth1 的 IP 地址为 10.1.3.1。
5. 在 Vsys2 中，配置 eth2 的 IP 地址为 10.1.2.1，配置 veth2 的 IP 地址为 10.1.3.2。
6. 创建虚拟网络 Vnet1，将 Vsys1 和 veth1 划入 Vnet1，将 Vsys2 和 veth2 也划入 Vnet1。
7. 在 Vsys1 和 Vsys2 中分别配置访问策略，允许 PC 之间通讯。
8. 在Vsys1上配置一条到PC2的静态路由，下一跳为10.1.3.2；在Vsys2上配置一条到PC1的静态路由，下一跳为 10.1.3.1。
9. 设置 PC1 的网关为 10.1.1.1，设置 PC2 的网关为 10.1.2.1。

3. 混合模式

混合模式能够同时实现数据流的二层转发和三层路由功能。

图 64 混合模式典型拓扑



此范例的配置步骤包括：

1. 将 eth1 和 veth1 划入 VLAN1，再将 VLAN1 划入 Vsys1。
2. 将 eth2 设置为三层接口，创建三层虚拟接口 veth2，然后将 eth2 和 veth2 划入 Vsys2。
3. 在 Vsys2 中，配置 eth2 的 IP 地址为 10.1.1.1/24，配置 veth2 的 IP 地址为 192.168.1.1/24。
4. 创建虚拟网络 Vnet1，将 Vsys1 和 veth1 划入 Vnet1，将 Vsys2 和 veth2 也划入 Vnet1。
5. 在 Vsys1 和 Vsys2 中分别配置访问策略，允许 PC 之间通讯。
6. 设置 PC1 的网关为 192.168.1.1，设置 PC2 的网关为 10.1.1.1。

13.4. 范例

本小节包含以下范例：

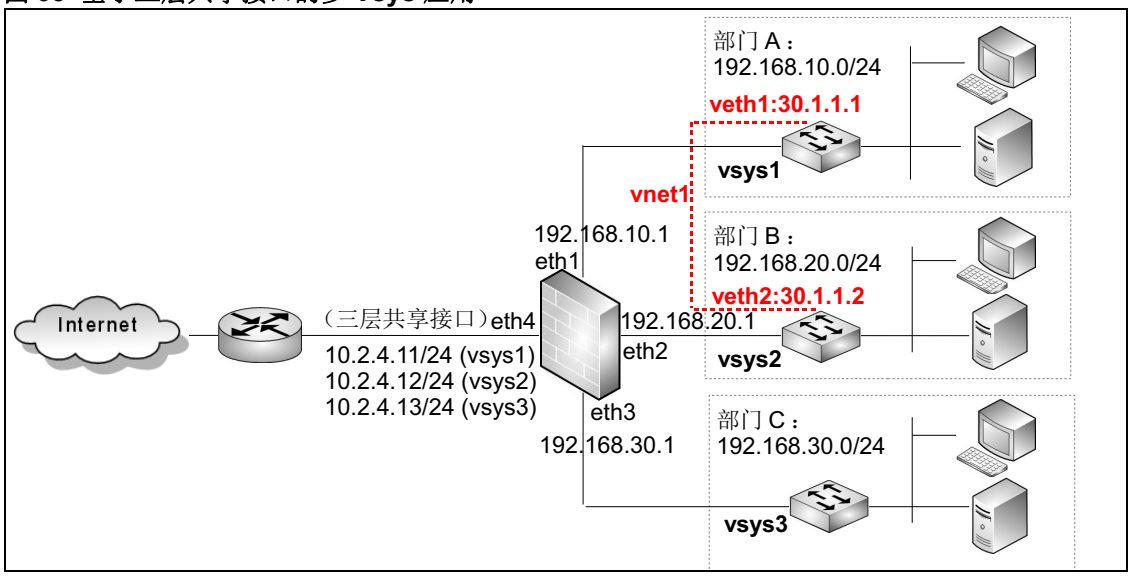
- 范例 1：基于三层共享接口的多 Vsys 应用
- 范例 2：基于 Trunk 接口的多 Vsys 应用

范例 1：基于三层共享接口的多 Vsys 应用

如下图所示，某公司有三个部门：A、 B、 C。它们处于不同的网段且需要有不同的安全配置，而且整个公司只有一个网络出口接入互联网。

- 为了让这三个部门有各自不同的安全配置，可为每个部门分别创建一个虚拟系统。
- 为了让三个部门可以同时访问互联网，需要将外网出口作为共享接口分配给这三个虚拟系统共用。
- 为了让部门 A 和 B 能够相互通讯，可以在他们之间创建一个虚拟网络，将这两个部门所在的虚拟系统连在一起。

图 65 基于三层共享接口的多 Vsys 应用

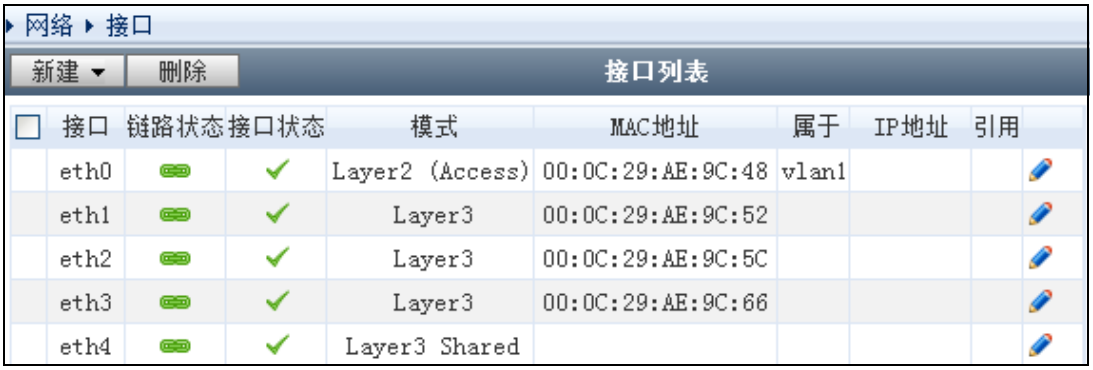


本范例包含以下配置：

1. 创建三层接口
2. 创建虚拟系统，划分接口，设置管理 IP
3. 添加 Vsys 1-3 的管理权限
4. 配置虚拟系统
5. 创建虚拟网络
6. 创建虚拟系统管理员

1. 创建三层接口

1. 选择**网络 > 接口**，将 eth1、eth2、eth3 设置为三层接口，将 eth4 设置为三层共享接口。



接口	链路状态	接口状态	模式	MAC地址	属于	IP地址	引用	
eth0		✓	Layer2 (Access)	00:0C:29:AE:9C:48	vlan1			
eth1		✓	Layer3	00:0C:29:AE:9C:52				
eth2		✓	Layer3	00:0C:29:AE:9C:5C				
eth3		✓	Layer3	00:0C:29:AE:9C:66				
eth4		✓	Layer3 Shared					

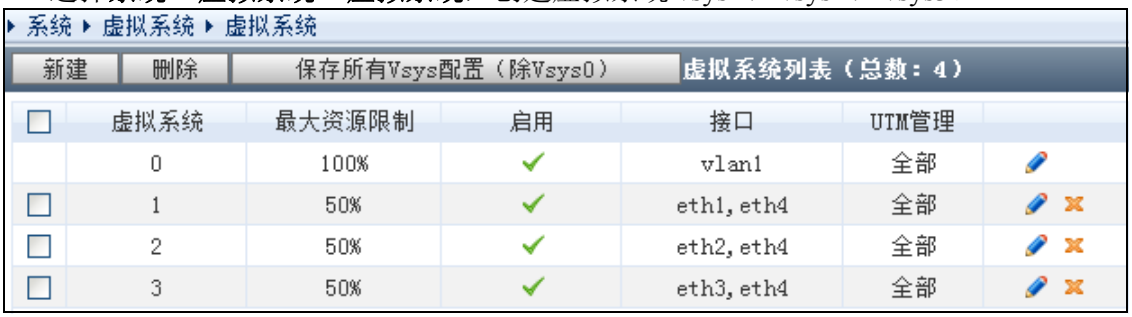
2. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet 1
NetEye@root-system-if-eth1] working-type layer3-interface
NetEye@root-system-if-eth1] exit
NetEye@root-system] interface ethernet 2
NetEye@root-system-if-eth2] working-type layer3-interface
NetEye@root-system-if-eth2] exit
NetEye@root-system] interface ethernet 3
NetEye@root-system-if-eth3] working-type layer3-interface
NetEye@root-system-if-eth3] exit
NetEye@root-system] interface ethernet 4
NetEye@root-system-if-eth4] working-type layer3-shared-interface
NetEye@root-system-if-eth4] exit
NetEye@vsys1-system] end
NetEye@vsys1> save config
```

2. 创建虚拟系统，划分接口，设置管理 IP

1. 选择**系统 > 虚拟系统 > 虚拟系统**，创建虚拟系统 vsys1、 vsys2、 vsys3。



2. 分别设置 Vsys 管理接口和 IP 为：
   - vsys1：eth1 （192.168.10.1/24）
   - vsys2：eth2 （192.168.20.1/24）。
   - vsys3：eth3 （192.168.30.1/24）。
3. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] vsys 1 resource-limit 50
NetEye@root-system-vsys1] hold ethernet 1
NetEye@root-system-vsys1] hold ethernet 4
NetEye@root-system-vsys1] exit
NetEye@root-system] vsys 2 resource-limit 50
NetEye@root-system-vsys2] hold ethernet 2
NetEye@root-system-vsys2] hold ethernet 4
NetEye@root-system-vsys2] exit
NetEye@root-system] vsys 3 resource-limit 50
NetEye@root-system-vsys3] hold ethernet 3
NetEye@root-system-vsys3] hold ethernet 4
NetEye@root-system-vsys3] exit
NetEye@root-system] vsys 1
NetEye@root-system-vsys1] manage-ip-address 192.168.10.1 255.255.255.0
ethernet 1
NetEye@root-system-vsys1] exit
NetEye@root-system] vsys 2
NetEye@root-system-vsys2] manage-ip-address 192.168.20.1 255.255.255.0
ethernet 2
NetEye@root-system-vsys2] exit
NetEye@root-system] vsys 3
NetEye@root-system-vsys3] manage-ip-address 192.168.30.1 255.255.255.0
ethernet 3
NetEye@root-system-vsys4] end
NetEye@root> save config
```

3. 添加 Vsys 1-3 的管理权限

1. 选择**系统>认证>管理用户**，点击Neusoft对应的 按钮，为根系统管理员Neusoft添加vsys1、 vsys2 和 vsys3 的管理权限。

2. 点击**确定**。
3. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] user administrator admin allowed-vsys vsys1
NetEye@root-system] user administrator admin allowed-vsys vsys2
NetEye@root-system] user administrator admin allowed-vsys vsys3
NetEye@root-system] end
NetEye@root> save config
```

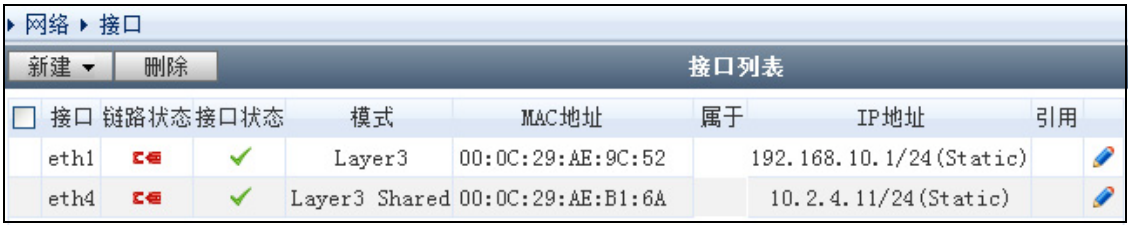
4. 配置虚拟系统

WebUI

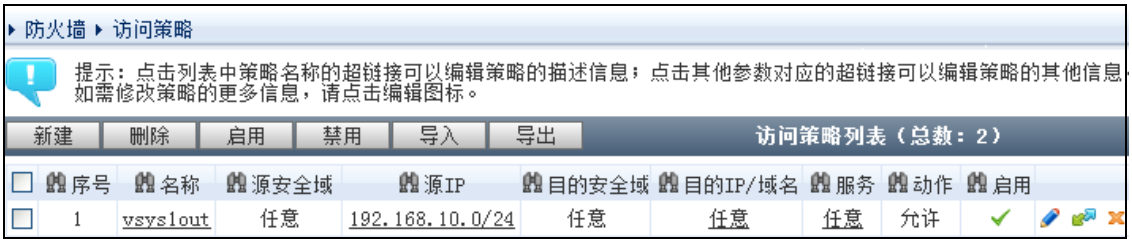
1. 选择**系统 > 虚拟系统 > 虚拟系统**，点击页面底端的**切换虚拟系统**链接。

2. 点击虚拟系统 vsys1 对应的按钮，进入虚拟系统 vsys1。

   a. 选择**网络 > 接口**，进入**接口**页面，设置 eth1 的 IP 地址设置为 192.168.10.1/24，设置 eth4 的 IP 地址为 10.2.4.11/24。



   b. 选择**防火墙 > 访问策略**，进入**访问策略**页面，添加一条允许 192.168.10.0/24 网段到任意目的地址的访问策略。



3. 切换到 vsys2，并进行以下操作：

   a. 选择**网络 > 接口**，进入接口页面，设置 eth2 的 IP 地址设置为 192.168.20.1/24，设置 eth4 的 IP 地址为 10.2.4.12/24。

   b. 选择**防火墙 > 访问策略**，进入访问策略页面，添加一条允许 192.168.20.0/24 网段到任意目的地址的访问策略。

4. 切换到 vsys3，并进行以下操作：

   a. 选择**网络 > 接口**，进入接口页面，设置 eth3 的 IP 地址设置为 192.168.30.1/24，设置 eth4 的 IP 地址为 10.2.4.13/24。

   b. 选择**防火墙 > 访问策略**，进入访问策略页面，添加一条允许 192.168.30.0/24 网段到任意目的地址的访问策略。

5. 点击。

CLI

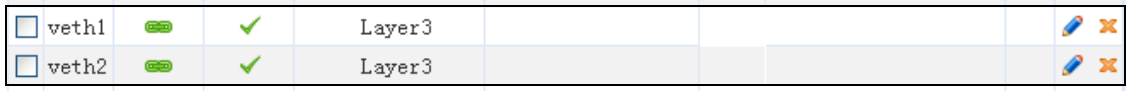
```
NetEye@root> switch vsys vsys1
NetEye@vsys1> configure mode override
NetEye@vsys1-system] interface ethernet 1
NetEye@vsys1-system-if-eth1] ip address 192.168.10.1 255.255.255.0
NetEye@vsys1-system-if-eth1] exit
NetEye@vsys1-system] interface ethernet 4
NetEye@vsys1-system-if-eth4] ip address 10.2.4.11 255.255.255.0
NetEye@vsys1-system-if-eth4] exit
NetEye@vsys1-system] policy access vsys1out any 192.168.10.0/24 any
any any any permit enable
NetEye@vsys1-system] end
NetEye@vsys1> save config
NetEye@vsys1> switch vsys vsys2
NetEye@vsys2> configure mode override
NetEye@vsys2-system] interface ethernet 2
NetEye@vsys2-system-if-eth2] ip address 192.168.20.1 255.255.255.0
NetEye@vsys2-system-if-eth2] exit
NetEye@vsys2-system] interface ethernet 4
NetEye@vsys2-system-if-eth4] ip address 10.2.4.12 255.255.255.0
NetEye@vsys2-system-if-eth4] exit
NetEye@vsys2-system] policy access vsys2out any 192.168.20.0/24 any
any any any permit enable
NetEye@vsys2-system] end
NetEye@vsys2> save config
NetEye@vsys2> switch vsys vsys3
NetEye@vsys3> configure mode override
NetEye@vsys3-system] interface ethernet 3
NetEye@vsys3-system-if-eth3] ip address 192.168.30.1 255.255.255.0
NetEye@vsys3-system-if-eth3] exit
NetEye@vsys3-system] interface ethernet 4
NetEye@vsys3-system-if-eth4] ip address 10.2.4.13 255.255.255.0
NetEye@vsys3-system-if-eth4] exit
NetEye@vsys3-system] policy access vsys3out any 192.168.30.0/24 any
any any any permit enable
NetEye@vsys3-system] end
NetEye@vsys3> save config
```

5. 创建虚拟网络

- 5.1. 创建虚拟接口
- 5.2. 将虚拟接口划入虚拟系统
- 5.3. 创建虚拟网络
- 5.4. 设置 Vsys 的虚拟接口 IP、静态路由和访问策略

5.1. 创建虚拟接口

1. 选择**系统 > 虚拟系统 > 虚拟系统**，点击 Vsys 0 对应的图标切换到根系统。
2. 选择**网络 > 接口**，创建三层虚拟接口 veth1 和 veth2：



3. 点击。

CLI

```
NetEye@vsys4> switch vsys root
NetEye@root> configure mode override
NetEye@root-system] veth 1
NetEye@root-system-veth1] working-type layer3-interface
NetEye@root-system-veth1] exit
NetEye@root-system] veth 2
NetEye@root-system-veth2] working-type layer3-interface
NetEye@root-system-veth2] end
NetEye@root> save config
```

5.2. 将虚拟接口划入虚拟系统

1. 选择**系统>虚拟系统>虚拟系统**，将虚拟接口veth1和veth2分别划入vsys1和vsys2：

2. 点击。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] vsys 1
NetEye@root-system-vsys1] hold veth 1
NetEye@root-system-vsys1] exit
NetEye@root-system] vsys 2
NetEye@root-system-vsys2] hold veth 2
NetEye@root-system-vsys2] end
NetEye@root> save config
```

5.3. 创建虚拟网络

1. 选择**系统 > 虚拟系统 > 虚拟网络**，创建虚拟网络 vnet1，将 vsys1 和 veth1 划入 vnet1，将 vsys2 和 veth2 也划入 vnet1：

2. 点击 。

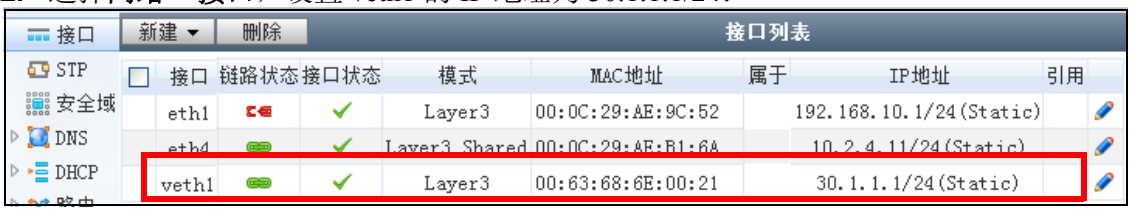
CLI

```
NetEye@root> configure mode override
NetEye@root-system] vnet 1
NetEye@root-system-vnet1] hold veth 1
NetEye@root-system-vnet1] hold veth 2
NetEye@root-system-vnet1] end
NetEye@root> save config
```

5.4. 设置 Vsys 的虚拟接口 IP、静态路由和访问策略

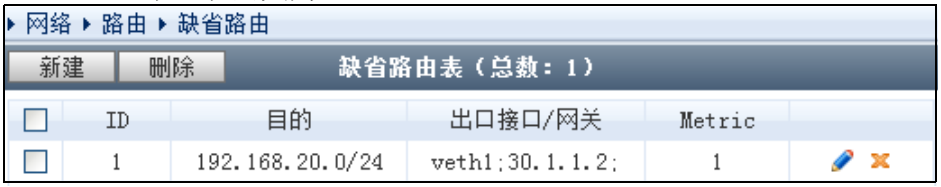
1. 选择**系统 > 虚拟系统 > 虚拟系统**，点击页面底端的**切换虚拟系统**链接，点击 Vsys 1 对应的 图标，进入虚拟系统 vsys1。

2. 选择**网络 > 接口**，设置 veth1 的 IP 地址为 30.1.1.1/24：

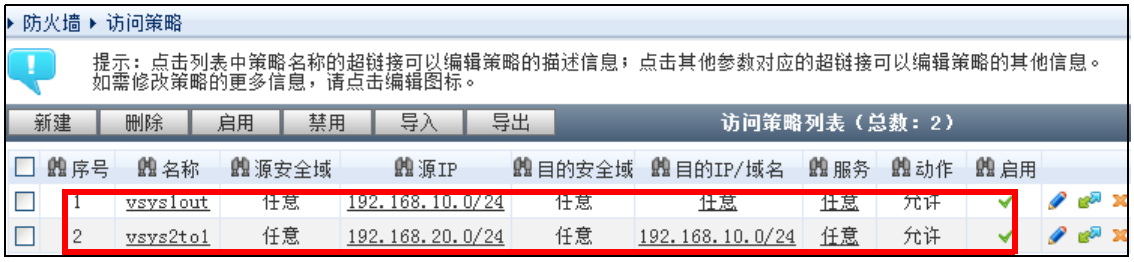


3. 点击**确定**。

4. 选择**网络 > 路由 > 缺省路由**，添加到 192.168.20.0/24 网段的静态路由，出口接口为 veth1，下一跳网关为 30.1.1.2：



5. 选择**防火墙 > 访问策略**，添加一条访问策略 vsys2to1，允许 192.168.20.0/24 到 192.168.10.0/24 的访问：



6. 切换到 vsys2，并进行以下配置：
   a. 选择网络 > 接口，设置 veth2 的 IP 地址为 30.1.1.2/24。
   b. 选择网络 > 路由 > 缺省路由，添加到 192.168.10.0/24 网段的静态路由，出口接口为 veth2，下一跳网关为 30.1.1.1。
   c. 选择防火墙 > 访问策略，添加一条访问策略，允许 192.168.10.0/24 到 192.168.20.0/24 的访问。
7. 点击 。

CLI

```
NetEye@root> switch vsys vsys1
NetEye@vsys1> configure mode override
NetEye@vsys1-system] veth 1
NetEye@vsys1-system-veth1] ip address 30.1.1.1 255.255.255.0
NetEye@vsys1-system-veth1] exit
NetEye@vsys1-system] route 192.168.20.0 255.255.255.0 interface veth1
gateway 30.1.1.2
NetEye@vsys1-system] policy access vsys2to1 any 192.168.20.0 any
192.168.10.0 any any permit enable
NetEye@vsys1-system] end
NetEye@vsys1> save config
NetEye@vsys1> switch vsys vsys2
NetEye@vsys2> configure mode override
NetEye@vsys2-system] veth 2
NetEye@vsys2-system-veth2] ip address 30.1.1.2 255.255.255.0
NetEye@vsys2-system-veth2] exit
NetEye@vsys2-system] route 192.168.10.0 255.255.255.0 interface veth2
gateway 30.1.1.1
NetEye@vsys2-system] policy access vsys1to2 any 192.168.10.0 any
192.168.20.0 any any permit enable
NetEye@vsys2-system] end
NetEye@vsys2> save config
```

6. 创建虚拟系统管理员

1. 选择**系统 > 虚拟系统 > 虚拟系统**，点击 Vsys 0 对应的 图标切换到根系统。
2. 选择**系统 > 认证 > 管理用户**，为 vsys1 添加 Vsys 管理员 vsys1ad，密码为 test_123：

3. 点击**确定**。
4. 分别为 vsys2、 vsys3 添加 Vsys 管理员 vsys2ad、 vsys3ad，密码均为 test_123。
5. 点击 。
6. 以 Vsys 管理员身份登录虚拟系统进行管理，登录方式同根系统管理员登录根系统。

提示：若想通过 Ping 命令检测网络的连通性，还需要到各 Vsys 中开启 Ping 服务。

CLI

```
NetEye@vsys2> switch vsys root
NetEye@root> configure mode override
NetEye@root-system] user administrator vsys1ad vsys-administrator
vsys vsys1 authtype local password simple
Password(6-128): <test_123>
Repeat Password(6-128): <test_123>
NetEye@root-system] user administrator vsys1ad logintype
web,ssh,telnet
NetEye@root-system] user administrator vsys2ad vsys-administrator
vsys vsys2 authtype local password simple
Password(6-128): <test_123>
```

```
Repeat Password(6-128): <test_123>
NetEye@root-system] user administrator vsys2ad logintype
web,ssh,telnet
NetEye@root-system] user administrator vsys3ad vsys-administrator
vsys vsys3 authtype local password simple
Password(6-128): <test_123>
Repeat Password(6-128): <test_123>
NetEye@root-system] user administrator vsys3ad logintype
web,ssh,telnet
NetEye@root-system] end
NetEye@root> save config
```

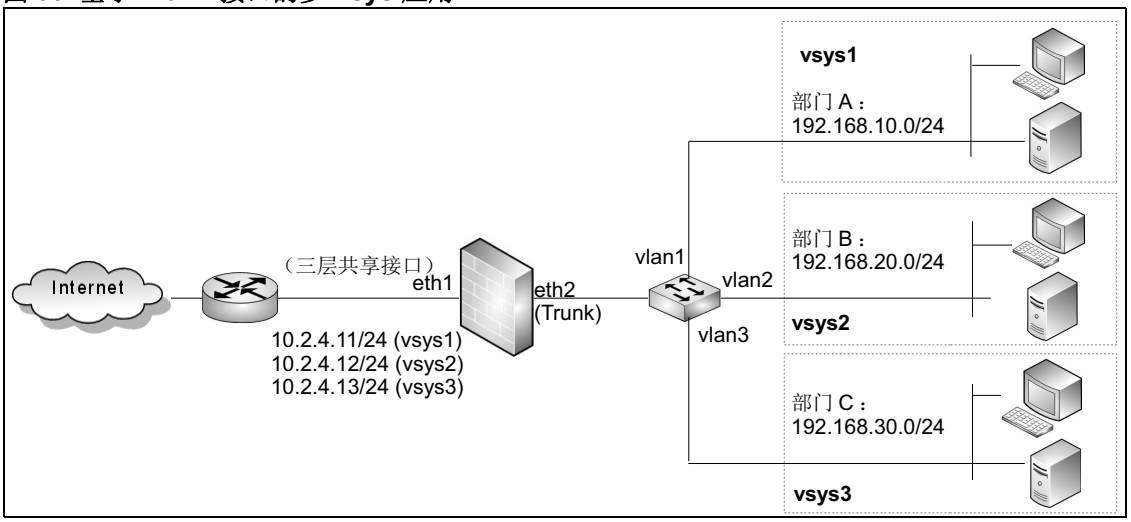
范例 2：基于 Trunk 接口的多 Vsys 应用

如下图所示，某公司有三个部门 A、 B、 C。这三个部门分属于不同的 IP 网段，但它们有不同的安全配置和服务需求，而整个公司只有一个网络出口连接互联网，且只有一个网络入口连接内网交换机。

- 为了让这三个部门网络可以有自己的安全配置，可以为每个部门单独创建一个虚拟系统。
- 为了让这三个部门的员工都可以访问互联网，可以将出口接口作为共享接口分配给这三个虚拟系统共用。
- 为了让部门A和B之间也能够相互通讯，可以在A和B之间创建一个虚拟网络，将两个部门的虚拟系统连接起来。

可为这三个部门分别创建一个虚拟系统，并，同时将入口接口设为 Trunk 模式。

图 66 基于 Trunk 接口的多 Vsys 应用



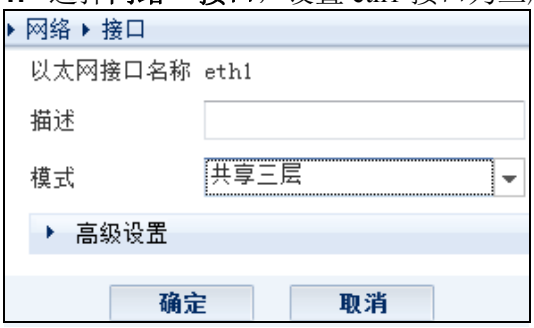
本范例包含以下配置：

1. 创建三层接口
2. 创建虚拟系统
3. 添加 Vsys 管理权限
4. 为 Vsys 设置接口 IP 和访问策略

提示：关于如何创建 Vsys 管理员和设置虚拟系统管理 IP 地址，请参见范例 1。

1. 创建三层接口

1. 选择**网络 > 接口**，设置 eth1 接口为三层共享接口。



2. 点击**确定**。
3. 创建VLAN接口vlan1、vlan2和vlan3，设置eth2接口为二层接口Trunk模式，将vlan1、vlan2 和 vlan3 划入 eth2。

4. 在内网交换机上设置相应的 Trunk 口和 VLAN。
5. 点击**确定**。
6. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] interface ethernet 1
NetEye@root-system-if-eth1] working-type layer3-shared-interface
NetEye@root-system-if-eth1] exit
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] exit
NetEye@root-system] vlan 2
NetEye@root-system-vlan2] exit
NetEye@root-system] vlan 3
NetEye@root-system-vlan3] exit
NetEye@root-system] interface ethernet 2
NetEye@root-system-if-eth2] port mode trunk
NetEye@root-system-if-eth2] port trunk allowed vlan 1,2,3
NetEye@root-system] end
NetEye@root> save config
```

2. 创建虚拟系统

1. 选择**系统 > 虚拟系统 > 虚拟系统**，点击**新建**，创建虚拟系统 vsys1、vsys2 和 vsys3，将 eth1 和 vlan1 划入 vsys1、 eth1 和 vlan2 划入 vsys2、 eth1 和 vlan3 划入 vsys3。

2. 点击 。

CLI

```
NetEye@root> configure mode override
NetEye@root-system] vsys 1 resource-limit 50
NetEye@root-system-vsys1] hold ethernet 1
NetEye@root-system-vsys1] hold vlan 1
NetEye@root-system-vsys1] exit
NetEye@root-system] vsys 2 resource-limit 50
NetEye@root-system-vsys2] hold ethernet 1
NetEye@root-system-vsys2] hold vlan 2
NetEye@root-system-vsys2] exit
NetEye@root-system] vsys 3 resource-limit 50
NetEye@root-system-vsys3] hold ethernet 1
NetEye@root-system-vsys3] hold vlan 3
NetEye@root-system] end
NetEye@root> save config
```

3. 添加 Vsys 管理权限

1. 点击**虚拟系统**页面底端的**管理用户**超链接，跳转到**管理用户**页面，点击 Neusoft 对应的 按钮，进入编辑页面，为 Neusoft 添加管理 vsys1、 vsys2 和 vsys3 的权限。

2. 点击**确定**。
3. 点击 。

CLI

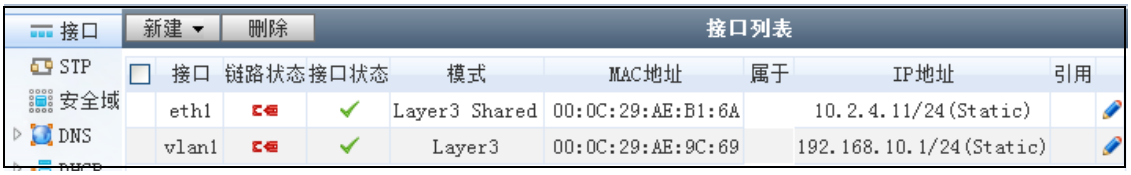
```
NetEye@root> configure mode override
NetEye@root-system] user administrator admin allowed-vsys vsys1
NetEye@root-system] user administrator admin allowed-vsys vsys2
NetEye@root-system] user administrator admin allowed-vsys vsys3
NetEye@root-system] end
NetEye@root> save config
```

4. 为 Vsys 设置接口 IP 和访问策略

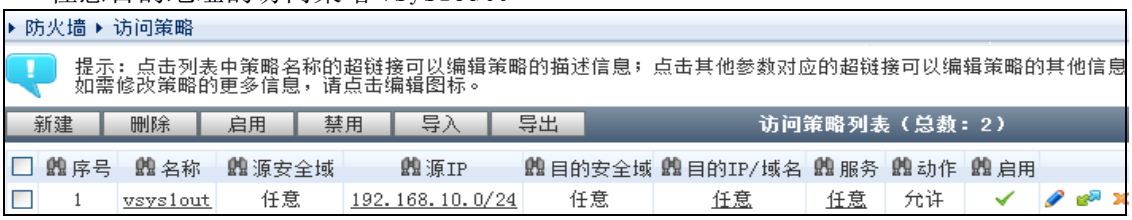
1. 选择**系统 > 虚拟系统 > 虚拟系统**，点击页面底端的**切换虚拟系统**超链接，进入**切换虚拟系统**页面。

2. 点击虚拟系统 1 对应的按钮，切换到虚拟系统 vsys1。

3. 选择**网络>接口**，设置eth1的IP地址为10.2.4.11/24，设置vlan1的IP地址为192.168.10.1/24。



4. 选择**防火墙 > 访问策略**，进入**访问策略**页面，添加一条允许 192.168.10.0/24 网段到任意目的地址的访问策略 vsys1out。



5. 切换到 vsys2，并进行以下配置：

   a. 选择网络>接口，进入接口页面，设置eth1的IP地址为10.2.4.12/24，设置vlan2的IP地址为 192.168.20.1/24。

   b. 选择防火墙 > 访问策略，进入访问策略页面，添加一条允许 192.168.20.0/24 网段到任意目的地址的访问策略 vsys2out。

6. 切换到 vsys3，并进行以下配置：

   a. 选择网络>接口，进入接口页面，设置eth1的IP地址为10.2.4.13/24，设置vlan3的IP地址为 192.168.30.1/24。

   选择防火墙 > 访问策略，进入访问策略页面，添加一条允许 192.168.30.0/24 网段到任意目的地址的访问策略 vsys3out。

7. 点击。

提示：如果想通过 Ping 命令检查网络连通性，还需要到各个虚拟系统中开启 Ping 服务。

CLI

```
NetEye@root> switch vsys vsys1
NetEye@vsys1> configure mode override
NetEye@vsys1-system] interface ethernet 1
NetEye@vsys1-system-if-eth1] ip address 10.2.4.11 255.255.255.0
NetEye@vsys1-system-if-eth1] exit
NetEye@vsys1-system] vlan 1
NetEye@vsys1-system-vlan1] ip address 192.168.10.1 255.255.255.0
NetEye@vsys1-system-vlan1] exit
NetEye@vsys1-system] policy access vsys1out any 192.168.10.0 any any any any permit enable
NetEye@vsys1-system] end
NetEye@vsys1> save config
NetEye@vsys1> switch vsys vsys2
NetEye@vsys2> configure mode override
NetEye@vsys2-system] interface ethernet 1
NetEye@vsys2-system-if-eth1] ip address 10.2.4.12 255.255.255.0
NetEye@vsys2-system-if-eth1] exit
NetEye@vsys2-system] vlan 2
NetEye@vsys2-system-vlan2] ip address 192.168.20.1 255.255.255.0
NetEye@vsys2-system-vlan2] exit
NetEye@vsys2-system] policy access vsys2out any 192.168.20.0 any any any any permit enable
NetEye@vsys2-system] end
NetEye@vsys2> save config
NetEye@vsys2> switch vsys vsys3
NetEye@vsys3> configure mode override
NetEye@vsys3-system] interface ethernet 1
NetEye@vsys3-system-if-eth1] ip address 10.2.4.13 255.255.255.0
NetEye@vsys3-system-if-eth1] exit
NetEye@vsys3-system] vlan 3
NetEye@vsys3-system-vlan3] ip address 192.168.30.1 255.255.255.0
NetEye@vsys3-system-vlan3] exit
NetEye@vsys3-system] policy access vsys3out any 192.168.30.0 any any any any permit enable
NetEye@vsys3-system] end
NetEye@vsys3> save config
```

13.5. 配置参数说明

本节介绍以下内容的相关参数：

- 13.5.1. 虚拟系统
- 13.5.2. 虚拟网络
- 13.5.3. 虚拟系统中可配置的功能

13.5.1. 虚拟系统

表 271 虚拟系统参数

参数	说明
虚拟系统	虚拟系统标识。虚拟系统名称由 vsys+ 虚拟系统标识组成。虚拟系统标识的取值范围为 1 ～ 255。
最大资源限制	根系统管理员划分给虚拟系统的最大资源百分比。取值范围为 1 ～ 100。
启用	虚拟系统是否处于启用状态。✔表示启用，✘表示禁用。
接口	根系统管理员划分给虚拟系统的三层或三层共享接口，包括三层或三层共享以太网接口、三层虚拟接口、 VLAN 接口、三层或三层共享以太网通道、三层或三层共享冗余接口以及 PPPoE 接口。
UTM 管理	根系统管理员为虚拟系统划分的 UTM 功能。可划分的 UTM 功能包括防病毒、反垃圾邮件、 IPS、 URL 过滤和应用控制。
描述	长度 0~255 字节， UTF-8 字符。不能包含以下字符：？ " ’ \ < > &
启用虚拟系统	启用或禁用虚拟系统。
管理 IP 地址	选择一个三层接口作为虚拟系统的管理口，同时设置一个 IPv4 或 IPv6 地址作为管理 IP 地址。
保存所有 Vsys 配置 （除 Vsys0）	保存除 root 外的所有 Vsys 配置。
管理用户	用于跳转到管理用户页面，为虚拟系统创建或指定管理用户。
切换虚拟系统	用于跳转到切换虚拟系统页面，进行虚拟系统切换。

13.5.2. 虚拟网络

表 272 虚拟网络参数

参数	说明
ID	虚拟网络标识。取值范围为 1 ～ 255 之间的整数。
虚拟系统	虚拟网络连接的虚拟系统。
接口	虚拟系统接入虚拟网络使用的虚拟接口。
描述	长度 0~255 字节， UTF-8 字符 （除？ " ’ \ < > &）。
链接虚拟接口列表	添加虚拟接口，将对应的虚拟系统接入虚拟网络。

13.5.3. 虚拟系统中可配置的功能

虚拟系统下可配置的功能包括：

- **主页**
- **系统 > 概述 > 访问设置**
- **系统 > 维护 > 备份 / 恢复 / 集中管理**
- **系统 > 认证 / 证书 / 对象**
- **系统 > 高可用性 > 虚拟路由器 / 虚拟路由器探测组**
- **系统 > 虚拟系统**：只能切换虚拟系统。
- **系统 > 服务配置 > 访问设置**（root 管理用户登录设置除外）**/ 标题信息**
- **系统 > 日志配置**
- **网络 > 接口 / 安全域**：仅能添加 Loopback 接口、编辑已添加的以太网接口。
- **网络 >DNS**
- **网络 >DHCP**
- **网络 > 路由 / 地址转换 / 多播 /IPv6**
- **防火墙**：包括策略和攻击防御。
- **UTM> 概要信息**
- **UTM> 出口控制 > 策略**
- **UTM> 出口控制 > 应用控制**
- **UTM> 出口控制 >URL 过滤 > 常规设置**：仅能查询 URL 分类。
- **UTM> 出口控制 >URL 过滤 > 防护配置 / 黑白名单**
- **UTM> 出口控制 >DNS 域名黑名单 / 页面过滤**
- **UTM> 客户端防护 / 服务器防护**
- **UTM> 防病毒 > 信任 URL/ 信任 Web 服务器 / 信任客户端**
- **UTM> 反垃圾邮件 > 允许列表 / 阻断列表 / 关键字列表**
- **UTM> 通知消息**
- **UTM>QoS**
- **VPN**：包括 IPSec VPN 和 SSL VPN。
- **监控**：仅提供当前所在系统的监控信息。

14 监控

NISG 的监控功能对系统信息进行全面的监控，使管理员能够更好地维护系统性能和安全。本章结构如下：

- 14.1 拓扑
- 14.2 流量统计
- 14.3 虚拟系统
- 14.4 STP
- 14.5 路由
- 14.6 NAT
- 14.7 ARP
- 14.8 CAM
- 14.9 DHCP IP 地址绑定状态
- 14.10 DHCPv6 客户端
- 14.11 DNS 缓存
- 14.12 高可用性
- 14.13 系统利用率
- 14.14 在线用户
- 14.15 IPSec VPN 隧道
- 14.16 多播
- 14.17 报警 / 日志

14.1 拓扑

拓扑监控显示安全域、三层接口以及二层接口间的网络拓扑关系。

选择**监控** > **拓扑**。

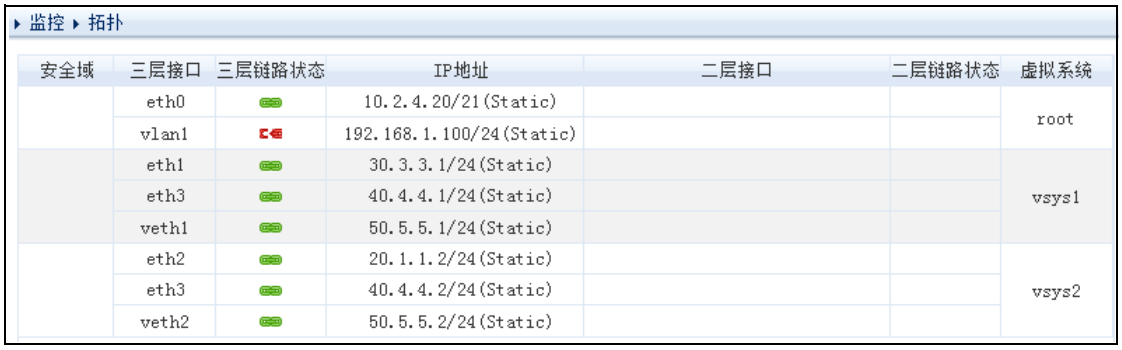


表 273 拓扑参数

参数	说明
安全域	三层接口所属的安全域。
三层接口	安全域包含的接口。 三层安全域包含的是三层接口，二层安全域对应的是 VLAN 接口。
IP 地址	接口对应的 IP 地址。 IPv4 地址仅显示主 IP 地址， IPv6 地址则显示所有 IP 地址。 三层安全域对应的是三层接口的 IP 地址。二层安全域对应的是 VLAN 接口的 IP 地址。
二层接口	三层接口包含的二层接口。
链路状态	对应二层接口或三层接口的链路状态。 • 接口已连接。 • 连接已断开。
虚拟系统	安全域所属的虚拟系统。

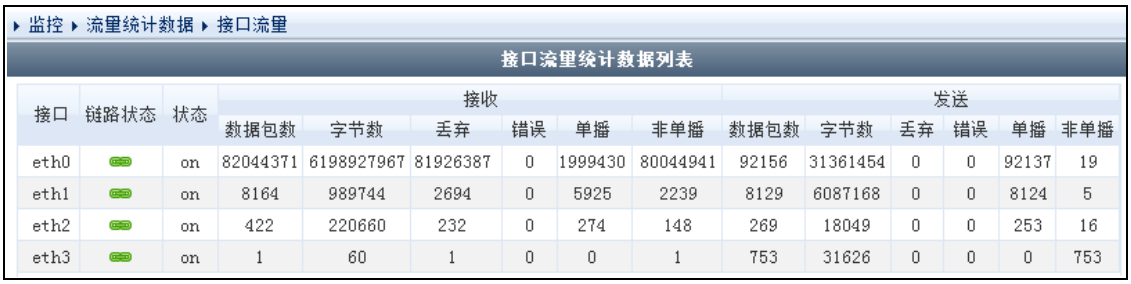
14.2 流量统计

NISG 的流量统计监控使管理员能够及时发现系统瓶颈或隐患，全面考察系统的稳定性和可靠性。流量统计监控以下内容：

- 14.2.1 接口流量
- 14.2.2 应用排名
- 14.2.3 URL 排名
- 14.2.4 用户排名
- 14.2.5 IP 地址排名

14.2.1 接口流量

选择**监控** > **流量统计数据** > **接口流量**。



接口	链路状态	状态	接收						发送					
			数据包数	字节数	丢弃	错误	单播	非单播	数据包数	字节数	丢弃	错误	单播	非单播
eth0		on	82044371	6198927967	81926387	0	1999430	80044941	92156	31361454	0	0	92137	19
eth1		on	8164	989744	2694	0	5925	2239	8129	6087168	0	0	8124	5
eth2		on	422	220660	232	0	274	148	269	18049	0	0	253	16
eth3		on	1	60	1	0	0	1	753	31626	0	0	0	753

表 274 接口流量参数

参数	说明
接口	接口名称。
链路状态	接口的连接状态。 • — 接口已连接。 • — 连接已断开。
状态	接口的启禁用状态。
接收数据包数	接口接收的数据包数。
接收字节数	接口接收的字节数。
接收丢弃 / 错误 / 单播 / 非单播包数	接口接收的数据包中丢失 / 错误 / 单播 / 非单播包数。
发送数据包数	接口转发的数据包数。
发送字节数	接口转发的字节数。
发送丢弃 / 错误 / 单播 / 非单播包数	接口转发的数据包中丢失 / 错误 / 单播 / 非单播包数。

14.2.2 应用排名

选择**监控** > **流量统计数据** > **应用排名**，进入**应用排名**页面查看应用排名实时信息。管理员还可以设置应用显示条数、刷新方法 （手动和自动）及刷新时间间隔。

14.2.3 URL 排名

选择**监控** > **流量统计数据** > **URL 排名**，进入 **URL 排名**页面查看 URL 排名实时信息。管理员还可以设置 URL 显示条数、刷新方法 （手动和自动）及刷新时间间隔。

14.2.4 用户排名

选择**监控** > **流量统计数据** > **用户排名**，进入**用户排名**页面查看用户排名实时信息。管理员还可以设置用户显示条数、刷新方法 （手动和自动）及刷新时间间隔。

14.2.5 IP 地址排名

选择**监控** > **流量统计数据** > **IP 地址排名**，进入 **IP 地址排名**页面查看 IP 地址排名实时信息。管理员还可以设置 IP 地址显示条数、刷新方法 （手动和自动）及刷新时间间隔。

14.3 虚拟系统

显示所有虚拟系统的信息。关于虚拟系统的详细信息，请参见第 13 章，虚拟系统。

选择**监控** > **虚拟系统**。

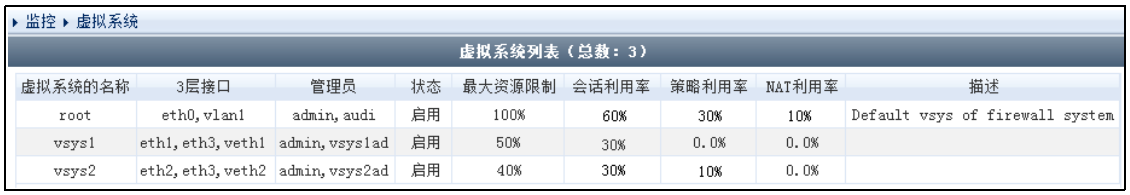


表 275 虚拟系统参数

参数	说明
虚拟系统名称	虚拟系统的名称。
三层接口	虚拟系统包含的三层接口。
管理员	虚拟系统的管理员。
状态	虚拟系统的启禁用状态。
最大资源限制	虚拟系统分配到的资源百分比。
会话利用率	虚拟系统可以使用的会话表资源百分比。
策略利用率	虚拟系统可以使用的策略资源百分比。
NAT 利用率	虚拟系统可以使用的 NAT 资源百分比。
描述	虚拟系统的描述信息。

14.4 STP

NISG 提供 STP 生成树协议的监控功能，实时显示各个 VLAN 和实例中二层接口的工作状态。关于 STP 的详细信息，请参见 4.19 STP。

选择**监控** > **STP**。要查看 STP 监控信息，要先启用 STP。

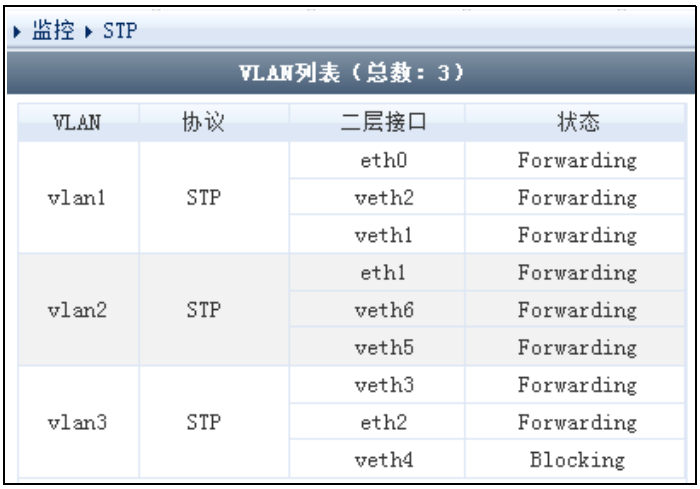


表 276 STP 参数

参数	说明
VLAN	启用 STP 的 VLAN。
协议	VLAN 上开启的协议类型，包括 STP 和 RSTP。
二层接口	VLAN 包含的二层接口，包括二层以太网接口、二层 Channel 接口、二层冗余接口和二层虚拟接口。
状态	VLAN 中二层接口的工作状态，包括禁用、阻塞、侦听、学习、转发和丢弃。

14.5 路由

NISG 的路由监控功能使管理员能够了解缺省路由、策略路由及多播路由的实时信息。关于路由的详细信息，请参见第 5 章，路由。

选择**监控** > **路由**或点击**默认路由表**超链接进入**缺省路由**页面。

表 277　缺省路由参数

参数	说明
类型	路由类型，包括直连路由 （Connected）和静态路由 （Static）。
目的 IP 地址	数据包经过 NISG 发往的目的主机或目的网络 IPv4 或 IPv6 地址。
路由信息	路由过程的详细信息。

选择**监控** > **路由**或点击**策略路由**超链接进入**策略路由**页面。

表 278　策略路由策略参数

参数	说明
名称	策略路由策略名称。
目的 IP 地址	数据包经过 NISG 发往的目的主机或目的网络 IPv4 或 IPv6 地址。
路由信息	路由过程的详细信息。

选择**监控** > **路由**或点击**多播路由**超链接进入**多播路由**页面。

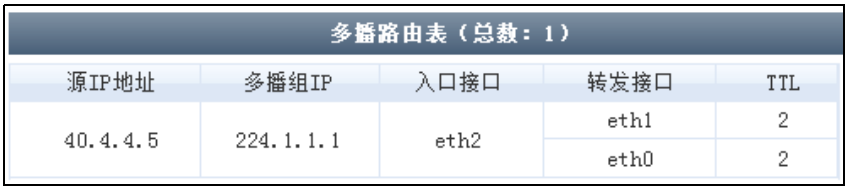


表 279　多播路由参数

参数	说明
源 IP 地址	多播数据包的源 IP 地址。
多播组 IP	目的多播组的 IP 地址。
入口接口	NISG 接收多播数据包的三层接口。
转发接口	NISG 转发多播数据包的三层接口。
TTL	多播数据包在被丢弃前能经过路由设备的最大数目。

14.6 NAT

NISG 的地址转换监控功能，管理员可以对实时地址转换信息进行监控。关于地址转换的详细信息，请参见第 6 章，地址转换。

选择**监控** > **NAT**。

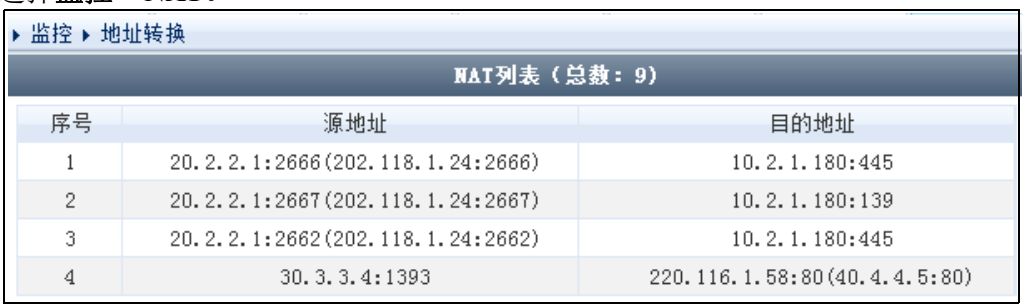


表 280 地址转换参数

参数	说明
源地址	数据包初始源 IP 地址及转换后源 IP 地址 （括号内）。
目的地址	数据包初始目的 IP 地址及转换后目的 IP 地址 （括号内）。

14.7 ARP

NISG 提供对 ARP 表和代理 ARP 表的实时监控。关于更多信息，请参见 4.10 ARP。

14.7.1 ARP 表

选择**监控** > **ARP** > **ARP 表**。点击**刷新**手动刷新 ARP 表信息。点击 进行关键字筛选。

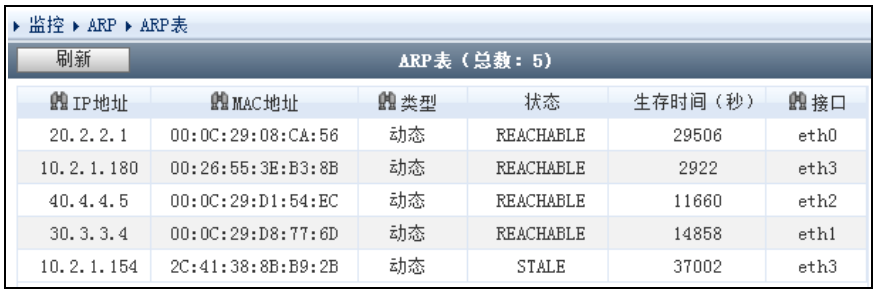


表 281 ARP 表参数

参数	说明
IP 地址	目的主机 IP 地址。该 IP 地址不能是环回地址、多播地址、指向子网的广播地址或受限制的广播地址。
MAC 地址	与 IP 地址相对应的 MAC 地址。该 MAC 地址不能是广播或多播 MAC 地址。
类型	ARP 表项类型，包括静态、动态及代理三种。
状态	ARP 表项状态： • INCOMPLETE：已发送 ARP 请求但还没有应答。 • REACHABLE：可用。 • STALE：可用，但生存时间过长，应再次查询学习。 • FAILED：不可用，该状态不可见。
生存时间 （秒）	动态 ARP 表项存活时间。
接口	表项所属的三层接口。接口包括除隧道接口、 PPPoE 接口和环回接口以外三层接口。

14.7.2 代理 ARP 表

选择**监控** > **ARP** > 代理 **ARP 表**。点击**刷新**，手动刷新代理 ARP 表信息。点击 进行关键字筛选。

表 282 代理 ARP 表参数

参数	说明
IP 地址	目的主机 IP 地址。
MAC 地址	与 IP 地址对应的 MAC 地址。
接口	表项所属三层接口。接口包括除隧道接口、 PPPoE 接口和环回接口以外三层接口。

14.8 CAM

NISG 提供对 CAM 表的监控功能，显示概要信息和地址表实时信息。关于 CAM 的详细信息，请参见 4.11 CAM。

选择**监控** > **CAM**。点击**刷新**，手动刷新地址表信息。点击 进行关键字筛选。

表 283 统计信息参数

参数	说明
动态地址个数	CAM 表中当前动态表项的个数。
静态地址 （用户自定义）个数	CAM 表中当前静态表项的个数。
系统自身绑定地址个数	CAM 表中当前系统自身型的表项的个数。
多播地址个数	CAM 表中当前多播表项的个数。
MAC 地址数最大数	CAM 表中可以包含的最多 MAC 地址个数。
MAC 地址总数	CAM 表中当前 MAC 地址的合计个数。

表 284 地址表参数

参数	说明
目的地址	数据包的目的 MAC 地址。
地址类型	CAM 表项类型，包括 dynamic、 static、 local 和 multicast。
三层接口信息	表项所属 VLAN。
目的端口	接收数据包的目的端口。
超时时间 （秒）	动态 CAM 表项的超时时间，单位为秒。取值范围为 10-30000 秒，缺省为 300 秒。

14.9 DHCP IP 地址绑定状态

显示 NISG 中开启 DHCP 服务器功能的接口与其分配的 IP 地址的信息。关于 DHCP 的详细信息，请参见 4.16 DHCP 服务器。

选择**监控** > **DHCP IP 地址绑定状态**。在**子网**下拉框中选择作用域，查看 DHCP IP 地址绑定状态。

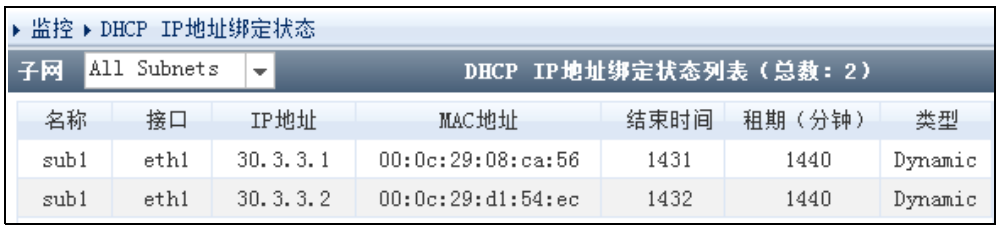


表 285 DHCP IP 地址绑定状态参数

参数	说明
名称	提供 IP 地址的作用域名称。
接口	启用 DHCP 功能的三层接口。
IP 地址	DHCP 服务器分配给 DHCP 客户端的 IP 地址。
MAC 地址	与相应 IP 地址绑定的 DHCP 客户端的 MAC 地址。
结束时间	DHCP 客户端租用 IP 地址的结束时间。
租期 （分钟）	在作用域内分配的 IP 地址租期时间。
类型	在作用域内分配的 IP 地址类型，包括动态分配的 IP 地址 （Dynamic）和固定分配的 IP 地址 （Reserved）。

14.10 DHCPv6 客户端

NISG 提供对 DHCPv6 客户端的实时监控。关于 DHCPv6 的详细信息，请参见 4.18 DHCPv6。

选择**监控** > **DHCPv6 客户端**。

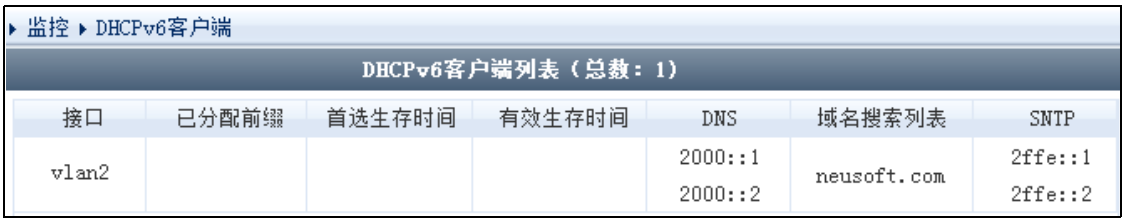


表 286 DHCPv6 客户端参数

参数	说明
接口	NISG 上开启 DHCP 客户端功能的接口。
已分配前缀	客户端获取到的前缀。
首选生存时间	获取到的前缀的首选生存期，单位为秒。
有效生存时间	获取到的前缀的有效生存期，单位为秒。
DNS	客户端获取到的 DNS 服务器地址。
域名搜索列表	客户端获取到的域名搜索列表。
SNTP	客户端获取的的 SNTP 服务器地址，用于同步客户端的系统时间。

14.11 DNS 缓存

NISG 提供对 DNS 动态缓存进行实时监控。关于 DNS 缓存的详细信息，请参见 4.15 DNS 缓存。

选择**监控** > **DNS 缓存**。

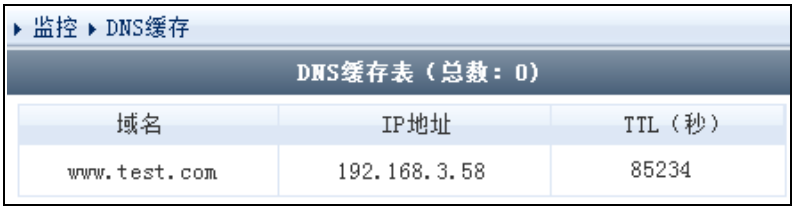


表 287 DNS 动态缓存参数

参数	说明
域名	动态缓存域名。
IP 地址	动态缓存条目中与域名对应的 IPv4 或 IPv6 地址。
TTL （秒）	动态缓存的生存时间。

14.12 高可用性

NISG 提供对虚拟路由器、虚拟路由器探测组及集群进行实时监控。关于高可用性的更多信息，请参见第 12 章，高可用性。

14.12.1 虚拟路由器

显示虚拟路由器及 IP 探测状态实时信息。

选择**监控** > **高可用性** > **虚拟路由器**。从 **VRID** 下拉框选择虚拟路由器标识号查看信息。

表 288 虚拟路由器参数

参数	说明
探测项	NISG 探测的项目，包括： • 选举接口：即本地和对端 NISG 之间通信的接口。 • 备用 IP：即本地和对端 NISG 的备用 IP 地址。 • 状态：即本地 NISG 和对端 NISG 的工作状态，即主和备。 • 运行时间：两次探测行为的时间间隔。 • 组 ID：虚拟路由器探测组 ID。
本地	本地 NISG 探测项目信息。
远程	远端 NISG 探测项目信息。

表 289 IP 探测状态参数

参数	说明
类型	IP 探测类型，包括 ARP Ping、 Ping 和 TCP Ping。
接口	IP 探测的当前设备上的某个三层接口。
IP 地址	NISG 通过指定接口要探测的目的 IP 地址。
端口	IP 探测类型为 TCP Ping 时需要的探测端口。
状态	表示探测的 IP 地址是否可达。 • ✔ — 探测地址可达。 • ✘ — 探测地址不可达。

14.12.2 虚拟路由器探测组

显示虚拟路由器探测组及 IP 探测状态实时信息。

选择**监控** > **高可用性** > **虚拟路由器探测组**。从**组 ID** 下拉框中选择虚拟路由器探测组查看监控信息。

表 290 虚拟路由器探测组

参数	说明
探测项	虚拟路由器探测组成员。
本地	本地 NISG 探测项目信息。
远程	对端 NISG 探测项目信息。

表 291 IP 探测状态参数

参数	说明
类型	IP 探测类型，包括 ARP Ping、 Ping 和 TCP Ping。
接口	IP 探测的当前设备上的某个三层接口。
IP 地址	NISG 通过指定接口要探测的目的 IP 地址。
端口	IP 探测类型为 TCP Ping 时需要的探测端口。
状态	表示探测的 IP 地址是否可达。 • ✔ — 探测地址可达。 • ✘ — 探测地址不可达。

14.12.3 集群

选择**监控** > **高可用性** > **集群**。

表 292 集群参数

参数	说明
探测项	NISG 探测的项目，包括： • 接口：集群内用于传递同步数据的网络接口。 • IP 地址：同步接口的 IP 地址。 • 集群状态：集群内成员的工作状态。 • 配置同步：配置信息同步的启用状态。 • 运行信息同步：运行信息同步的启用状态。 • 系统时间同步：系统时间同步的启用状态。
本地	本地 NISG 探测项目信息。
远程	对端 NISG 探测项目信息。

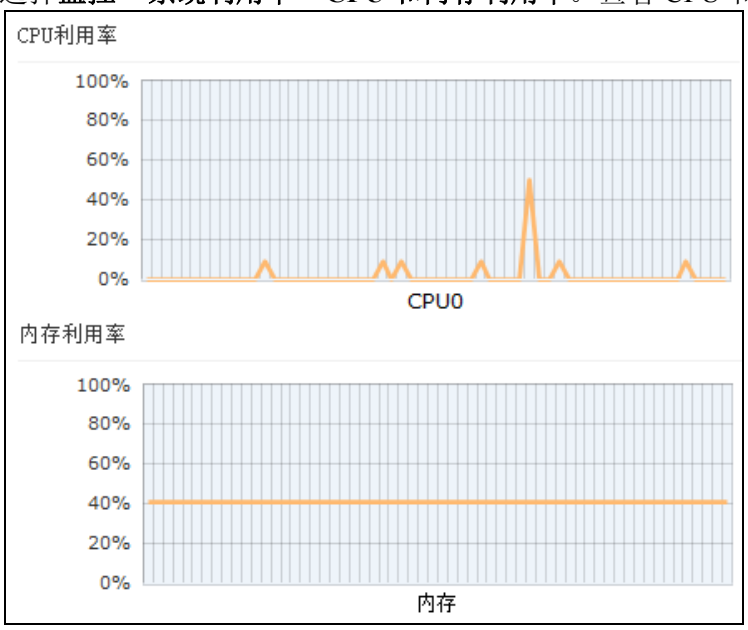
14.13 系统利用率

本节介绍 NISG 的系统资源利用率监控功能，管理员可以对 CPU 和内存及进程利用情况实时进行监控。

14.13.1 CPU 和内存利用率

CPU 和内存利用率显示当前系统的 CPU 和内存使用情况。

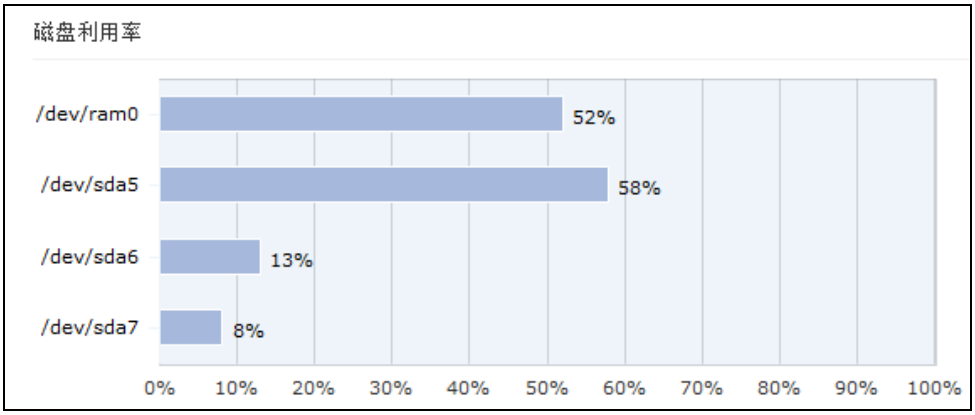
选择**监控** > **系统利用率** > **CPU 和内存利用率**。查看 CPU 和内存使用情况。



14.13.2 磁盘利用率

磁盘利用率监控显示当前系统磁盘的使用情况和日志存储空间的利用率。

选择**监控** > **系统利用率** > **磁盘利用率**，进入**磁盘利用率**页面查看磁盘和日志存储空间利用率。



14.13.3 进程

NISG 提供进程监控功能，管理员可以通过监视和控制进程来管理 CPU 和内存资源。

选择**监控** > **系统利用率** > **进程**。

表 293 进程参数

参数	说明
USER	发起或执行进行的用户。
PID	被内核使用的识别系统进行的唯一标识。
%CPU	活动进程占用 CPU 的百分比。
%MEM	活动进程占用内存的百分比。
VSZ	进程占用虚拟内存的大小，单位为 KB。
RSS	进程占用内存的大小，单位为 KB。
TTY	当前进程的控制终端设备类型。
STATE	进程的状态。
START	进程的启动时间。
TIME	进程目前的执行时间。
COMMAND	进程对应的命令。

14.14 在线用户

NISG 提供在线网络用户监控功能，管理员可以查询在线 WebAuth 用户和 SSL VPN 用户的实时信息。关于网络用户的更多信息，请参见 3.14 网络用户。

14.14.1 WebAuth 用户

选择**监控** > **在线用户** > **WebAuth 用户**。点击**刷新**，手动刷新在线 WebAuth 用户实时信息。勾选某个 WebAuth 用户对应的复选框，点击**离线**强制某个在线 WebAuth 用户下线。点击 进行关键字筛选。

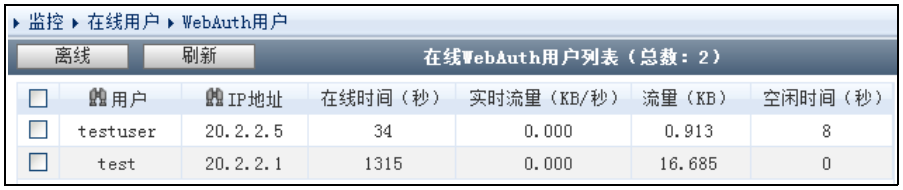


表 294 WebAuth 用户参数

参数	说明
用户	在线的 WebAuth 用户。
IP 地址	在线 WebAuth 用户的登录 IP 地址。
在线时间 （秒）	WebAuth 用户的在线时长，单位为秒。
实时流量 （KB/ 秒）	在线 WebAuth 用户产生的实时流量。
流量 （KB）	在线 WebAuth 用户产生的总流量。
空闲时间 （秒）	在线 WebAuth 用户在空闲时间内不产生流量，则断开该网络连接，单位为秒。

14.14.2 SSL VPN 用户

选择**监控** > **在线用户** > **SSL VPN 用户**。点击**刷新**，手动刷新在线用户实时信息。勾选某个用户对应的复选框，点击**离线**，强制某个在线用户下线。点击 进行关键字筛选。

表 295 SSL VPN 用户参数

参数	说明
用户	在线的 SSL VPN 用户。
用户组	在线 SSL VPN 用户所属的用户组。
登录类型	在线 SSL VPN 用户的登录类型。 NISG 支持通过隧道和 Web-portal 登录。
隧道 / 入口页面	在线 SSL VPN 用户使用的隧道或入口页面。
IP 地址	SSL VPN 用户登录使用的 IP 地址。
在线时间 （秒）	SSL VPN 用户的在线时长，单位为秒。
发送 （字节）	在线 SSL VPN 用户发送的字节数。
接收 （字节）	在线 SSL VPN 用户接收到的字节数。
空闲时间 （秒）	在线 SSL VPN 用户在空闲时间内不产生网络流量，则断开该网络连接，单位为秒。

14.15 IPSec VPN 隧道

管理员可以对自动密钥隧道、手动密钥隧道、加速卡统计信息、软加密统计信息及隧道组进行监控。关于 IPSec VPN 隧道的详细信息，请参见第 11 章，虚拟专用网。

14.15.1 自动密钥隧道

选择**监控** > **IPSec VPN 隧道** > **自动密钥隧道**，在**隧道类型**下拉框中选择**全部**、**静态 IP 地址**、**动态 IP 地址**、**拨号用户**或**拨号用户组**，查看自动密钥隧道信息。当选择**拨号用户组**时，还可以选择要查看的用户组。点击，查看自动密钥隧道信息。

表 296 自动密钥隧道参数

参数	说明
名称	自动密钥隧道名称。
状态	自动密钥隧道状态。 • 开启：VPN 隧道可以转发数据包。 • 关闭：VPN 隧道不能转发数据包。 • 协商：VPN 隧道处于协商状态。
对端类型	自动密钥隧道对端类型，包括静态 IP 地址、动态 IP 地址，拨号用户和拨号用户组。
对端	自动密钥隧道对端标识信息。
隧道添加时间	自动密钥隧道的添加时间。
接收数据包数	自动密钥隧道接收的数据包个数。
发送数据包数	自动密钥隧道发送的数据包个数。

14.15.2 手动密钥隧道

选择**监控** > **IPSec VPN 隧道** > **手动密钥隧道**。点击，查看手动密钥隧道信息。

表 297 手动密钥隧道参数

参数	说明
名称	手动密钥隧道名称。
状态	手动密钥隧道的启禁用状态。
对端	手动密钥隧道的对端 IP 地址。
隧道创建时间	手动密钥隧道的添加时间。
接收数据包数	手动密钥隧道接收的数据包个数。
发送数据包数	手动密钥隧道发送的数据包个数。

14.15.3 加速卡统计

选择**监控** > **IPSec VPN 隧道** > **加速卡统计**。

表 298 加速卡统计信息

参数	说明
名称	加速卡的名称。
状态	加速卡的启禁用状态。
加密数据包数	加速卡加密的数据包数。
加密字节数	加速卡加密的字节数。
解密数据包数	加速卡解密的数据包数。
解密字节数	加速卡解密的字节数。
错误数	发送或接收加密数据包时，被检测到的错误包次数。

14.15.4 软加密统计

选择**监控** > **IPSec VPN 隧道** > **软加密统计**。

表 299 软加密统计信息

参数	说明
加密数据包数	软加密数据包的个数。
加密字节数	软加密字节数。
解密数据包数	软加密解密的数据包个数。
解密字节数	软加密解密的字节数。
错误数	发送或接收软加密数据包时，被检测到的错误包次数。

14.15.5 隧道组

选择**监控** > **IPSec VPN 隧道** > **隧道组**。

表 300 隧道组参数

参数	说明
隧道组 ID	隧道组唯一标识。
启用	隧道组的使用状态： • ✗ — 隧道组未启用。 • ✓ — 隧道组已启用。
VPN 隧道	与当前隧道组关联的 IPSec VPN 隧道。
优先级	隧道组中 IPSec VPN 隧道的优先级。
VPN 隧道状态	隧道组中 IPSec VPN 隧道的当前状态。

14.16 多播

NISG 中提供对 DVMRP 邻居及 ICMP Snooping 的实时信息进行监控。关于多播的详细信息，请参见 5.1.2 三层多播和 5.1.3 二层多播。

14.16.1 DVMRP 邻居

选择**监控** > **多播** > **DVMRP 邻居**。

表 301 DVMRP 邻居信息

参数	说明
IP 地址	DVMRP 邻居的 IP 地址。
超时时间	DVMRP 邻居的超时值，单位为秒。
生成 ID	DVMRP 邻居的多播路由标识。
版本	DVMRP 协议的版本。
索引	DVMRP 的邻居编号。

14.16.2 IGMP Snooping 状态

选择**监控** > **多播** > **IGMP Snooping 状态**。

表 302 IGMP Snooping 状态信息

参数	说明
VLAN	接收多播数据包的接口信息。
状态	VLAN 中 IGMP Snooping 状态，包括开启和关闭。
二层接口	VLAN 包含的二层接口。
IGMP 版本	IGMP 的版本号有三种，分别是 v1、 v2 和 Auto。缺省版本为 Auto。
IGMP 模式	和 NISG 直接连接的网络的类型： • 多播路由器：与 NISG 相连的是多播路由器。多播数据包向该类型的接口发送。 • 主机：该类型的接口相连的是主机。 • 自动协商：接口通过接收的数据包动态地识别网络类型。 默认类型是自动协商。
多播 CAM 表	VLAN 对应的多播 CAM 表。

14.17 报警 / 日志

管理员可以对系统日志、防病毒报警、反垃圾邮件报警、 URL 过滤报警、 IPS 及应用控制报警进行实时监控。

14.17.1 系统日志

选择**监控** > **报警 / 日志** > **系统日志**。点击**刷新**获取最新的系统日志信息。点击 进行关键字筛选。

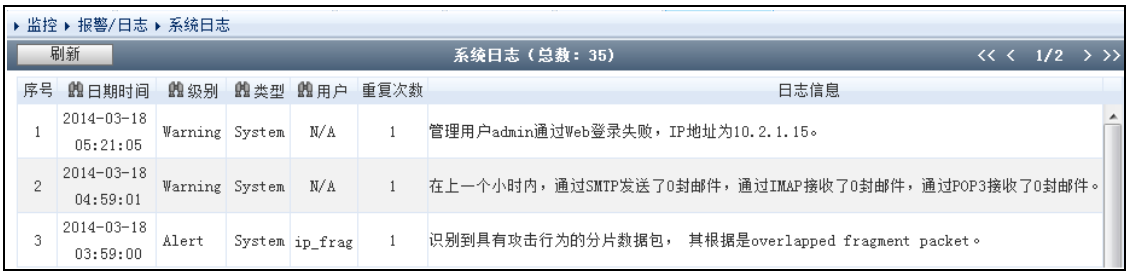


表 303 系统日志参数

参数	说明
日期时间	系统日志产生的日期和时间。
级别	系统日志的安全等级，包括 Emergency、 Alert、 Critical、 Error、 Waring、 Notice、 Informational 和 Debugging。
类型	产生系统日志的模块类型，包括 Management、 Session、 NAT、 FW、 VPN、 IPS、 Anti-Virus、 Anti-Spam、 URL Filtering 和 Application Control。
用户	触发日志产生的用户。
重复次数	系统日志的重复次数。 NISG 对重复产生的日志进行合并标明日志产生的次数。
日志信息	系统日志主体部分，描述事件具体信息。

14.17.2 防病毒报警

选择**监控** > **报警 / 日志** > **防病毒报警**。点击**刷新**获取最新的防病毒报警信息。点击 进行关键字筛选。

表 304 防病毒报警参数

参数	说明
日期时间	检测到病毒文件的日期和时间。
配置防护文件	病毒文件匹配的防病毒策略所引用的防护配置。
文件名	病毒文件名。
文件类型	病毒文件类型。
病毒	检测到的病毒名称。
服务	传输病毒文件的协议，包括 HTTP、 SMTP、 IMAP、 POP3 和 FTP。
源 IP	发送病毒文件的源 IP 地址。
状态	文件被认定为病毒的原因。
描述	病毒文件的详细信息。
动作	对文件进行处理所执行的动作，包括放行和阻断。

14.17.3 反垃圾邮件报警

选择**监控** > **报警 / 日志** > **反垃圾邮件报警**。点击**刷新**获取最新的反垃圾邮件报警信息。点击 进行关键字筛选。

表 305 反垃圾邮件报警参数

参数	说明
日期时间	邮件被检测为垃圾邮件的日期和时间。
配置防护文件	垃圾邮件匹配的反垃圾邮件策略所引用的防护配置。
服务	传输邮件的协议，包括 SMTP 和 POP3。
源 IP	邮件报文的源 IP 地址。
发件人	邮件的发件人。
主题	邮件的主题。
附件	邮件的附件名。
状态	邮件被认定为垃圾邮件的原因。
信息	邮件被认定为垃圾邮件的详细信息。
收件人	邮件的收件人。
动作	对邮件进行处理所执行的动作，包括放行、阻断和标记。

14.17.4 URL 过滤报警

选择**监控** > **报警 / 日志** > **URL 过滤报警**。点击**刷新**获取最新的 URL 过滤报警信息。点击 进行关键字筛选。

表 306 URL 过滤报警参数

参数	说明
日期时间	日志产生的日期和时间。
源 IP	HTTP 请求的源 IP 地址。
URL	HTTP 请求的 URL 信息。
分类	HTTP 请求的分类信息。
信息	HTTP 请求被隔离的详细信息。
动作	对 HTTP 请求的处理所执行的动作，包括放行和阻断。

14.17.5 IPS 报警

选择**监控** > **报警 / 日志** > **IPS 报警**。点击**刷新**获取最新的 IPS 报警信息。点击 进行关键字筛选。

表 307 IPS 报警参数

参数	说明
日期时间	日志产生的日期和时间。
配置防护文件	攻击匹配的攻击签名规则所引用的防护配置。
源 IP	发起攻击的源 IP 地址。
源端口	发起攻击的源端口。
目的 IP	攻击目标的目的 IP 地址。
目的端口	攻击目标的目的端口。
名称	攻击匹配的攻击签名规则集名称。
类别	攻击匹配的攻击签名规则类别。
严重级别	匹配攻击签名规则的攻击的严重程度，包括 High （Critical）、 Medium （Error）、Low （Warning）和 Info （Notification）。
服务	匹配攻击签名规则的攻击使用的服务。
规则 ID	攻击匹配的攻击签名规则标识。
信息	IPS 报警的详细信息。
动作	对攻击行为的处理所执行的动作，包括放行、阻断和拒绝。

14.17.6 应用控制报警

选择**监控** > **报警 / 日志** > **应用控制报警**。点击**刷新**获取最新的应用控制报警信息。点击 进行关键字筛选。

表 308 应用控制报警参数

参数	说明
日期时间	日志产生的日期和时间。
配置防护文件	应用请求匹配的应用控制策略所引用的防护配置。
源 IP	应用请求的源 IP 地址。
源端口	应用请求的源端口。
目的 IP	应用请求的目的 IP 地址。
目的端口	应用请求的目的端口。
协议类型	应用使用的协议类型，如 DNS、 HTTP、 SMTP、 POP3、 IMAP 和 FTP。
应用	匹配应用控制策略的应用名称。
分类	应用所属分类，包括交际类、商务类、多媒体类、网络构建类、通用互联网类。
子分类	应用所属子分类，包括 IP 协议、网络共享等。
风险等级	应用对系统的潜在风险等级。
动作	对该应用请求的处理所执行的动作，包括放行和阻断。

15 报表

本章介绍 NISG 的报表特性。章节结构如下：

- 15.1 概述，介绍报表概念和功能。
- 15.2 基本配置步骤，介绍报表基本配置步骤。不是每个场景都需要所有配置步骤。
- 15.3 配置参数说明，介绍报表配置参数的详细信息。

15.1 概述

报表是基于 WebUI 的一种应用，统计 NISG 记录的实时数据，最终以图表的形式展现给用户。本节介绍报表的基本信息，包括：

- 15.1.1 记录的数据类别
- 15.1.2 报表内容及格式
- 15.1.3 定期生成报表
- 15.1.4 查看 / 下载 / 邮件发送报表结果
- 15.1.5 报表保留数目

15.1.1 记录的数据类别

报表可以记录以下类别相关的数据：

系统；流量； Web 安全；邮件安全；防病毒；攻击；应用；用户

15.1.2 报表内容及格式

- 报表文件包括封皮、目录及统计数据 （以线图、条形图、圆饼图和表格形式展示）。
- 在**计划**页面**内容设置**区域手动添加报表要生成的数据类型。
- 报表封皮使用默认 Logo 或导入 JPG 图片。上传的图片必须小于 100 K，分辨率至少为 96 dpi。如果导入多个图片，系统仅保留最后一个。
- 报表可以以英文或简体中文显示。
- 报表可以以 PDF 或 HTML 格式显示。

15.1.3 定期生成报表

管理员可以制定具体的报表生成计划，以使 NISG 按照计划在规定的时间自动地生成报表。每个虚拟系统最多支持 10 个报表计划。

NISG 提供一个报表计划列表和报表计划预览日历，管理员可以在列表中查看已创建的计划，也可以在日历中查看到不同类型的报表计划： 代表每天计划， 代表每周计划， 代表每月计划。

15.1.4 查看 / 下载 / 邮件发送报表结果

NISG 生成报表后，管理员可以：

- 查看报表结果。
- 下载报表结果至本地。
- 邮件发送报表结果。设置 SMTP 服务器，通过邮件发送报表结果至指定用户。关于设置报表结果发送者和接收者的更多信息，请参见 15.3 配置参数说明。

15.1.5 报表保留数目

设置报表可保留的数目， 5-20 条，缺省为 10 条。

15.2 基本配置步骤

本节介绍报表相关的基本配置步骤：

- 15.2.1 配置常规设置
- 15.2.2 创建报表生成计划
- 15.2.3 管理报表结果

15.2.1 配置常规设置

选择**监控 > 报表 > 常规设置**。

1. 在**报表配置**区域，选择报表要记录的数据类型。

2. 设置 SMTP 服务器及发件人信息。

3. 设置保留报表数目。

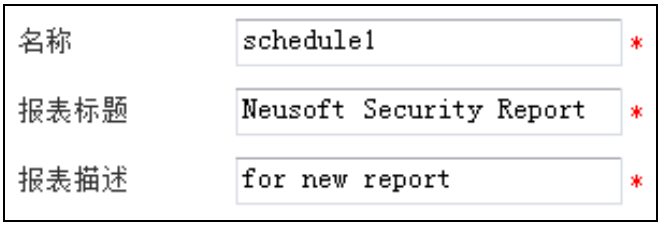
4. 使用默认 Logo 或者点击**导入**上传 Logo。导入后的 Logo 将在**预览**区域显示。

5. 点击**确定**。
6. 点击 。

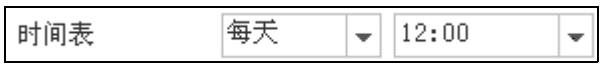
15.2.2 创建报表生成计划

选择**监控 > 报表 > 计划**。

1. 点击**新建**。设置报表基本信息。

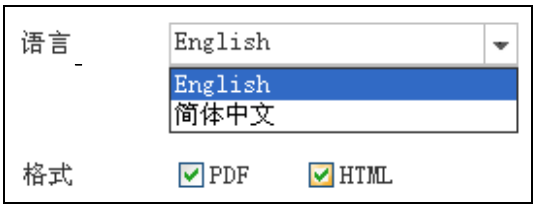


2. 设置报表生成时间表，可以设置每天、每周、每月生成。

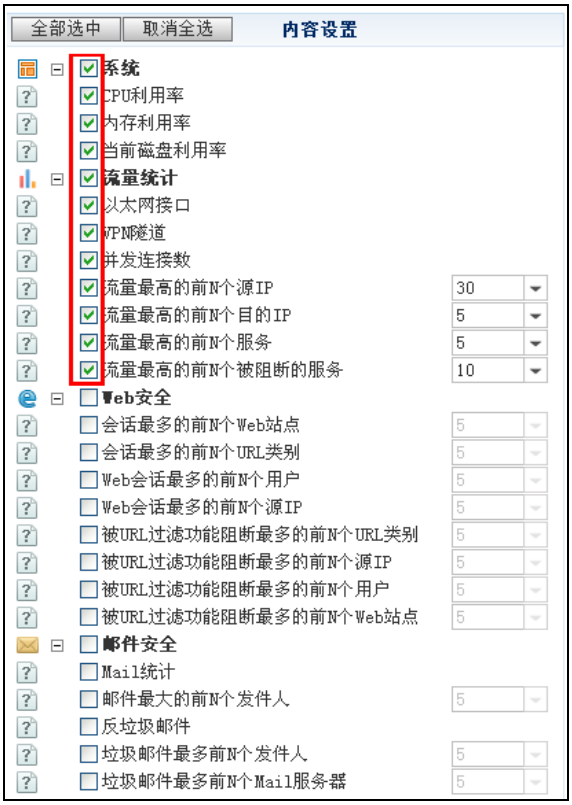


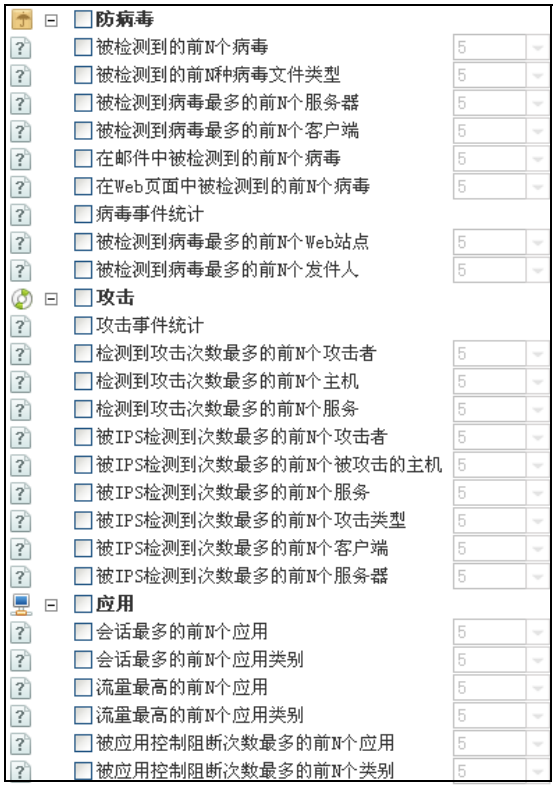
3. 点击**添加**创建报表收件人。

4. 设置报表显示语言及格式。



5. 设置报表要记录的具体内容，类别包括系统、流量统计、Web 安全、邮件安全、防病毒、攻击及应用。





提示：在**内容设置**区域选择记录的内容所属的类别在**常规设置 > 报表配置**区域也要选择，否则对应内容将不会在报表中显示。

6. 设置要记录的用户统计信息。

   如需额外为每类用户显示前 3 个用户的前 5 个应用信息，点击，在弹出的窗口中，勾选**显示前 3 个用户应用统计**复选框。

提示：要记录用户统计信息，需要在**常规设置 > 报表配置**区域勾选**流量**。

7. 选择特定用户或 IP 地址要记录的内容。首先添加特定用户或 IP 地址。

   NISG 可以对特定用户或 IP 地址（最多 5 个）的信息进行统计。点击**特定用户**对应的，在弹出的**用户列表**区域点击**添加**，设定用户或 IP 地址。

提示：只可以选择 NISG 上已存在的网络用户。

8. 查看报表示例图。

   点击图标，查看相应的报表统计信息的示例图。点击**计划**页面底部的**查看报表样例**按钮查看报表样例，也可以将此报表样例保存到本地。

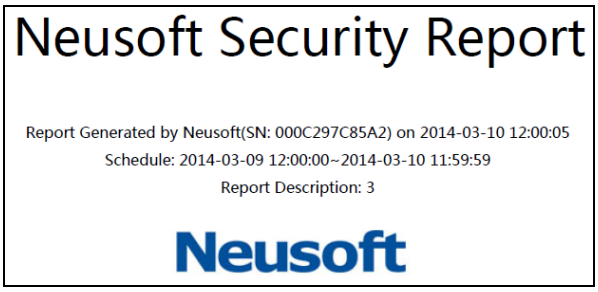
15.2.3 管理报表结果

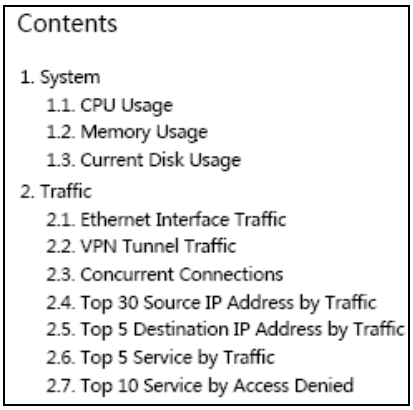
选择**监控** > **报表** > **结果**。

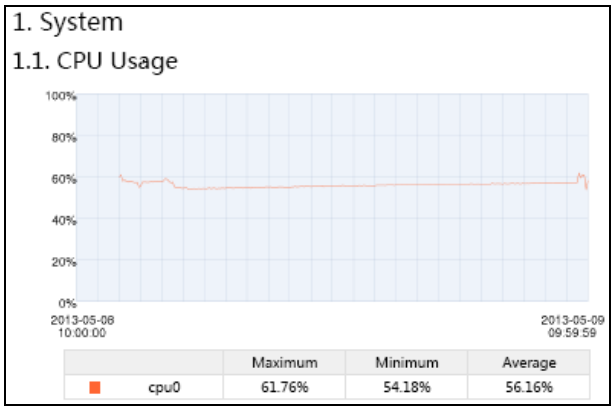
1. 删除报表结果或下载并保存报表结果至本地。

2. 查看报表结果。

   关于报表结果的详细信息，请参见 15.3.4 全局内容参数和 15.3.5 特定用户内容参数。







15.3 配置参数说明

本节介绍报表的配置参数，包括：

- 15.3.1 SMTP 服务器参数
- 15.3.2 报表计划参数
- 15.3.3 报表结果参数
- 15.3.4 全局内容参数
- 15.3.5 特定用户内容参数

15.3.1 SMTP 服务器参数

管理员可以对 NISG 进行配置并要求它通过邮件将报表发送给用户。

表 309 SMTP 服务器和发件人配置信息

参数	说明
地址	SMTP 服务器地址，可以是域名或 IP 地址。
端口	SMTP 服务器端口号。 1-65535。
安全连接	用于启用或禁用 SSL 加密。缺省为禁用。如果启用安全连接，服务器端口号需设置为 465。
发送人	发件人邮件地址。 5~255 字节。
身份认证	用于启用或禁用身份认证。缺省为禁用。 如果 SMTP 服务器要求身份认证，则必须启用身份认证并配置发件人用户名和密码： • 用户名：长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #。 • 密码：0 ～ 255 个字节。可以由 ASCII [33-62] [64-126] 字符组成。
主题	邮件主题。长度 0-64 字节， UTF-8 字符。不能包含以下字符：? ' \ 。

15.3.2 报表计划参数

表 310 报表计划配置信息

参数	说明
名称	长度 1-63 字节， UTF-8 字符。不能包含空格和以下字符：？, " ' \ < > & #。 同一虚拟系统内的报表名称须唯一。
报表标题	长度 1 ～ 63 个字节。 UTF-8 字符。
报表描述	长度 0 ～ 255 个字节。 UTF-8 字符。不能包含以下字符：? " ' \ < > & 。
时间表	用于设置报表生成时间。缺省的时间表为每天 01:00 生成报表。 • 如选择每周生成，缺省为每周一 01:00。 • 如选择每月生成，缺省为每月 1 日 01:00。
收件人列表	列出报表收件人邮件地址。报表生成后， NISG 会自动将生成的报表发送给收件人。 管理员最多可以添加 32 个收件人地址。

表 310 报表计划配置信息 (*续*)

参数	说明
语言	报表显示语言，英文或简体中文，缺省为英文。
格式	报表输出格式， PDF 或 HTML 或两种格式都选。
内容设置	设置在报表中要显示的内容。 用户可以选择与以下主题相关的内容：系统、流量统计、 Web 安全、邮件安全、防病毒、攻击、应用以及用户。 所有内容选项在缺省情况下都是禁用的。关于每个选项的信息，请参见 15.3.4 全局内容参数和 15.3.5 特定用户内容参数。

15.3.3 报表结果参数

所有报表结果按照生成时间倒序显示在**报表结果列表**中。

表 311 报表结果信息

参数	说明
时间	报表生成的时间。
名称	报表生成计划中配置的报表名称。
状态	显示报表是否生成成功。 状态包括：成功、失败、正在生成中。
信息	显示以下两种报表生成信息： • 报表生成失败。 • 连接 SMTP 邮件服务器失败。 “-” 表示报表已成功生成或正在生成中。
报告文件	为管理员提供下载报表的链接。

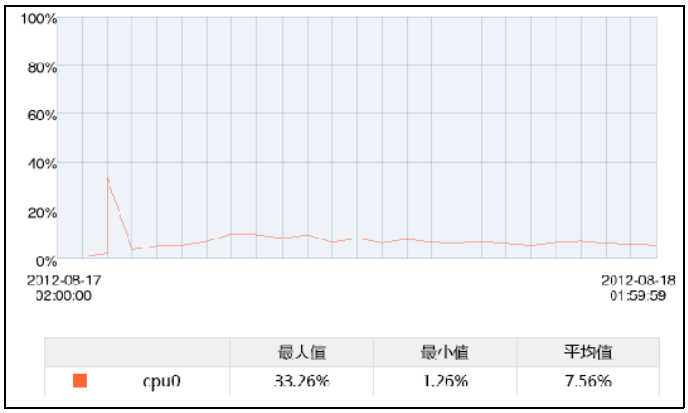
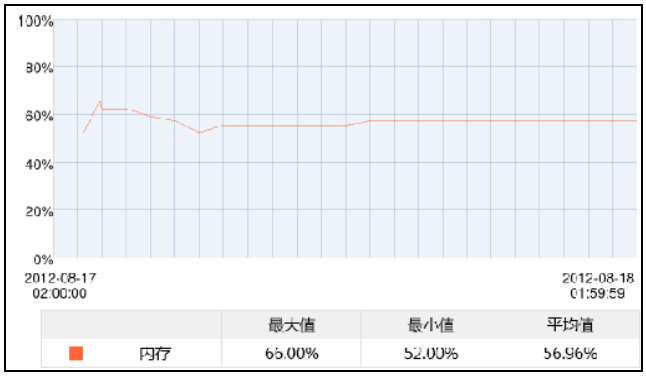
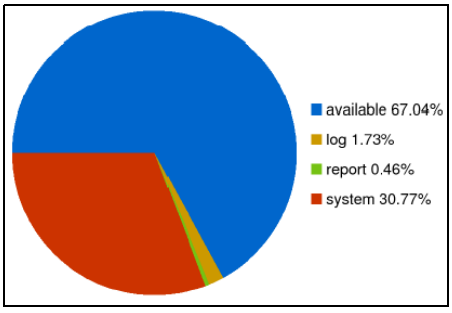
15.3.4 全局内容参数

本节介绍报表中显示的具体内容并给出报表示例。管理员可以选择与以下主题相关的内容：

- 15.3.4.1 系统
- 15.3.4.2 流量统计
- 15.3.4.3 Web 安全
- 15.3.4.4 邮件安全
- 15.3.4.5 防病毒
- 15.3.4.6 攻击
- 15.3.4.7 应用
- 15.3.4.8 用户

15.3.4.1 系统

表 312 系统信息

类型	描述
CPU 利用率	NISG 每 5 分钟统计一次 CPU 利用率并显示平均值。如果系统有多个内核或多个 CPU，那么每个内核或 CPU 会单独显示。  线图中纵坐标为 CPU 利用率百分比。图中绘制图的点为 5 分钟内的均值。
内存利用率	NISG 每 5 分钟统计一次系统内存利用率并显示平均值。  线图中纵坐标为内存利用率百分比。图中绘制图的点为 5 分钟内的均值。
当前磁盘利用率	NISG 统计生成报表时的磁盘使用情况。 

15.3.4.2 流量统计

表 313 流量信息

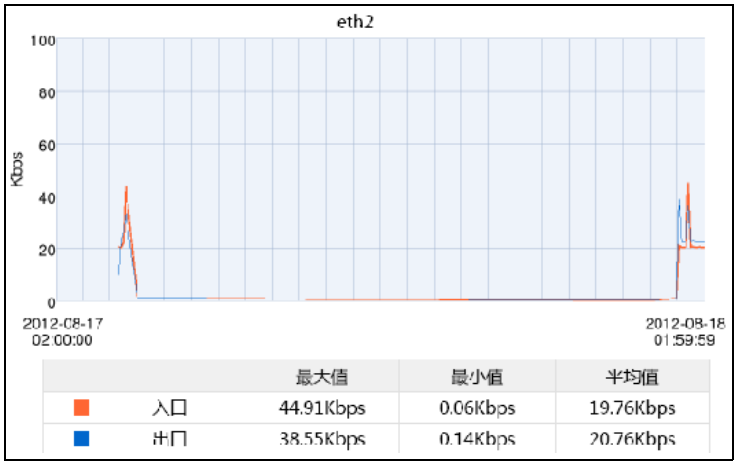
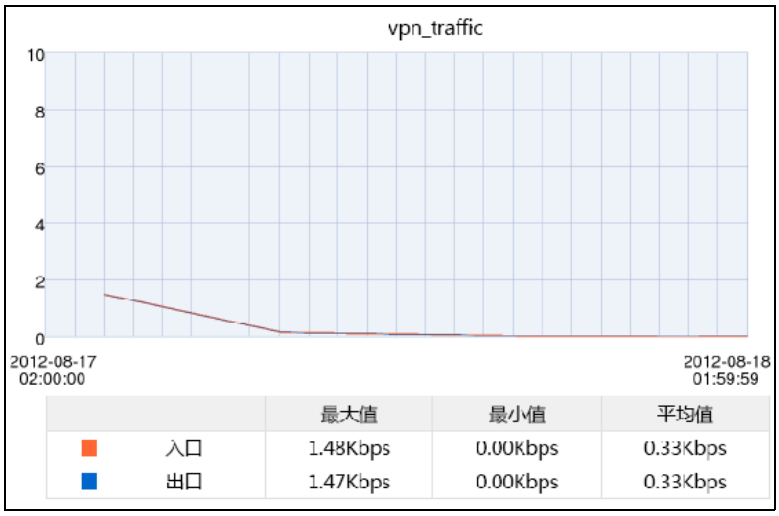
类型	描述
以太网接口	NISG 每 5 分钟统计一次入口和出口以太网接口的流量信息。  线图中绘制图的点为 5 分钟内的均值。
VPN 隧道	NISG 每五分钟统计一次 VPN 隧道入口和出口接口的流量信息。报表中只显示自动密钥隧道配置中前 10 个已经启用的网段到网段隧道的信息。  线图中绘制图的点为 5 分钟内的均值。

表 313 流量信息 (*续*)

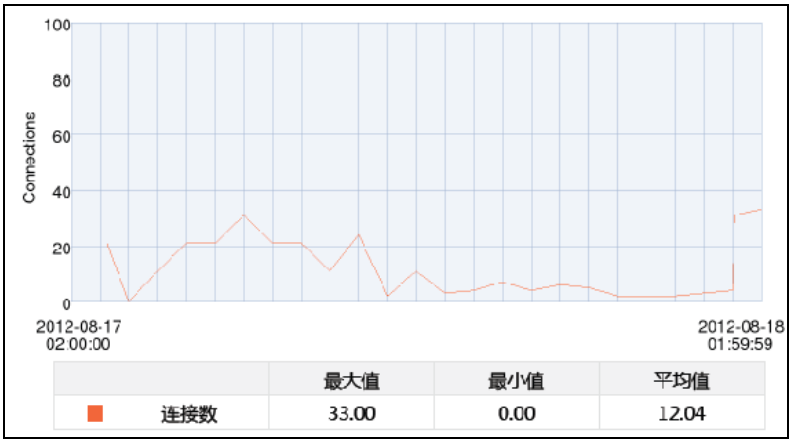
类型	描述
并发连接数	NISG 每 5 分钟统计一次并发连接总数。  线图中绘制图的点为 5 分钟内的总值。
流量最高的前 N 个源 IP	NISG 统计流量最高的前 N 个源 IP 地址的信息。 序列 | 源IP地址 | 流量(KB) | 百分比 1 | 192.168.111.2 | 1902 | 8.34% 2 | 192.168.111.3 | 1706 | 7.48% 3 | 192.168.111.4 | 1560 | 6.84% 4 | 192.168.111.5 | 1329 | 5.83% 5 | 192.168.111.6 | 1290 | 5.66% 说明： • 流量 （KB）：来自某一特定源 IP 地址的总流量。 • 百分比：来自某一特定源 IP 地址的总流量占系统总流量的比例。
流量最高的前 N 个目的 IP	NISG 统计流量最高的前 N 个目的 IP 地址的信息。 序列 | 目地IP地址 | 流量(KB) | 百分比 1 | 192.168.101.2 | 1902 | 8.34% 2 | 192.168.101.3 | 1706 | 7.48% 3 | 192.168.101.4 | 1560 | 6.84% 4 | 192.168.101.5 | 1329 | 5.83% 5 | 192.168.101.6 | 1290 | 5.66% 说明： • 流量 （KB）：发往某一特定目的 IP 地址的总流量。 • 百分比：发往某一特定目的 IP 地址的总流量占系统总流量的比例。

表 313 流量信息 (*续*)

类型	描述
流量最高的前 N 个服务	NISG 统计流量最高的前 N 种服务的信息。 序列 | 端口 | 服务名称 | 流量(KB) | 百分比 1 | UDP:12 | UDP_ANY | 1840 | 8.07% 2 | TCP:13 | TCP_ANY | 1577 | 6.91% 3 | UDP:14 | UDP_ANY | 1376 | 6.03% 4 | TCP:15 | TCP_ANY | 1157 | 5.07% 5 | UDP:16 | UDP_ANY | 1104 | 4.84% 说明： • 端口：目的端口号。如果无端口则显示协议号，如 Other：44。 • 服务名称：使用特定目的端口的服务对象的名称。 • 流量 （KB）：发往某一特定目的端口的总流量。 • 百分比：发往某一特定目的端口的总流量占系统总流量的比例。
流量最高的前 N 个被阻断的服务	NISG 统计被访问策略阻断次数最多的前 N 个服务。 序列 | 端口 | 服务 | 阻断次数 | 百分比 1 | OTHER:1231 | | 23 | 10.95% 2 | OTHER:1232 | | 19 | 9.05% 3 | OTHER:1235 | | 16 | 7.62% 4 | OTHER:1240 | | 12 | 5.71% 5 | OTHER:1247 | | 11 | 5.24% 说明： • 阻断次数：某一特定目的端口被访问策略阻断的总次数。 • 百分比：某一特定目的端口被访问策略阻断的总次数占所有端口被访问策略阻断的总次数的比例。

15.3.4.3 Web 安全

表 314 Web 安全信息

类型	描述
会话最多的前 N 个 Web 站点	被访问次数最多的前 N 个网站的信息。 序列 | 域名 | 会话数 | 百分比 1 | www.baidu.com_1 | 23 | 11.56% 2 | www.baidu.com_2 | 19 | 9.55% 3 | www.baidu.com_3 | 16 | 8.04% 4 | www.baidu.com_4 | 13 | 6.53% 5 | www.baidu.com_5 | 12 | 6.03% 说明： • 会话数：某一特定网站被访问的总次数。 • 百分比：某一特定网站被访问的总次数占所有网站被访问的总次数的比例。
会话最多的前 N 个 URL 类别	被访问次数最多的前 N 种 URL 类别的信息。 序列 | URL分类 | 会话数 | 百分比 1 | 烟酒 | 39 | 8.57% 2 | 匿名技术 | 33 | 7.25% 3 | 艺术 | 31 | 6.81% 4 | 商业 | 27 | 5.93% 5 | 运输 | 26 | 5.71%
Web 会话最多的前 N 个用户	访问 Web 次数最多的前 N 名用户的信息。 序列 | 用户名 | 会话数 | 百分比 1 | test1 | 45 | 22.61% 2 | test2 | 41 | 20.60% 3 | test3 | 33 | 16.58% 4 | test4 | 30 | 15.08% 5 | user*default | 26 | 13.07% 说明： 百分比：某一特定用户访问 Web 的总次数占所有用户访问 Web 的总次数的比例。
Web 会话最多的前 N 源 IP	访问 Web 次数最多的前 N 个源 IP 地址的信息。 序列 | 源IP地址 | 会话数 | 百分比 1 | 192.168.60.2 | 31 | 15.58% 2 | 192.168.60.3 | 27 | 13.57% 3 | 192.168.60.4 | 23 | 11.56% 4 | 192.168.60.5 | 19 | 9.55% 5 | 192.168.60.6 | 18 | 9.05% 说明： 百分比：某一特定源 IP 地址访问 Web 的总次数占所有 Web 访问总次数的比例。

表 314 Web 安全信息 (*续*)

类型	描述
被 URL 过滤功能阻断最多的前 N 个 URL 类别	被 URL 过滤功能阻断次数最多的前 N 个 URL 类别的信息。 序列 | URL分类 | 阻断的URL过滤 | 百分比 1 | 烟酒 | 39 | 8.57% 2 | 匿名技术 | 33 | 7.25% 3 | 艺术 | 31 | 6.81% 4 | 商业 | 27 | 5.93% 5 | 运输 | 26 | 5.71% 说明： • 阻断的 URL 过滤：某一特定 URL 类别被 URL 过滤功能阻断的总次数。 • 百分比：某一特定 URL 类别被 URL 过滤功能阻断的总次数占所有被 URL 过滤功能阻断的 URL 类别的总次数的比例。
被 URL 过滤功能阻断最多的前 N 个源 IP	被 URL 过滤功能阻断次数最多的前 N 个源 IP 地址的信息。 序列 | 源IP地址 | 阻断的URL过滤 | 百分比 2 | 192.168.60.3 | 52 | 11.43% 3 | 192.168.60.4 | 50 | 10.99% 4 | 192.168.60.5 | 46 | 10.11% 5 | 192.168.60.6 | 45 | 9.89%
被 URL 过滤功能阻断最多的前 N 个用户	被 URL 过滤功能阻断次数最多的前 N 个用户的信息。 序列 | 用户名 | 阻断的URL过滤 | 百分比 1 | test1 | 90 | 19.78% 2 | test2 | 84 | 18.46% 3 | test3 | 76 | 16.70% 4 | test4 | 71 | 15.60% 5 | user*default | 68 | 14.95%
被 URL 过滤功能阻断最多的前 N 个 Web 站点	被 URL 过滤功能阻断次数最多的前 N 个 Web 站点的信息。 序列 | 域名 | 阻断的URL过滤 | 百分比 1 | www.baidu.com_6 | 12 | 18.18% 2 | www.baidu.com_12 | 8 | 12.12% 3 | www.baidu.com_18 | 7 | 10.61% 4 | www.baidu.com_30 | 3 | 4.55% 5 | www.baidu.com_24 | 3 | 4.55%

15.3.4.4 邮件安全

表 315 邮件安全信息

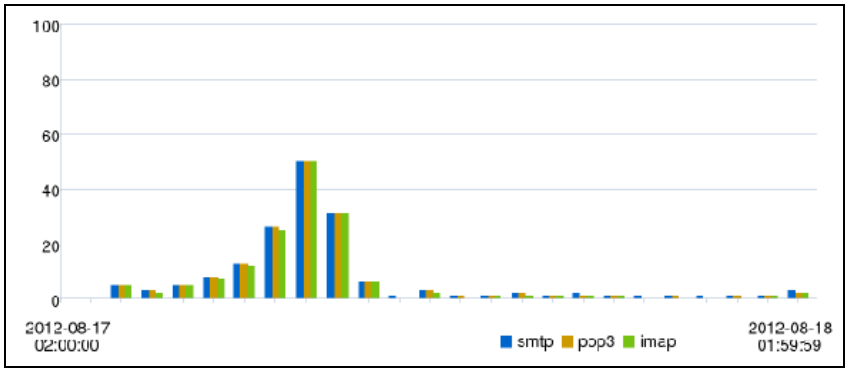
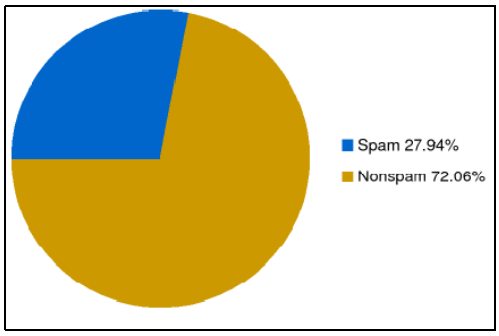
类型	描述
Mail 统计	NISG 统计使用 SMTP、POP3 和 IMAP 三种协议的邮件个数。在每天报表中，每小时统计一次邮件总数；每周报表中，每 6 小时统计一次总数；每月报表中，每 24 小时统计一次。  以上柱形图为每天报表示例。纵坐标为收和发两套邮件数，图中绘制图的点为一小时内的总数。
邮件最大的前 N 个发件人	发送邮件个数最多的前 N 个发件人的信息。 序列 | 发件人 | 邮件数量 | 百分比 1 | bbbb_1@hmail.com | 30 | 17.96% 2 | bbbb_5@hmail.com | 18 | 10.78% 3 | bbbb_9@hmail.com | 15 | 8.98% 4 | bbbb_13@hmail.com | 13 | 7.78% 5 | bbbb_17@hmail.com | 13 | 7.78% 说明： • 邮件数量：某一特定发件人发送邮件的总数。 • 百分比：某一特定发件人发送邮件的总数占所有邮件总数的比例。
反垃圾邮件	垃圾邮件占邮件总数的比例。 

表 315 邮件安全信息

类型	描述
垃圾邮件最多前 N 个发件人	发送垃圾邮件个数最多的前 N 个发件人的信息。 序列 | 发件人 | 垃圾邮件数量 | 百分比 2 | bbbb_2@hmail_2.com | 16 | 9.09% 3 | bbbb_3@hmail_3.com | 13 | 7.39% 4 | bbbb_4@hmail_0.com | 11 | 6.25% 5 | bbbb_5@hmail_1.com | 11 | 6.25%
垃圾邮件最多前 N 个 Mail 服务器	发送垃圾邮件个数最多的前 N 个邮件服务器的信息。 序列 | 邮件服务器域名 | 垃圾邮件数量 | 百分比 1 | hmail_1.com | 57 | 32.39% 2 | hmail_2.com | 48 | 27.27% 3 | hmail_3.com | 37 | 21.02% 4 | hmail_0.com | 34 | 19.32%

15.3.4.5 防病毒

表 316 防病毒信息

类型	描述
被检测到的前 N 个病毒	被检测出次数最多的前 N 个病毒的信息。 序列 | 病毒名称 | 检测到的病毒数量 | 百分比 1 | Eicar-Signature_1.UNOFFICIAL | 23 | 10.09% 2 | Eicar-Signature_2.UNOFFICIAL | 19 | 8.33% 3 | Eicar-Signature_3.UNOFFICIAL | 17 | 7.46% 4 | Eicar-Signature_4.UNOFFICIAL | 14 | 6.14% 5 | Eicar-Signature_5.UNOFFICIAL | 13 | 5.70% 说明： • 检测到的病毒数量：某一特定病毒被检测出的总次数。 • 百分比：在某一特定病毒被检测出的总次数占检测出病毒总次数的比例。
被检测到的前 N 种病毒文件类型	被检测出病毒次数最多的前 N 种文件类型的信息。 序列 | 文件类型 | 检测到的病毒数量 | 百分比 1 | rar | 50 | 21.93% 2 | zip | 46 | 20.18% 3 | txt | 38 | 16.67% 4 | dat | 35 | 15.35% 5 | jpg | 31 | 13.60%
被检测到病毒最多的前 N 个服务器	被服务器保护检测出病毒次数最多的前 N 个服务器的信息。 序列 | 服务器IP/域名 | 服务器类型 | 检测到的病毒数量 | 百分比 1 | hmail_2.com | POP3 | 21 | 19.27% 2 | hmail_0.com | HTTP | 14 | 12.84% 3 | hmail_2.com | SMTP | 12 | 11.01% 4 | hmail_2.com | FTP | 11 | 10.09% 5 | hmail_0.com | IMAP | 11 | 10.09% 说明： • 检测到的病毒数量：某一特定服务器被服务器保护检测出病毒的总次数。 • 百分比：某一特定服务器被服务器保护检测出病毒的总次数占服务器保护检测出病毒的总次数的比例。

表 316 防病毒信息 (*续*)

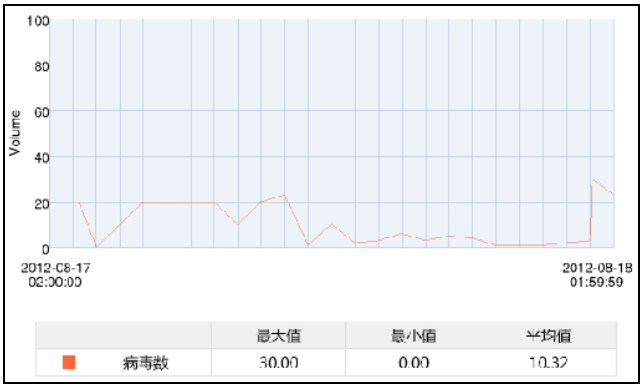
类型	描述
被检测到病毒最多的前 N 个客户端	被客户端保护检测出病毒次数最多的前 N 个客户端的信息。 序列 | 客户端IP | 检测到的病毒数量 | 百分比 1 | 192.1.2.2 | 33 | 27.73% 2 | 192.1.2.4 | 27 | 22.69% 3 | 192.1.2.6 | 21 | 17.65% 4 | 192.1.2.10 | 19 | 15.97% 5 | 192.1.2.8 | 19 | 15.97% 说明： • 检测到的病毒数量：某一特定客户端被客户端保护检测出病毒的总次数。 • 百分比：某一特定客户端被客户端保护检测出病毒的总次数占客户端保护检测出病毒的总次数的比例。
在邮件中被检测到的前 N 个病毒	在邮件中被检测到次数最多的前 N 个病毒的信息。 序列 | 病毒名称 | 检测到的病毒数量 | 百分比 1 | Eicar-Signature_1.UNOFFICIAL | 23 | 15.65% 2 | Eicar-Signature_2.UNOFFICIAL | 19 | 12.93% 3 | Eicar-Signature_3.UNOFFICIAL | 17 | 11.56% 4 | Eicar-Signature_6.UNOFFICIAL | 12 | 8.16% 5 | Eicar-Signature_7.UNOFFICIAL | 11 | 7.48%
在 Web 页面中被检测到的前 N 个病毒	在 Web 页面中被检测到次数最多的前 N 个病毒的信息。 序列 | 病毒名称 | 检测到的病毒数量 | 百分比 1 | Eicar-Signature_4.UNOFFICIAL | 14 | 34.15% 2 | Eicar-Signature_9.UNOFFICIAL | 11 | 26.83% 3 | Eicar-Signature_14.UNOFFICIAL | 8 | 19.51% 4 | Eicar-Signature_19.UNOFFICIAL | 8 | 19.51%
病毒事件统计	NISG 每 5 分钟统计一次检测出的病毒的总数。  线图中纵坐标为检测出病毒的总次数。图中绘制图的点为 5 分钟内的总次数。

表 316 防病毒信息 (*续*)

类型	描述
被检测到病毒最多的前 N 个站点	被检测出病毒次数最多的前 N 个网站的信息。 序列 | 网站名称 | 检测到的病毒数量 | 百分比 1 | hmail_0.com | 14 | 34.15% 2 | hmail_1.com | 11 | 26.83% 3 | hmail_2.com | 8 | 19.51% 4 | hmail_3.com | 8 | 19.51%
被检测到病毒最多的前 N 个发件人	在邮件中检测出病毒次数最多的前 N 个发件人的信息。 序列 | 发件人 | 检测到的病毒数量 | 百分比 No. | Sender | Viruse Detected | Rate 3 | bbbb_3@hmail_3.com | 17 | 11.56% 4 | bbbb_6@hmail_2.com | 12 | 8.16% 5 | bbbb_7@hmail_3.com | 11 | 7.48%

15.3.4.6 攻击

表 317 攻击信息

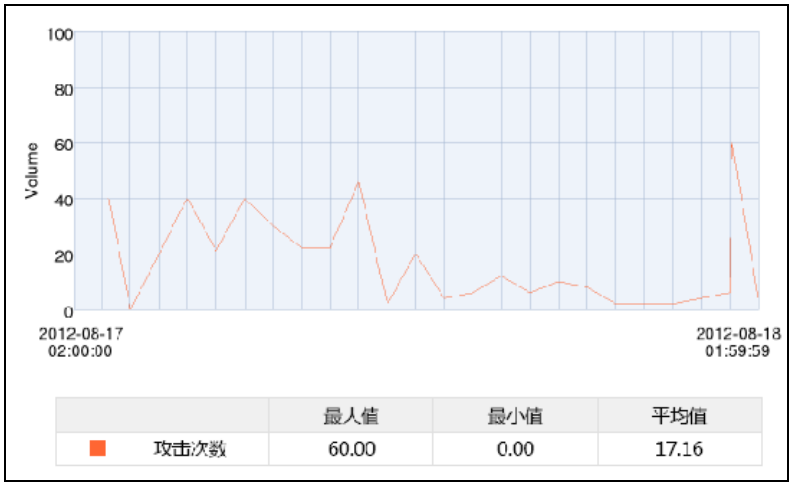
类型	描述
攻击事件统计	NISG 每 5 分钟统计一次攻击发生的总数。  线图中纵坐标为攻击发生的总次数。图中绘制图的点为 5 分钟内的总次数。
检测到攻击次数最多的前 N 个攻击者	被检测到攻击次数最多的前 N 个攻击者的信息。 序列 | 攻击者 | 检测到的攻击数量 | 百分比 1 | 10.168.1.2 | 31 | 8.40% 2 | 192.169.3.2 | 29 | 7.86% 3 | 10.168.1.3 | 27 | 7.32% 4 | 192.169.2.3 | 24 | 6.50% 5 | 10.168.1.4 | 22 | 5.96% 说明： • 攻击者：攻击者的 IP 地址。 • 检测到的攻击数量：某一特定攻击者发起攻击的总次数。 • 百分比：某一特定攻击者发起攻击的总次数占检测到攻击总次数的比例。
检测到攻击次数最多的前 N 个主机	被攻击次数最多的前 N 个主机的信息。 序列 | 受攻击主机 | 检测到的攻击数量 | 百分比 1 | 10.2.1.2 | 31 | 8.40% 2 | 192.169.2.2 | 29 | 7.86% 3 | 10.2.1.3 | 27 | 7.32% 4 | 192.169.3.3 | 24 | 6.50% 5 | 10.2.1.4 | 22 | 5.96%

表 317 攻击信息 (*续*)

类型	描述
检测到攻击次数最多的前 N 个服务	被攻击次数最多的前 N 个服务的信息。 序列 | 端口 | 服务 | 检测到的攻击数量 | 百分比 1 | TCP:280 | TCP_ANY | 23 | 8.42% 2 | OTHER:1231 | | 23 | 8.42% 3 | OTHER:1232 | | 19 | 6.96% 4 | UDP:281 | UDP_ANY | 18 | 6.59% 5 | OTHER:1235 | | 15 | 5.49% 说明： • 端口：目的端口号。如果无端口则显示协议号，如 Other：44。 • 服务：使用特定目的端口的服务对象的名称。
被 IPS 检测到次数最多的前 N 个攻击者	被 IPS 检测出发起攻击次数最多的前 N 个攻击者的信息。 序列 | 攻击者 | 检测到的攻击数量 | 百分比 1 | 10.168.1.2 | 31 | 8.40% 2 | 192.169.3.2 | 29 | 7.86% 3 | 10.168.1.3 | 27 | 7.32% 4 | 192.169.2.3 | 24 | 6.50% 5 | 10.168.1.4 | 22 | 5.96% 说明： • 检测到的攻击数量：IPS 检测出的某一特定攻击者发起攻击的总次数。 • 百分比：IPS 检测出的某一特定攻击者发起攻击的总次数占 IPS 检测到攻击总次数的比例。
被 IPS 检测到次数最多的前 N 个被攻击的主机	被 IPS 检测到被攻击次数最多的前 N 个主机的信息。 序列 | 受攻击主机 | 检测到的攻击数量 | 百分比 1 | 192.169.2.2 | 29 | 16.29% 2 | 192.169.3.3 | 24 | 13.48% 3 | 192.169.2.4 | 21 | 11.80% 4 | 192.169.3.5 | 17 | 9.55% 5 | 192.169.2.6 | 16 | 8.99%
被 IPS 检测到次数最多的前 N 个服务	被 IPS 检测到被攻击次数最多的前 N 个服务的信息。 序列 | 端口 | 服务 | 检测到的攻击数量 | 百分比 1 | TCP:280 | TCP_ANY | 23 | 28.05% 2 | UDP:281 | UDP_ANY | 18 | 21.95% 3 | TCP:285 | TCP_ANY | 10 | 12.20% 4 | UDP:286 | UDP_ANY | 9 | 10.98% 5 | TCP:290 | TCP_ANY | 5 | 6.10%

表 317 攻击信息 (*续*)

类型	描述
被 IPS 检测到次数最多的前 N 个攻击类型	被 IPS 检测出发起攻击次数最多的前 N 个攻击类型的信息。 序列 | 攻击类型 | 检测到的攻击数量 | 百分比 1 | 未知 | 104 | 58.43% 2 | 输入验证错误 | 44 | 24.72% 3 | 跨站脚本(CSS/XSS) | 30 | 16.85%
被 IPS 检测到次数最多的前 N 个客户端	客户端保护中 IPS 检测到被攻击次数最多的前 N 个客户端的信息。 序列 | 客户端IP | 检测到的攻击数量 | 百分比 1 | 192.169.2.2 | 29 | 30.85% 2 | 192.169.2.4 | 21 | 22.34% 3 | 192.169.2.6 | 16 | 17.02% 4 | 192.169.2.10 | 14 | 14.89% 5 | 192.169.2.8 | 14 | 14.89% 说明： • 检测到的攻击数量：客户端保护中 IPS 检测出的某一特定主机被攻击的总次数。 • 百分比：客户端保护中 IPS 检测出的某一特定主机被攻击的总次数占客户端保护中 IPS 检测出攻击的总次数的比例。
被 IPS 检测到次数最多的前 N 个服务器	服务器保护中 IPS 检测到被攻击次数最多的前 N 个服务器的信息。 序列 | 服务器IP/域名 | 检测到的攻击数量 | 百分比 1 | 192.169.3.3 | 24 | 28.57% 2 | 192.169.3.5 | 17 | 20.24% 3 | 192.169.3.7 | 15 | 17.86% 4 | 192.169.3.1 | 14 | 16.67% 5 | 192.169.3.9 | 14 | 16.67% 说明： • 检测到的攻击数量：服务器保护中 IPS 检测出的某一特定服务器被攻击的总次数。 • 百分比：服务器保护中 IPS 检测出的某一特定服务器被攻击的总次数占服务器保护中 IPS 检测到攻击总次数的比例。

15.3.4.7 应用

表 318 应用信息

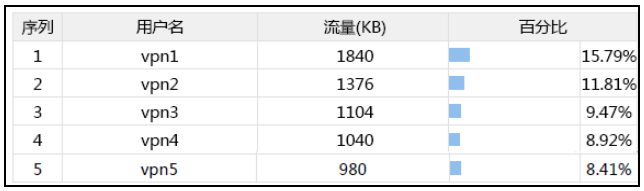
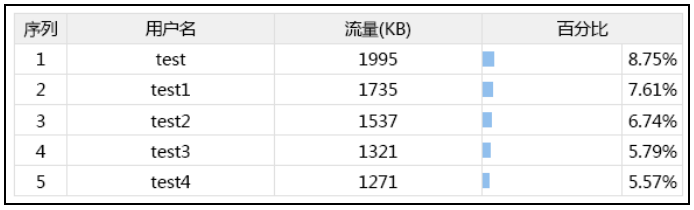
类型	描述
会话最多的前 N 个应用	会话数最多的应用的信息。 序列 | 应用 | 会话数 | 百分比 1 | 魔兽世界 | 23 | 10.04% 2 | NNTP | 19 | 8.30% 3 | Daytime | 16 | 6.99% 4 | IMAP | 13 | 5.68% 5 | MSN | 12 | 5.24% 说明： • 应用：应用的名称。 • 会话数：某一特定应用的会话总数。 • 百分比：某一特定应用的会话总数占所有应用会话数的比例。
会话最多的前 N 个应用类别	会话数最多的前 N 种应用类别的信息。 序列 | 应用分类 | 会话数 | 百分比 1 | 即时通讯 | 39 | 17.03% 2 | 游戏 | 30 | 13.10% 3 | 管理软件 | 30 | 13.10% 4 | 互联网实用类 | 27 | 11.79% 5 | 电子邮件 | 23 | 10.04%
流量最高的前 N 个应用	产生流量最高的前 N 个应用的信息。 序列 | 应用 | 流量(KB) | 百分比 1 | POP2 | 2923 | 12.82% 2 | POP3 | 2538 | 11.13% 3 | 魔兽世界 | 2361 | 10.35% 4 | NNTP | 2166 | 9.50% 5 | Daytime | 2137 | 9.37% 说明： • 流量 （KB）：某一特定应用产生的总流量。 • 百分比：某一特定应用产生的总流量占所有应用流量的比例。
流量最高的前 N 个应用类别	产生流量最高的前 N 个应用类别的信息。 序列 | 应用分类 | 流量(KB) | 百分比 1 | 电子邮件 | 8619 | 37.79% 2 | 即时通讯 | 4176 | 18.31% 3 | 游戏 | 2361 | 10.35% 4 | 互联网实用类 | 2166 | 9.50% 5 | 管理软件 | 2137 | 9.37%

表 318 应用信息 (*续*)

类型	描述
被应用控制阻断次数最多的前 N 个应用	被应用控制阻断会话数最多的前 N 个应用的信息。 序列 | 应用 | 会话数 | 百分比 1 | POP2 | 35 | 14.64% 2 | POP3 | 29 | 12.13% 3 | 魔兽世界 | 26 | 10.88% 4 | NNTP | 23 | 9.62% 5 | Daytime | 22 | 9.21% 说明： • 会话数：某一特定应用的会话被应用控制阻断的总数。 • 百分比：某一特定应用的会话被应用控制阻断的总数占所有应用被应用控制阻断的会话总数的比例。
被应用控制阻断次数最多的前 N 个类别	被应用控制阻断会话数最多的前 N 个应用类别的信息。 序列 | 应用分类 | 会话数 | 百分比 1 | 电子邮件 | 97 | 40.59% 2 | 即时通讯 | 38 | 15.90% 3 | 游戏 | 26 | 10.88% 4 | 互联网实用类 | 23 | 9.62% 5 | 管理软件 | 22 | 9.21%

15.3.4.8 用户

表 319 用户信息

类型	描述
流量最高的前 N 个 IPSec VPN 用户	产生流量最高的前 N 个 IPSec VPN 用户的信息。  说明： • 流量 （KB）：某一特定 IPSec VPN 用户产生的总流量。 • 百分比：某一特定 IPSec VPN 用户产生的总流量占 IPSec VPN 用户总流量的比例。
流量最高的前 N 个 SSL VPN 用户	产生流量最高的前 N 个 SSL VPN 用户的信息。 说明： • 流量 （KB）：某一特定 SSL VPN 用户产生的总流量。 • 百分比：某一特定 SSL VPN 用户产生的总流量占 SSL VPN 用户总流量的比例。
流量最高的前 N 个用户	产生流量最高的前 N 个 VPN 用户和 WebAuth 用户的信息。  说明： • 流量 （KB）：某一特定用户产生的总流量。 • 百分比：某一特定用户产生的总流量占用户总流量的比例。
流量最高的前 N 个 WebAuth 用户	产生流量最高的前 N 个 WebAuth 用户的信息。 说明： • 流量 （KB）：某一特定 WebAuth 用户产生的总流量。 • 百分比：某一特定 WebAuth 用户产生的总流量占所有 WebAuth 用户总流量的比例。

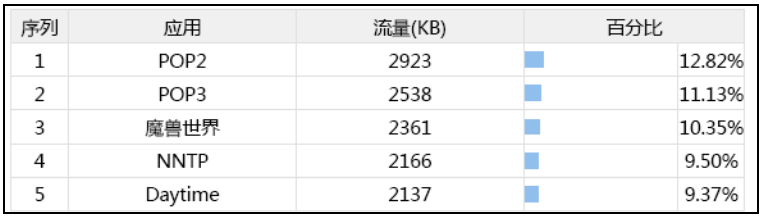
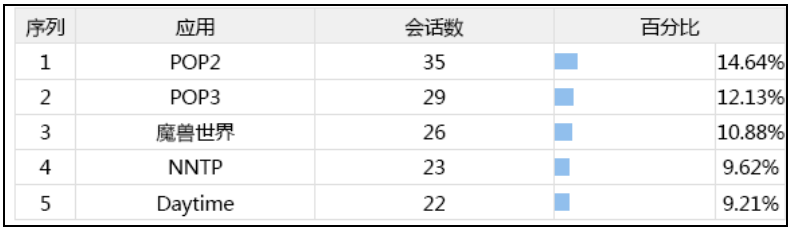
15.3.5 特定用户内容参数

管理员可以为特定用户或源 IP 地址选择与以下主题相关的内容：

- 15.3.5.1 应用
- 15.3.5.2 Web 安全

15.3.5.1 应用

表 320 特定用户应用信息

类型	描述
流量最高的前 N 个应用	被指定用户或 IP 地址访问并产生最高流量的前 N 个应用的信息。  说明： • 流量 （KB）某一特定应用产生的总流量。 • 百分比：某一特定应用产生的总流量占此用户或源 IP 地址所有应用流量的比例。
被应用控制阻断次数最多的前 N 个应用	被指定用户或源 IP 地址访问且会话被应用控制阻断次数最多的前 N 个应用的信息。  说明： • 会话数：某一特定应用的会话被应用控制阻断的总数。 • 百分比：某一特定应用的会话被应用控制阻断的总数占此用户或源 IP 地址被应用控制阻断的会话总数的比例。

15.3.5.2 Web 安全

表 321 特定用户 Web 安全信息

类型	描述
会话最多的前 N 个 Web 站点	被指定用户或 IP 地址访问次数最多的前 N 个网站的信息。 序列 | 域名 | 会话数 | 百分比 1 | www.baidu.com_1 | 23 | 11.56% 2 | www.baidu.com_2 | 19 | 9.55% 3 | www.baidu.com_3 | 16 | 8.04% 4 | www.baidu.com_4 | 13 | 6.53% 5 | www.baidu.com_5 | 12 | 6.03% 说明： • 会话数：某一特定网站的被访问的总次数。 • 百分比：某一网站被访问的总次数占此用户或源 IP 地址访问所有网站总次数的比例。
会话最多的前 N 个 URL 类别	被指定用户或 IP 地址访问的次数最多的前 N 种 URL 类别的信息。 序列 | URL分类 | 会话数 | 百分比 1 | 烟酒 | 39 | 8.57% 2 | 匿名技术 | 33 | 7.25% 3 | 艺术 | 31 | 6.81% 4 | 商业 | 27 | 5.93% 5 | 运输 | 26 | 5.71% 说明： • 会话数：某一特定 URL 类别被访问的总次数。 • 百分比：某一 URL 类别被访问的总次数占此用户或源 IP 地址访问所有 URL 类别的总次数的比例。
被 URL 过滤功能阻断最多的前 N 个 URL 类别	被指定用户或 IP 地址访问且被 URL 过滤功能阻断次数最多的前 N 个 URL 类别的信息。 序列 | URL分类 | 阻断的URL过滤 | 百分比 1 | 烟酒 | 39 | 8.57% 2 | 匿名技术 | 33 | 7.25% 3 | 艺术 | 31 | 6.81% 4 | 商业 | 27 | 5.93% 5 | 运输 | 26 | 5.71% 说明： • 阻断的 URL 过滤：某一特定 URL 类别被 URL 过滤功能阻断的总次数。 • 百分比：某一特定 URL 类别被 URL 过滤功能阻断的总次数占此用户或源 IP 地址访问的所有 URL 类别被 URL 过滤功能阻断的总次数的比例。
被 URL 过滤功能阻断最多的前 N 个 Web 站点	被指定用户或 IP 地址访问且被 URL 过滤功能阻断次数最多的前 N 个 Web 站点的信息。 序列 | 域名 | 阻断的URL过滤 | 百分比 1 | www.baidu.com_6 | 12 | 18.18% 2 | www.baidu.com_12 | 8 | 12.12% 3 | www.baidu.com_18 | 7 | 10.61% 4 | www.baidu.com_30 | 3 | 4.55% 5 | www.baidu.com_24 | 3 | 4.55% 说明： 百分比：某一特定网站被 URL 过滤功能阻断的总次数占此用户或源 IP 地址访问的所有网站被 URL 过滤功能阻断的总次数的比例。

A MIB 库

NISG 支持：

- 公共 MIB 库
- 私有 MIB 库

公共 MIB 库

下面给出了本产品的公共 MIB 库。

表 322 公共 MIB 库

1. system

1.1. systemInfo

1	sysDescr	实体的文本描述，它应该包含系统硬件类型、软件操作系统和网络软件的全名和版本标识。该描述应只包含可打印的 ASCII 字符。
2	sysObjectID	通过厂商权威认证的包含在实体中的网络管理子系统的标识。该值置于 SMI 的厂商子树（1.3.6.1.4.1）中，对被管实体究竟是什么给出一个简单、清晰的说明。例如：厂商 'Flintstones. Inc.' 被分配子树 1.6.1.4.1.4242, 那么就可分配标识符 1.3.6.1.4.1.4242.1.1 到 'Fred Router'。
3	sysUpTime	系统最近一次重新初始化网络管理部分至现在的时间 （以百分之一秒计）。
4	sysContact	该受管节点的联系人的文本标识，以及有关如何与该人员联系的信息。
5	sysName	该受管节点的名字。按照惯例，这是该节点的标准域名。
6	sysLocation	该节点的物理位置 （例如 'telephone closet, 3rd floor'）。
7	sysServices	表明此实体可能提供的服务集的值。该值是一个和数。此和数先取值零，然后对于该节点为其执行事务的每个层 （L，范围为 1 至 7），则添加 2 的 （L - 1）次幂到总和。例如，一个仅执行路由选择功能的节点的值为 4 （2^ （3-1））。相反，主机对之提供应用程序服务的节点的值为 72 （2^ （4-1） + 2^ （7-1））。 注意：在因特网协议套件的上下文中，值的计算应该根据： 层 功能 1 物理的 （如转发器） 2 数据链路和子网 （例如网桥） 3 网际网 （如支持 IP） 4 端对端 （如支持 TCP） 7 应用程序 （例如支持简单管理传输协议）。
8	sysORLastChange	当任意 sysORID 实例改变状态或值时， sysUpTime 的当前值。

表 322 公共 MIB 库

	1.2. sysORTable/sysOREntry	
9	sysORIndex	辨别 sysORTable 中对象的索引值。
10	sysORID	SNMPv2 支持的 MIB 模型的权威标识。
11	sysORDescr	sysORID 相应的文本描述。
12	sysORUpTime	此概念行最近一次初始化时的 sysUpTime 值。
	2. interfaces	
	2.1. ifTable/ifEntry	
13	ifIndex	用于各接口的特定值，范围在 1 和 ifNumber 之间；在网络管理实体的重新初始化到下一次重新初始化的时间里，该值应该保持不变。
14	ifDescr	包含接口信息的文本字符串。此字符串应包括制造商名称，产品名称和硬件接口的版本号。
15	ifType	根据网络层协议栈的物理 / 链路协议区分的接口类型。
16	ifMtu	通过接口传送 / 接受的最大数据报，单位是字节。这是网络上传送的最大数据报。
17	ifSpeed	接口流量带宽的估计，单位是 b/s。对于那些带宽不变或者不能被准确估算的接口，该对象应包含标称带宽。
18	ifPhysAddress	在协议栈里紧挨网络层的协议层的接口地址。对于没有这种地址的接口 ，该目标应该包含长度为零的字符串。
19	ifAdminStatus	接口的希望值。（3）测试状态表明没有操作包流过。
20	ifOperStatus	接口当前的操作状态，（3）测试状态表明没有操作包流过。
21	ifLastChange	从 snmpd 系统启动到接口状态改变 （插拔网线）的时间。如果期间接口状态没有改变，则该值为 0。
22	ifInOctets	该接口上收到的 8 位字节的总数 （包括结构字符）。
23	ifInUcastPkts	发送给高层的单播分组数。
24	ifInNUcastPkts	发送给高层协议的非单播 （多播或广播）分组数。
25	ifInDiscards	为了阻止发往高层而被丢弃的输入分组数。一种可能的原因是为了增大缓冲空间。
26	ifInErrors	收到的由于差错被丢弃的输入分组数。
27	ifInUnknownProtos	收到的由于未知协议或是不支持的协议被丢弃的分组数。
28	ifOutOctets	接口输出的 8 位字节总数 （包括结构字符）。
29	ifOutUcastPkts	从高层接收到的单播分组数 （包括被丢弃的和未发送的）。
30	ifOutNUcastPkts	从高层接收到的非单播 （如多播或广播）分组数 （包括被丢弃的和未发送的）。
31	ifOutDiscards	为了阻止发往高层而被丢弃的输出分组数。一种可能的原因是为了增大缓冲空间。
32	ifOutErrors	发出的由于差错被丢弃的输出分组数。
33	ifOutQLen	当前输出数据包队列长度。
34	ifSpecific	MIB 定义的参考信息，特别针对实现接口的特殊介质，如果接口是通过以太网实现的，则该对象的值指的是针对以太网定义的文档；如果没有此信息，则它的值应设为 OBJECT IDENTIFIER { 0 0 }, 它是一个有效的对象标识符，任何 asn.1 和误码率必须能够生成并识别这个值。
	2.2. interfacesInfo	
35	ifNumber	系统当前的网络接口数量 (不考虑当前状态)。

表 322 公共 MIB 库

	3. at	
	3.1. atIfTable/atIfEntry	
36	atIfIndex	由索引号识别的接口和由 ifIndex 识别的接口相同 （该等价关系在这个接口上有效）。
37	atPhysAddress	独立媒介的物理地址。若设置为长度为 0 的字符串，则表示无效表项。就是说，该项目有效地区分了所指项目辨识的接口和所指项目辨识的映射。代理程序是否将无效的项目从表格中删除要依每个执行而定。因此，管理站必须准备从与当前不在用的项目相对应的代理程序哪儿接收表格式的信息。对此类项目的正确理解需要对有关的 atPhysAddress 对象的检查。
38	atNetAddress	对应于独立媒介的物理地址的网络地址 （例如 IP 地址）。
	4. ip	
	4.1. IpGroup	
39	ipForwarding	该实体是否作为 IP 网关传输数据报（此实体收到的）。IP 网关传输数据报， IP 主机不传输。注意，对一些受控节点，此对象代表可能出现的值的子集。因此，如果一个管理站试图改变该对象的值时，主体可能会返回一个 'badValue' 的响应。
40	ipDefaultTTL	当传输层不提供 TTL 值时，输入到 IP 报头 TTL 域中的默认值。
41	ipInReceives	从所有接口上接收的 IP 数据报总数 (包括错误的数据包) 。
42	ipInHdrErrors	由于 IP 报头错误而丢弃的输入数据报数 (例如，校验和差错，版本不匹配，格式错误，TTL 超时，选项错误等）。
43	ipInAddrErrors	由于 IP 报头目的域中 IP 地址无效而丢弃的输入数据报数。它包括无效地址 （如 0.0.0.0）和不支持类的地址 （如 Class E）。对于没有 IP 网关和不传送数据报的实体，它指的是由于目的地址不是本地地址而被丢弃的数据报数。
44	ipForwDatagrams	由于本实体不是最终 IP 地址，而需要找到一条路径来转发的 IP 数据报数。如果该实体不是网关，那么这个数值只包括通过该实体的 IP 包。
45	ipInUnknownProtos	由于未知或者不支持的协议而被丢弃的发往本地的 IP 数据报数。
46	ipInDiscards	由于资源限制而丢弃的数据报数 （如缺乏缓冲空间）。注意，该数据不包含等待重组的数据报。
47	ipInDelivers	成功发送到 IP 用户协议层 （包括 ICMP）的 IP 数据报数。
48	ipOutRequests	传递给 IP 用户协议层 （包括 ICMP）来传输的 IP 数据报总数。注意，不包括已经在 ipForwDatagrams 中计入的那些。
49	ipOutDiscards	由于资源限制而丢弃的数据报数 （如缺乏缓冲空间）。注意，如果这种报文满足丢弃标准，那么该数据包含在 ipForwDatagrams 中计入的那些。
50	ipOutNoRoutes	由于没有路由来传送而丢弃的 IP 数据报数。注意，该数据包括满足 ‘ 无路由 ’ 条件的计入 ipForwDatagrams 中的数。注意，它还包括由于默认的网关关闭，主机不能传送的数据报。
51	ipReasmTimeout	在等待重组时已收到的数据报片被保留的最大秒数。
52	ipReasmReqds	收到的需要进行重组的 IP 数据报片的数目。
53	ipReasmOKs	已成功重组的 IP 数据报数。
54	ipReasmFails	IP 重组算法检测到的失败次数 （超时，错误，等等）。注意，他不一定是被丢弃的 IP 数据片数，因为有的算法 （特别是在 RFC815 种的算法）找不到数据片数。
55	ipFragOKs	被成功分片的 IP 数据报数。
56	ipFragFails	需要进行分片，但由于设置了 “ 不分片 ” 标志而不能分片的 IP 数据报数。
57	ipFragCreates	由分片而产生的 IP 数据报片的数目。

表 322 公共 MIB 库

	4.2. ipAddrTable/ipAddrEntry	
58	ipAdEntAddr	该实体地址信息所属的 IP 地址。
59	ipAdEntIfIndex	索引值唯一决定了可用的接口。由索引特定值识别的接口和由 ifIndex 识别的接口相同。
60	ipAdEntNetMask	对应这个 IP 地址的子网掩码。它是一个 IP 地址，其中所有网络位设为 1，主机位设为 0。
61	ipAdEntBcastAddr	ip 广播地址中的最低位的值，通常是 1。这个值适用于子网和网络广播地址，所用的实体就是这个 （逻辑）接口。
62	ipAdEntReasmMaxSize	在这个接口上收到的、能够进行重组的、最长的 IP 数据报。
	4.3. ipRouteTable/ipRouteEntry	
63	ipRouteDest	该路由的目的 IP 地址。默认路由为 0.0.0.0。在表中可能出现多路由对应单一目的地的情况，但是它依赖表准入机制，此机制由网络管理协议决定。
64	ipRouteIfIndex	本地接口定义的索引值。这个接口是路由应该到达的下一跳。这个由特定索引值定义的接口和由 ifIndex 定义的是一样的。
65	ipRouteMetric1	主要的选路度量。这个度量的意义取决于选路协议 (ipRouteProto)。 -1 表示未使用。
66	ipRouteMetric2	备用的选路度量。这个度量的意义取决于选路协议 (ipRouteProto)。 -1 表示未使用。
67	ipRouteMetric3	备用的选路度量。这个度量的意义取决于选路协议 (ipRouteProto)。 -1 表示未使用。
68	ipRouteMetric4	备用的选路度量。这个度量的意义取决于选路协议 (ipRouteProto)。 -1 表示未使用。
69	ipRouteNextHop	路由器下一跳的 IP 地址 （如果路由器绑定一个接口，这个接口是通过广播媒体实现的，那么这个值就是该接口上代理的 IP 地址的值）。
70	ipRouteType	路由类型。注意，直接值 （3）和间接值 （4）指的是在 IP 结构上直接和间接路由。设置该值无效 （2）会导致在 ipRouteTable 中的相应的对象值无效。也就是说，它有效地区分了所指项目辨识的目的和所指项目辨识的路由。代理程序是否将无效的项目从表格中删除要依每个执行而定。因此，管理站必须准备从与当前不在用的项目相对应的代理程序哪儿接收表格式的信息。对此类项目的正确理解需要检查相关的 ipRouteType 对象。
71	ipRouteProto	学习到的路由机制。网关路由协议的共享值不意味着主机应该支持这些协议。
72	ipRouteAge	自从路由上次被更新或确定是正确的以后所经历的秒数。注意， 'too old' 没有意义，除非根据学习到的路由的相关信息来推断。
73	ipRouteMask	在和 ipRouteDest 相比较之前，掩码要与目的 IP 地址进行逻辑 “ 与 ”，对于不支持任意子网掩码的系统，代理服务器创建 ipRouteMask 的值，通过检验 ipRouteDest 域值是否属于 A， B， C 类网，然后利用： mask network 255.0.0.0 class-A 255.255.0.0 class-B 255.255.255.0 class-C 如果 ipRouteDest 的值为 0.0.0.0 （一个默认路由），那么其掩码值也为 0.0.0.0。应该注意的是所有 IP 路由子系统默认使用这个机制。
74	ipRouteMetric5	备用的选路度量。这个度量的意义取决于选路协议 (ipRouteProto)。 -1 表示未使用。
75	ipRouteInfo	MIB 定义的参考信息，特别针对该路由的路由协议，如在路由中的 ipRouteProto 值，如果没有此信息，则它的值应设为 OBJECT IDENTIFIER { 0 0 }, 它是一个有效的对象标识符，任何 asn.1 和误码率必须能够生成并识别这个值。
	4.4. ipNetToMediaTable/ipNetToMediaEntry	
76	ipNetToMediaIfIndex	该接口上的等价性有效。由索引特定值识别的接口和由 ifIndex 识别的接口相同。

表 322 公共 MIB 库

77	ipNetToMediaPhysAddress	独立媒介的物理地址。
78	ipNetToMediaNetAddress	对应独立媒介物理地址的 IP 地址。
79	ipNetToMediaType	映射的类型：输入影响 ipNetToMediaTable 的有效值。就是说，有效地区分了所指项目辨识的接口和所指项目辨识的映射。代理程序是否将无效的项目从表格中删除要依每个执行而定。因此，管理站必须准备从与当前不在用的项目相对应的代理程序哪儿接收表格式的信息。对此类项目的正确理解需要对有关的 ipNetTomediaType 对象的检查。
	4.5. ipRoutingDiscards	
80	ipRoutingDiscards	所选择的选路表项即使是有效的但也要丢弃的数目。一种可能的原因可能是为其他路由器释放缓存空间。
	4.6. ipCidrRouteNumber	
81	ipCidrRouteNumber	当前有效的 ipCidrRouteTable 记录的个数。
	4.7. ipCidrRouteTable/ipCidrRouteEntry	
82	ipCidrRouteDest	路由的目的 IP 地址。此对象不会取组播地址值 （D 类）。如果 X 与相应 ipCidrRouteMask 对象的值逻辑与不等于 X，那么值 X 必须被丢弃。
83	ipCidrRouteMask	在和 ipCidrRouteDest 相比较之前，掩码要与目的 IP 地址进行逻辑 “ 与 ”。对于不支持任意子网掩码的系统，代理服务器参考 IP 地址类创建 ipCidrRouteMask 的值，如果 X 与相应 ipCidrRouteMask 对象的值逻辑与不等于 ipCidrRouteDest，那么值 X 必须被丢弃。
84	ipCidrRouteTos	策略是被 IP 的 TOS 域所指定的。 IP 的 TOS 的编码是通过下面的描述来说明。如果没有更多特殊的策略应用， 0 表示缺省路径。 +-----+-----+-----+-----+-----+-----+-----+-----+ | | | | | PRECEDENCE | TYPE OF SERVICE | 0 | | | | | +-----+-----+-----+-----+-----+-----+-----+-----+ IP TOS IP TOS Field Policy Field Policy Contents Code Contents Code 0 0 0 0 ==> 0 0 0 0 1 ==> 2 0 0 1 0 ==> 4 0 0 1 1 ==> 6 0 1 0 0 ==> 8 0 1 0 1 ==> 10 0 1 1 0 ==> 12 0 1 1 1 ==> 14 1 0 0 0 ==> 16 1 0 0 1 ==> 18 1 0 1 0 ==> 20 1 0 1 1 ==> 22 1 1 0 0 ==> 24 1 1 0 1 ==> 26 1 1 1 0 ==> 28 1 1 1 1 ==> 30。
85	ipCidrRouteNextHop	下一跳路由的地址，否则是 0.0.0.0。
86	ipCidrRouteIfIndex	本地接口定义的 ifIndex 值。
87	ipCidrRouteType	路由类型。注意，本地 （3）对应的是路由的下一跳是最终目的；远程 （4）对应的是下一跳是非最终目的。
88	ipCidrRouteProto	选路协议。网关路由协议包含的值不意味主机应该支持这些协议。
89	ipCidrRouteAge	自从路由上次被更新或确定是正确的以后所经历的秒数。

表 322 公共 MIB 库

90	ipCidrRouteInfo	在 ipCidrRouteProto 中指定的选路协议的 MIB 定义的引用。 MIB 定义的参考信息，特别针对该路由的路由协议，如在路由中的 ipRouteProto 值，如果没有此信息，则它的值应设为 OBJECT IDENTIFIER { 0 0 }, 它是一个有效的对象标识符，任何 asn.1 和误码率必须能够生成并识别这个值。
91	ipCidrRouteNextHopAS	下一跳的自治系统的数目。这个对象的含义是被在路由的 ipCidrRouteProto 值所指定的路由协议来决定的。当这个对象是未知的或者是和他的值没有关系，那么应该被设置为 0。
92	ipCidrRouteMetric1	主要的选路度量。这个度量的意义取决于选路协议 (ipCidrRouteProto)。 -1 表示未使用。
93	ipCidrRouteMetric2	备用的选路度量。这个度量的意义取决于选路协议 (ipCidrRouteProto)。 -1 表示未使用。
94	ipCidrRouteMetric3	备用的选路度量。这个度量的意义取决于选路协议 (ipCidrRouteProto)。 -1 表示未使用。
95	ipCidrRouteMetric4	备用的选路度量。这个度量的意义取决于选路协议 (ipCidrRouteProto)。 -1 表示未使用。
96	ipCidrRouteMetric5	备用的选路度量。这个度量的意义取决于选路协议 (ipCidrRouteProto)。 -1 表示未使用。
97	ipCidrRouteStatus	它排列出可变的状态，通常是列出安装和卸载的约定。

5. icmp

5.1. IcmpGroup

98	icmpInMsgs	收到的 ICMP 报文总数。注意，该值应该包括所有 icmpInErrors 计入的数。
99	icmpInErrors	收到的有差错的 ICMP 报文数 （例如，无效的 ICMP 检验和，错误长度等）。
100	icmpInDestUnreachs	收到的 ICMP 目的站不可达报文数。
101	icmpInTimeExcds	收到的 ICMP 超时报文数。
102	icmpInParmProbs	收到的 ICMP 参数问题报文数。
103	icmpInSrcQuenchs	收到的 ICMP 源站抑制报文数。
104	icmpInRedirects	收到的 ICMP 重定向报文数。
105	icmpInEchos	收到的 ICMP 回显请求报文数。
106	icmpInEchoReps	收到的 ICMP 回显应答报文数。
107	icmpInTimestamps	收到的 ICMP 时间戳请求报文数。
108	icmpInTimestampReps	收到的 ICMP 时间戳应答报文数。
109	icmpInAddrMasks	收到的 ICMP 地址掩码请求报文数。
110	icmpInAddrMaskReps	收到的 ICMP 地址掩码应答报文数。
111	icmpOutMsgs	输出的 ICMP 报文总数。注意，该值应该包括所有 icmpOutErrors 计入的数。
112	icmpOutErrors	由于 ICMP 报文中一个问题 （例如，缓存空间不足）而未发送的 ICMP 报文数。该值应该不包括 ICMP 层外部发现的错误，如无效的 IP 发送合成数据报。在某些情况下，可能没有类型的错误计入此计数器的值。
113	icmpOutDestUnreachs	发送的 ICMP 目的站不可达报文数。
114	icmpOutTimeExcds	发送的 ICMP 超时报文数。
115	icmpOutParmProbs	发送的 ICMP 参数问题报文数。
116	icmpOutSrcQuenchs	发送的 ICMP 源站抑制报文数。
117	icmpOutRedirects	发送的 ICMP 重定向报文数。对于主机，此对象应总为零，因为主机不发送重定向报文。
118	icmpOutEchos	发送的 ICMP 回显请求报文数。
119	icmpOutEchoReps	发送的 ICMP 回显应答报文数。

表 322 公共 MIB 库

120	icmpOutTimestamps	发送的 ICMP 时间戳请求报文数。
121	icmpOutTimestampReps	发送的 ICMP 时间戳应答报文数。
122	icmpOutAddrMasks	发送的 ICMP 地址掩码请求报文数。
123	icmpOutAddrMaskReps	发送的 ICMP 地址掩码应答报文数。

6. tcp

6.1. TcpGroup

124	tcpRtoAlgorithm	用来计算重传超时值的算法。
125	tcpRtoMin	以毫秒计的最小重传 （TCP 允许的）超时值。此类对象的更精确的语义取决于确定重传超时的算法，尤其是当超时算法是 rsre(3) 时，此类对象可视为 LBOUND 量 （RFC793 所述）。
126	tcpRtoMax	以毫秒计的最小重传 （TCP 允许的）超时值。此类对象的更精确的语义取决于确定重传超时的算法，尤其是当超时算法是 rsre(3) 时，此类对象可视为 UBOUND 量 （RFC793 所述）。
127	tcpMaxConn	支持的最大的 TCP 连接数。若为动态的，则值为 -1。
128	tcpActiveOpens	TCP 连接从 CLOSED 状态直接到 SYN_SENT 状态的转变次数。
129	tcpPassiveOpens	TCP 连接从 LISTEN 状态直接到 SYN_SENT 状态的转变次数。
130	tcpAttemptFails	从 SYN_SENT 或 SYN_RCVD 到 CLOSED 的状态变迁数，加上从 SYN_RCVD 到 LISTEN 的状态变迁数。
131	tcpEstabResets	从 ESTABLISHED 或 CLOSE_WAIT 状态到 CLOSED 的状态变迁数。
132	tcpCurrEstab	当前在 ESTABLISHED 或 CLOSE_WAIT 状态的连接数。
133	tcpInSegs	收到的报文段的总数 （包括错误的）。该值包括收到的当前建立联系的段。
134	tcpOutSegs	发送的报文段的总数，但将仅包含重传字节的除外。
135	tcpRetransSegs	重传的报文段的总数，即传输的 TCP 段的数目，包含一个或多个先前传送的字节。

6.2. tcpConnTable/tcpConnEntry

136	tcpConnState	此 TCP 连接的状态。管理站设置的唯一值是 deleteTCB(12)。因此，如果管理站试图给此对象设定其他值，那么代理会适当的返回一个 'badValue' 响应；如果一个管理站设定次对象的值为 deleteTCB(12)，那么它将删除对应受控节点的连接的 TCB(RFC793 中所述)，导致立即的连接中断。作为一个特定的执行选项， RST 段从受控节点发给其它 TCP 终点 (注意，尽管 RST 段不能可靠的发出)。
137	tcpConnLocalAddress	此 TCP 连接的本地 IP 地址。 0.0.0.0 代表监听进程愿意在任何接口接受连接。
138	tcpConnLocalPort	此 TCP 连接的本地端口号。
139	tcpConnRemAddress	此 TCP 连接的远程 IP 地址。
140	tcpConnRemPort	此 TCP 连接的远程端口号。
141	tcpInErrs	收到的具有一个差错 （如无效的检验和）的报文段总数。
142	tcpOutRsts	具有 RST 标志置位的报文段的总数。

7. udp

7.1. UdpStats

143	udpInDatagrams	发给 UDP 用户的 UDP 数据报输入数。
144	udpNoPorts	没有发送到有效端口的 UDP 数据报个数。

表 322 公共 MIB 库

145	udpInErrors	接收到的由于其他原因造成无法发送的 UDP 数据报的个数 (不包含每发送到有效端口的原因)。
146	udpOutDatagrams	发给该实体的 UDP 数据报输出数。
	7.2. udpTable/udpEntry	
147	udpLocalAddress	监听进程的本地 IP 地址。 0.0.0.0 代表接受任何接口的数据报。
148	udpLocalPort	监听进程的本地端口号。
	8. transmission	
	8.1. dot3	
149	dot3StatsIndex	标识一个接口是以太网媒介的唯一的索引值。由索引特定值识别的接口和由 ifIndex 识别的接口相同。
150	dot3StatsAlignmentErrors	在一个特定接口上接收到的并且没有通过 FCS 校验的帧的计数值，它们的长度不是整字节数。当 alignmentError 状态被 MAC 服务器返回给 LLC(或其他 MAC 用户)，此对象代表的数值增加。由 IEEE802.3 管理层协议，收到的帧 (由多重错误条件获得) 完全根据 LLC 的错误状态来计数。
151	dot3StatsFCSErrors	在一个特定接口上接收到的并且没有通过 FCS 校验的帧的计数值，它们的长度不是整字节数。当 frameCheckError 状态被 MAC 服务器返回给 LLC(或其他 MAC 用户)，此对象代表的数值增加。由 IEEE802.3 管理层协议，收到的帧 (由多重错误条件获得) 完全根据 LLC 的错误状态来计数。
152	dot3StatsSingleCollisionFrames	在一个特定接口上成功发送的帧的计数值，此时发送正好被两个或更多个冲突所抑制。帧可由此对象实例计数，也可由相应的其它实例计数，如 ifOutUcastPkts，ifOutMulticastPkts 和 ifOutBroadcastPkts ；但是它不能由 dot3StatsMultipleCollisionFrames 对象实例计数。参考 IEEE 802.3 管理层。
153	dot3StatsMultipleCollisionFrames	在一个特定接口上成功发送的帧的计数值，此时发送正好被两个或更多个冲突所抑制。帧可由此对象实例计数，也可由相应的其它实例计数，如 ifOutUcastPkts，ifOutMulticastPkts 和 ifOutBroadcastPkts ；但是它不能由 dot3StatsSingleCollisionFrames 对象实例计数。参考 IEEE 802.3 管理层。
154	dot3StatsSQETestErrors	SQE TEST ERROR 在一个特定接口上被接收的次数的计数值。该 SQE TEST ERROR 是根据规则进行检查的 SQE 检测机制 （如 IEEE Std. 802.3， 2000 版， 7.2.4.6. 章节中 PLS 载波传感器功能意义所述）。该计数器不会因为接口以大于 10Mb/s 的速度运行或者在全双工模式下运行而增加。当管理系统的重新初始化时，此计数器的值不连续，其他情况下，该值由 ifCounterDiscontinuityTime 给出。
155	dot3StatsDeferredTransmissions	因为媒介忙，所以在一个特定接口上第一次发送尝试被延迟的帧的计数值，计数值不包括在冲突中卷入的帧的数目。当接口运行在全双工模式下时，此计数器不增加；当管理系统的重新初始化时，此计数器的值不连续，其他情况下，该值由 ifCounterDiscontinuityTime 给出。
156	dot3StatsLateCollisions	在一个包的传送过程中，在一个特定接口上在比 slotTime 更近的时间内探测的冲突的次数的数目。此对象表示的数中的冲突也被认为是一个通用的冲突，为了统计其他相关冲突。当接口运行在全双工模式下时，此计数器不增加；当管理系统的重新初始化时，此计数器的值不连续，其他情况下，该值由 ifCounterDiscontinuityTime 给出。
157	dot3StatsExcessiveCollisions	由于在一个特定接口上过多的冲突导致发送失败的帧的个数。
158	dot3StatsInternalMacTransmitErrors	由于在一个特定接口上内在的 MAC 子层传送错误导致发送失败的帧的个数。如果该帧不被 dot3StatsLateCollisions 对象，或 dot3StatsCarrierSenseErrors 对象，或 dot3StatsExcessiveCollisions 对象的实例所计数，那么它只被该对象的实例所计数。此对象实例代表数量的准确定义是特别执行。特别的，此对象实例代表在一特定接口上的传输错误数量 （不以其它方式计算）。参考 IEEE 802.3 管理层。

表 322 公共 MIB 库

159	dot3StatsCarrierSenseErrors	当在一个特定接口上试图去传送一个帧的时候，载波传感器的条件缺失，或从未满足的次数的数目。当每次尝试传输时，即使载波传感器条件不定，对象实例表示的数值也至少递增一次。
160	dot3StatsFrameTooLongs	在一个特定接口上接收到的超过最大允许帧大小的帧的个数。当 MAC 服务向 LLC(或其他 MAC 用户）返回 frameTooLong 状态时，增加该对象实例的计数值。收到的帧 (由多重错误条件获得) 完全根据 LLC 的错误状态来计数。参考 IEEE 802.3 管理层。
161	dot3StatsInternalMacReceiveErrors	由于一个内在 MAC 子层接收错误而在特定接口上产生帧接收失败的帧的个数。只有在该计数器不被 dot3StatsFrameTooLongs 对象，或 dot3StatsAlignmentErrors 对象，或 dot3StatsFCSErrors 对象的相关实例计数时，该对象实例才对帧数进行计数。此对象实例代表数量的准确定义是特别执行。特别的，此对象实例代表在一特定接口上的传输错误数量 （不以其它方式计算）。参考 IEEE 802.3 管理层。
162	dot3StatsEtherChipSet	该对象包含一个对象标识符，该标识符用来识别实现接口的芯片集。以太网接口由几种不同的芯片组成。 MIB 实现者决定了通过该对象标识哪一块芯片。实现者应该标识通常被称为 MAC 的芯片。如果没有这样容易标识的芯片，实现者应该标识那些集中了发送、接收统计和错误指示的芯片。这将允许管理工作站与统计和生成统计的芯片相关联，这样就给了它分析芯片中的任何已知异常事件的能力。
	9. snmp	
163	snmpInPkts	通过传送服务发送到 SNMP 实体的消息总数。
164	snmpOutPkts	从 SNMP 实体发送到传输服务器的全部 snmp 消息数。
165	snmpInBadVersions	发送到 SNMP 实体 （用于不支持的 SNMP 版本）SNMP 消息总数。
166	snmpInBadCommunityNames	发送到 SNMP 实体 （使用上述实体未知的 SNMP 共用名）的 SNMP 消息总数。
167	snmpInBadCommunityUses	发送到 SNMP 实体 （表示消息中命名的 SNMP 公共名所不允许的 SNMP 操作）的 SNMP 消息总数。
168	snmpInASNParseErrs	SNMP 实体在对所接收的 SNMP 消息进行解码时遇到的 ASN.1 或基本编码规则 （BER）错误总数。
169	snmpInTooBigs	发给 SNMP 实体的具有 toobig 错误状态的 SNMP PDU 数量。
170	snmpInNoSuchNames	发给 SNMP 实体的具有 noSuchName 错误状态的 SNMP PDU 数量。
171	snmpInBadValues	发给 SNMP 实体的具有 badValue 错误状态的 SNMP PDU 数量。
172	snmpInReadOnlys	发给 SNMP 实体的具有只读错误状态的 SNMP PDU 数量。注意，这是一个生成包含只读错误状态 SNMP PDU 的协议错误。例如，该对象用来检测 SNMP 的误执行。
173	snmpInGenErrs	发给 SNMP 实体的具有 genErr 错误状态的 SNMP PDU 数量。
174	snmpInTotalReqVars	通过 SNMP 的 Get-Request 和 Get-Next 获取的 MIB 对象的数量。
175	snmpInTotalSetVars	通过 SNMP 的 Set-Request PDU 修改的 MIB 对象的数量。
176	snmpInGetRequests	SNMP 实体接收并处理的 SNMP Get-Request PDU 数量。
177	snmpInGetNexts	SNMP 实体接收并处理的 SNMP Get-Next PDU 数量。
178	snmpInSetRequests	SNMP 实体接收并处理的 SNMP Set-Request PDU 数量。
179	snmpInGetResponses	SNMP 实体接收并处理的 SNMP Get-Response PDU 数量。
180	snmpInTraps	SNMP 实体接收并处理的 SNMP Trap PDU 数量。
181	snmpOutTooBigs	SNMP 实体产生的具有 tooBig 错误状态的 SNMP PDU 数量。
182	snmpOutNoSuchNames	SNMP 实体产生的具有 noSuchName 错误状态的 SNMP PDU 数量。
183	snmpOutBadValues	SNMP 实体产生的具有 badValue 错误状态的 SNMP PDU 数量。

表 322 公共 MIB 库

184	snmpOutGenErrs	SNMP 实体产生的具有 genErr 错误状态的 SNMP PDU 数量。
185	snmpOutGetRequests	SNMP 实体产生的 SNMP GetRequest PDU 数量。
186	snmpOutGetNexts	SNMP 实体产生的 SNMP Get-Next PDU 数量。
187	snmpOutSetRequests	SNMP 实体产生的 SNMP SetNext PDU 数量。
188	snmpOutGetResponses	SNMP 实体产生的 SNMP GetResponse PDU 数量。
189	snmpOutTraps	SNMP 实体产生的 SNMP GetTrap PDU 数量。
190	snmpEnableAuthenTrap	表明是否允许 SNMP 实体生成 authenticationFailure 陷阱。此对象的值覆盖任何配置信息；它提供可以禁用所有 authenticationFailure 陷阱的方法。注意，我们极力推荐您将该对象存储在非易失性内存中，从而使它在跨越网络管理系统重新初始化时保持不变。
191	snmpSilentDrops	发送到被静默删除的 SNMP 实体的 GetRequest-PDU、 GetNextRequest-PDU、 GetBulkRequest-PDU、 SetRequest-PDU 和 InformRequest-PDU 的总数。其被静默删除的原因是由于包含备用 Response-PDU （带有空的变量绑定字段）的回答大小大于本地约束，或大于与请求创始者关联的最大消息大小。
192	snmpProxyDrops	发送到被静默删除的 SNMP 实体的 GetRequest-PDU、 GetNextRequest-PDU、 GetBulkRequest-PDU、 SetRequest-PDU 和 InformRequest-PDU 的总数。其被静默删除的原因是在某种意义上给代理服务器的信息传输失败 （暂停除外）而导致没有 Response-PDU 返回。

10. host

10.1. hrSystemInfo

193	hrSystemUptime	从设备上次完成初始化后到当前的一个时间统计。注意，它不同于 MIB-II [3] 中的 sysUpTime, 后者指的是网络管理模块启动的时间。
194	hrSystemDate	设备时间 （系统硬件时间和日期）。
195	hrSystemInitialLoadDevice	hrDeviceEntry 中一个设备的序号，主机将从这个设备引导初始化系统或者启动配置参数。
196	hrSystemInitialLoadParameters	当初始化操作系统时由其它设备提供给本地设备的参数 （路径、参数）。
197	hrSystemNumUsers	指的是系统当前存储的用户会话数。它是一个集合 （需要用户认证和工作控制的进程）。
198	hrSystemProcesses	系统当前载入和运行的进程数量。
199	hrSystemMaxProcesses	系统支持的最大进程数量。如果最大值不固定，那么该值应为 0。对于有固定最大值的系统，当到达最大值时，它能帮助诊断发生的错误。

10.2. hrStorageInfo

200	hrMemorySize	主机内存大小，单位是 KB。

10.3. hrStorageTable/hrStorageEntry

201	hrStorageIndex	每个逻辑存储区域的唯一值。
202	hrStorageType	该实体的存储类型。
203	hrStorageDescr	存储区域类型的描述。
204	hrStorageAllocationUnits	存储设备的存储单元大小 （单位字节）。如果该实体监控部分，块，缓冲区，或者数据包，例如，这个值通常将会比一大。否则，这个数将为一。
205	hrStorageSize	该存储区域包含多少个存储单元，以 hrStorageAllocationUnits 为单位。
206	hrStorageUsed	已用的存储空间大小，用存储单元的数目来表示。以 hrStorageAllocationUnits 为单位。

表 322 公共 MIB 库

207	hrStorageAllocationFailures	由于存储空间不足引起的存储失败的次数。注意，这个对象有一个 SYNTAX 值，它没有一个确定的初始值。建议设为 0。
	10.4. hrDeviceTable/hrDeviceEntry	
208	hrDeviceIndex	一个设备唯一的标示 （序号）。每个设备对应的值必须保持连续性，至少从重新初始化到下一次重新初始化。
209	hrDeviceType	设备类型说明。如果这个值是 ' hrDeviceProcessor { hrDeviceTypes 3 }' ，那么在对应设备的 'hrProcessorTable' 中会存储一个登陆。如果这个值是 ' hrDeviceNetwork { hrDeviceTypes 4 }'，那么在对应设备的 'hrNetworkTable' 中会存储一个登陆。如果这个值是 ' hrDeviceNetwork { hrDeviceTypes 5 }'，那么在对应设备的 'hrPrinterTable' 中会存储一个登陆。如果这个值是 'hrDeviceNetwork { hrDeviceTypes 6}' ，那么在对应设备的 hrDiskStorageTable 中会存储一个登陆。
210	hrDeviceDescr	设备描述信息，它应该包括设备制造商，版本，序列号等。
211	hrDeviceID	该设备的产品 ID。
212	hrDeviceStatus	设备的当前操作状态，包含如下的 5 个状态：unknow （1），不明状态； running （2），正常工作状态，没有已知的错误； warning （3），被检测出存在非正常的错误，但是仍然可操作； test(4), 设备处于测试模式，暂时不可用； down （5），设备未启用。
213	hrDeviceErrors	侦测到的设备错误次数。注意，这个对象有一个 SYNTAX 值，它没有一个确定的初始值。建议设为 0。
	10.5. hrProcessorTable/hrProcessorEntry	
214	hrProcessorFrwID	主机包含的处理器列表。注意，这个表的内容会少，只有当 hrDeviceType 的对应值是 hrDeviceProcessor 时，概念条目才存在。
215	hrProcessorLoad	处理器负载：最后一分钟处理器出于利用时间的百分比。
	10.6. hrNetworkTable/hrNetworkEntry	
216	hrNetworkIfIndex	网络设备的 ifInde 值。
	10.7. hrDiskStorageTable/hrDiskStorageEntry	
217	hrDiskStorageAccess	一个说明，表示这个长期存储设备是可读写的还是只读的。这应该反映了媒体类型，任何写保护机制，以及任何设备配置，影响整个装置。
218	hrDiskStorageMedia	存储设备的媒介类型。
219	hrDiskStorageRemoveble	表明媒介磁盘是否可以从设备中移除。
220	hrDiskStorageCapacity	存储设备容量。
	10.8. hrPartitionTable/hrPartitionEntry	
221	hrPartitionIndex	存储设备的分区索引序号。每个存储设备的值必须保持连续，或者至少重一个重新初始化到下一个重新初始化。
222	hrPartitionLabel	关于这个分区的一个文本描述。
223	hrPartitionID	一个分区在操作系统中的唯一标示。对于一些系统，该值采用二进制表示。
224	hrPartitionSize	分区大小。
225	hrPartitionFSIndex	该分区所挂接的文件系统的索引序号，如果该分区没有设置到文件系统中，则此项值为 0。注意多个分区可能指向一个文件系统，指这一文件系统放在那些分区。多重文件系统可能不会放在一个分区。
	10.9. hrFSTable/hrFSEntry	
226	hrFSIndex	文件系统索引序号；从一次初始化到下一次重新初始化的时间里，该值应该保持不变。
227	hrFSMountPoint	文件系统根路径名。

表 322 公共 MIB 库

228	hrFSRemoteMountPoint	网络文件系统的主机名或者地址，也可以包含文件系统参数，如果该文件系统不是网络文件系统，此处应该为 0 长度的字符串。
229	hrFSType	定义这个文件系统的对象的值。
230	hrFSAccess	说明由操作系统逻辑配置的系统文件是可读写的还是只读的。这不代表任何本地入口控制策略，除了作为一个整体适用于这个文件系统。
231	hrFSBootable	文件系统可启动标志。
232	hrFSStorageIndex	该文件系统在 hrStorageEntry 中的索引。如果没有这样的信息可用，那么该值为零。相关存储条目，将有助于追踪这个文件系统适用率以及诊断可能发生的错误当它超出空间时。
233	hrFSLastFullBackupDate	上次将此文件系统完整备份到其他存储设备的时间。如果这个信息未知，那么这个变量应该有对应于一月一日年 0000，00:00:00.0 的值，其十六进制码（hex）为 00 00 01 01 00 00 00 00。
234	hrFSLastPartialBackupDate	上次将此文件系统中的部分分区备份到其他存储设备的时间。该信息能确保定期进行备份工作。如果这个信息未知，那么这个变量应该有对应于一月一日年 0000， 00:00:00.0 的值，其十六进制码 （hex）为 00 00 01 01 00 00 00 00。

10.10. hrSWRunTable/hrSWRunEntry

235	hrSWRunIndex	设备上运行的软件索引序号。无论如何，它都应该是系统自带的，特定的识别号码。
236	hrSWRunName	该运行的软件的文本描述，包括厂商，版本和它的通用名称。如果该软件安装在设备上，这个名字应该和 hrSWInstalledName 中的名字对应。
237	hrSWRunID	该运行的软件产品的 ID 号。
238	hrSWRunPath	该软件被加载时的存储路径 （例如：某盘符）。
239	hrSWRunParameters	该软件初始化时的加载参数。
240	hrSWRunType	软件类型。
241	hrSWRunStatus	软件运行状态 。invalid(4) 不可用，当把软件设置成该状态将使其停止运行，并被卸载。

10.11. hrSWRunPerfTable/hrSWRunPerfEntry

242	hrSWRunPerfCPU	该软件使用的系统 cpu 的 1/100 秒数。注意，在一个多进程的系统里，在一个 1/100 秒的实际时间 （挂钟），该值可能会增加超过一个 1/100 秒数。
243	hrSWRunPerfMem	分配给这个进程的系统内存的总数。
244	hrSWInstalledLastChange	上次 hrSWInstalledTable 中条目发生增加删除改名时的 sysUpTime 的值。因为这个表可能会包含很多条目和对象的投票表决，所以它允许一个管理站决定什么时候重载有用的表。
245	hrSWInstalledLastUpdateTime	上次 hrSWInstalledTable 被完整更新时的 sysUpTime 的值。由于缓冲的数据将成为一个流行的实施策略，恢复此对象将让一个管理站获得保证，即在这个表中没有数据早于显示时间。

10.12. hrSWInstalledTable/hrSWInstalledEntry

246	hrSWInstalledIndex	主机上安装的软件的索引序号。该值范围从 1 到主机上安转的软件总数之间。
247	hrSWInstalledName	已安转的软件的文本描述，包括软件名称，厂商，版本，序列号等。
248	hrSWInstalledID	已安装的软件产品的 ID。
249	hrSWInstalledType	软件类型。
250	hrSWInstalledDate	在目录列表中列出的软件的最后修改日期。

表 322 公共 MIB 库

11. ifMIB

11.1. ifXTable/ifXEntry

251	ifName	接口名称。该值应该是已分配本地设备的接口名称，适用于进入该设备 'console' 的命令。它可能是一个名字 （如 'le0'），或者一个简单的端口号 （如 1），这都取决于设备的接口命名规则。如果有若干条目在 iftable 一起代表一个单一的接口 （由设备命名），那么，每一个都会有相同的 ifName 名 。如果没有本地名字，或此对象没被用，那么，这种对象包含一个 0 长度字符串。
252	ifInMulticastPkts	交付给高层的多播分组数。从这个子层传到较高子层的数据包数。对于一个 MAC 层协议，它包括组和功能地址。
253	ifInBroadcastPkts	交付给高层的广播分组数。
254	ifOutMulticastPkts	从高层接收到的多播分组数。包括被丢弃的和未发出的。对于一个 MAC 层协议，它包括组和功能地址。
255	ifOutBroadcastPkts	从高层接收到的广播分组数。包括被丢弃的和未发出的。
256	ifHCInOctets	该接口上收到的 8 位组，包括结构字符。该对象是一个 64 位版本的 ifInOctets。
257	ifHCInUcastPkts	交付给高层的单播分组数。该对象是一个 64 位版本的 ifInUcastPkts。
258	ifHCInMulticastPkts	交付给高层的多播分组数。对于一个 MAC 层协议，它包括组和功能地址。该对象是一个 64 位版本的 ifInMulticastPkts。
259	ifHCInBroadcastPkts	交付给高层的广播分组数，该对象是一个 64 位版本的 ifInBroadcastPkts。
260	ifHCOutOctets	该接口上输出的 8 位组，包括结构字符。该对象是一个 64 位版本的 ifOutOcters。
261	ifHCOutUcastPkts	从高层接收到的单播分组数。它包括组和功能地址。该对象是一个 64 位版本的 ifOutUcastPkts。
262	ifHCOutMulticastPkts	从高层接收到的多播分组数。包括被丢弃的和未发出的。对于一个 MAC 层协议，它包括组和功能地址。该对象是一个 64 位版本的 ifOutMulticastPkts。
263	ifHCOutBroadcastPkts	从高层接收到的广播分组数。包括被丢弃的和未发出的。该对象是一个 64 位版本的 ifOutBroadcastPkts。
264	ifLinkUpDownTrapEnable	指出网卡 up 或 down 时是否会产生 trap。默认情况下为 Enable(1)。不会运行在其他接口 （定义为 ifStackTable）之上。反之为 disabled(2)。
265	ifHighSpeed	对接口当前带宽的估算值，单位为每秒 1M 位。如果这个对象的值是 n 则接口的速度可能在 n-500000 到 n+499999 之间。对于那些带宽不变的或没有正确估算值的接口，这个对象应该包括额定带宽。对于没有带宽概念的低层来说，该对象的值为 0。
266	ifPromiscuousMode	是否是混杂模式，如果是混杂模式则为 true，否则为 false。如果合法，设定此对象真值（1）将要求接口重置。 ifPromiscuousMode 的值不会影响广播和组播的接受。
267	ifConnectorPresent	该对象的借口子层有物理连接，那么值为 true （1），否则为 false （2）。
268	ifAlias	网络管理为接口指定的别名。并为接口提供一种非易失性 ‘ 处理 ’。接口的第一个例子，ifAlias 值是长度为 0 的字符串。
269	ifCounterDiscontinuityTime	从 snmpd 系统最近一次启动到接口计数器断开的 sysUpTime 值。相关计数器是指该接口 ifTable 或 ifXTable 中的任意 Counter32 或 Counter64 对象。如果从系统启动到现在都没有计数器中断发生，则该对象值为 0。

12. snmpV2

12.1. snmpEngineGroup

270	snmpEngineID	SNMP 引擎的特定管理的 ID。
271	snmpEngineBoots	SNMP 引擎自从最后一次配置后，到目前被初始化的次数。

表 322 公共 MIB 库

272	snmpEngineTime	自从最后一次 snmpEngineBoots 发生变化到现在的时间。当递增该对象值会引起它超过最大值。 snmpEngineBoots 是递增的，当重新初始化，这个对象值也随之为 0。
273	snmpEngineMaxMessageSize	snmp 引擎能接收、发送、处理的最大的消息长度 （8 位组），它是所有可传输最大消息值和引擎支持的消息值中的最小值。
	12.2. snmpMPDGroup	
274	snmpUnknownSecurityModels	因为引擎的安全模型不支持或不识别而丢弃的收到的包。
275	snmpInvalidMsgs	引擎收到的因为封装有问题而丢弃的包的数量。
276	snmpUnknownPDUHandlers	因为应用进程不能处理该 pdu 类型而丢弃的包的数量。
	12.3. usmMIBBasicGroup	
277	usmStatsUnsupportedSecLevels	被 SNMP 丢弃的那些收到的因为无法知道安全级别和其他不可用的包。
278	usmStatsNotInTimeWindows	被丢弃的因为他们超出权威的 SNMP 引擎窗口的数据包。
279	usmStatsUnknownUserNames	由于 SNMP 引擎不识别的用户而丢弃的包的数量。
280	usmStatsUnknownEngineIDs	由于 SNMP 引擎不识别的 snmpEngineID 而丢弃的包的总数。
281	usmStatsWrongDigests	由于不是 SNMP 引擎所期望的摘要值而被丢弃的包的总数。
282	usmStatsDecryptionErrors	SNMP 引擎丢弃的包 （因不能解码）的数量。
	12.4. vacmBasicGroup	
283	vacmGroupName	该表项所属组名 （如 securityModel 和 securityName 的组合）。在 vacmAccessTable 中索引这个组名来选择一个访问控制策略。然而，这个表中的值不能说明这个事例值存在于 vacmAccessTable 表中。
284	vacmSecurityToGroupStorageType	此概念行的存储类型。概念行有 'permanent' 值，不需要注销行里的任何列对象。
285	vacmSecurityToGroupStatus	该概念行状态。直到事例中所有对应列得到妥善配置， vacmSecurityToGroupStatus 的对应值才为 notReady。特别，一个新建的行不能被激活，直到 vacmGroupName 被设置。RowStatus TC[RFC2579] 要求该描述条款必须说明能够在何种情况下对此行的对象进行修改。此部对象值应该对该行其他对象的可修改性没有影响。
286	vacmAccessContextMatch	如果设置为 exact， contextName 必须与 vacmAccessContextPrefix 精确匹配。如果设置为 prefix， contextName 只需与 vacmAccessContextPrefix 前面几个字符匹配即可。它允许一个简单的通配符格式。
287	vacmAccessReadViewName	读访问所用的授权 MIB viewName。如果该值为空串，表示没有任何活动视图被配置成可读的。如果该值为空串，或没有主动的 MIB 视图有 vacmViewTreeFamilyViewName 值，表示没有允许的访问。
288	vacmAccessWriteViewName	写访问所用的授权 MIB viewName。如果该值为空串，表示没有任何活动视图被配置成可写的。本概念行的存储类型。概念行有 ‘permanent’ 值，不需要注销行里的任何列对象。如果该值为空串，或没有主动的 MIB 视图有 vacmViewTreeFamilyViewName 值，表示没有允许的访问。
289	vacmAccessNotifyViewName	notify 访问所用的授权 MIB viewName。如果该值为空串，表示没有任何活动视图 被配置成允许 notify 访问的。如果该值为空串，或没有主动的 MIB 视图有 vacmViewTreeFamilyViewName 值，表示没有允许的访问。

表 322 公共 MIB 库

290	vacmAccessStorageType	本概念行的存储类型。概念行有 'permanent' 值，不需要注销行里的任何列对象。
291	vacmAccessStatus	本概念行状态。 RowStatus TC[RFC2579] 要求该描述条款必须说明能够在何种情况下对此行的对象进行修改。此部对象值应该对该行其他对象的可修改性没有影响。
292	vacmViewSpinLock	配合 SNMP 命令生成器来协调 Set 操作 （创建或则修改视图）的一种咨询锁。当产生或修改一个现有视图时，它对与其他视图用途的潜在的相互作用的了解起到重要作用。该 vacmViewSpinLock 应该被找回。被创建的视图名应由 SNMP 命令生成器通过参考 vacmViewTreeFamilyTable 决定。最后，该视图名会被创建 （包括咨询锁）。如果另一个 SNMP 命令生成器同时改变了视图，那么旋转锁值也将改变，那么这个生成会失败，因为它指定旋转锁值错误。因为它是一个咨询锁，该锁不被强迫使用。
293	vacmViewTreeFamilyMask	位掩码，与 vacmViewTreeFamilySubtree 一起定义视图子树。该位掩码的每个位都对应一个 vacmViewTreeFamilySubtree 的分标识，字节字符串值中最重要的一位的 i 次方字节对应于 （8*i-7）次方字节分标识 （如有必要，见下文）。次重要的一位的 i 次方字节对应于 8*i 次方字节分标识，其中 i 的范围从 1 到 16。当决定是否一个对象标识符是视图子树时，该位掩码的每一位指定是否相应的分标识必须匹配。 '1' 表示精确匹配； '0' 表示 'wild card'。
294	vacmViewTreeFamilyType	指明 vacmViewTreeFamilySubtree 与 vacmViewTreeFamilyMask 一道定义的 MIB 视图子树是包含在 MIB view 内，还是排除在 MIB view 外。
295	vacmViewTreeFamilyStorageType	本概念行的存储类型。概念行有 'permanent' 值，不需要注销行里的任何列对象。
296	vacmViewTreeFamilyStatus	本概念行状态。 RowStatus TC[RFC2579] 要求该描述条款必须说明能够在何种情况下对此行的对象进行修改。此部对象值应该对该行其他对象的可修改性没有影响。

私有 MIB 库

下面给出了本产品的私有 MIB 库。

表 323 私有 MIB 库

	1. fwSystemInfoGroup	
1	fwProductName	产品名字
2	fwProductVer	产品版本
3	fwRegMsg	注册信息
4	fwName	系统名称
	2. fwRunningStatGroup	
5	fwCpuUsage	CPU 的使用率
6	fwMemUsage	内存的使用率
	3. fwChannelGroup **fwChannelTable/fwChannelEntry**	
7	fwChannelIndex	通道的索引
8	fwChannelName	通道名称
9	fwChannelStat	通道状态
10	fwChannelMode	通道的模式
11	fwChannelNativeVlan	通道的缺省 VLAN
12	fwChannelIncludePorts	通道包含的端口
13	fwChannelBelowInterfaces	通道所属接口
	4. fwVlanGroup **fwVlanTable/fwVlanEntry**	
14	fwVlanIndex	VLAN 的索引
15	fwVlanName	VLAN 的名称
16	fwVlanStat	VLAN 的状态
17	fwVlanMTU	VLAN 的 MTU
18	fwVlanMAC	VLAN 的 MAC 地址
19	fwVlanIP	VLAN 的 IP 地址
20	fwVlanBelowVsys	VLAN 所属的虚拟系统
21	fwVlanIncludePorts	VLAN 包含的端口
22	fwVlanTXPackets	VLAN 发送的数据包数量
23	fwVlanRXPackets	VLAN 接收的数据包数量
24	fwVlanTXBytes	VLAN 发送的字节数

表 323 私有 MIB 库 (*续*)

25	fwVlanRXBytes	VLAN 接收的字节数
	5. fwVsysGroup	
	fwVsysTable/fwVsysEntry	
26	fwVsysIndex	Vsys 索引
27	fwVsysName	Vsys 名称
28	fwVsysStat	Vsys 状态
29	fwVsysResourcePercent	Vsys 资源百分比
30	fwIncludeVlans	包含的 VLAN 数
	6. fwSecureZoneGroup	
	fwSecureZoneTable/fwSecureZoneEntry	
31	fwSecureZoneIndex	安全域的索引
32	fwSecureZoneName	安全域的名称
33	fwSecureZoneInternalRule	安全域的域内策略 （是否允许安全间相互访问）
34	fwSecureZoneIncludeInterfaces	安全域包含的接口
35	fwSecureZoneIncludePorts	安全域包含的端口
	7. fwUserGroup	
	fwUserTable/fwUserEntry	
36	fwUserIndex	用户索引
37	fwUserName	用户名
38	fwUserBelowVsys	用户所属的 Vsys
	8. fwVPNTunnelGroup	
	8.1. fwVPNAutoTunnelTable/fwVPNAutoTunnelEntry	
39	fwVPNAutoTunnelIndex	VPN 自动隧道索引
40	fwVPNAutoTunnelName	VPN 自动隧道名称
41	fwVPNAutoTunnelState	VPN 自动隧道状态
42	fwVPNAutoTunnelRemoteType	自动隧道对端类型：动态 IP、静态 IP、用户和用户组
43	fwVPNAutoTunnelRemoteInfo	自动隧道对端信息 （根据对端类型的不同，可能是一个动态 IP、静态 IP、用户或用户组。）
	8.2. fwVPNManualTunnelTable/fwVPNManualTunnelEntry	
44	fwVPNManualTunnelIndex	VPN 手动隧道索引
45	fwVPNManualTunnelName	VPN 手动隧道名称
46	fwVPNManualTunnelState	VPN 手动隧道状态
47	fwVPNManualTunnelRemoteType	手动隧道对端类型：静态 IP

表 323 私有 MIB 库 (*续*)

48	fwVPNManualTunnelRemoteInfo	手动隧道对端信息：静态 IP
	9. fwChassisGroup	
	9.1. fwChassisSerialNumber	
49	fwChassisSerialNumber	设备的序列号
	9.2. fwChassisMBType	
50	fwChassisMBType	设备主板的类型
	9.3. fwChassisMBRevNumber	
51	fwChassisMBRevNumber	设备主板的修正号
	9.4. fwChassisMBSerialNumber	
52	fwChassisMBSerialNumber	设备主板的序列号
	9.5. fwCardTable/fwCardEntry	
53	fwCardIndex	CF 卡的索引
54	fwCardOperStatus	CF 卡的运作状态
	10. fwStorageGroup	
	fwSIMMTotal	
55	fwSIMMTotal	SIMM 内存的总容量
	11. fwProcessGroup	
	11.1. fwProcessorUtilization	
56	fwProcessorUtilization	自系统启动起 CPU 利用率的平均值
	11.2. fwProcessTable/fwProcessEntry	
57	fwProcessID	进程 ID
58	fwProcessParentID	父进程 ID
59	fwProcessOwner	进程的拥有者 （用户）
60	fwProcessMemory	进程内存占用量 （兆位）
61	fwProcessPercentCPU	进程 CPU 占用率
62	fwProcessName	进程名称
	12. fwAssetGroup	
	12.1. fwAssetChassisSerialNumber	
63	fwAssetChassisSerialNumber	设备的序列号
	12.2. fwCPUModel	
64	fwCPUModel	设备中 CPU 型号
	12.3. fwCPUMfr	
65	fwCPUMfr	设备中 CPU 的制造厂商

表 323 私有 MIB 库 (*续*)

	12.4. fwCPUFreq	
66	fwCPUFreq	CPU 的频率
	12.5. fwKernMaxMem	
67	fwKernMaxMem	内核内存最大的容量
	12.6. fwMotherBoardSerNum	
68	fwMotherBoardSerNum	主板的序列号
	12.7. fwMotherBoardRev	
69	fwMotherBoardRev	主板的修正序列号
	12.8. fwMotherBoardModel	
70	fwMotherBoardModel	主板的型号
	12.9. fwOSRelease	
71	fwOSRelease	当前操作系统的释放序号
	12.10. fwOSVersion	
72	fwOSVersion	当前操作系统的版本号
	12.11. fwProductModel	
73	fwProductModel	当前系统的产品型号
	12.12. fwAssetTable/fwAssetEntry	
74	fwPkgIndex	安装并运行的软件索引
75	fwPkgName	软件的名称
76	fwPkgMajorVersion	软件的主版本号
77	fwPkgMinorVersion	软件的小版本号
	12.13. fwDiskDriveTableModel/fwDiskDriveEntry	
78	fwDiskDriveIndex	磁盘的索引
79	fwDiskSysDriveIndex	操作系统中标识该磁盘的索引
80	fwDiskDriveModel	磁盘型号
81	fwDiskDriveCapacity	磁盘的容量
82	fwDiskDriveLocation	磁盘的位置
	12.14. fwBiosVendor	
83	fwBiosVendor	BIOS 的供应商
	12.15. fwBiosVersion	
84	fwBiosVersion	BIOS 版本
	12.16. fwBiosDate	
85	fwBiosDate	BIOS 时间

表 323 私有 MIB 库 (*续*)

13. fwCounterSessionGroup

fwCounterSessionTable/fwCounterSessionEntry

86	fwCounterIndex	接口索引
87	fwCounterInterfaceName	接口名称
88	fwCounterSessions	从系统启动到现在的会话总数
89	fwCounterMacTblFull	MAC 表被完全填满的次数
90	fwCounterDroppedPkts	丢弃的数据包数量
91	fwCounterLoggedPkts	记录到日志中的数据包数量
92	fwCounterRejectedPkts	由于策略限制而拒绝的数据包数量
93	fwCounterRejectedBytes	由于策略限制而拒绝的数据包总字节数
94	fwCounterDroppedByVlanPkts	由于 VLAN 原因 （如缺少 VLAN 头）丢弃的数据包数量
95	fwCounterDroppedNoInBufPkts	由于接收缓存不足丢弃的数据包数量
96	fwCounterDroppedNoOutBufPkts	由于发送缓存不足丢弃的数据包数量
97	fwCounterOutPkts	发送数据包的数量
98	fwCounterOutBytes	发送数据包的总字节数
99	fwCounterOutCollErr	发送冲突包数量
100	fwCounterInPkts	接收数据包的数量
101	fwCounterInBytes	收到的数据包的字节数
102	fwCounterInCollErrPkts	接收冲突包数量
103	fwCounterInCrcErrPkts	接收数据包中 CRC 校验错误的数量
104	fwCounterInArpReq	接收到的 ARP 请求数量
105	fwCounterOutArpReq	发送的 ARP 请求数量
106	fwCounterInSelfPkts	被本地协议栈接收的数据包数量
107	fwCounterInVpnPkts	接收到的 VPN 数据包数量
108	fwCounterInIpPkts	接收到的 IP 数据包的数量
109	fwCounterInIpBytes	接收到的 IP 数据包字节数 （整个以太网帧长度）
110	fwCounterInNipPkts	接收到的非 IP 数据包数量
111	fwCounterInNipBytes	接收到的非 IP 数据包字节数 （整个以太网帧长度）
112	fwCounterInTcpPkts	接收到的 TCP 数据包数量
113	fwCounterInTcpBytes	接收到的 TCP 数据包字节数 （整个以太网帧长度）
114	fwCounterInUdpPkts	接收到的 UDP 数据包数量
115	fwCounterInUdpBytes	接收到的 UDP 数据包字节数 （整个以太网帧长度）
116	fwCounterInIcmpPkts	接收到的 ICMP 数据包数量

表 323 私有 MIB 库 (*续*)

117	fwCounterInMiscProtoPkts	接收到的非 TCP、 UDP 和 ICMP 协议数据包的数量
118	fwCounterInLess64Pkts	数据包长度小于等于 64 字节的数据包数量
119	fwCounterInLess256Pkts	数据包长度大于 64 字节但小于等于 256 字节的数据包数量
120	fwCounterInLess1024Pkts	数据包长度大于 256 字节但小于等于 1024 字节的数据包数量
121	fwCounterInBigger1024Pkts	数据包长度大于 1024 字节的数据包数量
122	fwCounterTcpSynPkts	接收到的 TCP 标志位为 SYN 的数据包数量
123	fwCounterTcpSynAckPkts	接收到的 TCP 标志位为 SYN 和 ACK 的数据包数量
124	fwCounterTcpAckPkts	接收到的 TCP 标志位为 ACK 的数据包数量
125	fwCounterTcpFinPkts	接收到的 TCP 标志位为 FIN 的数据包数量
126	fwCounterTcpRstPkts	接收到的 TCP 标志位为 RST 的数据包数量
127	fwCounterNipDenyPkts	由于非 IP 包过滤策略限制而拒绝的数据包数量
128	fwCounterIpMacDenyPkts	由于 IP-MAC 绑定策略限制而拒绝的数据包数量
129	fwCounterRouteDenyPkts	由于路由而丢弃的数据包数量
130	fwCounterSnatDenyPkts	由于源 NAT 策略限制而拒绝的数据包数量
131	fwCounterDnatDenyPkts	由于目的 NAT 策略限制而拒绝的数据包数量
132	fwCounterDroppedDtsIpLimit	被基于目的 IP 的会话策略限制而丢弃的数据包数量
133	fwCounterDroppedSrsIpLimit	被基于源 IP 的会话策略限制而丢弃的数据包数量
134	fwCounterDroppedSessionLimit	被基于会话的会话策略限制而丢弃的数据包数量
135	fwCounterDroppedNoNatResPkts	由于 NAT 资源不足而丢弃的数据包数量
136	fwCounterDroppedNoGatePkts	由于没有可用网关而丢弃的封包数量
137	fwCounterDroppedIpfilterPkts	由于 IP 包过滤策略限制而丢弃的数据包数量
138	fwCounterPacketsIcmpFlood	ICMP 泛滥攻击的数据包数量
139	fwCounterPacketsSynFlood	SYN 泛滥攻击的数据包数量
140	fwCounterPacketsUdpFlood	UDP 泛滥攻击的数据包数量
141	fwCounterPacketsTcpRstScan	RST 端口扫描的数据包数量
142	fwCounterPacketsWinnuke	WinNuke 攻击的数据包数量
143	fwCounterPacketsSmurf	SMURF 攻击的数据包数量
144	fwCounterPacketsLand	LAND 攻击的数据包数量
145	fwCounterPacketsPingOfDeath	Ping-of-Death 攻击的数据包数量
146	fwCounterPacketsTearDrop	Teardrop 攻击的数据包数量
147	fwCounterPacketsFinScan	Fin 扫描的数据包数量
148	fwCounterPacketsXmasScan	XMAS 扫描的数据包数量
149	fwCounterPacketsNullScan	NULL 扫描的数据包数量

表 323 私有 MIB 库 (*续*)

150	fwCounterPacketsSynScan	SYN 端口扫描的数据包数量
151	fwCounterPacketsIpSweep	IP 地址探测攻击的数据包数量
152	fwCounterPacketsSynFinSet	TCP 标志位 SYN 和 FIN 同时置位的非法数据包的数量
153	fwCounterPacketsFinWithoutAck	没有 ACK 置位的 FIN 数据包的数量
154	fwCounterNonSynFlags	会话的第一个数据包没有 SYN 标志的数据包数量
155	fwCounterIpoptTimeStamp	设置 IP 时间戳选项的 IP 数据包数量
156	fwCounterIpoptRecordRoute	设置记录路由选项的 IP 数据包数量
157	fwCounterIpoptTraceRoute	设置 IP 追踪路由选项的 IP 数据包数量
158	fwCounterIpoptLooseSourceRoute	设置 IP 松散源路由选项的 IP 数据包数量
159	fwCounterIpoptStrictSourceRoute	设置 IP 严格源路由选项的 IP 数据包数量
160	fwCounterIpoptOther	设置其他 IP 选项的数据包数量
161	fwCounterIpSpoofing	IP 欺骗攻击的数据包数量
162	fwCounterIpFrag	被阻塞的 IP 分片包的数量
163	fwCounterIcmpFrag	被阻塞的 ICMP 分片包的数量
164	fwCounterIcmpLargePacket	被阻塞的 ICMP 数据包的数量
165	fwCounterSourceRouteFilter	被源路由选项过滤掉的数据包的数量
166	fwCounterTcpWithoutFlag	没有控制标志的 TCP 数据包的数量
167	fwCounterUnknowProto	被阻塞的未知协议的数据包数量
168	fwCounterSynFrag	被阻塞的 SYN Fragment 攻击的数据包数量
169	fwCounterActiveRaTunnels	当前已经连接的远程访问隧道数量
170	fwCounterActiveTunnels	当前状态为 OPEN 的隧道数量，包括远程访问和网段到网段隧道
171	fwCounterIkeConcurent	IKE 并发协商数 （当前处于协商状态的隧道数）
172	fwCounterIkeFailures	IKE 协商第一阶段失败的总次数
173	fwCounterIkeSuccesses	IKE 协商第一阶段成功的总次数
174	fwCounterDecPkts	解密包总数
175	fwCounterDecBytes	解密的总字节数
176	fwCounterDecErr	解密错误的数据包数量
177	fwCounterEncPkts	加密数据包总数
178	fwCounterEncBytes	加密的总字节数
179	fwCounterEncErr	加密错误的数据包总数
180	fwCounterVpnAccelEncBytes	加速卡加密的总字节数
181	fwCounterVpnAccelEncErr	加速卡加密错误总数
182	fwCounterVpnAccelDecBytes	加速卡解密总字节数

表 323 私有 MIB 库 (*续*)

183	fwCounterVpnAccelDecErr	加速卡解密错误总数
184	fwCounterCreatSessionHttp	HTTP 总共创建的会话数
185	fwCounterCurSessionHttp	HTTP 当前连接的会话数
186	fwCounterCreatSessionSmtp	SMTP 总共创建的会话数
187	fwCounterCurSessionSmtp	SMTP 当前连接的会话数
188	fwCounterCreatSessionPop3	POP3 总共创建的会话数
189	fwCounterCurSessionPop3	POP3 当前连接的会话数
190	fwCounterCreatSessionImap	IMAP 总共创建的会话数
191	fwCounterCurSessionImap	IMAP 当前连接的会话数
192	fwCounterCreatSessionFtp	FTP 总共创建的会话数
193	fwCounterCurSessionFtp	FTP 当前连接的会话数
194	fwCounterCreatSessionTelnet	TELNET 总共创建的会话数
195	fwCounterCurSessionTelnet	TELNET 当前连接的会话数

14. fwAnti-VirusCounterGroup

196	fwCounterHttpBlckByFiletype	基于 HTTP 协议的数据中，由于文件类型被禁止转发而被阻断的文件个数
197	fwCounterHttpBlckByVirus	基于 HTTP 协议的数据中，被检测出病毒的文件个数
198	fwCounterHttpScanned	基于 HTTP 协议的数据中，进行病毒检测的文件个数
199	fwCounterFtpBlckByFiletype	基于 FTP 协议的数据中，由于文件类型被禁止转发而被阻断的文件个数
200	fwCounterFtpBlckByVirus	基于 FTP 协议的数据中，被检测出病毒的文件个数
201	fwCounterFtpScanned	基于 FTP 协议的数据中，进行病毒检测的文件个数
202	fwCounterSmtpBlckByFiletype	基于 SMTP 协议的数据中，由于文件类型被禁止转发而被阻断的文件个数
203	fwCounterSmtpBlckByVirus	基于 SMTP 协议的数据中，被检测出病毒的文件个数
204	fwCounterSmtpScanned	基于 SMTP 协议的数据中，进行病毒检测的文件个数
205	fwCounterPop3BlckByFiletype	基于 POP3 协议的数据中，由于文件类型被禁止转发而被阻断的文件个数
206	fwCounterPop3BlckByVirus	基于 POP3 协议的数据中，被检测出病毒的文件个数
207	fwCounterPop3Scanned	基于 POP3 协议的数据中，进行病毒检测的文件个数
208	fwCounterImapBlckByFiletype	基于 IMAP 协议的数据中，由于文件类型被禁止转发而被阻断的文件个数
209	fwCounterImapBlckByVirus	基于 IMAP 协议的数据中，被检测出病毒的文件个数
210	fwCounterImapScanned	基于 IMAP 协议的数据中，进行病毒检测的文件个数

表 323 私有 MIB 库 (*续*)

211	fwCounterTotalBlckByFiletype	基于所有协议的数据中，由于文件类型被禁止转发而被阻断的文件个数
212	fwCounterTotalBlckByVirus	基于所有协议的数据中，被检测出病毒的文件个数
213	fwCounterTotalScanned	基于所有协议的数据中，进行病毒检测的文件个数
	15. fwAnti-SpamCounterGroup	
214	fwCounterBlckByIpBlacklist	被 IP 地址阻断列表阻断的邮件个数
215	fwCounterBlckBySenderBlacklist	被发件人阻断列表阻断的邮件个数
216	fwCounterBlckByWordBlacklist	被垃圾邮件关键字列表阻断的邮件个数
217	fwCounterBlckByContent	由于邮件内容被阻断的垃圾邮件个数
218	fwCounterBlckTotal	所有被阻断的垃圾邮件个数
	16. fwWeb-ProtectionCounterGroup	
219	fwCounterNewSessionRateHttp	HTTP 新建会话率 （sessions/s）
220	fwCounterWordFilteringHttp	被 HTTP 页面关键字过滤阻断的会话数
221	fwCounterFormatSizeHttp	HTTP 协议格式和长度异常的会话数
222	fwCounterMethodsHttp	被 Method 阻断的会话数
223	fwCounterASIIOnlyReqHttp	含有非 ASCII 字符的 HTTP 请求连接数
224	fwCounterHeaderSpoofingHttp	发生首部替换的数量
225	fwCounterDirectoryListingHttp	发生 HTTP 目录 Listing 操作的次数
226	fwCounterErrConcealmentHttp	被错误码隐藏阻断的 HTTP 连接数
227	fwCounterSQLInjection	被 SQL 注入防御阻断的 HTTP 连接数
228	fwCounterCmdInjection	被命令注入防御阻断的 HTTP 连接数
229	fwCounterLDAPInjection	被 LDAP 注入防御阻断的 HTTP 连接数
230	fwCounterCrossSiteScripting	跨站脚本攻击次数
231	fwCounterErrPageHttp	为用户返回错误提示页面次数
232	fwCounterAttackDefenseHttp	HTTP 攻击数量
	17. fwMail-ProtectionCounterGroup	
233	fwCounterNewSessionRateSmtp	SMTP 新建会话率 （sessions/s）
234	fwCounterNewSessionRatePop3	POP3 新建会话率 （sessions/s）
235	fwCounterNewSessionRateImap	IMAP 新建会话率 （sessions/s）
236	fwCounterFormatSizeSmtp	SMTP 协议格式和长度异常的会话数
237	fwCounterBlckCmdsSmtp	被 SMTP 阻断的非法命令数
238	fwCounterFormatSizePop3	POP3 协议格式和长度异常的会话数
239	fwCounterBlckCmdsPop3	被 POP3 阻断的非法命令数

表 323 私有 MIB 库 (*续*)

240	fwCounterFormatSizeImap	IMAP 协议格式和长度异常的会话数
241	fwCounterBlckCmdsImap	被 IMAP 阻断的非法命令数
242	fwCounterAttackDefenseSmtp	基于 SMTP 协议的攻击数量
243	fwCounterAttackDefensePop3	基于 POP3 协议的攻击数量
244	fwCounterAttackDefenseImap	基于 IMAP 协议的攻击数量
	18. fwDeep-InspectionCounterGroup	
245	fwCounterNewSessionRateFtp	FTP 新建会话率 （sessions/s）
246	fwCounterNewSessionRateTelnet	Telnet 新建会话率 （sessions/s）
247	fwCounterBlckbyBlacklistDns	被 DNS 域名黑名单阻断的会话数
248	fwCounterBlckCmdsTelnet	Telnet 用户自定义命令阻断的会话数
249	fwCounterAttackDefenseDI	DI 引擎攻击检测的总数量
250	fwCounterBackdoorDI	DI 检测到的后门攻击次数
	19. fwUrl-FilteringCounterGroup	
251	fwCounterBlckByBlacklist	被 URL 黑名单阻断的 URL 个数
252	fwCounterBlckByAnonymizers	被 Anonymizers URL 分类阻断的 HTTP 连接数
253	fwCounterBlckByBotnets	被 Botnets URL 分类阻断的 HTTP 连接数
254	fwCounterBlckByHacking	被 Hacking URL 分类阻断的 HTTP 连接数
255	fwCounterBlckByMalware	被 Malware URL 分类阻断的 URL 个数
256	fwCounterBlckByNetworkErrors	被 NetworkErrors URL 分类阻断的 URL 个数
257	fwCounterBlckByParkedDomains	被 ParkedDomains URL 分类阻断的 URL 个数
258	fwCounterBlckByPhishingFraud	被 PhishingFraud URL 分类阻断的 URL 个数
259	fwCounterBlckBySpamSites	由于包含 SpamSites URL 分类阻断的 URL 个数
260	fwCounterBlckByTranslators	被 Translators URL 分类阻断的 URL 个数
261	fwCounterBlckByAdvertisementsPop-Ups	被 Advertisements & Pop-Ups URL 分类阻断的 URL 数
262	fwCounterBlckByAlcoholTobacco	被 Alcohol & Tobacco URL 分类阻断的 URL 个数
263	fwCounterBlckByArts	被 Arts URL 分类阻断的 URL 个数
264	fwCounterBlckByBusiness	被 Business URL 分类阻断的 URL 个数
265	fwCounterBlckByChat	被 Chat URL 分类阻断的 URL 个数
266	fwCounterBlckByChildAbuseImages	被 Child Abuse Images URL 分类阻断的 URL 个数
267	fwCounterBlckByCompromised	被 Compromised URL 分类阻断的 URL 个数
268	fwCounterBlckByComputersTechnology	被 Computers & Technology URL 分类阻断的 URL 数
269	fwCounterBlckByCriminalActivity	被 Criminal Activity URL 分类阻断的 URL 个数
270	fwCounterBlckByCults	被 cults URL 分类阻断的 URL 个数

表 323 私有 MIB 库 (*续*)

271	fwCounterBlckByDatingPersonals	被 Dating & Personals URL 分类阻断的 URL 个数
272	fwCounterBlckByDownloadSites	被 Download Sites URL 分类阻断的 URL 个数
273	fwCounterBlckByEducation	被 Education URL 分类阻断的 URL 个数
274	fwCounterBlckByEntertainment	被 Entertainment URL 分类阻断的 URL 个数
275	fwCounterBlckByFashionBeauty	被 Fashion & Beauty URL 分类阻断的 URL 个数
276	fwCounterBlckByFinance	被 Finance URL 分类阻断的 URL 个数
277	fwCounterBlckByForumsNewsgroups	被 Forums & Newsgroups URL 分类阻断的 URL 个数
278	fwCounterBlckByGambling	被 Gambling URL 分类阻断的 URL 个数
279	fwCounterBlckByGames	被 Games URL 分类阻断的 URL 个数
280	fwCounterBlckByGeneral	被 General URL 分类阻断的 URL 个数
281	fwCounterBlckByGovernment	被 Government URL 分类阻断的 URL 个数
282	fwCounterBlckByGreetingCards	被 Greeting Cards URL 分类阻断的 URL 个数
283	fwCounterBlckByHateIntolerance	被 Hate & Intolerance URL 分类阻断的 URL 个数
284	fwCounterBlckByHealthMedicine	被 Health & Medicine URL 分类阻断的 URL 个数
285	fwCounterBlckByIllegalDrugs	被 Illegal Drugs URL 分类阻断的 URL 个数
286	fwCounterBlckByIllegalSoftware	被 Illegal Software URL 分类阻断的 URL 个数
287	fwCounterBlckByImageSharing	被 Image Sharing URL 分类阻断的 URL 个数
288	fwCounterBlckByInformationSecurity	被 Information Security URL 分类阻断的 URL 个数
289	fwCounterBlckByInstantMessaging	被 Instant Messaging URL 分类阻断的 URL 个数
290	fwCounterBlckByJobSearch	被 Job Search URL 分类阻断的 URL 个数
291	fwCounterBlckByLeisureRecreation	被 Leisure & Recreation URL 分类阻断的 URL 个数
292	fwCounterBlckByNews	被 News URL 分类阻断的 URL 个数
293	fwCounterBlckByNon-profitsNGOs	被 Non-profits & NGOs URL 分类阻断的 URL 个数
294	fwCounterBlckByNudity	被 Nudity URL 分类阻断的 URL 个数
295	fwCounterBlckByPeertoPeer	被 Peer-to-Peer URL 分类阻断的 URL 个数
296	fwCounterBlckByPersonalSites	被 Personal Sites URL 分类阻断的 URL 个数
297	fwCounterBlckByPolitics	被 Politics URL 分类阻断的 URL 个数
298	fwCounterBlckByPornographyOrSexuallyExpliclt	被 Pornography/Sexually Explicit URL 分类阻断的 URL 个数
299	fwCounterBlckByPrivateIPAddresses	被 Private IP Addresses URL 分类阻断的 URL 个数
300	fwCounterBlckByRealEstate	被 Real Estate URL 分类阻断的 URL 个数
301	fwCounterBlckByReligion	被 Religion URL 分类阻断的 URL 个数
302	fwCounterBlckByRestaurantsDining	被 Restaurants & Dining URL 分类阻断的 URL 个数
303	fwCounterBlckBySchoolCheating	被 School Cheating URL 分类阻断的 URL 个数

表 323 私有 MIB 库 (*续*)

304	fwCounterBlckBySearchEnginesPortals	被 Search Engines & Portals URL 分类阻断的 URL 数
305	fwCounterBlckBySexEducation	被 Sex Education URL 分类阻断的 URL 个数
306	fwCounterBlckByShopping	被 Shopping URL 分类阻断的 URL 个数
307	fwCounterBlckBySocialNetworking	被 Social Networking URL 分类阻断的 URL 个数
308	fwCounterBlckBySports	被 Sports URL 分类阻断的 URL 个数
309	fwCounterBlckByStreamingMediaDownloads	被 Streaming Media & Downloads URL 分类阻断的 URL 个数
310	fwCounterBlckByTasteless	被 Tasteless URL 分类阻断的 URL 个数
311	fwCounterBlckByTransportation	被 Transportation URL 分类阻断的 URL 个数
312	fwCounterBlckByTravel	被 Travel URL 分类阻断的 URL 个数
313	fwCounterBlckByViolence	被 Violence URL 分类阻断的 URL 个数
314	fwCounterBlckByWeapons	被 Weapons URL 分类阻断的 URL 个数
315	fwCounterBlckByWebBasedEmail	被 Web-based Email URL 分类阻断的 URL 个数
316	fwCounterBlckTotal	被 URL 过滤阻断的连接总数