H3C SecBlade FW/VPN 单板

命令手册

杭州华三通信技术有限公司

http://www.h3c.com.cn

资料版本：T1-081944-20070416-1.03

产品版本：COMWARE 3.10

声明

Copyright ©2006-2007 杭州华三通信技术有限公司及其许可者 版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

H3C、H3C、Aolynk、Aolynk、H^{3}Care、H3care、TOP G、TOPG、IRF、NetPilot、Neocean、NeoVTL、SecPro、SecPoint、SecEngine、SecPath、Comware、Secware、Storware、NQA、VVG、V^{2}G、V^{n}G、PSPT、XGbus、N-Bus、TiGem、InnoVision、HUASAN、华三均为杭州华三通信技术有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。如需要获取最新手册，请登录http://www.h3c.com.cn。

技术支持

用户支持邮箱：customer_service@h3c.com

技术支持热线电话：800-810-0504（固话拨打）

400-810-0504（手机、固话均可拨打）

网址：http://www.h3c.com.cn

前 言

相关手册

手册名称	用途
《H3C SecBlade FW/VPN 单板操作手册》	该手册介绍了 H3C SecBlade 系列 FW/VPN 单板的功能特性、工作原理和配置及操作指导。

本书简介

本手册各章节内容如下：

- **简介。**该部分主要介绍了交换机和 SecBlade 进行协同工作前先要在交换机中对 SecBlade 进行的相关配置命令。
- **VPN。**该部分包括 L2TP 和 GRE 的配置命令，动态 VPN 的配置命令、IPSec 和 IKE 配置命令以及 PKI 的配置命令。
- **安全。**该部分包括 AAA 及 RADIUS/HWTACACS 配置命令、访问控制列表配置命令、防火墙配置命令、地址转换配置命令、Web 和邮件过滤配置命令、攻击防范与报文统计配置命令以及日志维护统计配置命令等。
- **可靠性。**该部分主要介绍了 VRRP 的配置命令。
- **附录。**主要对 H3C Secblade FW/VPN 单板的所有配置命令在命令手册中的位置作了一个索引，方便用户查找。

🕮 **说明：**

由于各型号产品软件规格存在一定差异，所有涉及产品规格的问题需要和杭州华三通信技术有限公司技术支持部联系确认。

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | … }	表示从两个或多个选项中选取一个。
[x | y | …]	表示从两个或多个选项中选取一个或者不选。
{ x | y | … }*	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | …]*	表示从两个或多个选项中选取多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入 1～n 次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

⚠ **小心、注意**：提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。

警告：该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。

🕮 **说明、提示、窍门、思考**：对操作内容的描述进行必要的补充和说明。

简介

目 录

第 1 章 SecBlade配置命令 1-1
1.1 SecBlade配置命令 1-1
1.1.1 default-login-user 1-1
1.1.2 display secblade module 1-1
1.1.3 map to slot 1-2
1.1.4 secblade aggregation slot 1-3
1.1.5 secblade module 1-3
1.1.6 secblade slot 1-4
1.1.7 secblade-interface 1-4
1.1.8 security-vlan 1-5

第1章 SecBlade 配置命令

1.1 SecBlade 配置命令

1.1.1 default-login-user

【命令】

default-login-user

undo default-login-user

【视图】

SecBlade 的系统视图

【参数】

无

【描述】

default-login-user 命令用来使能 SecBlade 默认用户登录功能，**undo default-login-user** 命令用来禁止 SecBlade 默认用户登录功能。

为了方便用户登录，SecBlade 中内建了一个名为“SecBlade”，密码为“SecBlade”的用户。

缺省情况下，使能 SecBlade 默认用户登录功能，即允许使用内建的用户登录到 SecBlade。

🕮 **说明：**

此条命令是在 SecBlade 单板上配置的。

【举例】

禁止默认用户登录功能。

```
[SecBlade_FW] undo default-login-user
```

1.1.2 display secblade module

【命令】

display secblade module [*sec-mod-name*]

【视图】

交换机的任意视图

【参数】

sec-mod-name：模块名。

【描述】

display secblade module 命令用来显示 SecBlade 模块的相关信息。

【举例】

显示模块 newsec 的相关信息。

```
[H3C]display secblade module newsec
module newsec:
   security-vlan: 10,20,30
   secblade-interface: Vlan-interface192
   vlan passing: 10,20,30,192
   map to slot: 5
```

1.1.3 map to slot

【命令】

map to slot *slot-number*

undo map to slot *slot-number*

【视图】

交换机的 SecBlade 模块视图

【参数】

slot-number：SecBlade 单板所在的槽位号。

【描述】

map to slot 命令用来将当前模块映射到 *slot-number* 对应的单板，**undo map to slot** 命令用来取消 SecBlade 模块和 SecBlade 单板之间的映射。

缺省情况下，未将任何模块映射到任何单板。

【举例】

将当前模块映射到槽位 2 上的 SecBlade 单板。

```
[H3C-secblade-newsec] map to slot 2
```

1.1.4 secblade aggregation slot

【命令】

secblade aggregation slot *slot-number*

undo secblade aggregation slot *slot-number*

【视图】

交换机的系统视图

【参数】

slot-number：SecBlade 单板所在的槽位号。

【描述】

secblade aggregation slot 命令用来设置 SecBlade 接口的聚合，**undo secblade aggregation slot** 命令用来取消接口聚合。

SecBlade 单板与交换机的连接是通过 2 个内部 GigabitEthernet 接口，可将这 2 个接口聚合为一个逻辑接口，以提供更大的接口带宽。

缺省情况下，未对接口进行聚合，且只有一个 GigabitEthernet 接口可以使用。

🕮 **说明：**

当用户通过 **Secblade aggregation slot** 命令用来设置 SecBlade 接口的聚合时，如果聚合资源不充分的情况下，SecBlade 会抢占其它聚合组已占有的资源。

【举例】

设置 2 号槽位上的 SecBlade 单板的接口聚合。

```
[H3C] secblade aggregation slot 2
```

1.1.5 secblade module

【命令】

secblade module *sec-mod-name*

undo secblade module *sec-mod-name*

【视图】

交换机的系统视图

【参数】

sec-mod-name ：SecBlade 的模块名，模块名必须以字母或数字开头。

【描述】

secblade module 命令用来创建 SecBlade 模块，并进入 SecBlade 模块视图，以配置 SecBlade 模块的属性。

undo secblade module 命令用来删除 SecBlade 模块。如果该模块已经 map 到 SecBlade 单板，则不允许删除。

【举例】

进入 SecBlade 模块视图。

```
[H3C] secblade module newsec
[H3C-secblade-newsec]
```

1.1.6 secblade slot

【命令】

secblade slot *slot-number*

【视图】

交换机的用户视图

【参数】

slot-number：SecBlade 单板所在的槽位号。

【描述】

secblade slot 命令用来登录到 SecBlade 上。

【举例】

登录到 2 号槽位上的 SecBlade 单板。

```
<H3C> secblade slot 2
```

1.1.7 secblade-interface

【命令】

secblade-interface vlan-interface *interface-number*

undo secblade-interface vlan-interface *interface-number*

【视图】

交换机的 SecBlade 模块视图

【参数】

interface-number：指定接口号。

【描述】

secblade-interface 命令用来设置交换机与 SecBlade 相连接的三层接口，**undo secblade-interface** 命令用来删除交换机与 SecBlade 相连接的三层接口。

缺省情况下，没有设置交换机与 SecBlade 相连接的三层接口。

此处指定的 VLAN 接口所对应的 VLAN 不能包含在 **security-vlan** 中。

【举例】

设置交换机的 VLAN 40 接口为交换机与 SecBlade 相连接的三层接口。

```
[H3C-secblade-newsec] secblade-interface vlan-interface 40
```

1.1.8 security-vlan

【命令】

security-vlan *vlan-range*

undo security-vlan *vlan-range*

【视图】

交换机的 SecBlade 模块视图

【参数】

vlan-range：VLAN 范围

【描述】

security-vlan 命令用来指定 *vlan-range* 中所有的 VLAN 都需要 SecBlade 进行保护，**undo security-vlan** 命令用来取消 SecBlade 对 *vlan-range* 中 VLAN 的保护。

缺省情况下，没有 VLAN 受到保护。

📖 **说明：**

当某个 VLAN 被配置为 Super VLAN 后，不能再将此 VLAN 配置为 Security VLAN。

【举例】

设置 VLAN 10、20、30 收到 SecBlade 保护。

```
[H3C-secblade-newsec] security-vlan 10 20 30
```

VPN

目 录

第 1 章 L2TP配置命令 1-1
1.1 L2TP配置命令 1-1
1.1.1 allow l2tp 1-1
1.1.2 debugging l2tp 1-2
1.1.3 display l2tp session 1-3
1.1.4 display l2tp tunnel 1-4
1.1.5 display l2tp user 1-5
1.1.6 interface virtual-template 1-6
1.1.7 l2tp enable 1-6
1.1.8 l2tp-auto-client enable 1-7
1.1.9 l2tp-group 1-7
1.1.10 l2tpmoreexam enable 1-8
1.1.11 mandatory-chap 1-9
1.1.12 mandatory-lcp 1-9
1.1.13 reset l2tp session 1-10
1.1.14 reset l2tp tunnel 1-11
1.1.15 reset l2tp user 1-11
1.1.16 session idle-time 1-12
1.1.17 start l2tp 1-12
1.1.18 start l2tp tunnel 1-13
1.1.19 tunnel authentication 1-14
1.1.20 tunnel avp-hidden 1-15
1.1.21 tunnel flow-control 1-15
1.1.22 tunnel keepstanding 1-16
1.1.23 tunnel name 1-17
1.1.24 tunnel password 1-17
1.1.25 tunnel timer hello 1-18
第 2 章 GRE配置命令 2-1
2.1 GRE配置命令 2-1
2.1.1 debugging tunnel 2-1
2.1.2 destination 2-1
2.1.3 display interface tunnel 2-2
2.1.4 gre checksum 2-4
2.1.5 gre key 2-4
2.1.6 interface tunnel 2-5
2.1.7 keepalive 2-6
2.1.8 source 2-6
2.1.9 tunnel-protocol gre 2-7

第 3 章 IPSec配置命令 3-1
3.1 IPSec配置命令 3-1
3.1.1 ah authentication-algorithm 3-1
3.1.2 debugging ike dpd 3-2
3.1.3 debugging ipsec 3-2
3.1.4 display ike dpd 3-3
3.1.5 display ipsec policy 3-4
3.1.6 display ipsec policy-template 3-7
3.1.7 display ipsec proposal 3-8
3.1.8 display ipsec sa 3-9
3.1.9 display ipsec statistics 3-12
3.1.10 display ipsec tunnel 3-13
3.1.11 dpd 3-14
3.1.12 encapsulation-mode 3-15
3.1.13 esp authentication-algorithm 3-16
3.1.14 esp encryption-algorithm 3-17
3.1.15 ike dpd 3-18
3.1.16 interval-time 3-18
3.1.17 ipsec policy 3-19
3.1.18 ipsec policy 3-20
3.1.19 ipsec policy-template 3-21
3.1.20 ipsec proposal 3-22
3.1.21 ipsec sa global-duration 3-23
3.1.22 pfs 3-24
3.1.23 proposal 3-25
3.1.24 reset ipsec sa 3-26
3.1.25 reset ipsec statistics 3-27
3.1.26 sa authentication-hex 3-28
3.1.27 sa duration 3-29
3.1.28 sa encryption-hex 3-30
3.1.29 sa spi 3-32
3.1.30 sa string-key 3-33
3.1.31 security acl 3-35
3.1.32 time-out 3-35
3.1.33 transform 3-36
3.1.34 tunnel local 3-37
3.1.35 tunnel remote 3-38
3.2 加密卡配置命令 3-39
3.2.1 debugging encrypt-card host 3-39
3.2.2 display encrypt-card fast-switch 3-40
3.2.3 display interface encrypt 3-40
3.2.4 encrypt-card backuped 3-41
3.2.5 encrypt-card fast-switch 3-42
3.2.6 interface encrypt 3-43
3.2.7 ipsec card-proposal 3-43

3.2.8 reset counters interface encrypt 3-44
3.2.9 reset encrypt-card fast-switch 3-45
3.2.10 reset encrypt-card sa 3-46
3.2.11 reset encrypt-card statistics 3-46
3.2.12 reset encrypt-card syslog 3-47
3.2.13 snmp-agent trap enable encrypt-card 3-48
3.2.14 use encrypt-card 3-48
第 4 章 IKE配置命令 4-1
4.1 IKE配置命令 4-1
4.1.1 authentication-algorithm 4-1
4.1.2 authentication-method 4-1
4.1.3 debugging ike 4-2
4.1.4 dh 4-3
4.1.5 display ike peer 4-4
4.1.6 display ike proposal 4-4
4.1.7 display ike sa 4-5
4.1.8 encryption-algorithm 4-6
4.1.9 exchange-mode 4-7
4.1.10 id-type 4-8
4.1.11 ike encrypt-card dh-computation disabled 4-8
4.1.12 ike local-name 4-9
4.1.13 ike next-payload check disabled 4-10
4.1.14 ike peer 4-10
4.1.15 ike-peer 4-11
4.1.16 ike proposal 4-11
4.1.17 ike sa keepalive-timer interval 4-13
4.1.18 ike sa keepalive-timer timeout 4-13
4.1.19 ike sa nat-keepalive-timer interval 4-14
4.1.20 local 4-15
4.1.21 local-address 4-15
4.1.22 nat traversal 4-16
4.1.23 pre-shared-key 4-17
4.1.24 peer 4-17
4.1.25 remote-address 4-18
4.1.26 remote-name 4-18
4.1.27 reset ike sa 4-19
4.1.28 sa duration 4-20
第 5 章 PKI配置命令 5-1
5.1 PKI域配置命令 5-1
5.1.1 ca identifier 5-1
5.1.2 certificate request entity 5-1
5.1.3 certificate request from 5-2
5.1.4 certificate request mode 5-3
5.1.5 certificate request polling 5-3

5.1.6 certificate request url 5-4
5.1.7 crl check disable 5-5
5.1.8 crl update-period 5-5
5.1.9 crl url 5-6
5.1.10 ldap-server 5-6
5.1.11 pki domain 5-7
5.1.12 root-certificate fingerprint 5-8
5.2 PKI实体配置命令 5-8
5.2.1 fqdn 5-8
5.2.2 common-name 5-9
5.2.3 country 5-10
5.2.4 ip 5-10
5.2.5 locality 5-11
5.2.6 organization 5-11
5.2.7 organization-unit 5-12
5.2.8 state 5-12
5.2.9 pki entity 5-13
5.3 PKI证书操作命令 5-13
5.3.1 pki delete-certificate 5-13
5.3.2 pki import-certificate 5-14
5.3.3 pki request-certificate 5-15
5.3.4 pki retrieval-certificate 5-15
5.3.5 pki retrieval-crl 5-16
5.3.6 pki validate-certificate 5-16
5.4 PKI显示与调试命令 5-17
5.4.1 debugging pki 5-17
5.4.2 display pki certificate 5-21
5.4.3 display pki crl 5-23
第 6 章 动态VPN配置命令 6-1
6.1 动态VPN配置命令 6-1
6.1.1 algorithm-suite 6-1
6.1.2 authentication-client method 6-2
6.1.3 authentication-server method 6-2
6.1.4 data algorithm-suite 6-3
6.1.5 data ipsec-sa duration 6-4
6.1.6 debugging dvpn 6-4
6.1.7 display dvpn ipsec-sa 6-5
6.1.8 display dvpn map 6-6
6.1.9 display dvpn session 6-7
6.1.10 display dvpn info 6-7
6.1.11 display dvpn online-user 6-9
6.1.12 dvpn class 6-9
6.1.13 dvpn client register-dumb 6-10
6.1.14 dvpn client register-interval 6-10

6.1.15 dvpn client register-retry 6-11
6.1.16 dvpn dvpn-id 6-12
6.1.17 dvpn interface-type 6-12
6.1.18 dvpn policy 6-13
6.1.19 dvpn policy 6-13
6.1.20 dvpn register-type 6-14
6.1.21 dvpn security 6-15
6.1.22 dvpn server 6-15
6.1.23 dvpn server authentication-client method 6-16
6.1.24 dvpn server map age-time 6-17
6.1.25 dvpn server pre-shared-key 6-17
6.1.26 dvpn service enable 6-18
6.1.27 local-user 6-18
6.1.28 public-ip 6-19
6.1.29 pre-shared-key 6-20
6.1.30 private-ip 6-20
6.1.31 reset dvpn all 6-21
6.1.32 reset dvpn map 6-21
6.1.33 reset dvpn session 6-22
6.1.34 reset dvpn statistics 6-22
6.1.35 session algorithm-suite 6-23
6.1.36 session idle-time 6-24
6.1.37 session keepalive-interval 6-24
6.1.38 session setup-interval 6-25
6.1.39 tunnel-protocol udp dvpn 6-25

第1章 L2TP 配置命令

1.1 L2TP 配置命令

1.1.1 allow l2tp

【命令】

allow l2tp virtual-template *virtual-template-number* **remote** *remote-name* [**domain** *domain-name*]

undo allow

【视图】

L2TP 组视图

【参数】

virtual-template-number：指定用于创建新的虚拟访问接口（virtual access interface）时所用的虚拟模板接口，取值范围是整数 0～1023。

remote-name：指定发起连接请求的隧道对端的名称，对大小写有区别，取值为字符串，长度为 1～30。

domain-name：指定企业的名称，取值为字符串，长度为 1～30。

【描述】

allow l2tp 命令用来指定接受呼叫时隧道对端的名称及所使用的 Virtual-Template，**undo allow** 命令用来取消隧道对端的名称及所使用的 Virtual-Template。

缺省情况下，为禁止接受呼入。

此命令在 LNS 端使用。

在 L2TP 多域应用中，必须配置参数 *domain-name*。

使用 L2TP 组号 1 时（缺省的 L2TP 组号），可以不指定通道对端名 *remote-name*，在组 1 下进行配置时，本命令的格式为：

allow l2tp virtual-template *virtual-template-number* [**remote** *remote-name*] [**domain** *domain-name*]

如果在 L2TP 组 1 的配置模式下，仍指定对端名称，则 L2TP 组 1 不作为缺省的 L2TP 组。如在 Windows 2000 beta 2 版本中，VPN 连接的本端名称为 NONE，则 SecBlade 收到的对端名称为 NONE。为了接收这种不知名的对端发起的通道请求连接，或者用于测试目的，可以设置一个缺省的 L2TP 组。

命令 **allow l2tp** 使用在 LNS 侧，如果配置了通道对端名称，必须确保通道对端的名称和 LAC 侧配置的本端名称一致。

相关配置可参考命令 **l2tp-group**。

【举例】

接受名称为 AS8010 的对端（LAC）发起的 L2TP 隧道连接请求，并在 virtual-template 1 上创建 virtual-access 接口。

```
[SecBlade_VPN-l2tp2] allow l2tp virtual-template 1 remote AS8010
```

将 L2TP 组 1 作为缺省的 L2TP 组，接受任何对端发起的 L2TP 通道连接请求，并根据 virtual-template 1 创建 virtual-access 接口。

```
[SecBlade_VPN] l2tp-group 1
[SecBlade_VPN-l2tp1] allow l2tp virtual-template 1
```

1.1.2 debugging l2tp

【命令】

debugging l2tp { **all** | **control** | **dump** | **error** | **event** | **hidden** | **payload** | **time-stamp** }

undo debugging l2tp { **all** | **control** | **dump** | **error** | **event** | **hidden** | **payload** | **time-stamp** }

【视图】

用户视图

【参数】

all：表示打开所有 L2TP 调试信息开关。

control：表示打开控制报文调试开关。

dump：表示打开 PPP 报文调试开关。

error：表示打开差错信息的调试开关。

event：表示打开事件调试信息开关。

hidden：表示打开隐藏 AVP 的调试开始信息开关。

payload：表示打开 L2TP 数据报文调试开关。

time-stamp：表示打开显示时间戳的调试开关。

【描述】

debugging l2tp 命令用来打开 L2TP 调试信息开关，**undo debugging l2tp** 命令用来关闭 L2TP 调试信息开关。

【举例】

打开所有 L2TP 调试信息开关。

```
<SecBlade_VPN> debugging l2tp all
```

1.1.3 display l2tp session

【命令】

display l2tp session

【视图】

所有视图

【参数】

无

【描述】

display l2tp session 命令用来显示当前的 L2TP 会话的信息。

该命令的输出信息，可以帮助用户确定当前建立的 L2TP 会话信息。

相关配置可参考命令 **display l2tp tunnel**。

【举例】

显示当前 L2TP 会话信息。

```
<SecBlade_VPN> display l2tp session
LocalSID      RemoteSID    LocalTID IdleTimeLeft
 1                    1             2        600
Total session = 1
```

表1-1 display L2tp session 显示信息的域描述

域	描述
Total session	Session 的数目
LocalSID	本端唯一标识一个会话的数值
RemoteSID	对端唯一标识一个会话的数值
LocalTID	隧道的本端标识号
Idle-Time-Left	会话距离超时挂断剩余时间

1.1.4 display l2tp tunnel

【命令】

display l2tp tunnel

【视图】

所有视图

【参数】

无

【描述】

display l2tp tunnel 命令用来显示当前的 L2TP 隧道的信息。

该命令的输出信息，可以帮助用户确定当前所建立的 L2TP 隧道信息。

相关配置可参考命令 **display l2tp session**。

【举例】

显示当前 L2TP 隧道信息。

```
<SecBlade_VPN> display l2tp tunnel
LocalTID RemoteTID RemoteAddress Port  Sessions  RemoteName keepstanding
 2        22849      11.1.1.1        1701      1       lns    YES
 Total tunnel = 1
```

表1-2 display l2tp tunnel 显示信息的域描述

域	描述
Total tunnel	Tunnel 的数目
LocalTID	本端唯一标识一个隧道的数值
RemoteTID	对端唯一标识一个隧道的数值
RemoteAddress	对端的 IP 地址
Port	对端的端口号
Sesssions	此隧道上的会话数目
Remote Name	对端的名称
KeepStanding	是否设置了连接保持功能

📖 **说明：**

SecBlade 作为 LNS 时，当存在域用户和非域用户时，对于非域用户触发的隧道，在设备上可能会显示错误的 L2TP 信息。

1.1.5 display l2tp user

【命令】

display l2tp user

【视图】

所有视图

【参数】

无

【描述】

display l2tp user 命令用来显示当前 L2TP 用户的信息。

相关配置可参考命令 **display l2tp tunnel**，**display l2tp session**。

【举例】

显示当前 L2TP 用户信息。

```
<SecBlade_VPN> display l2tp user
User Name        LocalSID  RemoteSID  LocalTID
w@h3c              1              1              2

 Total user = 1
```

表1-3 display L2tp user 显示信息的域描述

域	描述
User Name	用户名
LocalSID	会话连接的本端标识号
RemoteSID	会话连接的对端标识号
LocalTID	隧道的本端标识号
Total user	用户的数目

1.1.6 interface virtual-template

【命令】

interface virtual-template *virtual-template-number*

undo interface virtual-template *virtual-template-number*

【视图】

系统视图

【参数】

virtual-template-number：标识虚拟模板接口序号，取值为整数，范围是 0～1023。

【描述】

interface virtual-template 命令用来创建虚拟模板接口，**undo interface virtual-template** 命令用来删除虚拟模板接口。

缺省情况下，系统没有创建虚拟模板接口。

虚拟模板接口主要用于配置 SecBlade 在运行过程中动态创建的虚接口的工作参数，如 L2TP 逻辑接口。

相关配置可参考命令 **allow l2tp**。

【举例】

创建虚拟模板接口 1 并进入该视图。

```
[SecBlade_VPN] interface virtual-template 1
```

1.1.7 l2tp enable

【命令】

l2tp enable

undo l2tp enable

【视图】

系统视图

【参数】

无

【描述】

l2tp enable 命令用来启用 L2TP 功能，**undo l2tp enable** 命令用来禁止 L2TP 功能。

缺省情况下，L2TP 功能被禁止。

相关配置可参考命令 **l2tp-group**。

【举例】

在 SecBlade 上启用 L2TP 功能。

```
[SecBlade_VPN] l2tp enable
```

1.1.8 l2tp-auto-client enable

【命令】

l2tp-auto-client enable

undo l2tp-auto-client enable

【视图】

虚拟模板接口视图

【参数】

无

【描述】

l2tp-auto-client enable 命令用来使能 LAC 客户端建立 L2TP 隧道。**undo l2tp-auto-client enable** 命令用来取消 LAC 客户端建立 L2TP 隧道。

【举例】

进入虚拟模板接口视图。

```
[SecBlade_VPN] interface virtual-template 1
```

使能 LAC 客户端建立 L2TP 隧道。

```
[SecBlade_VPN-Virtual-Template1] l2tp-auto-client enable
```

1.1.9 l2tp-group

【命令】

l2tp-group *group-number*

undo l2tp-group *group-number*

【视图】

系统视图

【参数】

group-number：标识 L2TP 组号，取值为整数，范围为 1～1000。

【描述】

l2tp-group 命令用来创建 L2TP 组，**undo l2tp-group** 命令用来删除 L2TP 组。

缺省情况下，系统没有创建 L2TP 组。

使用 **l2tp-group** 命令创建一个 L2TP 组（L2TP 组 1 可以作为缺省的 L2TP 组）。使用 **undo l2tp-group** 命令删除 L2TP 组后，该组的所有配置信息也将被删除。

相关配置可参考命令 **allow l2tp**，**start l2tp**。

【举例】

创建 L2TP 组 2，并进入 L2TP 组 2 视图。

```
[SecBlade_VPN] l2tp-group 2
[SecBlade_VPN-l2tp2]
```

1.1.10 l2tpmoreexam enable

【命令】

l2tpmoreexam enable

undo l2tpmoreexam enable

【视图】

系统视图

【参数】

无

【描述】

本命令在 LNS 端配置。

l2tpmoreexam enable 命令用来启用 L2TP 多域功能，**undo l2tpmoreexam enable** 命令用来禁止 L2TP 多域功能。

缺省情况下，L2TP 多域功能被禁止。

使用 **l2tpmoreexam enable** 命令启用 L2TP 多域功能，只有启用该功能后才能开展 L2TP 多域业务。

相关配置可参考命令 **l2tp enable**。

【举例】

在 SecBlade（LNS 端）上启用 L2TP 多域功能。

```
[H3C] l2tpmoreexam enable
```

1.1.11 mandatory-chap

【命令】

mandatory-chap

undo mandatory-chap

【视图】

L2TP 组视图

【参数】

无

【描述】

mandatory-chap 命令用来强制 LNS 与用户端（Client）之间重新进行 CHAP 验证，**undo mandatory-chap** 命令用来禁止 CHAP 的重新验证。

缺省情况下，系统不进行 CHAP 的重新验证。

在 LAC 对用户端进行代理验证后，LNS 对用户端再次进行验证，可以增加安全性。如果使用 **mandatory-chap** 命令，则对于由接入服务器初始化隧道连接的 VPN 的用户端来说，会经过两次验证：一次是用户端在接入服务器端的验证，另一次是用户端在 LNS 端的验证。一些 PPP 用户端可能不支持进行第二次验证，这时，本端的 CHAP 验证会失败。

相关配置可参考命令 **mandatory-lcp**。

【举例】

强制进行 CHAP 验证。

```
[SecBlade_VPN-l2tp1] mandatory-chap
```

1.1.12 mandatory-lcp

【命令】

mandatory-lcp

undo mandatory-lcp

【视图】

L2TP 组视图

【参数】

无

【描述】

mandatory-lcp 命令用来在 LNS 与用户端（Client）之间重新进行链路控制协议（Link Control Protocol）的协商，**undo mandatory-lcp** 命令用来禁止 LCP 的重新协商。

缺省情况下，系统不重新进行 LCP 协商。

对于 NAS-Initialized VPN 的用户端，在一个 PPP 会话开始时，将先和网络接入服务器（NAS）进行 PPP 协商。如果协商通过，则由接入服务器初始化隧道连接，并把与用户端协商收集到的信息传给 LNS；LNS 根据收到的代理验证信息判断用户是否合法。使用 **mandatory-lcp** 命令可以强制 LNS 与用户端重新进行 LCP 协商，这就忽略 NAS 的代理验证信息。如果一些 PPP 用户端可能不支持 LCP 的重新协商，则 LCP 重新协商过程会失败。

相关配置可参考命令 **mandatory-chap**。

【举例】

允许进行 LCP 重新协商。

```
[SecBlade_VPN-l2tp1] mandatory-lcp
```

1.1.13 reset l2tp session

【命令】

reset l2tp session *session-id*

【视图】

用户视图

【参数】

session-id：会话连接的本端标识号。

【描述】

reset l2tp session 命令用于强制断开一个会话连接。当用户再次呼入时，会话可以重新建立。

相关配置可参考命令 **reset l2tp tunnel**。

【举例】

强制断开 L2TP 会话连接。

```
<SecBlade_VPN> reset l2tp session 1
```

1.1.14 reset l2tp tunnel

【命令】

reset l2tp tunnel { name *remote-name* | id *tunnel-id* }

【视图】

用户视图

【参数】

remote-name：隧道对端的名称。

tunnel-id：隧道本端的标识号。

【描述】

reset l2tp tunnel 命令用来断开指定的隧道（Tunnel）连接，同时断开隧道内的所有会话（Session）连接。

reset l2tp tunnel 命令用于强制断开一个隧道连接。当对端用户再次呼入时，隧道可以重新建立。通过指定隧道的对端名称来确定需要断开的隧道连接。如果没有符合条件的隧道连接存在，则对当前的隧道连接没有影响。如果有多个符合条件的隧道连接存在（同一个名称，不同 IP 地址），则断开所有符合条件的隧道连接。指定 *tunnel-id* 时，只断开对应的隧道连接。

相关配置可参考命令 **display l2tp tunnel**。

【举例】

断开对端名称为 AS8010 的 Tunnel 连接。

```
<SecBlade_VPN> reset l2tp tunnel name AS8010
```

1.1.15 reset l2tp user

【命令】

reset l2tp user *user-name*

【视图】

用户视图

【参数】

user-name： L2TP 的用户名。

【描述】

reset l2tp user 命令用于强制断开该用户的连接。当用户再次呼入时，可以重新接入。

相关配置可参考命令 **reset l2tp tunnel**，**reset l2tp session**。

【举例】

强制断开当前 L2TP 用户的连接。

```
<SecBlade_VPN> reset l2tp user H3C@h3c
```

1.1.16 session idle-time

【命令】

session idle-time *time*

undo session idle-time

【视图】

L2TP 组视图

【参数】

time：超时时间长度，以秒为单位，取值范围为 0～10000。缺省为 0，表示不超时。

【描述】

session idle-time 命令用来设置 L2TP 会话超时挂断的超时时间，并触发超时挂断功能。**undo session idle-time** 命令用来禁止 L2TP 会话超时断开。

缺省情况下，L2TP 会话不会超时。

【举例】

进入 L2TP 组视图。

```
[SecBlade_VPN] l2tp-group 1
```

设定 L2TP 会话超时挂断时间为 600 秒。

```
[SecBlade_l2tp1] session idle-time 600
```

1.1.17 start l2tp

【命令】

start l2tp { **ip** *ip-addr* [**ip** *ip-addr*] [**ip** *ip-addr*] **...** } { **domain** *domain-name* | **fullusername** *user-name* }

undo start

【视图】

L2TP 组视图

【参数】

ip *ip-addr*：隧道对端（LNS）的 IP 地址，最多可以设置五个，彼此形成备份 LNS。

domain-name：指定触发连接请求的用户域名，取值为字符串，长度为 1～30。

user-name：指定触发连接请求的用户全名，取值为字符串，长度为 1～80。

【描述】

start l2tp 命令用来指定本端作为 L2TP LAC 端时发起呼叫的触发条件，**undo start** 命令用来删除指定的触发条件。

此命令在 LAC 端使用。使用此命令指定 LNS 的 IP 地址，并支持多种触发连接请求。

- 可以根据用户域名来发起建立隧道的连接请求。比如用户所在公司的域名为 h3c.com，则可以指定包含 h3c.com 域名的用户为 VPN 用户。
- 可以直接通过用户全名来指定该用户为 VPN 用户。

如果发现是 VPN 用户，则本端（LAC）按照配置的 LNS 的先后顺序向某个 LNS 发送建立 L2TP 隧道的连接请求，当得到 LNS 的接收应答后，该 LNS 就作为隧道的对端；否则 LAC 向下一个 LNS 发起隧道连接请求。

这几种 VPN 用户判定方式之间可能存在冲突的情况，如对全用户名指定的 LNS 地址是 1.1.1.1，而根据域名指定的 LNS 地址为 1.1.1.2，有必要规定一下查找用户的先后顺序。查找的顺序为：先根据完整的用户名查看是否存在根据此用户名指定的 L2TP 组；如果没有找到，再根据域名进行查找。

当配置多个 LNS 时，因客户端 PPP 的超时时间不同，可能会导致不能与后续几个 IP 地址（备份 LNS）建立连接，故建议最多配置两个 LNS。

【举例】

根据域名 h3c.com 来判断 VPN 用户，对应的总部 L2TP 接入服务器的 IP 地址为 202.38.168.1。

```
[SecBlade_VPN-l2tp1] start l2tp ip 202.38.168.1 domain h3c.com
```

1.1.18 start l2tp tunnel

【命令】

start l2tp tunnel

【视图】

L2TP 组视图

【参数】

无

【描述】

start l2tp tunnel 命令用来启动 L2TP LAC 端发起呼叫。

此命令只在 LAC 端使用。

相关命令请参考 **tunnel keepstanding**。

【举例】

启动 LAC 按照配置的 LNS 的先后顺序发送建立 L2TP 隧道的连接请求，即先向地址为 1.1.1.1 的 LNS 发起，没有应答则顺序向下一个地址为 2.2.2.2 的 LNS 发起。

```
[SecBlade_VPN-l2tp1] start l2tp ip 1.1.1.1 ip 2.2.2.2 fullusername vpdnuser
[SecBlade_VPN-l2tp1] start l2tp tunnel
```

⚠ 注意：

该命令需要与 **tunnel keepstanding** 命令配合使用，否则隧道不会被建立。

1.1.19 tunnel authentication

【命令】

tunnel authentication

undo tunnel authentication

【视图】

L2TP 组视图

【参数】

无

【描述】

tunnel authentication 命令用来启用 L2TP 的隧道验证功能，**undo tunnel authentication** 命令用来取消 L2TP 隧道验证功能。

缺省情况下，系统对 L2TP 隧道进行验证。

L2TP 隧道验证是缺省允许的。一般情况下，为了安全起见，隧道两端都需要对对方进行验证。如果为了进行网络的连通性测试或者是接收不知名对端发起的连接，可以不进行隧道验证。

【举例】

设置不验证隧道对端。

```
[SecBlade_VPN-l2tp1] undo tunnel authentication
```

1.1.20 tunnel avp-hidden

【命令】

tunnel avp-hidden

undo tunnel avp-hidden

【视图】

L2TP 组视图

【参数】

无

【描述】

tunnel avp-hidden 命令用来配置对 AVP（Attribute Value Pair，属性值对）数据采用隐藏的方式进行传输，**undo tunnel avp-hidden** 命令用来恢复 AVP 数据的缺省传输方式。

缺省情况下，隧道采用明文方式传输 AVP 数据。

L2TP 协议的一些参数是通过 AVP 数据来传输的，如果用户对这些数据的安全性要求高，可以使用本命令将 AVP 数据的传输方式配置成为隐藏传输。

【举例】

设置 AVP 数据隐含传输。

```
[SecBlade_VPN-l2tp1] tunnel avp-hidden
```

1.1.21 tunnel flow-control

【命令】

tunnel flow-control

undo tunnel flow-control

【视图】

L2TP 组视图

【参数】

无

【描述】

tunnel flow-control 命令用来开启 L2TP 通道流控功能，**undo tunnel flow-control** 命令用来关闭通道流控功能。

缺省情况下，关闭 L2TP 通道流控功能。

使用此命令来开启 L2TP 通道流控功能，以达到流控目的。

【举例】

开启通道流控。

```
[SecBlade_VPN-l2tp1] tunnel flow-control
```

1.1.22 tunnel keepstanding

【命令】

tunnel keepstanding

undo tunnel keepstanding

【视图】

L2TP 组视图

【参数】

无

【描述】

tunnel keepstanding 命令用来配置 L2TP Tunnel 连接保持功能。**undo tunnel keepstanding** 命令用来取消 L2TP Tunnel 连接保持功能。

配置 L2TP Tunnel 连接保持功能后，即使隧道上没有 Session 也不会因超时而挂断。

⚠ 注意：

此命令需要在隧道两端同时配置才会生效。

缺省情况下，未配置隧道连接保持功能。

【举例】

进入 L2TP 组视图。

```
[SecBlade_VPN] l2tp-group 1
```

使能 L2TP Tunnel 连接保持功能。

```
[SecBlade_VPN-l2tp1] tunnel keepstanding
```

1.1.23 tunnel name

【命令】

tunnel name *name*

undo tunnel name

【视图】

L2TP 组视图

【参数】

name：标识隧道本端的名称，取值为字符串，长度为 1～30。

【描述】

tunnel name 命令用来指定隧道本端的名称，**undo tunnel name** 命令用来恢复本端名称为缺省值。

缺省情况下，系统的本端名称为 SecBlade 的名称。

当创建一个 L2TP 组时，本端名称将被初始化成 SecBlade 的名称。

LNS 根据 LAC 的 tunnel 名来选择其本端的 L2TP 组，如果 tunnel 名相同，LNS 将以第一个符合配置的组建立隧道。所以若要建立多条隧道，需要配置不同的 tunnel 名。

相关配置可参考命令 **sysname**。

【举例】

设置隧道本端名称为 itsme。

```
[SecBlade_VPN-l2tp1] tunnel name itsme
```

1.1.24 tunnel password

【命令】

tunnel password { **simple** | **cipher** } *password*

undo tunnel password

【视图】

L2TP 组视图

【参数】

simple：密码以明文方式显示。

cipher：密码以密文方式显示。

password：标识隧道验证时使用的密码，取值为字符串，长度为 1～16。

【描述】

tunnel password 命令用来指定隧道验证时的密码，**undo tunnel password** 命令用来取消隧道验证的密码。

缺省情况下，系统的隧道验证密码为空。

【举例】

设置隧道验证的密码为 yougotit，并且以密文方式显示。

```
[SecBlade_VPN-l2tp1] tunnel password cipher yougotit
```

1.1.25 tunnel timer hello

【命令】

tunnel timer hello *hello-interval*

undo tunnel timer hello

【视图】

L2TP 组视图

【参数】

hello-interval：LAC 或 LNS 在没有报文接收时发送 Hello 报文的时间间隔，取值为整数，单位为秒，范围为 60～1000。

【描述】

tunnel timer hello 命令用来设置隧道中 Hello 报文发送时间间隔，**undo tunnel timer hello** 命令用来恢复隧道中 Hello 报文发送时间间隔为缺省值。

缺省情况下，Hello 报文每隔 60 秒发送一次。

在 LNS 和 LAC 侧，可以分别配置不同的 Hello 报文时间间隔。

【举例】

设置发送 Hello 报文的时间间隔为 99 秒

```
[SecBlade_VPN-l2tp1] tunnel timer hello 99
```

第2章 GRE 配置命令

2.1 GRE 配置命令

2.1.1 debugging tunnel

【命令】

debugging tunnel

undo debugging tunnel

【视图】

用户视图

【参数】

无

【描述】

debugging tunnel 命令用来打开 tunnel 调试信息开关，**undo debugging tunnel** 命令用来关闭 tunnel 调试信息开关。

【举例】

打开 tunnel 调试信息开关。

```
<SecBlade_VPN> debugging tunnel
```

2.1.2 destination

【命令】

destination *ip-addr*

undo destination

【视图】

Tunnel 接口视图

【参数】

ip-addr：标识 Tunnel 对端使用的实际物理接口的 IP 地址。

【描述】

destination 命令用来指定 Tunnel 接口进行封装时对添加的 IP 报头填入的目的端 IP 地址，**undo destination** 命令用来删除设置的目的地址。

缺省情况下，系统不指定隧道的目的地址。

指定的隧道目的地址是接收 GRE 报文的实际物理接口的 IP 地址，该地址必须与对端 Tunnel 接口指定的源地址相同，并且要保证到对端物理接口的路由可达。

不能对两个或两个以上使用同种封装协议的 Tunnel 接口配置完全相同的源地址和目的地址。

相关配置可参考命令 **interface tunnel**，**source**。

【举例】

在 SecBlade_VPN1 的 GigabitEthernet0/0.1 接口（IP 地址是 193.101.1.1）和 SecBlade_VPN2 的 GigabitEthernet0/0.2 接口（IP 地址是 192.100.1.1）间建立 tunnel 连接。

```
[SecBlade_VPN1-Tunnel0] source 193.101.1.1
[SecBlade_VPN1-Tunnel0] destination 192.100.1.1
[SecBlade_VPN2-Tunnel1] source 192.100.1.1
[SecBlade_VPN2-Tunnel1] destination 193.101.1.1
```

2.1.3 display interface tunnel

【命令】

display interface tunnel [*number*]

【视图】

所有视图

【参数】

number：Tunnel 接口的编号，范围为 0～1023。

【描述】

display interface tunnel 命令用来显示 Tunnel 接口的工作状态。

执行 **display interface tunnel** 命令显示指定 Tunnel 接口的源地址、目的地址（收发 GRE 报文的实际物理接口地址）、封装模式、识别关键字及端到端校验等信息。

相关配置可参考命令 **source**，**destination**，**gre key**，**gre checksum**，**tunnel-protocol**。

【举例】

显示当前 Tunnel 通道接口信息。

```
<SecBlade_VPN> display interface tunnel 2
Tunnel2 current state :UP
Line protocol current state :DOWN
Description : Tunnel0 Interface
The Maximum Transmit Unit is 64000
Internet Address is 192.168.2.1/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 192.168.0.1 (GigabitEthernet0/0.1), destination 202.38.16.188
Tunnel keepalive disable
Tunnel protocol/transport GRE/IP, key disabled
Checksumming of packets disabled
    Last 300 seconds input:  0 bytes/sec, 0 packets/sec
    Last 300 seconds output:  0 bytes/sec, 0 packets/sec
    0 packets input,  0 bytes
    0 input error
    0 packets output,  0 bytes
    0 output error
```

表2-1 display interface tunnel 2 显示信息的域描述

域	描述
Tunnel2 current state	Tunnel 接口的当前状态
Line protocol current state	Tunnel 接口协议的当前状态
Description	Tunnel 接口描述信息
The Maximum Transmit Unit	Tunnel 接口的 MTU 值
Internet Address	Tunnel 接口的 IP 地址
Encapsulation	封装 GRE 协议形成隧道
Loopback	是否启动回环测试
Tunnel source	Tunnel 源地址
destination	Tunnel 目的地址
Tunnel keepalive	是否启用 Tunnel Keepalive 功能
Tunnel protocol/transport	Tunnel 封装协议和传输协议
key	Tunnel 接口的识别关键字
Checksumming of packets	Tunnel 端到端校验
Last 300 seconds input	离现在最近的 5 分钟内，每秒输入的字节数和报文数
Last 300 seconds output	离现在最近的 5 分钟内，每秒输出的字节数和报文数

域	描述
packets input, bytes	总计输入的报文数和字节数
packets output, bytes	总计输出的报文数和字节数
input error	在所有输入的报文中，出现错误的报文数
output error	在所有输出的报文中，出现错误的报文数

2.1.4 gre checksum

【命令】

gre checksum

undo gre checksum

【视图】

Tunnel 接口视图

【参数】

无

【描述】

gre checksum 命令用来设置隧道两端进行端到端校验，从而验证报文的正确性，并丢掉验证不通过的报文，**undo gre checksum** 命令用来取消校验。

缺省情况下，禁止 Tunnel 两端进行端到端校验。

隧道两端可以根据实际应用需要，配置校验和或禁止校验和。如果本端配置了校验和而对端没有配置，则本端将不会对接收到的报文进行校验和检查，但对发送的报文计算校验和；相反，如果本端没有配置校验和而对端已配置，则本端将对从对端发来的报文进行校验和检查，但对发送的报文不计算校验和。

相关配置可参考命令 **interface tunnel**。

【举例】

SecBlade_VPN1 和 SecBlade_VPN2 接口之间建立隧道，在隧道两端设置校验。

```
[SecBlade_VPN1-Tunnel3] gre checksum
[SecBlade_VPN2-Tunnel2] gre checksum
```

2.1.5 gre key

【命令】

gre key *key-number*

undo gre key

【视图】

Tunnel 接口视图

【参数】

key-number：标识隧道两端的识别关键字，取值为整数，范围为 0～4294967295。

【描述】

gre key 命令用来设置 Tunnel 接口的识别关键字，通过这种弱安全机制防止错误识别、接收其它地方来的报文，**undo gre key** 命令用来取消当前配置。

缺省情况下，系统不设置隧道的识别关键字。

如果在隧道两端设置了 *key-number*，则要求在一条隧道的两端必须指定相同的 *key-number*；或隧道两端都不设置 *key-number*。

相关配置可参考命令 **interface tunnel**。

【举例】

SecBlade_VPN1 和 SecBlade_VPN2 之间建立隧道，设置隧道的识别关键字。

```
[SecBlade_VPN1-Tunnel3] gre key 123
[SecBlade_VPN2-Tunnel2] gre key 123
```

2.1.6 interface tunnel

【命令】

interface tunnel *number*

undo interface tunnel *number*

【视图】

系统视图

【参数】

number：Tunnel 接口号，范围 0～1023。

【描述】

interface tunnel 命令用来创建一个 Tunnel 接口，并进入该 Tunnel 接口视图，**undo interface tunnel** 命令用来删除指定的 Tunnel 接口。

缺省情况下，系统无 Tunnel 接口。

执行 **interface tunnel** 命令进入指定隧道的接口视图。如果 Tunnel 接口尚未创建，则先创建再进入接口视图。

Tunnel 接口号只具有本地意义，隧道两端可以使用相同或不同的接口号。

相关配置可参考命令 **source**，**destination**，**gre key**，**gre checksum**，**tunnel-protocol**。

【举例】

创建接口 Tunnel3。

```
[SecBlade_VPN] interface tunnel 3
```

2.1.7 keepalive

【命令】

keepalive [*seconds* [*times*]]

undo keepalive

【视图】

Tunnel 接口视图

【参数】

seconds：keepalive 报文发送周期，缺省为 10 秒，取值范围为 1～32767。

times：keepalive 报文的最大传送次数，缺省为 3 次，取值范围为 1～255。

【描述】

keepalive 命令用来使能 GRE 的 keepalive 功能，并配置 keepalive 报文发送周期及最大发送次数，**undo keepalive** 命令用来关闭 keepalive 功能。

缺省情况下，不启用 GRE 的 keepalive。当配置了该命令后，SecBlade 会从 tunnel 口定期发送 GRE 的 keepalive 报文。如果超时时间内对端设备没有回应，则本端 SecBlade 重新发送 keepalive 报文。如果超过最大传送次数后仍然没有接受到对端的回应，则本端 tunnel 口的协议状态将变为 down。

相关配置可参考命令 **interface tunnel**。

【举例】

配置 GRE keepalive 的报文发送周期 20s，最大传送次数为 5 次。

```
[SecBlade_VPN-Tunnel0] keepalive 20 5
```

2.1.8 source

【命令】

source { *ip-addr* | *interface-type interface-num* }

undo source

【视图】

Tunnel 接口视图

【参数】

ip-addr：使用 A.B.C.D 的地址形式来指定发出 GRE 报文的实际接口的 IP 地址；

interface-type interface-num：接口类型及接口号。

【描述】

source 命令用来指定 Tunnel 接口进行封装时对添加的 IP 报头填入的源端 IP 地址，**undo source** 命令用来删除设置的源地址。

缺省情况下，系统不指定隧道的源地址。

指定的隧道源地址是发出 GRE 报文的实际接口地址，该地址应和隧道对端指定的目的地址一致。

不能对两个或两个以上使用同种封装协议的 Tunnel 接口配置完全相同的源地址和目的地址。

当前该配置不支持插卡热插拔事件，即拔掉插卡后，相应的配置仍然存在，需要手工删除。

相关配置可参考命令 **interface tunnel**，**destination**。

【举例】

在 SecBlade_VPN1 上配置 Tunnel5 接口，此接口封装的报文实际出口为 GigabitEthernet0/0.1 接口（接口 IP 地址为 192.100.1.1）。

```
[SecBlade_VPN1-Tunnel5] source 192.100.1.1
```

或使用接口形式：

```
[SecBlade_VPN1-Tunnel5] source GigabitEthernet0/0.1
```

2.1.9 tunnel-protocol gre

【命令】

tunnel-protocol gre

【视图】

Tunnel 接口视图

【参数】

无

【描述】

tunnel-protocol gre 命令用来设置 Tunnel 接口为 GRE 封装模式。

缺省情况下，是 GRE 模式。在 GRE 模式下，用户只能看见和执行 GRE 有关的配置命令；在其他模式下，用户才能看见和执行相应的配置命令。

相关配置可参考命令 **interface tunnel**。

【举例】

SecBlade_VPN1 和 SecBlade_VPN2 之间建立隧道，配置封装协议为 GRE，传输协议为 IP。

```
[SecBlade_VPN1-Tunnel3] tunnel-protocol gre
[SecBlade_VPN2-Tunnel2] tunnel-protocol gre
```

第3章 IPSec 配置命令

3.1 IPSec 配置命令

3.1.1 ah authentication-algorithm

【命令】

ah authentication-algorithm { **md5** | **sha1** }

undo ah authentication-algorithm

【视图】

IPSec 提议（ipsec proposal）视图

【参数】

md5：设置采用 MD5 认证算法。

sha1：设置采用 SHA-1 认证算法。

【描述】

命令 **ah authentication-algorithm** 用来设置 IPSec 安全提议中 AH（Authentication Header）协议采用的认证算法，命令 **undo ah authentication-algorithm** 用来恢复缺省的认证算法。

缺省情况下，在 IPSec 安全提议中 AH 协议采用 MD5 认证算法。

AH 协议没有加密的功能，只对报文进行认证。

MD5 算法使用 128 位的消息摘要（message－digest），SHA-1 算法使用 160 位的消息摘要（message－digest）。MD5 算法的计算速度比 SHA-1 算法快，而 SHA-1 算法的安全强度比 MD5 算法高。

在安全隧道的两端设置安全策略时，所引用的提议中，AH 协议必须设置成采用同样的认证算法。

只有先使用 **transform** 命令选择了 ah 或 ah-esp 安全协议后，才能够配置 AH 认证算法。

相关配置可参考命令 **ipsec proposal**，**proposal**，**sa spi**，**transform**。

【举例】

在配置安全提议 prop1 时，设定 AH 协议采用 SHA-1 算法。

```
[SecBlade_VPN] ipsec proposal prop1
```

```
[SecBlade_VPN-ipsec-proposal-prop1] transform ah
[SecBlade_VPN-ipsec-proposal-prop1] ah authentication-algorithm sha1
```

3.1.2 debugging ike dpd

【命令】

debugging ike dpd

undo debugging ike dpd

【视图】

用户视图

【参数】

无

【描述】

debugging ike dpd 命令打开 IKE DPD 调试开关，**undo debugging ike dpd** 命令用来关闭 IKE DPD 调试开关。

【举例】

打开 IKE DPD 调试开关。

```
<SecBlade_VPN> debugging ike dpd
```

3.1.3 debugging ipsec

【命令】

debugging ipsec { **all** | **sa** | **misc** | **packet** [**policy** *policy-name* [*seq-number*] | **parameters** *ip-address protocol spi-number*] }

undo debugging ipsec { **all** | **sa** | **misc** | **packet** [**policy** *policy-name* [*seq-number*] | **parameters** *ip-address protocol spi-number*] }

【视图】

用户视图

【参数】

all：打开 ipsec 所有的调试开关。

sa：显示安全联盟的调试信息。

packet：显示 IPSec 数据报文的调试信息。

policy *policy-name*：显示安全策略名为 *policy-name* 的 IPSec 调试信息。

seq-number：显示安全策略顺序号为 *seq-number* 的 IPSec 调试信息。

parameters：显示由目的地址 *ip-address*、*protocol*（**ah** 或 **esp**）、SPI（*spi-number*）所唯一确定的一个安全联盟的调试信息。

misc：显示 IPSec 其他调试信息。

【描述】

debugging ipsec 命令用来打开 IPSec 调试开关，**undo debugging ipsec** 命令用来关闭 IPSec 调试开关。

缺省情况下，关闭 IPSec 调试开关。

【举例】

打开 IPSec 的安全联盟的调试开关。

```
<SecBlade_VPN> debugging ipsec sa
```

3.1.4 display ike dpd

【命令】

display ike dpd [*dpd-name*]

【视图】

所有视图

【参数】

dpd-name：DPD 结构名。

【描述】

display ike dpd 命令用来显示配置的 DPD 结构信息。

【举例】

显示配置的 DPD 结构信息。

```
[SecBlade_VPN] display ike dpd
---------------------------
 IKE dpd: aaa
   references: 0
   interval-time: 10
   time_out: 5
---------------------------
---------------------------
 IKE dpd: xhy
   references: 1
   interval-time: 10
```

```
time_out: 5
```

表3-1 display ike dpd 命令显示信息描述表

字段	描述
IKE dpd	IKE DPD 结构名
references	引用计数
interval-time	触发 DPD 查询的时间间隔
time_out	单次 DPD 查询的超时间隔

3.1.5 display ipsec policy

【命令】

display ipsec policy [**brief** | **name** *policy-name* [*seq-number*]]

【视图】

所有视图

【参数】

brief：表示显示所有安全策略的简要信息。

name：表示显示名字为 *policy-name*，顺序号为 *seq-number* 的安全策略的信息。

policy-name：指定安全策略的名字。

seq-number：指定安全策略的顺序号。

如果不指定任何参数，则表示要显示所有安全策略的详细信息。如果指定了 *name policy-name*，而没有指定 *seq-number*，则表示要显示指定的安全策略组的信息。

【描述】

display ipsec policy 命令用来显示安全策略的信息。

brief 参数表示将显示所有安全策略的简要信息，显示格式为简要格式（参见下面的举例）。利用 **brief** 参数可以快速查看所有的安全策略。简要信息包括：安全策略名及顺序号、协商方式、访问控制列表号、提议、本端地址、对端地址。

其它子命令均显示安全策略的详细信息，显示格式为详细格式（参见下面的举例）。

相关配置可参考命令 **ipsec policy**（系统视图）。

【举例】

显示所有安全策略的简要信息。

```
[SecBlade_VPN] display ipsec policy brief
IPsec-Policy-Name     Mode    acl          Local-Address  Remote-Address
```

```
-------------------------------------------------------------------------
policy1-1             isakmp  3000                        172.16.2.1
policy2-1             manual  3001       172.16.2.1       172.16.2.2
```

表3-2 IPSec 安全策略简要信息描述表

域名	描述
IPsec-Policy-Name	安全策略组的名字和安全策略顺序号（其中策略组名和策略顺序号之间用“-”隔开）
Mode	安全策略采用的协商方式
acl	安全策略引用的访问控制列表
Local Address	本端的 IP 地址
Remote Address	对端的 IP 地址
ike-peer name	在 ISAKMP 协商模式下，安全策略所引用的 IKE 对等体的名称（manual 模式下无此信息显示）

显示所有安全策略的信息。

```
[SecBlade_VPN] display ipsec policy
==========================================
IPsec Policy Group: "policy1"
Using interface: {GigabitEthernet0/0.1}
==========================================

  ----------------------------
  IPsec policy name: "policy1"
  sequence number: 1
  mode: isakmp
  ----------------------------
    security data flow : 3000
    selector mode: standard
    ike-peer name:  ikepeer
    perfect forward secrecy: DH group 1
    proposal name:  proposal1
    IPsec sa local duration(time based): 3600 seconds
    IPsec sa local duration(traffic based): 1843200 kilobytes

==========================================
IPsec Policy Group: "policy2"
Using interface: {GigabitEthernet0/0.2}
==========================================
```

```
-----------------------------
IPsec policy name: "policy2"
sequence number: 1
mode: manual
-----------------------------
  security data flow : 3001
  tunnel local  address: 172.16.2.1
  tunnel remote address: 172.16.2.2
  proposal name: proposal2
  inbound AH setting:
    AH spi:
    AH string-key:
    AH authentication hex key:
  inbound ESP setting:
    ESP spi:
    ESP string-key:
    ESP encryption hex key:
    ESP authentication hex key:
  outbound AH setting:
    AH spi:
    AH string-key:
    AH authentication hex key:
  outbound ESP setting:
    ESP spi:
    ESP string-key:
    ESP encryption hex key:
    ESP authentication hex key: :
```

表3-3 PSec 安全策略详细信息显示描述表

域名	描述
IPsec policy name	安全策略的名称
sequence number	安全策略的序号
mode	安全策略的协商方式：isakmp 或 manual
security data flow	安全策略引用的访问控制列表
selector mode	表明数据流的保护方式
ike-peer name	引用的 IKE 对等体的名称
perfect forward secrecy	完善的前向安全性（PFS）的配置信息
proposal name	安全策略引用的提议的名字
IPsec sa local duration(time based)	IPSec 安全联盟的生存周期（基于时间的）

域名	描述
IPsec sa local duration(traffic based)	IPSec 安全联盟的生存周期（基于流量的）
tunnel local address	隧道的本端 IP 地址
tunnel remote address	隧道的对端 IP 地址
inbound AH setting	入方向的 AH 协议的设置
inbound ESP setting	入方向的 ESP 协议的设置
outbound AH setting	出方向的 AH 协议的设置
outbound ESP setting	出方向的 ESP 协议的设置

3.1.6 display ipsec policy-template

【命令】

display ipsec policy-template [**brief** | **name** *template-name* [*seq-number*]]

【视图】

所有视图

【参数】

brief：表示显示所有安全策略模板的简要信息。

name：表示显示名字为 *template-name*，顺序号为 *seq-number* 的安全策略模板的信息。

template-name：指定安全策略模板的名字。

seq-number：指定安全策略模板的顺序号。

如果不指定任何参数，则表示要显示所有安全策略模板的详细信息。如果指定了 **name** *template-name*，而没有指定 *seq-number*，则表示要显示指定的安全策略模板组的信息。

【描述】

命令 **display ipsec policy-template** 用来显示安全策略模板的信息。

brief 子命令表示将显示所有安全策略模板的简要信息，显示格式为简要格式（参见下面的举例）。利用 **brief** 子命令，可以快速查看所有的安全策略模板。简要信息包括：安全策略模板名及顺序号、访问控制列表号、对端地址。

其它子命令均显示安全策略模板的详细信息。

相关配置可参考命令 **ipsec policy-template**（系统视图）。

【举例】

显示所有安全策略模板的简要信息。

```
[SecBlade_VPN] display ipsec policy-template brief
Policy-template-Name     acl            Remote-Address
-----------------------------------------------------
test-tplt300             2200
```

表3-4 IPSec 安全策略模板简要信息描述表

域名	描述
Policy-template-Name	安全策略模板的名字和顺序号
acl	安全策略模板引用的访问控制列表
Remote Address	对端的 IP 地址

3.1.7 display ipsec proposal

【命令】

display ipsec proposal [*proposal-name*]

【视图】

所有视图

【参数】

proposal-name：指定提议的名字。

【描述】

命令 **display ipsec proposal** 显示提议的配置信息，如果没有指定提议的名字，则显示所有的提议的信息。

相关配置可参考命令 **ipsec proposal**，**display ipsec sa**，**display ipsec policy**。

【举例】

显示所有的提议。

```
[SecBlade_VPN] display ipsec proposal
IPsec proposal name: prop2
     encapsulation mode: tunnel
     transform: ah-new
 ah protocol: authentication sha1-hmac-96
IPsec proposal name: prop1
     encapsulation mode: transport
     transform: esp-new
```

```
esp protocol: authentication md5-hmac-96, encryption des
```

表3-5 IPSec 安全提议信息显示描述表

域名	描述
IPsec proposal name	提议的名字
encapsulation mode	提议采用的模式，包括两种：传输（transport）和隧道（tunnel）模式
transform	提议采用的安全协议，包括两种：AH 协议和 ESP 协议
ah protocol	AH 协议采用的认证算法
esp protocol	ESP 协议采用的认证算法和加密算法

3.1.8 display ipsec sa

【命令】

display ipsec sa [**brief** | **remote** *ip-address* | **policy** *policy-name* [*seq-number*] | **duration**]

【视图】

所有视图

【参数】

brief：表示显示所有的安全联盟的简要信息。

remote *ip-address*：表示显示对端地址为 *ip-address* 的安全联盟的信息。

policy：表示显示由指定安全策略创建的安全联盟的信息。

policy-name：指定安全策略的名称。

seq-number：指定安全策略的顺序号。

duration：表示显示全局的安全联盟生存周期。

【描述】

display ipsec sa 命令用来显示安全联盟的相关信息。

使用 **brief** 参数显示所有的安全联盟的简要信息，显示格式为简要格式（参见下面的举例），简要信息包括：源地址、目的地址、安全参数索引、协议、算法。其中，算法的显示以“E:”开头的表示加密算法，以“A:”开头的表示认证算法。利用 **brief** 参数可以快速查看所有已经建立的安全联盟。

使用 **remote** 和 **policy** 参数均显示安全联盟的详细信息，显示格式是先显示安全策略的部分信息，再显示此安全策略中的安全联盟的详细信息。

使用 **duration** 参数显示全局的安全联盟的生存时间，包括“基于时间”和“基于流量”两种类型。参见下面的举例。

当未指定任何参数时，显示所有的安全联盟的信息。

相关配置可参考命令 **reset ipsec sa**，**ipsec sa global-duration**，**display ipsec policy**。

【举例】

下面是 **display ipsec sa brief** 命令的输出：

```
[SecBlade_VPN] display ipsec sa brief
Total IPSec SAs: 2
Src Address  Dst Address  SPI    Protocol     Algorithm
-------------------------------------------------------
10.1.1.1     10.1.1.2     300    ESP        E:DES; A:HMAC-MD5-96
10.1.1.2     10.1.1.1     400    ESP        E:DES; A:HMAC-MD5-96
```

表3-6 IPSec 安全联盟简要信息显示描述表

域名	描述
Src Address	本端的 IP 地址
Dst Address	对端的 IP 地址
SPI	安全参数索引
Protocol	IPSec 采用的安全协议
Algorithm	安全协议采用的认证算法和加密算法，其中，以“E:”开头表示加密算法；以“A:”开头表示认证算法

显示安全联盟的全局生存时间。

```
[SecBlade_VPN] display ipsec sa duration
     Ipsec sa global duration（traffic based）: 1843200 kilobytes
     Ipsec sa global duration（time based）: 3600 seconds
```

下面是 **display ipsec sa** 命令的输出：

```
[SecBlade_VPN] display ipsec sa
==============================
Interface: GigabitEthernet0/0.1
    path MTU: 1500
==============================

  ----------------------------
  IPsec policy name: "1"
  sequence number: 1
  mode: isakmp
```

```
-----------------------------
  Created by: "Encrypt-card"
  connection id: 5
  encapsulation mode: tunnel
  perfect forward secrecy: None
  tunnel:
      local  address: 2.1.1.1
      remote address: 2.1.1.3
  flow:    (8 times matched)
      sour addr: 192.168.1.0/255.255.255.0  port: 0  protocol: IP
      dest addr: 10.1.1.0/255.255.255.0  port: 0  protocol: IP

  [inbound AH SAs]
    spi: 1369228154 (0x519cc37a)
    proposal: AH-SHA1HMAC96
    sa remaining key duration (bytes/sec): 1887436256/3594
    max received sequence-number: 4
    udp encapsulation used for nat traversal: N

  [inbound ESP SAs]
    spi: 2673492781 (0x9f5a432d)
    proposal: ESP-ENCRYPT-3DES ESP-AUTH-MD5
    sa remaining key duration (bytes/sec): 1887436448/3594
    max received sequence-number: 4
    udp encapsulation used for nat traversal: N

  [outbound ESP SAs]
    spi: 1109683945 (0x42246ee9)
    proposal: ESP-ENCRYPT-3DES ESP-AUTH-MD5
    sa remaining key duration (bytes/sec): 1887436256/3594
    max sent sequence-number: 5
    udp encapsulation used for nat traversal: N

  [outbound AH SAs]
    spi: 3969283528 (0xec9675c8)
    proposal: AH-SHA1HMAC96
    sa remaining key duration (bytes/sec): 1887436160/3594
    max sent sequence-number: 5
    udp encapsulation used for nat traversal: N
```

表3-7 IPSec 安全联盟详细信息显示描述表

域名	描述
Interface	应用了安全策略的接口
path MTU	从该接口发送出去的最大 IP 数据报文长度
IPsec policy	采用的安全策略，包括策略名、顺序号和协商方式
Created by	"Encrypt-card"表示使用加密卡进行加密；"Host"表示使用软件加密
connection id	安全通道标识符
encapsulation mode	IPSec 采用的模式，有两种：传输（transport）和隧道（tunnel）模式
perfect forward secrecy	是否使用完善的前向安全（Perfect Forward Secrecy）特性
tunnel local	本端的 IP 地址
tunnel remote	对端的 IP 地址
sour addr	安全策略所引用的 ACL 的源地址
dest addr	安全策略所引用的 ACL 的目的地址
inbound	输入端 SA 的信息
transform	安全策略所引用的提议
sa remaining key duration	安全联盟剩余的存活时间
max received sequence-number	接收的报文最大序列号（安全协议提供的防重放功能）
udp encapsulation used for nat traversal	是否使用 IKE NAT 穿越
outbound	输出端 SA 的信息
max sent sequence-number	发送的报文最大序列号（安全协议提供的防重放功能）

3.1.9 display ipsec statistics

【命令】

display ipsec statistics

【视图】

所有视图

【参数】

无

【描述】

显示 IPSec 处理报文的统计信息。包括输入输出的安全报文数、字节数、被丢弃的报文数以及被丢弃的报文的详细说明。

相关配置可参考命令 **reset ipsec statistics**。

【举例】

显示 IPSec 的报文统计信息。

```
[SecBlade_VPN] display ipsec statistics
the security packet statistics:
    input/output security packets: 5124/8231
    input/output security bytes: 52348/64356
    input/output dropped security packets: 0/0
    dropped security packet detail:
      no enough memory: 0
      can't find SA: 0
      queue is full: 0
      authentication is failed: 0
      wrong length: 0
      replay packet: 0
      too long packet: 0
      wrong SA: 0
      other error packet: 0
```

表3-8 IPSec 处理报文的统计信息显示描述表

域名	描述
input/output security packets	受安全保护的输入/输出数据包
input/output security bytes	受安全保护的输入/输出字节数
input/output dropped security packets	被丢弃了的受安全保护的输入/输出数据包

3.1.10 display ipsec tunnel

【命令】

display ipsec tunnel

【视图】

所有视图

【参数】

无

【描述】

display ipsec tunnel 命令用来显示 IPSec 的隧道信息。

【举例】

显示 IPSec 的隧道信息。

```
<H3C> display ipsec tunnel
    -----------------------------------------------
    Connection ID : 5
    Perfect forward secrecy: None
    SA's SPI :
        Inbound :  1369228154 (0x519cc37a) [AH]
                   2673492781 (0x9f5a432d) [ESP]
        Outbound : 1109683945 (0x42246ee9) [ESP]
                   3969283528 (0xec9675c8) [AH]
    Tunnel :
        Local Address:  2.1.1.1  Remote Address : 2.1.1.3
    Flow :     (8 times matched)
        Sour Addr : 0.0.0.0/0.0.0.0  Port: 0  Protocol : IP
        Dest Addr : 0.0.0.0/0.0.0.0  Port: 0  Protocol : IP
```

3.1.11 dpd

【命令】

dpd *dpd-name*

undo dpd

【视图】

ike-peer 视图

【参数】

dpd-name：DPD 结构名。

【描述】

dpd 命令用来为 IKE Peer 指定 DPD 结构，**undo dpd** 用来取消 IKE Peer 的 DPD 结构。

指定的 DPD 结构应预先建立好，否则将返回错误信息。执行 **dpd** 命令时，该 DPD 结构的引用计数器加 1；执行 **undo dpd** 命令时，该 DPD 结构的引用计数器减 1。

相关配置可参考命令 **ike dpd**。

【举例】

指定 IKE Peer1 的 DPD 结构为 aaa

```
[SecBlade_VPN-ike-peer-peer1] dpd aaa
```

取消 IKE Peer1 的 DPD 结构。

```
[SecBlade_VPN-ike-peer-peer1] undo dpd
```

3.1.12 encapsulation-mode

【命令】

encapsulation-mode { **transport** | **tunnel** }

undo encapsulation-mode

【视图】

安全提议视图

【参数】

transport：设置 IP 报文的封装形式采用传输模式。

tunnel：设置 IP 报文的封装形式采用隧道模式。

【描述】

命令 **encapsulation-mode** 用来设置安全协议对 IP 报文的封装形式，有传输模式（**transport**）和隧道模式（**tunnel**）两种，命令 **undo encapsulation-mode** 用来恢复到缺省的报文封装形式。

缺省情况使用 **tunnel**，即隧道模式。

使用 IPSec 对 IP 报文进行加密或认证有两种封装形式，分别是传输模式和隧道模式。对于传输模式，不增加新 IP 头，原始报文的源地址和目的地址就是安全隧道的端点；对于隧道模式，IPSec 对整个 IP 报文进行保护，并在原 IP 报文的前面增加一个新的 IP 头，新 IP 头的源地址和目的地址分别是安全隧道的两个端点的 IP 地址。

通常，在两个 SecBlade、路由器或防火墙之间，总是使用隧道模式。在一端被加密的报文，只有另一端能够解密。因此，必须对 IP 报文进行隧道封装，即增加一个新的 IP 头，进行隧道封装后的 IP 报文被发送到另一端，才能够被解密。

传输模式适合两台主机之间的通讯，或者是一台主机和一个 SecBlade 或路由器之间的通讯。在传输模式下，对报文进行加密和解密的两台设备本身必须是报文的原始发送者和最终接收者。在两个 SecBlade、路由器或防火墙之间的数据流量，绝大部分都不是其本身的通讯量，因此，不使用传输模式。

在安全隧道的两端设置的安全策略所引用的提议必须设置成采用同样的报文封装形式。

相关配置可参考命令 **ah authentication-algorithm**，**ipsec proposal**，**esp encryption-algorithm**，**esp authentication-algorithm**，**proposal**，**transform**。

【举例】

设置名为 prop2 的提议采用传输模式对 IP 报文进行封装。

```
[SecBlade_VPN] ipsec proposal prop2
[SecBlade_VPN-ipsec-proposal-prop2] encapsulation-mode transport
```

3.1.13 esp authentication-algorithm

【命令】

esp authentication-algorithm { **md5** | **sha1** }

undo esp authentication-algorithm

【视图】

安全提议视图

【参数】

md5：采用 MD5 认证算法，密钥长度 128 位。

sha1：采用 SHA-1 认证算法，密钥长度 160 位。

【描述】

命令 **esp authentication-algorithm** 用来设置 ESP 协议采用的认证算法，命令 **undo esp authentication-algorithm** 用来设置 ESP 协议不对报文进行认证。

缺省情况下，使用 **md5**，即 MD5 认证算法。

MD5 算法的计算速度比 SHA-1 算法快，而 SHA-1 算法的安全强度比 MD5 算法高。

ESP 协议允许对报文同时进行加密和认证，或只加密，或只认证。

ESP 协议采用的加密算法和认证算法不能同时设置为空。

注意：**undo esp authentication-algorithm** 命令不是恢复认证算法为缺省算法，而是设置认证算法为空，即不认证。当加密算法不为空时，**undo esp authentication-algorithm** 命令才起作用。

在安全隧道的两端设置的安全策略所引用的提议必须设置成采用同样的认证算法。

相关配置可参考命令 **ipsec proposal**，**esp encryption-algorithm**，**proposal**，**transform**。

【举例】

设定提议 prop1 采用 ESP 协议并使用 SHA-1 认证算法。

```
[SecBlade_VPN] ipsec proposal prop1
```

```
[SecBlade_VPN-ipsec-proposal-prop1] transform esp
[SecBlade_VPN-ipsec-proposal-prop1] esp authentication-algorithm sha1
```

3.1.14 esp encryption-algorithm

【命令】

esp encryption-algorithm { **3des** | **des** | **aes** }

undo esp encryption-algorithm

【视图】

安全提议视图

【参数】

des：即数据加密标准 DES（Data Encryption Standard），是国际通用的加密算法，密钥长度 56 位。

3des：即 3DES（Triple DES），也是一种国际通用的加密算法，密钥长度 168 位。

aes：即 AES（Advanced Encryption Standard），是 IETF 标准要求的一种加密算法，CMW 实现的密钥长度是 128 位、192 位和 256 位。

【描述】

命令 **esp encryption-algorithm** 用来设置 ESP 协议采用的加密算法，命令 **undo esp encryption-algorithm** 用来设置 ESP 协议不对报文进行加密。

缺省情况使用 **des**，即 DES 加密算法。

对于保密及安全性要求非常高的地方，采用 3DES 算法可以满足需要，但 3DES 加密速度比较慢；对于普通的安全要求，DES 算法则可以满足需要。

ESP 协议允许对报文同时进行加密和认证，或只加密，或只认证。

ESP 协议采用的加密算法和认证算法不能同时设置为空。当认证算法不为空时，**undo esp encryption-algorithm** 命令才起作用。

相关配置可参考命令 **ipsec proposal**，**esp authentication-algorithm**，**proposal**，**transform**。

【举例】

设定提议 prop1 采用 ESP 协议并使用 3DES 加密算法。

```
[SecBlade_VPN] ipsec proposal prop1
[SecBlade_VPN-ipsec-proposal-prop1] transform esp
[SecBlade_VPN-ipsec-proposal-prop1] esp encryption-algorithm 3des
```

3.1.15 ike dpd

【命令】

ike dpd *dpd-name*

undo ike dpd *dpd-name*

【视图】

系统视图

【参数】

dpd-name：DPD（Dead Peer Detection）结构名。

【描述】

ike dpd 命令用来创建 DPD 结构并进入 DPD 结构视图，**undo ike dpd** 命令用来删除一个 DPD 结构。

如 DPD 结构已经被 IKE Peer 引用，则不能删除。

相关配置可参考命令 **dpd**。

【举例】

创建一个名字为 aaa 的 DPD 结构。

```
[SecBlade_VPN] ike dpd aaa
```

删除一个名字为 aaa 的 DPD 结构。

```
[SecBlade_VPN] undo ike dpd aaa
```

3.1.16 interval-time

【命令】

interval-time *seconds*

undo interval-time

【视图】

DPD 结构视图

【参数】

seconds：触发 DPD 查询的时间间隔，取值范围 1～300 秒。缺省情况下，*seconds* 为 10 秒。

【描述】

interval-time 命令用来配置触发 DPD 查询的时间间隔，**undo interval-time** 命令用来恢复触发 DPD 查询的时间间隔为缺省值。

【举例】

设置 interval-time 为 20 秒。

```
[SecBlade_VPN-ike-dpd-aaa] interval-time 20
```

重置 interval-time 为 10 秒。

```
[SecBlade_VPN-ike-dpd-aaa]undo interval-time
```

3.1.17 ipsec policy

【命令】

ipsec policy *policy-name*

undo ipsec policy [*policy-name*]

【视图】

接口视图

【参数】

policy-name：指定应用在接口上的安全策略组的名字。在系统视图下，必须已经配置了名字为 *policy-name* 的安全策略组。

【描述】

命令 **ipsec policy** *policy-name* 用来在接口上应用名字为 *policy-name* 的安全策略组，命令 **undo ipsec policy** 用来从接口上取消应用的所有的或特定的安全策略组，使此接口不再具有 IPSec 的安全保护功能。

在一个接口上，只能应用一个安全策略组。如果要在接口上应用另一个安全策略组，必须先从接口上取消应用的安全策略组，再在接口上应用另外一个安全策略组。一个安全策略组可应用到多个接口上。

当从一个接口发送报文时，将按照顺序号从小到大的顺序查找安全策略组中每一条安全策略。如果报文匹配了一条安全策略引用的访问控制列表，则使用这条安全策略对报文进行处理；如果报文没有匹配安全策略引用的访问控制列表，则继续查找下一条安全策略；如果报文对所有安全策略引用的访问控制列表都不匹配，则报文直接被发送（IPSec 不对报文加以保护）。

想要实现在接口上不发送任何不加密的报文，需要结合防火墙和 IPSec 一起使用，用防火墙将不需要加密的报文全部丢弃。

当在所有接口上都删除了安全策略后，才会删除所有的 IKE SA，否则需要手工删除或等到 SA 超时。

相关配置可参考命令 **ipsec policy**（系统视图）。

【举例】

在 GigabitEthernet0/0.1 接口上应用名为 pg1 的安全策略组。

```
[SecBlade_VPN] interface GigabitEthernet0/0.1
[SecBlade_VPN- GigabitEthernet0/0.1] ipsec policy pg1
```

3.1.18 ipsec policy

【命令】

ipsec policy *policy-name seq-number* [**manual** | **isakmp** [**template** *template-name*]]

undo ipsec policy *policy-name* [*seq-number*]

【视图】

系统视图

【参数】

policy-name：安全策略的名字。命名规则为：长度为 1～15 个字符，不区分大小写，字符可以是英文字母或者数字，不能带减号“-”。

seq-number：安全策略的顺序号，取值范围 1～10000，值越小优先级越高。

manual：指定用手工方式建立安全联盟。

isakmp：指定通过 IKE 协商建立安全联盟。

template：指定采用策略模板动态创建安全联盟。

template-name：指定被引用的 template 的名字。此 *policy-name* 将引用 *template-name*。*template-name* 是一个策略模板。在此之前，名为 *template-name* 的安全策略模板必须已经创建。

【描述】

在系统视图下，命令 **ipsec policy** 用来创建或修改一条安全策略，并进入安全策略（ipsec policy）视图，命令 **undo ipsec policy** 用来删除安全策略。使用 **undo ipsec policy** *policy-name* 命令，用来删除名字为 *policy-name* 的安全策略组；使用 **undo ipsec policy** *policy-name seq-number* 命令，用来删除名字为 *policy-name*，顺序号为 *seq-number* 的一条安全策略。当安全策略被应用到接口时，则不允许将其删除。

缺省情况下，没有安全策略存在。

使用此命令创建安全策略时，必须指定协商方式；在安全策略创建后，不能修改协商方式，如果要修改安全策略的协商方式，只能先删除这条安全策略，在重新创建安全策略时，指定新的协商方式。

具有相同名字的安全策略一起组成一个安全策略组。由名字和顺序号一起确定一条唯一的安全策略。在一个安全策略组中最大可以设置 500 条安全策略。在一个安全策略组中，顺序号 *seq-number* 越小的安全策略，优先级越高。在一个接口上应用一个安全策略组，实际上是同时应用了安全策略组中所有的安全策略，从而能够对不同的数据流采用不同的安全联盟进行保护。

ipsec policy *policy-name seq-number* **isakmp template** *template-name* 命令创建一个安全策略，该策略由 IKE 协商建立安全联盟，而策略的参数根据 *template-name* 指定的策略模板来确定。在配置此命令前，必须已经使用命令 **ipsec policy-template** 创建策略模板。在协商过程中进行策略匹配时，策略模板中定义的参数必须相符，而策略模板中没有定义的参数由发起方来决定，响应方接受发起方的建议。策略模板中必须定义的参数是提议（proposal），其它参数为可选配置。

注意：IKE 不会用带有 **template** 参数的策略去发起协商。但可以用带有 **template** 参数的策略响应对方发起的协商。

相关配置可参考命令 **ipsec policy**（接口视图），**security acl**，**tunnel local**，**tunnel remote**，**sa duration**，**proposal**，**display ipsec policy**，**ipsec policy-template**，**ike-peer**。

【举例】

设置名字为 policy1，顺序号为 100，采用 ISAKMP 方式协商的安全策略。

```
[SecBlade_VPN] ipsec policy policy1 100 isakmp
[SecBlade_VPN-ipsec-policy-isakmp-policy1-100]
```

3.1.19 ipsec policy-template

【命令】

ipsec policy-template *policy-template-name seq-number*

undo ipsec policy-template *policy-template-name* [*seq-number*]

【视图】

系统视图

【参数】

template-name：为安全策略模板的名字。命名规则为：长度为 1～15 个字符，不区分大小写，字符可以是英文字母或者数字，不能带减号“-”。

seq-number：为此安全策略模板的顺序号，取值范围 1～10000。在一个安全策略模板中，顺序号越小的安全策略，优先级越高。

【描述】

命令 **ipsec policy-template** 用来创建或修改一个安全策略模板，并进入安全策略模板（ipsec policy template）视图，命令 **undo ipsec policy-template** 用来删除一个安全策略模板组或者安全策略模板组中的一个安全策略模板。使用 **undo ipsec policy-template** *template-name* 命令删除名字为 *template-name* 的安全策略模板组；使用 **undo ipsec policy-template** *template-name seq-number* 命令删除名字为 *template-name*、序号为 *seq-number* 的一个安全策略模板。

缺省情况下，没有安全策略模板存在。

创建一个策略模板以后，在使用 **ipsec policy** *policy-name seq-number* **isakmp template** *template-name* 命令创建一个安全策略时，通过 *template-name* 参数引用此模板。

IPsec 安全策略模板的参数与 IPSec ISAKMP 协商方式的安全策略的参数是一样的，包括所引用的 IPSec proposal、保护的数据流、PFS 特性、生存周期、隧道对端地址。但需要注意的是，proposal 参数是必须配置的，而其它参数是可选的。在 IKE 协商时，如果使用 IPSec 策略模板进行策略匹配，则配置的参数必须匹配，而没有配置的参数采用发起方的。

相关配置可参考命令 **ipsec policy**，**security acl**，**tunnel local**，**tunnel remote**，**proposal**，**display ipsec policy**，**ike-peer**。

【举例】

创建一个模板名字为 template1，顺序号为 100 的安全策略模板。

```
[SecBlade_VPN] ipsec policy-template template1 100
[SecBlade_VPN-ipsec-policy-template- template1-100]
```

3.1.20 ipsec proposal

【命令】

ipsec proposal *proposal-name*

undo ipsec proposal *proposal-name*

【视图】

系统视图

【参数】

proposal-name：指定 IPsec 提议的名字。命名规则为：长度为 1～15 个字符，不区分大小写。

【描述】

命令 **ipsec proposal** *proposal-name* 用来创建或修改一个名字为 *proposal-name* 的 IPsec 提议，并进入 IPsec 提议视图，命令 **undo ipsec proposal** *proposal-name* 用来删除一个名字为 *proposal-name* 的 IPsec 提议。

缺省情况下，系统没有任何提议。

IPsec 提议（Proposal）是用于实施 IPSec 安全时所采取的一系列的措施，提议包含了所采用的安全协议、加密和认证算法、报文封装形式。

在配置安全策略时，需要通过引用提议来确定在安全隧道的两端所采用的安全协议、加密和认证算法和报文封装形式。

在使用 ipsec proposal 命令创建一个新的 IPsec 安全提议后，其缺省参数为采用 ESP 协议、DES 加密算法、MD5 认证算法。

相关配置可参考命令 **ah authentication-algorithm**，**esp encryption-algorithm**，**esp authentication-algorithm**，**encapsulation-mode**，**proposal**，**display ipsec proposal**，**transform**。

【举例】

创建名为 newprop1 的提议。

```
[SecBlade_VPN] ipsec proposal newprop1
```

3.1.21 ipsec sa global-duration

【命令】

ipsec sa global-duration { **time-based** *seconds* | **traffic-based** *kilobytes* }

undo ipsec sa global-duration { **time-based** | **traffic-based** }

【视图】

系统视图

【参数】

time-based *seconds*：指定以时间为基准的全局生存周期，*seconds* 的取值范围是 30～604800，单位是秒，缺省值是 3600 秒。

traffic-based *kilobytes*：指定以流量为基准的全局生存周期，*kilobytes* 的取值范围是 256～4194303，单位是千字节，缺省值是 1843200 千字节，如果流量达到此值，则生存周期到期。

【描述】

命令 **ipsec sa global-duration** 用来设置全局的安全联盟生存周期，命令 **undo ipsec sa global-duration** 用来恢复全局的安全联盟生存周期的缺省值。

当 IKE 协商安全联盟时，如果采用的安全策略没有配置自己的生存周期，将采用此命令所定义的全局生存周期与对端协商。如果安全策略配置了自己的生存周期，则系统使用安全策略自己的生存周期与对端协商。IKE 为 IPSec 协商建立安全联盟时，采用本地设置的生存周期和对端提议的生存周期中较小的一个。

衡量生存周期有两种方式：“基于时间”的生存周期和“基于流量”的生存周期。基于时间的生存周期是从安全联盟建立开始到此安全联盟协商存活的时间；基于流量的生存周期是此安全联盟允许处理的最大流量。如果生存周期到达指定的时间或指定的流量，则安全联盟就会失效。安全联盟失效前，IKE 将为 IPSec 协商建立新的安全联盟，这样，在旧的安全联盟失效前新的安全联盟就已经准备好。在新的安全联盟开始协商而没有协商好之前，继续使用旧的安全联盟保护通信。在新的安全联盟协商好之后，则立即采用新的安全联盟保护通信。

使用该命令可以改变安全联盟的全局生存周期，改变全局生存周期以后，没有单独配置生存周期的安全联盟，在下次 IKE 协商中，会使用新的全局生存周期。

安全联盟的生存周期只对通过 IKE 协商的安全联盟起作用，对通过手工方式建立的安全联盟不起作用。

相关配置可参考命令 **sa duration**，**display ipsec sa duration**。

【举例】

设置全局的安全联盟生存时间为 2 小时。

```
[SecBlade_VPN] ipsec sa global-duration time-based 7200
```

设置全局的安全联盟生存时间为：传输 10M 字节的流量后，安全联盟即过期。

```
[SecBlade_VPN] ipsec sa global-duration traffic-based 10000
```

3.1.22 pfs

【命令】

pfs { **dh-group1** | **dh-group2** | **dh-group5** | **dh-group14** }

undo pfs

【视图】

安全策略视图、安全策略模板视图

【参数】

dh-group1：指定使用 768-bit Diffie-Hellman 组。

dh-group2：指定使用 1024-bit Diffie-Hellman 组。

dh-group5：指定使用 1536-bit Diffie-Hellman 组。

dh-group14：指定使用 2048bit Diffie-Hellman 组。

【描述】

命令 **pfs** 用来设置使用此安全策略发起协商时使用完善的前向安全（Perfect Forward Secrecy）特性，命令 **undo pfs** 用来设置在协商时不使用 PFS 特性。

缺省情况没有 PFS 特性。

此命令使 IPSec 在使用此安全策略发起一个协商时，在阶段 2 的协商中进行一次附加的密钥交换以提高通讯的安全性。本端和对端指定的 Diffie-Hellman 组必须一致，否则协商会失败。

此命令仅在通过 IKE 方式建立安全联盟时才可以进行配置。

相关配置可参考命令 **ipsec policy-template**，**ipsec policy**（系统视图），**ipsec policy**（接口视图），**tunnel local**，**tunnel remote**，**sa duration**，**proposal**。

【举例】

设置使用安全策略 shanghai 200 进行协商时使用 PFS 特性。

```
[SecBlade_VPN] ipsec policy shanghai 200 isakmp
[SecBlade_VPN-ipsec-policy-isakmp-shanghai-200] pfs group1
```

3.1.23 proposal

【命令】

proposal *proposal-name1* [*proposal-name2*...*proposal-name6*]

undo proposal [*proposal-name*]

【视图】

安全策略视图、安全策略模板视图

【参数】

proposal-name1，…，*proposal-name6*：所采用的提议名字。

【描述】

命令 **proposal** 用来设置安全策略所引用的提议，命令 **undo proposal** 用来取消安全策略引用的提议。

缺省情况下，不引用任何提议。

在使用此命令之前，必须已经配置了相应的安全提议。

如果安全策略是手工（**manual**）方式的，则安全策略在引用提议时只能指定一个安全提议。如果需要改变已配置好的安全提议，必须先使用命令 **undo proposal** 取消原先的安全提议，再设置新的安全提议。

如果安全策略是 IKE（**isakmp**）协商方式的，则一条安全策略最多可以引用六个安全提议，IKE 协商时将在安全策略中搜索能够完全匹配的安全提议。

如果是安全策略模板，则每个模板最多可以引用六个安全提议，IKE 协商时将搜索能够完全匹配的安全提议。

相关配置可参考命令 **ipsec proposal**，**ipsec policy**（系统视图），**ipsec policy**（接口视图），**security acl**，**tunnel local**，**tunnel remote**。

【举例】

设置名字为 prop1 的安全提议，采用 ESP 协议和缺省算法。并设置安全策略引用此名字为 prop1 的安全提议。

```
[SecBlade_VPN] ipsec proposal prop1
[SecBlade_VPN-ipsec-proposal-prop1] transform esp
[SecBlade_VPN-ipsec-proposal-prop1] quit
[SecBlade_VPN] ipsec policy policy1 100 manual
[SecBlade_VPN-ipsec-policy-manual-policy1-100] proposal prop1
```

3.1.24 reset ipsec sa

【命令】

reset ipsec sa [**remote** *ip-address* | **policy** *policy-name* [*seq-number*] | **parameters** *ip-address protocol spi-number*]

【视图】

用户视图

【参数】

remote *ip-address*：指定对端地址为 *ip-address*，地址为点分十进制格式。

policy：指定安全策略。

policy-name：指定安全策略的名字。命名规则为：长度为 1～15 个字符，不区分大小写，字符可以是英文字母或者数字。

seq-number：为可选参数，指定安全策略的顺序号。如果不指定 *seq-number*，则是指名字为 *policy-name* 的安全策略组中所有安全策略。

parameters：指定一个安全联盟 SA（Security Association）所对应的目的 IP 地址、安全协议、SPI（Security Parameter Index）。

ip-address：指定目的地址，格式为点分十进制的 IP 地址格式。

protocol：指定安全协议，可选关键字为 **ah** 或 **esp**，不区分大小写。ah 是指报文头认证（Authentication Header）协议，esp 是指封装安全协议（Encapsulation Security Protocol）。

spi-number：指定安全参数索引，取值范围是 256～4294967295。

【描述】

命令 **reset ipsec sa** 删除已经建立的安全联盟（无论是手工建立的还是通过 IKE 协商建立的）。如果未指定 **remote**、**policy**、**parameters**，则删除所有的安全联盟。

一个安全联盟由三元组目的 IP 地址、安全协议、SPI 唯一地标识，安全联盟可以通过手工建立，也可以通过 IKE（Internet Key Exchange）协商建立。

通过手工建立的安全联盟被删除后，系统会自动根据对应的手工安全策略建立新的安全联盟。

而通过 IKE 协商建立的安全联盟被删除后，如果有报文重新触发 IKE 协商，IKE 将重新协商建立新的安全联盟。

如果指定了 **parameters** 关键字，由于安全联盟是成对出现的，删除了一个方向的安全联盟，另一个方向的安全联盟也会被删除。

相关配置可参考命令 **display ipsec sa**。

【举例】

删除所有安全联盟。

```
<SecBlade_VPN> reset ipsec sa
```

删除对端地址为 10.1.1.2 的安全联盟。

```
<SecBlade_VPN> reset ipsec sa remote 10.1.1.2
```

删除安全策略模板 policy1 中的所有安全联盟。

```
<SecBlade_VPN> reset ipsec sa policy policy1
```

删除安全策略名字为 policy1、顺序号为 10 的安全联盟。

```
<SecBlade_VPN> reset ipsec sa policy policy1 10
```

删除对端地址为 10.1.1.2、安全协议为 AH、安全参数索引为 10000 的安全联盟。

```
<SecBlade_VPN> reset ipsec sa parameters 10.1.1.2 ah 10000
```

3.1.25 reset ipsec statistics

【命令】

reset ipsec statistics

【视图】

用户视图

【参数】

无

【描述】

命令 **reset ipsec statistics** 清除 IPSec 的报文统计信息，所有的统计信息都被设置成零。

相关配置可参考命令 **display ipsec statistics**。

【举例】

清除 IPSec 的报文统计信息。

```
<SecBlade_VPN> reset ipsec statistics
```

3.1.26 sa authentication-hex

【命令】

sa authentication-hex { **inbound** | **outbound** } { **ah** | **esp** } *hex-key*

undo sa authentication-hex { **inbound** | **outbound** } { **ah** | **esp** }

【视图】

手工方式安全策略视图

【参数】

inbound：设置入方向安全联盟的参数，IPSec 使用入方向安全联盟处理接收的报文。

outbound：设置出方向安全联盟的参数，IPSec 使用出方向安全联盟处理发送的报文。

ah：设置采用 AH 协议的安全联盟的参数。如果安全策略引用的提议规定了采用 AH 协议，使用 **ah** 关键字来设置安全联盟的参数。

esp：设置采用 ESP 协议的安全联盟的参数。如果安全策略引用的提议规定了采用 ESP 协议，使用 **esp** 关键字来设置安全联盟的参数。

hex-key：指定安全联盟的认证密钥，以 16 进制格式输入。如果使用 MD5 算法，密钥长度为 16 个字节；如果使用 SHA1 算法，密钥长度为 20 个字节。

【描述】

命令 **sa authentication-hex** 用来对 **manual** 方式安全策略手工设置安全联盟的认证密钥，命令 **undo sa authentication-hex** 用来删除设置的安全联盟的认证密钥。

此命令仅用于 **manual** 方式的安全策略。

对于 **isakmp** 方式的安全策略，IKE 将自动协商安全联盟的参数并创建安全联盟，不需要手工设置安全联盟的参数，该命令无效。

在配置 manual 方式的安全策略时，必须分别设置 **inbound** 和 **outbound** 两个方向安全联盟的参数。

在安全隧道的两端设置的安全联盟参数必须是完全匹配的。本端的入方向安全联盟的密钥必须和对端的出方向安全联盟的密钥一样；本端的出方向安全联盟密钥必须和对端的入方向安全联盟的密钥一样。

输入密钥有两种方式：16 进制方式和字符串方式。如果以字符串方式输入密钥，需要使用命令 **sa string-key**。如果分别以两种方式输入了密钥，则最后设定的密钥有效。在安全隧道的两端，应当以相同的方式输入密钥。如果一端以字符串方式输入密钥，另一端以 16 进制方式输入密钥，则不能通讯。

相关配置可参考命令 **ipsec policy**（系统视图），**ipsec policy**（接口视图），**security acl**，**tunnel local**，**tunnel remote**，**sa duration**，**proposal**。

【举例】

在采用 AH 协议及 MD5 算法的安全策略中，设置输入安全联盟的 SPI 为 10000，密钥为 0x112233445566778899aabbccddeeff00；输出安全联盟的 SPI 为 20000，密钥为 0xaabbccddeeff001100aabbccddeeff00。

```
[SecBlade_VPN] ipsec proposal prop_ah
[SecBlade_VPN-ipsec-proposal-prop_ah] transform ah
[SecBlade_VPN-ipsec-proposal-prop_ah] ah authentication-algorithm md5
[SecBlade_VPN-ipsec-proposal-prop_ah] quit
[SecBlade_VPN] ipsec policy tianjin 100 manual
[SecBlade_VPN-ipsec-policy-manual-tianjin-100] proposal prop_ah
[SecBlade_VPN-ipsec-policy-manual-tianjin-100] sa spi inbound ah 10000
[SecBlade_VPN-ipsec-policy-manual-tianjin-100]    sa    authentication-hex
inbound ah 112233445566778899aabbccddeeff00
[SecBlade_VPN-ipsec-policy-manual-tianjin-100] sa spi outbound ah 20000
[SecBlade_VPN-ipsec-policy-manual-tianjin-100]    sa    authentication-hex
outbound ah aabbccddeeff001100aabbccddeeff00
```

3.1.27 sa duration

【命令】

sa duration { **traffic-based** *kilobytes* | **time-based** *seconds* }

undo sa duration { **traffic-based** | **time-based** }

【视图】

安全策略视图、安全策略模板视图

【参数】

time-based *seconds*：指定以时间为基准的生存周期，*seconds* 的取值范围是 120～604800，单位是秒，缺省值是 3600 秒。

traffic-based *kilobytes*：指定以流量为基准的生存周期，*kilobytes* 的取值范围是 256～4194303，单位是千字节，缺省值是 1843200 千字节。

【描述】

命令 **sa duration** 用来为安全策略设置安全联盟的生存周期，命令 **undo sa duration** 用来取消设置的生存周期，即恢复使用设定的全局生存周期。

当 IKE 协商安全联盟时，如果采用的安全策略没有配置自己的生存周期，将采用全局生存周期与对端协商。如果安全策略配置了自己的生存周期，则系统使用安全策略自己的生存周期与对端协商。IKE 为 IPSec 协商建立安全联盟时，采用本地设置的生存周期和对端提议的生存周期中较小的一个。

衡量生存周期有两种方式：“基于时间”的生存周期和“基于流量”的生存周期。基于时间的生存周期是从安全联盟建立开始，此安全联盟存活的时间；基于流量的生存周期是此安全联盟允许处理的最大流量。如果生存周期到达指定的时间或指定的流量，则安全联盟就会失效。安全联盟失效前，IKE 将为 IPSec 协商建立新的安全联盟，这样，在旧的安全联盟失效前，新的安全联盟就已经准备好。在新的安全联盟开始协商而没有协商好之前，继续使用旧的安全联盟保护通信。在新的安全联盟协商好之后，则立即采用新的安全联盟保护通信。

安全联盟的生存周期只对通过 IKE 协商的安全联盟起作用，而对通过手工方式建立的安全联盟不起作用。

相关配置可参考命令 **ipsec sa global-duration**，**ipsec policy**（系统视图），**ipsec policy**（接口视图），**security acl**，**tunnel local**，**tunnel remote**，**proposal**。

【举例】

设置安全策略的安全联盟生存时间为两个小时，即 7200 秒。

```
[SecBlade_VPN] ipsec policy shenzhen 100 isakmp
[SecBlade_VPN-ipsec-policy-isakmp-shenzhen-100] sa duration time-based 7200
```

设置安全策略的安全联盟生存时间为 20M 字节，即 20,000 千字节。

```
[SecBlade_VPN] ipsec policy shenzhen 100 isakmp
[SecBlade_VPN-ipsec-policy-isakmp-shenzhen-100] sa duration traffic-based
20000
```

3.1.28 sa encryption-hex

【命令】

sa encryption-hex { **inbound** | **outbound** } **esp** *hex-key*

undo sa encryption-hex { **inbound** | **outbound** } **esp**

【视图】

手工方式安全策略视图

【参数】

inbound：设置入方向安全联盟的参数，IPSec 使用入方向安全联盟处理接收的报文。

outbound：设置出方向安全联盟的参数，IPSec 使用出方向安全联盟处理发送的报文。

esp：设置采用 ESP 协议的安全联盟的参数。如果安全策略引用的提议规定了采用 ESP 协议，使用 **esp** 关键字来设置安全联盟的参数。

hex-key：使用 ESP 协议时，指定安全联盟的加密密钥。以 16 进制格式输入，输入的密钥长度必须符合所采用的加密算法的要求。如果使用 DES 算法，密钥长度为 8 个字节；如果使用 3DES 算法，密钥长度为 24 个字节。

【描述】

命令 **sa encryption-hex** 用来对 **manual** 方式的安全策略手工设置安全联盟的加密密钥参数，命令 **undo sa encryption-hex** 用来删除设置的安全联盟的加密密钥参数。

此命令仅用于 **manual** 方式的安全策略，来手工设置安全联盟的参数，实现手工创建安全联盟。

对于 **isakmp** 方式的安全策略，IKE 将自动协商安全联盟的参数并创建安全联盟，不需要手工设置安全联盟的参数，该命令无效。

在为系统配置安全联盟时，必须分别设置 **inbound** 和 **outbound** 两个方向安全联盟的参数。

在安全隧道的两端设置的安全联盟参数必须是完全匹配的。本端的入方向安全联盟的加密密钥必须和对端的出方向安全联盟的加密密钥一样；本端的出方向安全联盟的加密密钥必须和对端的入方向安全联盟的加密密钥一样。

相关配置可参考命令 **ipsec policy**（系统视图），**ipsec policy**（接口视图），**security acl**，**tunnel local**，**tunnel remote**，**sa duration**，**proposal**。

【举例】

在采用 ESP 协议及 DES 加密算法的安全策略中，设置入方向安全联盟的 SPI 为 1001，加密算法的密钥为 0x1234567890abcdef ；输出安全联盟的 SPI 为 2001，加密算法的密钥为 0x abcdefabcdef1234。

```
[SecBlade_VPN] ipsec proposal prop_esp
[SecBlade_VPN-ipsec-proposal-prop_esp] transform esp
```

```
[SecBlade_VPN-ipsec-proposal-prop_esp] ah encryption-algorithm des
[SecBlade_VPN-ipsec-proposal-prop_esp] quit
[SecBlade_VPN] ipsec policy tianjin 100 manual
[SecBlade_VPN-ipsec-policy-manual-tianjin-100] proposal prop_esp
[SecBlade_VPN-ipsec-policy-manual-tianjin-100] sa spi inbound esp 1001
[SecBlade_VPN-ipsec-policy-manual-tianjin-100] sa encryption-hex inbound esp
1234567890abcdef
[SecBlade_VPN-ipsec-policy-manual-tianjin-100] sa spi outbound esp 2001
[SecBlade_VPN-ipsec-policy-manual-tianjin-100] sa encryption-hex outbound
esp abcdefabcdef1234
```

3.1.29 sa spi

【命令】

sa spi { **inbound** | **outbound** } { **ah** | **esp** } *spi-number*

undo sa spi { **inbound** | **outbound** } { **ah** | **esp** }

【视图】

手工方式安全策略视图

【参数】

inbound：设置入方向安全联盟的参数，IPSec 使用入方向安全联盟处理接收的报文。

outbound：设置出方向安全联盟的参数，IPSec 使用出方向安全联盟处理发送的报文。

ah：设置采用 AH 协议的安全联盟的参数。如果安全策略引用的提议规定了采用 AH 协议，使用 **ah** 关键字来设置安全联盟的参数。

esp：设置采用 ESP 协议的安全联盟的参数。如果安全策略引用的提议规定了采用 ESP 协议，使用 **esp** 关键字来设置安全联盟的参数。

spi-number：安全联盟三元组标识中的安全参数索引 SPI（Security Parameter Index），取值范围为 256～4294967295。在系统中，安全联盟的三元组标识<SPI、目的地址、安全协议>必须是唯一的。

【描述】

命令 **sa spi** 用来对 **manual** 方式的安全策略手工设置安全联盟的 SPI（安全参数索引）参数，命令 **undo sa spi** 用来删除设置的安全联盟的 SPI（安全参数索引）参数。

此命令仅用于 **manual** 方式的安全策略，用该命令手工设置安全联盟的参数，实现手工创建安全联盟。

对于 **isakmp** 方式的安全策略，IKE 将自动协商安全联盟的参数并创建安全联盟，不需要手工设置安全联盟的参数，该命令无效。

在为系统配置安全联盟时，必须分别设置 **inbound** 和 **outbound** 两个方向安全联盟的参数。

在安全隧道的两端设置的安全联盟参数必须是完全匹配的。本端的入方向安全联盟的 SPI 必须和对端的出方向安全联盟的 SPI 一样；本端的出方向安全联盟的 SPI 必须和对端的入方向安全联盟的 SPI 一样。

相关配置可参考命令 **ipsec policy**（系统视图），**ipsec policy**（接口视图），**security acl**，**tunnel local**，**tunnel remote**，**sa duration**，**proposal**。

【举例】

在采用 AH 协议及 MD5 算法的安全策略中设置输入安全联盟的 SPI 为 10000，输出安全联盟的 SPI 为 20000。

```
[SecBlade_VPN] ipsec proposal prop_ah
[SecBlade_VPN-ipsec-proposal-prop_ah] transform ah
[SecBlade_VPN-ipsec-proposal-prop_ah] ah authentication-algorithm md5
[SecBlade_VPN-ipsec-proposal-prop_ah] quit
[SecBlade_VPN] ipsec policy tianjin 100 manual
[SecBlade_VPN-ipsec-policy-manual-tianjin-100] proposal prop_ah
[SecBlade_VPN-ipsec-policy-manual-tianjin-100] sa spi inbound ah 10000
[SecBlade_VPN-ipsec-policy-manual-tianjin-100] sa spi outbound ah 20000
```

3.1.30 sa string-key

【命令】

sa string-key { **inbound** | **outbound** } { **ah** | **esp** } *string-key*

undo sa string-key { **inbound** | **outbound** } { **ah** | **esp** }

【视图】

手工方式安全策略视图

【参数】

inbound：设置入方向安全联盟的参数，IPSec 使用入方向安全联盟处理接收的报文。

outbound：设置出方向安全联盟的参数，IPSec 使用出方向安全联盟处理发送的报文。

ah：设置采用 AH 协议的安全联盟的参数。如果安全策略引用的提议规定了采用 AH 协议，使用 **ah** 关键字来设置安全联盟的参数。

esp：设置采用 ESP 协议的安全联盟的参数。如果安全策略引用的提议规定了采用 ESP 协议，使用 **esp** 关键字来设置安全联盟的参数。

string-key：指定安全联盟的密钥，以字符串格式输入，长度 1～255 个字符。对不同的算法，均可输入不超过长度范围的字符串，系统会根据输入的字符串自动生成符合算法要求的密钥。对于 ESP 协议，系统会自动地同时生成认证算法的密钥和加密算法的密钥。

【描述】

命令 **sa string-key** 用来对 **manual** 方式的安全策略手工设置安全联盟的参数，命令 **undo sa string-key** 用来删除设置的安全联盟的参数。

此命令仅用于 **manual** 方式的安全策略，用该命令手工设置安全联盟的参数，实现手工创建安全联盟。

对于 **isakmp** 方式的安全策略，IKE 将自动协商安全联盟的参数并创建安全联盟，不需要手工设置安全联盟的参数，该命令无效。

在为系统配置安全联盟时，必须分别设置 **inbound** 和 **outbound** 两个方向安全联盟的参数。

在安全隧道的两端设置的安全联盟参数必须是完全匹配的。本端入方向安全联盟的密钥必须和对端出方向安全联盟的密钥一样；本端出方向安全联盟的密钥必须和对端入方向安全联盟的密钥一样。

输入密钥有两种方式：16 进制方式和字符串方式。如果以 16 进制方式输入密钥需要使用命令 **sa authentication-hex**。如果分别以两种方式输入了密钥，则最后设定的密钥有效。在安全隧道的两端，应当以相同的方式输入密钥。如果一端以字符串方式输入密钥，另一端以 16 进制方式输入密钥，则不能正确地建立安全隧道。

相关配置可参考命令 **ipsec policy**（系统视图），**ipsec policy**（接口视图），**security acl**，**tunnel local**，**tunnel remote**，**sa duration**，**proposal**。

【举例】

在采用 AH 协议及 MD5 算法的安全策略中，设置输入安全联盟的 SPI 为 10000，密钥为字符串 abcdef；输出安全联盟的 SPI 为 20000，密钥为字符串 efcdab。

```
[SecBlade_VPN] ipsec proposal prop_ah
[SecBlade_VPN-ipsec-proposal-prop_ah] transform ah
[SecBlade_VPN-ipsec-proposal-prop_ah] ah authentication-algorithm md5
[SecBlade_VPN-ipsec-proposal-prop_ah] quit
[SecBlade_VPN] ipsec policy tianjin 100 manual
[SecBlade_VPN-ipsec-policy-manual-tianjin-100] proposal prop_ah
[SecBlade_VPN-ipsec-policy-manual-tianjin-100] sa spi inbound ah 10000
[SecBlade_VPN-ipsec-policy-manual-tianjin-100] sa string-key abcdef
[SecBlade_VPN-ipsec-policy-manual-tianjin-100] sa spi outbound ah 20000
```

```
[SecBlade_VPN-ipsec-policy-manual-tianjin-100] sa string-key efcdab
```

3.1.31 security acl

【命令】

security acl *acl-number*

undo security acl

【视图】

安全策略视图、安全策略模板视图

【参数】

acl-number：指定安全策略所引用的访问控制列表号，取值范围是 3000～3999。

【描述】

命令 **security acl** 用来设置安全策略引用的访问控制列表，命令 **undo security acl** 用来取消安全策略引用的访问控制列表。

缺省情况下，安全策略没有指定访问控制列表。

安全策略所保护的数据流由此命令指定的 acl 来定义。在实施 IPSec 安全策略时，系统首先检查通过接口的报文是否与 acl 中的规则匹配，如果匹配且是被访问控制列表允许（**permit**）的报文，则系统对报文进行 IPsec 保护后再发送。如果不匹配，或者访问控制列表拒绝（**deny**）的报文，则直接发送报文。

对于手工方式创建的安全策略，只支持保护访问控制列表下的一条规则，即只有最先匹配此访问控制列表的报文被保护，后续匹配此访问控制列表中其它规则的报文不会被保护。

相关配置可参考命令 **ipsec policy**（系统视图），**ipsec policy**（接口视图），**tunnel local**，**tunnel remote**，**sa duration**，**proposal**。

【举例】

设置安全策略引用 3001 号访问控制列表。

```
[SecBlade_VPN] acl number 3001
[SecBlade_VPN-acl-adv-3001] rule permit tcp source 10.1.1.1 0.0.0.255
destination 10.1.1.2 0.0.0.255
[SecBlade_VPN] ipsec policy beijing 100 manual
[SecBlade_VPN-ipsec-policy-manual-beijing-100] security acl 3001
```

3.1.32 time-out

【命令】

time-out *seconds*

undo time-out

【视图】

DPD 结构视图

【参数】

seconds：等待 DPD 应答报文的超时时间，取值范围 1～60 秒。缺省情况下，*seconds* 为 5 秒。

【描述】

time-out 命令用来配置等待 DPD 应答报文的超时时间，**undo time-out** 命令用来恢复等待 DPD 应答报文超时时间为缺省值。

【举例】

设置 time-out 为 2 秒。

```
[SecBlade_VPN-ike-dpd-aaa] time-out 2
```

重置 time-out 为 5 秒。

```
[SecBlade_VPN-ike-dpd-aaa] undo time-out
```

3.1.33 transform

【命令】

transform { **ah** | **ah-esp** | **esp** }

undo transform

【视图】

安全提议视图

【参数】

ah：设置采用 RFC2402 规定的 AH 协议。

ah-esp：设置先用 ESP 协议对报文进行保护，再用 AH 协议进行保护。

esp：设置采用 RFC2406 规定的 ESP 协议。

【描述】

命令 **transform** 用来设置提议采用的安全协议，命令 **undo transform** 用来恢复缺省的安全协议。

缺省情况使用 **esp**，即 RFC2406 规定的 ESP 协议。

如果采用 ESP 协议，则缺省的加密算法为 DES，认证算法为 MD5。

如果采用 AH 协议，则缺省的认证算法为 MD5。

如果指定参数 **ah-esp**，则 AH 缺省的认证算法为 MD5，ESP 协议缺省使用的加密算法为 DES，不使用认证算法。

AH 协议提供数据源认证、数据完整性校验和防报文重放功能。

ESP 协议提供数据源认证、数据完整性校验、防报文重放和数据加密功能。

在安全隧道的两端，IPsec 提议所使用的安全协议需要匹配。

不同安全协议在 transport 和 tunnel 模式下的数据封装形式如下图：

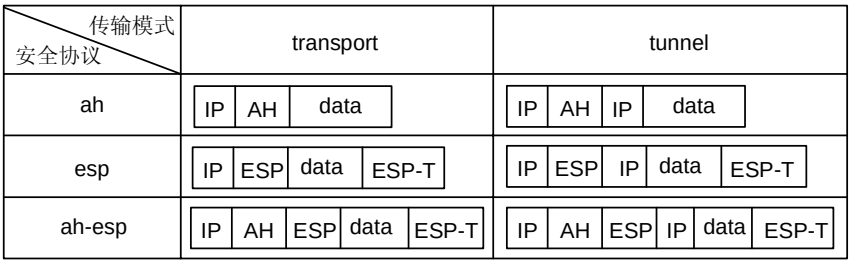

图3-1 安全协议数据封装格式

上图中的 data 为原 IP 报文。

相关配置可参考命令 **ah authentication-algorithm**，**ipsec proposal**，**esp encryption-algorithm**，**esp authentication-algorithm**，**encapsulation-mode**，**proposal**。

【举例】

设置一个采用 AH 协议的提议。

```
[SecBlade_VPN] ipsec proposal prop1
[SecBlade_VPN-ipsec-proposal-prop1] transform ah
```

3.1.34 tunnel local

【命令】

tunnel local *ip-address*

undo tunnel local

【视图】

手工方式安全策略视图

【参数】

ip-address：本端地址，格式为点分十进制格式。

【描述】

命令 **tunnel local** 用来设置安全策略的本端地址，命令 **undo tunnel local** 用来删除在安全策略中设定的本端地址。

缺省情况下，没有配置安全隧道的本端地址。

对于 **isakmp** 方式的安全策略，不需要设置本端地址，该命令无效。IKE 能够自动从应用该安全策略的接口上获取本端地址。

对于 **manual** 方式的安全策略，必须设置本端地址才能够创建安全联盟。安全隧道是建立在本端和对端之间的，故必须正确设置本端地址和对端地址才能成功地建立一条安全隧道。

相关配置可参考命令 **ipsec policy**（系统视图），**ipsec policy**（接口视图），**security acl**，**tunnel remote**，**sa duration**，**proposal**。

【举例】

设置安全策略的本地地址，该安全策略应用在 IP 地址为 10.0.0.1 的 GigabitEthernet0/0.1 接口上。

```
[SecBlade_VPN] ipsec policy guangzhou 100 manual
[SecBlade_VPN-ipsec-policy-manual-guangzhou-100] tunnel local 10.0.0.1
[SecBlade_VPN-ipsec-policy-manual-guangzhou-100] quit
[SecBlade_VPN] interface GigabitEthernet0/0.1
[SecBlade_VPN- GigabitEthernet0/0.1] ipsec policy guangzhou
```

3.1.35 tunnel remote

【命令】

tunnel remote *ip-address*

undo tunnel remote [*ip-address*]

【视图】

手工方式安全策略视图

【参数】

ip-address：安全策略的隧道对端地址，格式为点分十进制格式。

【描述】

命令 **tunnel remote** 用来设置安全策略的隧道对端地址，命令 **undo tunnel remote** 用来删除安全策略中设置的隧道对端地址。

缺省情况下，没有配置安全隧道的对端地址。

对于 **manual** 方式的安全策略，如果已经设置了对端地址，必须先删除原先的地址才能设置新的对端地址。

安全隧道是建立在本端和对端之间，在安全隧道的两端，均需要正确设置对端地址。

相关配置可参考命令 **ipsec policy**（系统视图），**ipsec policy**（接口视图），**security acl**，**tunnel local**，**sa duration**，**proposal**。

【举例】

设置安全策略的对端地址为 10.1.1.2。

```
[SecBlade_VPN] ipsec policy shanghai 10 manual
[SecBlade_VPN-ipsec-policy-shanghai-10] tunnel remote 10.1.1.2
```

3.2 加密卡配置命令

3.2.1 debugging encrypt-card host

【命令】

debugging encrypt-card host { **all** | **command** | **error** | **misc** | **packet** | **sa** }

undo debugging encrypt-card host { **all** | **command** | **error** | **misc** | **packet** | **sa** }

【视图】

用户视图

【参数】

all：打开加密卡上所有信息的调试开关。

command：打开加密卡上命令信息的调试开关。

error：打开加密卡上错误信息的调试开关。

misc：打开加密卡上其他信息的调试开关。

packet：打开加密卡上报文处理开关。

sa：打开加密卡上安全联盟信息调试开关。

【描述】

命令 **debugging encrypt-card** 用来打开加密卡侧 CMW 主体测试软件的调试信息开关，命令 **undo debugging encrypt-card** 用来关闭调试信息开关。

【举例】

打开加密卡侧 CMW 主体测试软件的命令调试开关。

```
<SecBlade_VPN> debugging encrypt-card host command
```

3.2.2 display encrypt-card fast-switch

【命令】

display encrypt-card fast-switch

【视图】

所有视图

【参数】

无

【描述】

display encrypt-card fast-switch 命令用来显示加密卡的快转表项。

【举例】

显示加密卡的快转表项。

```
[SecBlade_VPN] display encrypt-card fast-switch
  encrypt-card Fast-Forwarding cache:
Index SourIP   SourPort     DestIP   DestPort     Prot     TdbID    Type
18    1.1.1.2      8        1.1.1.1      0        1 0x00000024     encrypt
130   1.1.1.1      0        1.1.1.2      0        50 0x00000023    decrypt
```

表3-9 display encrypt-card fast-switch 命令显示信息描述表

域名	描述
Index	快转表项的索引
SourIP	源 IP
SourPort	源端口
DestIP	目的 IP
DestPort	目的端口
Prot	指协议号
TdbID	为加密这条流所使用的 TDB 的 ID
Type	有两种，encrypt 和 decrypt，指出方向（加密）和入方向（解密）

3.2.3 display interface encrypt

【命令】

display interface encrypt [*slot-id*]

【视图】

所有视图

【参数】

slot-id：SecBlade 槽位号，取值范围由 SecBlade 槽位数决定。槽位号采用三维数组表示，例如 x/y/z，其中 x 表示 SecBlade 的插槽编号，y/z 对于加密卡编号固定取值为 0。

【描述】

命令 **display interface encrypt** 用来显示加密卡接口信息。

该命令可以查询加密卡的状态、加密卡收发的报文总数、每秒丢弃的最大报文数以及过去 5 秒的相关的信息。

相关配置可参考 **interface encrypt**。

【举例】

显示 SecBlade5/0/0 槽位加密卡接口的信息。

```
[SecBlade_VPN] display interface Encrypt 5/0/0
Description :  Encrypt5/0/0 Interface
  Protocol Status:    READY
  Driver Status  :    READY
  Total Statistics
    Packets sent to card              :    10
    Packets received from card        :    9
    Bytes sent to card                :    1216
    Bytes received from card          :    584
    Dropped packets                 :    0
  Statistics during last 5 seconds
    Packets sent to card              :    0
    Packets received from card        :    0
    Bytes sent to card                :    0
    Bytes received from card          :    0
    Dropped packets                 :    0
```

以上信息显示了 SecBlade5/0/0 槽位加密卡的协议状态、驱动器状态、收发包总数、收发字节总数、每秒的最大丢包数以及在过去 5 秒中的相应的信息的统计。

3.2.4 encrypt-card backuped

【命令】

encrypt-card backuped

undo encrypt-card backuped

【视图】

系统视图

【参数】

无

【描述】

命令 **encrypt-card backuped** 用来使能加密卡的主机备份功能。命令 **undo encrypt-card backuped** 命令用来禁止加密卡的主机备份功能。缺省情况下，主机备份加密卡功能是被禁止的。

对于使用加密卡进行 IPSec 处理的安全联盟，若该加密卡状态正常，IPSec 就由该加密卡进行处理，当该加密卡状态异常时，如果已经开启了加密卡主机备份开关，并且CMW主体软件IPSec模块支持该安全联盟所使用的加密/认证算法，则由CMW主体软件 IPSec 模块替代加密卡对报文进行 IPSec 处理；若 CMW 主体软件 IPSec 模块不支持该安全联盟使用的算法，则报文被丢弃。

【举例】

使能加密卡主机备份功能

```
[SecBlade_VPN] encrypt-card backuped
```

3.2.5 encrypt-card fast-switch

【命令】

encrypt-card fast-switch

undo encrypt-card fast-switch

【视图】

系统视图

【参数】

无

【描述】

encrypt-card fast-switch 命令用来使能加密卡快转功能，**undo encrypt-card fast-switch** 命令用来关闭加密卡快转功能。

缺省情况下，关闭加密卡快转功能。

加密卡快转指的是对于[SourIP, SourPort, DestIP, DestPort, Prot] 五元组相同的一系列报文，SecBlade 在接收或发送第一个报文时就会创建一个快转表项，之后符合

此表项的所有报文都会直接被发往加密卡进行加密或解密，然后再由加密卡发往目的出口，这样省去了对每个报文逐一进行从 IP 到 IPSec 的处理，加速了处理过程。

⚠ 注意：

开启加密卡快转功能后，经过加密卡快转的报文将不进行 ACL 的统计计数。

【举例】

使能加密卡快转功能。

```
[SecBlade_VPN] encrypt-card fast-switch
```

3.2.6 interface encrypt

【命令】

interface encrypt *slot-id*

【视图】

系统视图

【参数】

slot-id：SecBlade 槽位号，取值范围由 SecBlade 槽位数决定。必须进入槽位为 *slot-id* 的加密卡接口。槽位号采用三维数组表示，例如 x/y/z，其中 x 表示 SecBlade 的插槽编号，y/z 对于加密卡编号固定取值为 0。

【描述】

命令 **interface encrypt** 用来进入加密卡接口视图。

进入加密卡的接口模式后，只能进行 **shutdown** 和 **undo shutdown** 命令的操作，分别对加密卡进行禁用和使能操作。

【举例】

进入槽位 5/0/0 的加密卡接口

```
[SecBlade_VPN] interface encrypt 5/0/0
[SecBlade_VPN-Encrypt5/0/0]
```

3.2.7 ipsec card-proposal

【命令】

ipsec card-proposal *proposal-name*

undo ipsec card-proposal *proposal-name*

【视图】

系统视图

【参数】

proposal-name：加密卡安全提议的名称，小于 16 个字符组成的字符串，不区分大小写。

【描述】

命令 **ipsec card-proposal** 用来创建并进入加密卡安全提议视图。命令 **undo ipsec card-proposal** 用来删除加密卡安全提议。

本命令适用于加密卡提议视图（相应的加密/解密/认证在加密卡上完成）；而主机软件同时还兼容应用于主机本身的安全提议视图（命令为 **ipsec proposal**），相应的加密/解密/认证处理由主机完成。在本视图下的操作中除了增加了 **use encrypt card** 命令用来指定加密卡安全提议使用的加密卡的槽位外，其他的配置与 **ipsec proposal** 命令完全相同。

在完成安全提议下的配置后，需要使用命令 **quit** 退回到系统视图进行其他信息的设置。

【举例】

创建名称为 card 的加密卡安全提议、使用 5/0/0 槽位的加密卡，并且进行安全和加密算法的配置。

```
[SecBlade_VPN] ipsec card-proposal card
[SecBlade_VPN-ipsec-card-proposal] use encrypt-card 5/0/0
[SecBlade_VPN-ipsec-card-proposal-card] transform ah-esp
[SecBlade_VPN-ipsec-card-proposal-card] ah authentication-algorithm sha1
[SecBlade_VPN-ipsec-card-proposal-card] esp authentication-algorithm sha1
[SecBlade_VPN-ipsec-card-proposal-card] esp encryption-algorithm 3des
[SecBlade_VPN-ipsec-card-proposal-card] quit
[SecBlade_VPN]
```

以上配置创建了名为 card 的加密卡安全提议，使用 SecBlade 槽位 5/0/0 上的加密卡，设置采用的安全协议为 ah-esp，ah 的认证算法为 sha1，esp 的认证和加密算法分别为 sha1 和 3des。最后退回到系统视图。

3.2.8 reset counters interface encrypt

【命令】

reset counters interface encrypt [*slot-id*]

【视图】

用户视图

【参数】

slot-id：SecBlade 槽位号，取值范围由 SecBlade 槽位数决定。槽位号采用三维数组表示，例如 x/y/z，其中 x 表示 SecBlade 的插槽编号，y/z 对于加密卡编号固定取值为 0。

【描述】

命令 **reset counters interface encrypt** 用来清除加密卡的统计信息。

加密卡的统计信息记录了从加密卡正常工作到清除前的所有的统计信息，在调试的过程中，往往需要通过一段时间的统计信息来分析问题，这样，就需要现将加密卡的统计信息清除，使加密卡的计数器重新开始计数来获得特定时间段的统计信息。

相关配置可参考命令 **ipsec card-proposal**。

【举例】

删除 5/0/0 槽位上加密卡的统计信息。

```
<SecBlade_VPN> reset counters interface encrypt-card 5/0/0
```

3.2.9 reset encrypt-card fast-switch

【命令】

reset encrypt-card fast-switch

【视图】

用户视图

【参数】

无

【描述】

reset encrypt-card fast-switch 命令用来清除加密卡的快速转发信息。

【举例】

清除加密卡的快速转发信息。

```
<SecBlade_VPN> reset encrypt-card fast-switch
```

3.2.10 reset encrypt-card sa

【命令】

reset encrypt-card sa [*slot-id*]

【视图】

用户视图

【参数】

slot-id：SecBlade 槽位号，取值范围由 SecBlade 槽位数决定。槽位号采用三维数组表示，例如 x/y/z，其中 x 表示 SecBlade 的插槽编号，y/z 对于加密卡编号固定取值为 0。

【描述】

命令 **reset encrypt-card sa** 用来删除指定加密卡上的安全联盟。

在调试的过程中为了仅输出需要的信息，可以通过 **reset encrypt-card sa** 命令删除加密卡上备份的主机安全联盟数据库的信息。

相关配置可参考命令 **ipsec card-proposal**。

📖 **说明：**

目前的加密卡尚不支持此命令。

【举例】

删除 5/0/0 槽位上加密卡上的安全联盟。

```
<SecBlade_VPN> reset encrypt-card sa 5/0/0
```

3.2.11 reset encrypt-card statistics

【命令】

reset encrypt-card statistics [*slot-id*]

【视图】

用户视图

【参数】

slot-id：SecBlade 槽位号，取值范围由 SecBlade 槽位数决定。槽位号采用三维数组表示，例如 x/y/z，其中 x 表示 SecBlade 的插槽编号，y/z 对于加密卡编号固定取值为 0。

【描述】

命令 **reset encrypt-card statistics** 用来清除加密卡处理过程中的统计信息。

加密卡记录了自上次复位至当前为止的协议处理情况，包括 ESP/AH 包的输入/输出个数、丢包统计、认证失败统计、错误 SA 统计、非法加密卡安全提议统计、非法协议统计等信息。

📖 **说明：**

目前的加密卡尚不支持此命令。

【举例】

清除 5/0/0 槽位上加密卡处理过程中的统计信息。

```
<SecBlade_VPN> reset encrypt-card statistic 5/0/0
```

3.2.12 reset encrypt-card syslog

【命令】

reset encrypt-card syslog [*slot-id*]

【视图】

用户视图

【参数】

slot-id：SecBlade 槽位号，取值范围由 SecBlade 槽位数决定。槽位号采用三维数组表示，例如 x/y/z，其中 x 表示 SecBlade 的插槽编号，y/z 对于加密卡编号固定取值为 0。

【描述】

命令 **reset encrypt-card syslog** 用来清除加密卡上所有的日志信息。

加密卡侧保留了日志历史信息，并以增量形式逐渐增多，每次查询加密卡日志时都会上报所有信息（包含很久以前的过时信息），不利于对日志的监控和定位问题，因此可以通过 **reset encrypt-card syslog** 命令及时清除加密卡日志缓冲区中的信息。

📖 **说明：**

目前的加密卡尚不支持此命令。

【举例】

删除 5/0/0 槽位加密卡上的所有日志信息。

```
<SecBlade_VPN> reset encrypt-card syslog 5/0/0
```

3.2.13 snmp-agent trap enable encrypt-card

【命令】

snmp-agent trap enable encrypt-card

undo snmp-agent trap enable encrypt-card

【视图】

系统视图

【参数】

无

【描述】

命令 **snmp-agent trap enable encrypt-card** 用来使能加密卡 SNMP 代理的 trap 监控信息开关。命令 **undo snmp-agent trap enable encrypt-card** 用来禁止加密卡 trap 信息开关。

使能 trap 信息后结合简单网络管理的配置，用户将能够在网管及 SecBlade 的控制台上查看加密卡复位信息、状态变迁信息和加密卡处理异常丢包等信息。

缺省情况下，加密卡 trap 信息开关是打开的。

【举例】

使能加密卡 trap 信息开关。

```
[SecBlade_VPN] snmp-agent trap enable encrypt-card
```

3.2.14 use encrypt-card

【命令】

use encrypt-card *slot-id*

undo use encrypt-card

【视图】

加密卡提议视图

【参数】

slot-id：SecBlade 槽位号，取值范围由 SecBlade 槽位数决定。槽位号采用三维数组表示，例如 x/y/z，其中 x 表示 SecBlade 的插槽编号，y/z 对于加密卡编号固定取值为 0。

【描述】

命令 **use encrypt-card** 用来指定某个加密卡提议所使用的加密卡所在的槽位。命令 **undo use encrypt-card** 用来取消某加密卡提议所使用的加密卡。

对于同一个加密卡提议，仅可以指定一块加密卡来进行处理，也就是说加密卡不支持多块加密卡轮循处理同一个加密卡安全提议；对于不同的加密卡安全提议可以指定相同的加密卡进行处理，即同一块加密卡可以处理多个加密卡安全提议。

相关配置可参考命令 **ipsec card-proposal**。

【举例】

加密卡提议 card 所使用的加密卡所在的槽位为 5/0/0。

```
[SecBlade_VPN] ipsec card-proposal card
[SecBlade_VPN-ipsec-card-proposal] use encrypt-card 5/0/0
```

第4章 IKE 配置命令

4.1 IKE 配置命令

4.1.1 authentication-algorithm

【命令】

authentication-algorithm { **md5** | **sha** }

undo authentication-algorithm

【视图】

IKE 提议视图

【参数】

md5：指定认证算法为 HMAC-MD5。

sha：指定认证算法为 HMAC-SHA1。

【描述】

命令 **authentication-algorithm** 用来指定一个供 IKE 提议使用的认证算法，命令 **undo authentication-algorithm** 用来设置认证算法为缺省值。

缺省使用 SHA1 认证算法。

相关配置可参考命令 **ike proposal**，**display ike proposal**。

【举例】

指定 IKE 提议 10 的认证算法为 MD5。

```
[SecBlade_VPN] ike proposal 10
[SecBlade_VPN-ike-proposal-10] authentication-algorithm md5
```

4.1.2 authentication-method

【命令】

authentication-method { **pre-share** | **rsa-signature** }

undo authentication-method

【视图】

IKE 提议视图

【参数】

pre-share：指定认证方法为预共享密钥（pre-shared-key）方法。

rsa-signature：指定认证方法为 PKI 数字签名方法。

【描述】

命令 **authentication-method** 用来指定一个供 IKE 提议使用的认证方法，命令 **undo authentication-method** 用来设置认证方法为缺省值。

缺省情况下，使用 pre-shared key 的认证方法。

使用此命令指定一个 IKE 策略使用的认证方法。目前我们实现了预共享密钥（pre-shared-key）和 PKI（rsa-signature）的认证方法。

使用 pre-shared-key 的认证方法时必须配置认证字，请参考命令 **pre-shared-key**。

在 IKE 协商中，如果发起方使用 RSA 数字签名验证方式，那么在 IKE 对等体（IKE Peer）中配置的 **id-type**，**remote-name** 将不生效，响应方只会根据 IKE 对等体中的 **remote-address** 来选择 IKE Peer，故当使用 RSA 数字签名验证方式时，发起方和响应方都要具体指定 **remote-address**，若未配置 **remote-address**，则默认为匹配所有地址。

相关配置可参考命令 **ike pre-shared-key**，**ike proposal**，**display ike proposal**，**pki domain**，**pki entity**。

📖 说明：

关于 PKI 的配置，请参考本手册中的“PKI 配置”。

【举例】

指定 IKE 提议 10 的认证方法为 pre-shared key。

```
[SecBlade_VPN] ike proposal 10
[SecBlade_VPN-ike-proposal-10] authentication-method pre-share
```

4.1.3 debugging ike

【命令】

debugging ike { **all** | **error** | **exchange** | **message** | **misc** | **transport**}

undo debugging ike { **all** | **error** | **exchange** | **message** | **misc** | **transport** }

【视图】

用户视图

【参数】

all：所有 IKE 调试功能。

error：IKE 错误信息。

exchange：IKE 交换模式调试信息。

message：IKE 消息包调试信息。

misc：IKE 所有其他调试信息。

transport：IKE 传输功能调试信息。

【描述】

命令 **debugging ike** 用来打开 IKE 调试开关，命令 **undo debugging ike** 用来关闭 IKE 调试开关。

缺省情况下，IKE 调试开关关闭。

【举例】

打开 IKE 错误信息调试开关。

```
<SecBlade_VPN> debugging ike error
```

4.1.4 dh

【命令】

dh { **group1** | **group2** | **group5** | **group14** }

undo dh

【视图】

IKE 提议视图

【参数】

group1：指定阶段 1 密钥协商时采用 768-bit 的 Diffie-Hellman 组。

group2：指定阶段 1 密钥协商时采用 1024-bit 的 Diffie-Hellman 组。

group5：指定阶段 1 密钥协商时采用 1536-bit 的 Diffie-Hellman 组。

group14：指定阶段 1 密钥协商时采用 2048-bit 的 Diffie-Hellman 组。

【描述】

命令 **dh** 用来配置 IKE 阶段 1 密钥协商时所使用的 DH 密钥交换参数，命令 **undo dh** 用来设置 Diffie-Hellman 组标识为缺省值。

缺省为 group1，即 768-bit 的 Diffie-Hellman 组。

相关配置可参考命令 **ike proposal**，**display ike proposal**。

【举例】

指定 IKE 提议 10 使用 768-bit 的 Diffie-Hellman 组。

```
[SecBlade_VPN] ike proposal 10
[SecBlade_VPN-ike-proposal-10] dh group1
```

4.1.5 display ike peer

【命令】

display ike peer [*peer-name*]

【视图】

所有视图

【参数】

peer-name：IKE 对等体名，取值范围为长度 1~15 的字符串。

【描述】

display ike peer 命令用来显示 IKE 对等体的相关配置信息。

【举例】

显示 ike 对等体的相关配置信息。

```
[SecBlade_VPN-ike-peer-good] display ike peer

---------------------------
 IKE Peer: good
   exchange mode: main on phase 1
   pre-shared-key:
   peer id type: ip
   peer ip address: 0.0.0.0 ~ 255.255.255.255
   peer name:
   nat traversal: disable
---------------------------
```

4.1.6 display ike proposal

【命令】

display ike proposal

【视图】

所有视图

【参数】

无

【描述】

命令 **display ike proposal** 用来显示每个 IKE 提议配置的参数。

IKE 提议按照优先级的先后顺序显示。

相关配置可参考命令 **authentication-method**，**ike proposal**，**encryption-algorithm**，**authentication-algorithm**，**dh**，**sa duration**。

【举例】

下面是一个配置了两条 IKE 提议后显示的例子。

```
[SecBlade_VPN] display ike proposal
priority authentication authentication encryption Diffie-Hellman duration
             method       algorithm    algorithm     group       (seconds)
------------------------------------------------------------------------------
 10       PRE_SHARED     SHA            DES_CBC    MODP_1024      5000
 11       PRE_SHARED     MD5            DES_CBC    MODP_768       50000
 default  PRE_SHARED     SHA            DES_CBC    MODP_768       86400
```

4.1.7 display ike sa

【命令】

display ike sa [**verbose** [**connection-id** *id* | **remote-address** *ip-address*]]

【视图】

所有视图

【参数】

verbose：显示 IKE 安全联盟的详细信息。

connection-id *id*：IKE 安全联盟的连接号。

remote-address *ip-address*：IKE 安全联盟的对端 IP 地址。

【描述】

命令 **display ike sa** 用来显示当前由 IKE 建立的安全隧道。

相关配置可参考命令 **ike proposal**。

【举例】

显示当前由 IKE 建立的安全通道。

```
[SecBlade_VPN] display ike sa
```

```
    Total IKE phase-1 SAs:  1
conn-id      peer          flag         phase     doi
1            202.38.0.2      RD|ST        1         IPSEC
2            202.38.0.2      RD|ST        2         IPSEC
flag meaning:
RD--READY ST--STAYALIVE RL--REPLACED FD—FADING TO--TIMEOUT
```

下表为显示信息各域的描述。

表4-1 IKE SA 显示信息描述

域名	描述
conn-id	安全通道的标识符
peer	此安全联盟的对端的 IP 地址
flag	显示此安全联盟的状态： RD（READY）：表示此 SA 已建立成功； ST（STAYALIVE）：表示此端是通道协商发起方； RL（REPLACED）：表示此通道已经被新的通道代替，一段时间后将被删除； FD（FADING）：表示此通道已发生过一次软超时，目前还在使用，在硬超时发生时，会删除此通道。 TO（TIMEOUT）：表示此 SA 在上次 keepalive 超时发生后还没有收到 keepalive 报文，如果在下次 keepalive 超时发生时仍没有收到 keepalive 报文，此 SA 将被删除。
phase	此 SA 所属阶段： Phase 1：建立安全通道进行通信的阶段，此阶段建立 ISAKMP SA； Phase 2：协商安全服务的阶段，此阶段建立 IPSec SA。
doi	SA 所属解释域

4.1.8 encryption-algorithm

【命令】

encryption-algorithm { **des-cbc** | **3des-cbc** | **aes-cbc** }

undo encryption-algorithm

【视图】

IKE 提议视图

【参数】

des-cbc：指定 IKE 安全提议采用的加密算法为 CBC 模式的 DES 算法，DES 算法采用 56 bits 的密钥进行加密。

3des-cbc：指定 IKE 安全提议采用的加密算法为 CBC 模式的 3DES 算法。3DES 算法采用 168 bits 的密钥进行加密。

aes-cbc：指定 IKE 安全提议采用的加密算法为 CBC 模式的 AES 算法。

【描述】

命令 **encryption-algorithm** 用来指定一个 IKE 提议使用的加密算法，命令 **undo encryption-algorithm** 用来设置加密算法为缺省值。

缺省情况下，使用 CBC 模式的 56-bit DES 加密算法。

相关配置可参考命令 **ike proposal**，**display ike proposal**。

【举例】

指定 IKE 提议 10 的加密算法为 CBC 模式的 56-bit DES。

```
[SecBlade_VPN] ike proposal 10
[SecBlade_VPN-ike-proposal-10] encryption-algorithm des-cbc
```

4.1.9 exchange-mode

【命令】

exchange-mode { **aggressive** | **main** }

undo exchange-mode

【视图】

ike-peer 视图

【参数】

aggressive：野蛮模式

main：主模式

【描述】

exchange-mode 命令用于选择 ike 阶段的协商模式，**undo exchange-mode** 命令用来恢复缺省的协商模式。缺省情况下使用主模式。

在主模式下，只能使用 ip 地址进行 IKE 协商建立 SA，这种模式用于隧道两端都有固定 IP 地址的情况。

在 IKE 野蛮模式下，不但可以使用 ip 地址进行协商，也可以使用名字进行 IKE 协商建立 SA。当安全隧道一端的 IP 地址为自动获取时（如一端用户为拨号方式），则协商模式必须配置为 **aggressive**。这种情况下，只要建立 SA 时使用的用户名和密码正确，就可以建立 SA。

当响应方使用策略模板接受发起方的协商请求时，会根据发起方的协商模式而进行选择。

相关配置可参考命令 **id-type**。

【举例】

配置 IKE 使用主模式。

```
[SecBlade_VPN] ike peer new_peer
[SecBlade_VPN-ike-peer-new_peer] exchange-mode main
```

4.1.10 id-type

【命令】

id-type { **ip** | **name** }

undo id-type

【视图】

ike-peer 视图

【参数】

ip：选择 IP 地址作为 ike 协商过程中使用的 ID。

name：选择名字作为 ike 协商过程中使用的 ID。

【描述】

id-type 命令用于选择 ike 协商过程中使用的 ID 的类型，**undo id-type** 命令恢复缺省设置。缺省情况下使用 ip 地址作为 ike 协商过程中使用的 ID。

在主模式下，只能使用 ip 地址进行 IKE 协商，建立 SA。

在 IKE 野蛮模式下，不但可以使用 ip 地址进行协商，也可以使用名字进行 IKE 协商，建立 SA。

相关配置可参考命令 **ike local-name**。

【举例】

配置使用名字作为 IKE 协商的依据。

```
[SecBlade_VPN] ike peer new_peer
[SecBlade_VPN-ike-peer-new_peer] id-type name
```

4.1.11 ike encrypt-card dh-computation disabled

【命令】

ike encrypt-card dh-computation disabled

undo ike encrypt-card dh-computation disabled

【视图】

系统视图

【参数】

无

【描述】

ike encrypt-card dh-computation disabled 命令用来禁止 DH 交换的硬件加速，改用软件处理。**undo ike encrypt-card dh-computation disabled** 命令用来使能 DH 交换的硬件加速。

缺省情况下，使能 DH 交换的硬件加速。

【举例】

禁止 DH 交换的硬件加速。

```
[H3C] ike encrypt-card dh-computation disabled
```

4.1.12 ike local-name

【命令】

ike local-name *name*

undo ike local-name

【视图】

系统视图

【参数】

name：指定 IKE 协商时的本端网关的名字，取值为 1～32 个字符。

【描述】

ike local-name 命令用于配置本端网关的名字，**undo ike local**-name 用来恢复本端网关的缺省名字。缺省情况下，直接使用 SecBlade 名作为本端网关的名字。

当 IKE 协商的发起端使用网关名字进行协商时（即配置了 **id-type name**），本端需要配置命令 **ike local**-name。

相关配置可参考命令 **remote-name**。

【举例】

```
[SecBlade_VPN] ike local-name beijing_VPN
```

4.1.13 ike next-payload check disabled

【命令】

ike next-payload check disabled

undo ike next-payload check disabled

【视图】

系统视图

【参数】

无

【描述】

ike next-payload check disabled 命令用来配置在 IPSec 协商过程中取消对最后一个 payload 的 next payload 域的检查，以便与某些公司的产品互通。**undo ike next-payload check disabled** 命令用来恢复缺省设置。

缺省情况下，检查 next payload 域。

next-payload 是指在 IKE 协商报文（由几个 payload 组装而成）的最后一个 payload 的通用头中 Next Payload 域。按协议规定该域必须为 0，但某些公司的设备会将该域赋其它值，为增强设备的互通性，可以通过 **ike next-payload check disabled** 命令取消 IPSec 协商过程对该域的检查。

【举例】

配置在 IPSec 协商过程中取消对最后一个 payload 的 next payload 域的检查。

```
[SecBlade_VPN] ike next-payload check disabled
```

4.1.14 ike peer

【命令】

ike peer *peer-name*

undo ike peer *peer-name*

【视图】

系统视图

【参数】

peer-name：ike 对等体名，最多 15 个字符。

【描述】

ike peer 命令用于配置一个 ike 对等体，并进入 ike peer 视图，**undo ike peer** 命令用于删除一个 ike 对等体。

【举例】

配置 ike 对等体为 new_peer，并进入 ike peer 视图。

```
[SecBlade_VPN] ike peer new_peer
[SecBlade_VPN-ike-peer-new]
```

4.1.15 ike-peer

【命令】

ike-peer *peer-name*

undo ike-peer [*peer-name*]

【视图】

安全策略视图、安全策略模板视图

【参数】

peer-name：ike 对等体名，最多 15 个字符。

【描述】

ike-peer 命令用于在安全策略或安全策略模板中引用 ike 对等体，**undo ike peer** 命令用于取消在安全策略或安全策略模板中引用 ike 对等体。

相关配置可参考命令 **ipsec policy**。

【举例】

配置在安全策略中引入 ike 对等体。

```
[SecBlade_VPN-ipsec-policy-isakmp-policy-10] ike-peer new_peer
```

4.1.16 ike proposal

【命令】

ike proposal *proposal-number*

undo ike proposal *proposal-number*

【视图】

系统视图

【参数】

proposal-number：IKE 提议序号，取值为 1～100。该序号同时表示优先级，数值越小，优先级越高。在进行 ike 协商的时候，会从序号最小的 Ike 提议进行匹配，如果匹配则直接使用，否则继续查找。

【描述】

命令 **ike proposal** 用来定义一个 IKE 提议。命令 **undo ike proposal** 用来删除一个 IKE 提议。

缺省情况下，系统提供一条缺省的 IKE 提议，此缺省的 IKE 提议具有最低的优先级。

在系统视图下，使用此命令后，将进入 IKE 提议视图。在 IKE 提议视图下，可以使用 **authentication-method** 、 **encryption-algorithm** 、 **dh** 、 **authentication-algorithm** 和 **sa duration** 命令为 IKE 提议定义一系列的参数，包括认证方法、加密算法、认证算法、DH 组标识和生存周期。

缺省的提议具有缺省的参数，如下：

```
Encryption algorithm: DES-CBC
Authentication algorithm: HMAC-SHA1
Authentication method: Pre-Shared Key
DH group ID: MODP_768
SA duration: 86400 seconds
```

这些参数在经过两端协商达成一致后，被用来建立一条安全通道。

配置的 IKE 提议将被用来建立安全通道。执行此命令会进入 IKE 提议视图，配置参数。

可以为进行 IKE 协商的每一端配置多条 IKE 提议，在协商时，将从优先级最高的提议开始，匹配双方都相同的提议。匹配的原则是：协商双方具有相同的加密算法、认证算法、认证方法和 DH 组标识，存活时间是由协商发起方决定的，两端不需要匹配。

相关配置可参考命令 **authentication-method**，**encryption-algorithm**，**dh**，**authentication-algorithm**，**sa duration**，**display ike proposal**。

【举例】

以下命令定义了一条 IKE 提议 10。

```
[SecBlade_VPN] ike proposal 10
[SecBlade_VPN-ike-proposal-10] authentication-algorithm md5
[SecBlade_VPN-ike-proposal-10] authentication-method pre-share
[SecBlade_VPN-ike-proposal-10] sa duration 5000
```

4.1.17 ike sa keepalive-timer interval

【命令】

ike sa keepalive-timer interval *seconds*

undo ike sa keepalive-timer interval

【视图】

系统视图

【参数】

seconds：指定通过 ISAKMP SA 向对端发送 Keepalive 报文的时间间隔。可以设定为 20 到 28800 之间的一个值。

【描述】

命令 **ike sa keepalive-timer interval** 用来配置通过 ISAKMP SA 向对端发送 Keepalive 报文的时间间隔，命令 **undo ike sa keepalive-timer interval** 用来使此功能失效。

缺省情况下，此功能无效。

配置通过 ISAKMP SA 向对端发送 Keepalive 报文的时间间隔。IKE 通过此报文维护 ISAKMP SA 的隧道状态。一般在对端使用命令 **ike sa keepalive-timer timeout** 配置了超时时间时，必须在本端配置此 Keepalive 报文发送时间间隔。当对端在配置的超时时间到后，如果对端的 ISAKMP SA 无 TIMEOUT 标记，则将其标记为 TIMEOUT，当对端再收到本端 keepalive-timer 时间到后发送的 keepalive 报文，将清除 TIMEOUT 标记；如果对端的 ISAKMP SA 已带有 TIMEOUT 标记，说明在超时时间内未收到 Keepalive 报文，则删除该 ISAKMP SA 以及对应的 IPSec SA。所以，在配置时，需使配置的超时时间比 Keepalive 报文发送时间长。

相关配置可参考命令 **ike sa keepalive-timer timeout**。

【举例】

配置本端向对端发送 Keepalive 报文的时间间隔为 20 秒。

```
[SecBlade_VPN] ike sa keepalive-timer interval 20
```

4.1.18 ike sa keepalive-timer timeout

【命令】

ike sa keepalive-timer timeout *seconds*

undo ike sa keepalive-timer timeout

【视图】

系统视图

【参数】

seconds：指定 ISAKMP SA 等待对端发送 Keepalive 报文的超时时间。可以设定为 20 到 28800 之间的一个值。

【描述】

命令 **ike sa keepalive-timer timeout** 用来配置一个 ISAKMP SA 等待 Keepalive 报文的超时时间，命令 **undo ike sa keepalive-timer timeout** 用来使此功能失效。

缺省情况下，此功能无效。

配置等待对端发送 Keepalive 报文的超时时间。IKE 通过此报文维护该条 ISAKMP SA 的链路状态。当对端在配置的超时时间到后，如果对端的 ISAKMP SA 无 TIMEOUT 标记，则将其标记为 TIMEOUT，当对端再收到本端 keepalive-timer 时间到后发送的 keepalive 报文，将清除 TIMEOUT 标记；如果对端的 ISAKMP SA 已带有 TIMEOUT 标记，说明在超时时间内未收到 Keepalive 报文，则删除该 ISAKMP SA 以及对应的 IPSec SA。所以，在配置时，需使配置的超时时间比 Keepalive 报文发送时间长。

在网络上，一般不会出现超过连续三次的报文丢失，所以，配置超时时间时，可以采用对端配置的 Keepalive 报文发送时间间隔的三倍。

相关配置可参考命令 **ike sa keepalive-timer interval**。

【举例】

配置本端等待对端发送 Keepalive 报文的超时时间为 20 秒。

```
[SecBlade_VPN] ike sa keepalive-timer timeout 20
```

4.1.19 ike sa nat-keepalive-timer interval

【命令】

ike sa nat-keepalive-timer interval *seconds*

undo ike sa nat-keepalive-timer interval

【视图】

系统视图

【参数】

seconds：IKE 对等体发送 NAT Keepalive 报文的时间间隔，范围为 5～300，单位为秒。

【描述】

ike sa nat-keepalive-timer interval 命令用来配置 IKE 对等体发送 NAT Keepalive 报文的时间间隔，**undo ike sa nat-keepalive-timer interval** 命令用来恢复发送 NAT Keepalive 报文的时间间隔为缺省值。

当配置此命令时，要确保配置的时间间隔小于 NAT 转换的超时时间。

缺省情况下，IKE 对等体发送 NAT Keepalive 报文的时间间隔为 20 秒。

【举例】

配置 IKE 对等体发送 NAT Keepalive 报文的时间间隔为 30 秒。

```
[SecBlade_VPN] ike sa nat-keepalive-timer interval 30
```

4.1.20 local

【命令】

local { **multi-subnet** | **single-subnet** }

undo local

【视图】

ike-peer 视图

【参数】

multi-subnet：指定多子网类型。

single-subnet：指定单子网类型。

【描述】

local 命令用来配置 IKE 协商时的子网类型，**undo local** 命令用来恢复缺省的子网类型。本命令用于与 NETSCREEN 设备互通时使用。

缺省情况下，为单子网类型。

【举例】

配置 IKE 协商时的子网类型为多子网类型。

```
[SecBlade_VPN-ike-peer-xhy] local multi-subnet
```

4.1.21 local-address

【命令】

local-address *ip-address*

undo local-address

【视图】

ike-peer 视图

【参数】

ip-address： IKE 协商时的本端网关的 IP 地址。

【描述】

local-address 命令用来配置 IKE 协商时的本端网关的 IP 地址，**undo local-address** 命令用来取消本端网关的 IP 地址。

一般情况下 **local-address** 不需要配置，只有当用户需要指定特殊的本端网关地址时才需要配置此命令。

【举例】

配置本端网关 IP 地址为 1.1.1.1。

```
[SecBlade_VPN-ike-peer-xhy] local-address 1.1.1.1
```

4.1.22 nat traversal

【命令】

nat traversal

undo nat traversal

【视图】

ike-peer 视图

【参数】

无

【描述】

nat traversal 用于配置 IPSec/IKE 的 NAT 穿越功能，**undo nat traversal** 用来取消 IPSec/IKE 的 NAT 穿越功能。

此命令适用于 IPSec/IKE 组建的 VPN 隧道中加入了 NAT 网关的情况。

为了节省 IP 地址空间，ISP 经常会在公网中加入 NAT 网关，以便于将私有 IP 地址分配给用户，此时可能会导致 IPSec/IKE 隧道的两端一端为公网地址，另一端为私网地址，所以必须在私网侧配置 NAT 穿越，保证隧道能够正常协商建立。

【举例】

```
[SecBlade_VPN] ike peer new_peer
[SecBlade_VPN-ike-peer-new_peer] nat traversal
```

4.1.23 pre-shared-key

【命令】

pre-shared-key *key*

undo pre-shared-key

【视图】

ike-peer 视图

【参数】

key：指定的身份认证字，取值范围为 1～128 个字符。

【描述】

pre-shared-key 命令用于配置 ike 协商所使用的身份认证字，**undo pre-shared-key** 命令用来取消 ike 协商所使用的身份认证字。

【举例】

配置 ike 协商所使用的身份认证字为 abcde。

```
[SecBlade_VPN] ike peer new_peer
[SecBlade_VPN-ike-peer-new_peer] pre-shared-key abcde
```

4.1.24 peer

【命令】

peer { **multi-subnet** | **single-subnet** }

undo peer

【视图】

ike-peer 视图

【参数】

multi-subnet：指定多子网类型。

single-subnet：指定单子网类型。

【描述】

peer 命令用来配置 IKE 协商时的子网类型，**undo peer** 命令用来恢复缺省的子网类型。本命令用于与 NETSCREEN 设备互通时使用。

缺省情况下，为单子网类型。

【举例】

配置 IKE 协商时的子网类型为多子网类型。

```
[SecBlade_VPN-ike-peer-xhy] peer multi-subnet
```

4.1.25 remote-address

【命令】

remote-address *low-ip-address* [*high-ip-address*]

undo remote-address

【视图】

ike-peer 视图

【参数】

low-ip-address：起始 IP 地址。

high-ip-address：结束 IP 地址。

【描述】

remote-address 用于配置对端网关设备的 IP 地址，**undo remote-address** 用来删除对端网关设备的 IP 地址。

当 IKE 协商的发起端使用地址进行协商时（即配置了 **id-type ip**），发起端会发送自己的 IP 地址给对端来标识自己的身份，而响应端使用 **remote-address** *low-ip-address* [*high-ip-address*]来验证发起端。若响应端只配置了 *low-ip-address* 时，*low-ip-address* 应与发起端上 **local-address** 命令所配的 IP 地址保持一致；若响应端配置了 *low-ip-address* 和 *high-ip-address*，即配置了一个地址范围时，此地址范围应包含发起端上 **local-address** 命令所配置的 IP 地址。IKE 协商的发起端不能配置 **remote-address** 为地址范围。

【举例】

配置对端网关设备 IP 地址为 10.0.0.1。

```
[SecBlade_VPN] ike peer new_peer
[SecBlade_VPN-ike-peer-new_peer] remote-address 10.0.0.1
```

4.1.26 remote-name

【命令】

remote-name *name*

undo remote-name

【视图】

ike-peer 视图

【参数】

name：指定 IKE 协商时对端的名字，取值范围为 1～32 字符。

【描述】

remote-name 用于配置对端网关的名字，**undo remote-name** 用来删除网关名称。

当 IKE 协商的发起端使用网关名字进行协商时（即配置了 **id-type name**），发起端会发送自己名字给对端来标识自己的身份，而对端使用 **remote-name** *name* 来验证发起端，故此时 *name* 应与发起端上 **ike local-name** 命令所配的名字保持一致。

【举例】

```
[SecBlade_VPN] ike peer new_peer
[SecBlade_VPN-ike-peer-new_peer] remote-name beijing
```

4.1.27 reset ike sa

【命令】

reset ike sa [*connection-id*]

【视图】

用户视图

【参数】

connection-id：指定要删除的安全隧道的连接 ID 号。如果未指定此参数，所有的阶段 1 的 SA 都会被删除。

【描述】

命令 **reset ike sa** 用来删除 IKE 建立的安全隧道。

如果未指定 *connection-id*，所有阶段 1 的 SA 都会被删除。删除本地的安全隧道时，如果阶段 1 的 ISAKMP SA 还存在，将在此安全通道的保护下，向对端发送删除消息，通知对方清除相应的安全联盟。

IKE 使用了两个阶段的 ISAKMP：第一阶段建立 IKE 安全联盟，即 ISAKMP SA；第二阶段使用这个已经建立的 ISAKMP SA 为 IPSec 协商安全联盟，即建立 IPSec SA。

相关配置可参考命令 **display ike sa**。

【举例】

删除一个到 202.38.0.2 的安全通道。

```
<SecBlade_VPN> display ike sa
    Total IKE phase-1 SAs:  1
conn-id      remote          flag         phase     doi
1            202.38.0.2      RD|ST        1         IPSEC
2            202.38.0.2      RD|ST        2         IPSEC
flag meaning:
RD--READY ST--STAYALIVE RL--REPLACED FD—FADING TO--TIMEOUT
<SecBlade_VPN> reset ike sa 2
<SecBlade_VPN> display ike sa
    Total IKE phase-1 SAs:  1
conn-id      remote        flag           phase      doi
1            202.38.0.2    RD|ST          1          IPSEC
flag meaning:
RD--READY ST--STAYALIVE RL--REPLACED FD—FADING TO—TIMEOUT
```

⚠ 注意：

如果先删除阶段 1 的 SA，那么在删除阶段 2 的 SA 时，就无法通知对方清除相应的 SA。

4.1.28 sa duration

【命令】

sa duration *seconds*

undo sa duration

【视图】

IKE 提议视图

【参数】

seconds：指定 ISAKMP SA 存活时间，sa duration 时间超时时 ISAKMP SA 将自动更新。可以设定为 60 秒到 604800 秒之间的一个值。

【描述】

命令 **sa duration** 用来指定一个 IKE 提议的 ISAKMP SA 存活时间，命令 **undo sa duration** 用来设置 ISAKMP SA 存活时间为缺省值。

缺省值为 86400 秒（一天）。

在设定的存活时间超时前，会提前协商另一个 SA 来替换旧的 SA。在新的 SA 还没有协商完之前，依然使用旧的 SA；在新的 SA 建立后，将立即使用新的 SA，而旧的 SA 在存活时间超时时，被自动清除。

相关配置可参考命令 **ike proposal**，**display ike proposal**。

【举例】

指定 IKE 提议 10 的 ISAKMP SA 存活时间 600 秒（10 分钟）。

```
[SecBlade_VPN] ike proposal 10
[SecBlade_VPN-ike-proposal-10] sa duration 600
```

第5章 PKI 配置命令

5.1 PKI 域配置命令

5.1.1 ca identifier

【命令】

ca identifier *name*

undo ca identifier

【视图】

PKI 域视图

【参数】

name：本设备信任的 CA 标识符。长度范围 1～63 字符。

【描述】

ca identifier 命令用来指定本设备信任的 CA，将本设备与名称为 *name* 的 CA 进行绑定。**undo ca identifier** 命令用来删除本设备信任的 CA。

缺省情况下，未指定本设备信任的 CA。

在未删除该 CA 之前，该设备证书的申请、获取、撤消及查询均是通过该 CA 执行。

【举例】

指定本设备信任的 CA 的名称。

```
[SecBlade_VPN-pki-domain-1] ca identifier new-ca
```

5.1.2 certificate request entity

【命令】

certificate request entity *entity-name*

undo certificate request entity

【视图】

PKI 域视图

【参数】

entity-name：申请证书所用的实体名称，该名称必须与 **pki entity** 命令定义的名字保持一致。长度范围 1～15 字符。

【描述】

certificate request entity 命令用来指定申请证书所用的实体名称，**undo certificate request entity** 命令用来取消申请证书所用的实体名称。

缺省情况下，未指定设备申请证书所使用的实体名称。

相关命令请参考 **pki entity**。

【举例】

指定设备申请证书时使用实体“en”

```
[SecBlade_VPN-pki-domain-1] certificate request entity en
```

5.1.3 certificate request from

【命令】

certificate request from { **ca** | **ra** }

undo certificate request from

【视图】

PKI 域视图

【参数】

ca：表示实体从 CA 注册申请证书。

ra：表示实体从 RA 注册申请证书。

【描述】

certificate request from 命令用来为实体指定是通过 CA 还是 RA 注册申请证书。**undo certificate request from** 命令用来删除所选定的证书注册受理机构。

RA 是 CA 证书发放管理的延伸，它负责证书申请者的信息录入、审核以及证书发放等工作，但其并无证书的签发功能。在一些小的 PKI 系统中，RA 的职能可由 CA 来完成，而不设立独立运行的 RA。

缺省情况下，未指定本设备证书申请的注册受理机构。PKI 安全策略推荐使用 RA 作为注册审理机构。

【举例】

指定实体从 CA 注册申请证书。

```
[SecBlade_VPN-pki-domain-1] certificate request from ca
```

5.1.4 certificate request mode

【命令】

certificate request mode { **manual** | **auto** [**key-length** *key-length* | **password** { **simple** | **cipher** } *password*]* }

undo certificate request mode

【视图】

PKI 域视图

【参数】

manual：表示用手工方式申请证书。

auto：表示用自动方式申请证书。

key-length：指定 RSA 密钥长度，最小长度为 512 位，最大长度为 2048 位。

simple：指定密码以明文形式显示。

cipher：指定密码以加密形式显示。

password：指定吊销证书时使用的密码，长度为 1～31 个字符。

【描述】

certificate request mode 命令用来指定证书申请是手工发起，还是自动发起。**undo certificate request mode** 命令用来恢复证书申请方式为缺省值。

如果是自动方式，则在本地没有自己的证书时自动向注册机构进行申请，而且在证书快要过期时自动申请新的证书。如果为手工方式，则需要手工完成各项证书申请工作。

缺省情况下，证书申请为手工方式。

相关命令请参考 **pki request-certificate**。

【举例】

指定证书申请为自动发起方式。

```
[SecBlade_VPN-pki-domain-1] certificate request mode auto
```

5.1.5 certificate request polling

【命令】

certificate request polling { **interval** *minutes* | **count** *count* }

undo certificate request polling { **interval** | **count** }

【视图】

PKI 域视图

【参数】

minutes：指定两次查询之间的时间间隔。单位分钟，取值范围为 5～60 分钟，缺省为 20 分钟。

count：重试次数。取值范围为 1～100，缺省为 50。

【描述】

certificate request polling 命令用来指定两次状态查询之间的时间间隔以及重传次数。**undo certificate request polling** 命令用来恢复缺省参数。

在发送证书申请后，如果 CA 采用手工验证申请，会需要很长时间才能发布证书，客户端需要定期发送状态查询，以便在证书签发后能及时获取到证书。

相关命令请参考 **display pki certificate**。

【举例】

指定两次状态查询之间的时间间隔和查询重试次数。

```
[SecBlade_VPN-pki-domain-1] certificate request polling interval 15
[SecBlade_VPN-pki-domain-1] certificate request polling count 40
```

5.1.6 certificate request url

【命令】

certificate request url *string*

undo certificate request url

【视图】

PKI 域视图

【参数】

string：表示证书申请的注册机构服务器位置 URL。长度范围 1～255 字符。内容包括服务器位置及 CA 的 CGI 命令接口脚本位置，格式为 *http://server_location /ca_script_location*。其中 *server_location* 一般用 IP 地址表示，若要用服务器名字表示，请配置 DNS 以实现网络 IP 地址和名称的转换匹配。

【描述】

certificate request url 命令用来指定本设备通过 SCEP 协议进行证书申请的服务器位置 URL，SCEP 是专门用于与认证权威机构进行通信的协议。**undo certificate request url** 命令用来删除证书申请的服务器位置。

缺省情况下，未指定证书申请机构的服务器位置 URL。

【举例】

指定证书申请的服务器位置。

```
[SecBlade_VPN-pki-domain-1] certificate request url
http://169.254.0.100/certsrv/mscep/mscep.dll
```

5.1.7 crl check disable

【命令】

crl check disable

undo crl check disable

【视图】

PKI 域视图

【参数】

无

【描述】

crl check disable 命令用来禁止 CRL 检查，**undo crl check disable** 命令用来使能 CRL 检查。

缺省情况下，使能 CRL 检查。

【举例】

禁止 CRL 检查。

```
[SecBlade_VPN-pki-domain-1] crl check disable
```

5.1.8 crl update-period

【命令】

crl update-period *hours*

undo crl update-period

【视图】

PKI 域视图

【参数】

hours：指定更新周期，单位为“小时”。

【描述】

crl update-period 指定 CRL 的更新周期，CRL 的更新周期是指本地从 CRL 存储服务器上下载 CRL 的时间间隔。**undo crl update-period** 命令用来恢复 CRL 更新周期为缺省值。

缺省情况下，根据 CRL 的有效期进行更新。

【举例】

指定 CRL 的更新周期为 20 小时。

```
[SecBlade_VPN-pki-domain-1] crl update-period 20
```

5.1.9 crl url

【命令】

crl url { *url-string* | **scep** }

undo crl url

【视图】

PKI 域视图

【参数】

url-string：表示 CRL 的发布点位置，长度范围 1～127 字符。格式为 *http://server_location* 或 *ldap://server_location*，其中 *server_location* 一般用 IP 地址表示，若要用服务器名字表示，请配置 DNS 以实现网络 IP 地址和名称的匹配。

scep：使用 SCEP 获取 CRL。

【描述】

crl url 命令用来设置 CRL 发布点位置 URL。**undo crl url** 命令用来撤消该 URL。

缺省情况下，未指定 CRL 发布点位置 URL。

【举例】

指定 CRL 库的 URL 位置。

```
[SecBlade_VPN-pki-domain-1] crl url
http://192.168.19.2/certenroll/win2000.crl
```

5.1.10 ldap-server

【命令】

ldap-server ip *ip-address* [**port** *port-num*] [**version** *version-number*]

undo ldap-server

【视图】

PKI 域视图

【参数】

ip-address：LDAP 服务器的 IP 地址。

port-num：LDAP 服务器的端口号。取值范围 1～65535，缺省为 389。

version-number：LDAP 版本号。可取值为 2 或 3，缺省为 2。

【描述】

ldap-server ip 命令设置 LDAP 服务器地址及端口。**undo ldap-server** 命令撤消 LDAP 服务器地址及端口。

缺省情况下，未指定 LDAP 服务器的 IP 地址及端口。

【举例】

指定 LDAP 服务器的位置。

```
[SecBlade_VPN-pki-domain-1] ldap-server ip 169.254.0 30
```

5.1.11 pki domain

【命令】

pki domain *name*

undo pki domain *name*

【视图】

系统视图

【参数】

name：该参数为本设备指定一个 PKI 域名字，用于表示本设备是属于哪一个 PKI 域，供其它命令引用时指定。长度范围 1～15 字符。

【描述】

pki domain 命令用来进入 PKI 域视图，在该视图中可配置 LDAP 服务器、证书申请及证书验证等参数。**undo pki domain** 命令用来删除指定的 PKI 域。

缺省情况下，未指定 PKI 域名。

【举例】

进入 PKI 域视图。

```
[SecBlade_VPN] pki domain 1
[SecBlade_VPN-pki-domain-1]
```

5.1.12 root-certificate fingerprint

【命令】

root-certificate fingerprint { **md5** | **sha1** } *string*

undo root-certificate fingerprint

【视图】

PKI 域视图

【参数】

md5：使用 MD5 指纹。

sha1：使用 SHA1 指纹。

string：指定所使用的指纹。当选择 MD5 指纹时，*string* 必须为 32 个字符，并且以 16 进制的形式输入；当选择 SHA1 指纹时，*string* 必须为 40 个字符，并且以 16 进制的形式输入。

【描述】

root-certificate fingerprint 命令用来配置验证 CA 根证书时所使用的指纹，**undo root-certificate fingerprint** 命令用来取消配置的指纹。

缺省情况下，未配置验证 CA 根证书时使用的指纹。

【举例】

配置验证 CA 根证书时使用的 MD5 指纹。

```
[SecBlade_VPN-pki-domain-1] root-certificate fingerprint md5
12EF53FA355CD23E12EF53FA355CD23E
```

配置验证 CA 根证书时使用的 SHA1 指纹。

```
[SecBlade_VPN-pki-domain-1] root-certificate fingerprint sha1
D1526110AAD7527FB093ED7FC037B0B3CDDDAD93
```

5.2 PKI 实体配置命令

5.2.1 fqdn

【命令】

fqdn *name-str*

undo fqdn

【视图】

PKI 实体视图

【参数】

name-str：实体的 FQDN 名。长度范围 1～255 字符。

【描述】

fqdn 命令用来指定实体的 FQDN 名称。**undo fqdn** 命令用来删除实体的 FQDN 名称。

缺省情况下，未指定实体 FQDN。

FQDN（Fully Qualified Domain Name）是实体在网络中的唯一标识，如 email 地址，可被解析为 IP 地址，一般形式为：user.domain。

【举例】

配置实体的 FQDN。

```
[SecBlade_VPN-pki-entity-1] fqdn pki.h3c.com
```

5.2.2 common-name

【命令】

common-name *name-str*

undo common-name

【视图】

PKI 实体视图

【参数】

name-str：实体的通用名称。长度范围 1～31 字符。

【描述】

common-name 命令用来指定实体的通用名。比如用户名字。**undo common-name** 命令用来删除实体的通用名。

缺省情况下，未指定实体通用名。

【举例】

配置实体的通用名。

```
[SecBlade_VPN-pki-entity-1] common-name pki test
```

5.2.3 country

【命令】

country *country-code-str*

undo country

【视图】

PKI 实体视图

【参数】

country-code-str：2 字节国家代码。

【描述】

country 命令用来指定实体所属的国家代码，代码用标准的 2 字符代码。例如，中国为“CN”。**undo country** 命令用来删除实体所属的国家代码。

缺省情况下，未指定实体所属国家代码。

【举例】

配置实体所属的国家代码。

```
[SecBlade_VPN-pki-entity-1] country CN
```

5.2.4 ip

【命令】

ip *ip-address*

undo ip

【视图】

PKI 实体视图

【参数】

ip-address：实体的 IP 地址。IP 地址为点分十进制形式，如 A.B.C.D。

【描述】

ip 命令用来指定实体的 IP 地址。**undo ip** 命令用来删除实体的 IP 地址。

缺省情况下，未指定实体 IP 地址。

【举例】

配置实体的 IP 地址。

```
[SecBlade_VPN-pki-entity-1] ip 161.12.2.3
```

5.2.5 locality

【命令】

locality *locality-str*

undo locality

【视图】

PKI 实体视图

【参数】

locality-str：地理区域的名称。长度范围 1～31 字符。

【描述】

locality 命令用来指定实体所在的地理区域的名称，比如城市名称。**undo locality** 命令用来删除实体所在的地理区域的名称。

缺省情况下，未指定实体所在地理区域。

【举例】

配置实体所在城市名称。

```
[SecBlade_VPN-pki-entity-1] locality bei jing
```

5.2.6 organization

【命令】

organization *org-str*

undo organization

【视图】

PKI 实体视图

【参数】

org-str：组织名称。长度范围 1～31 字符。

【描述】

organization 命令用来指定实体所属组织的名称。**undo organization** 命令用来删除实体所属组织的名称。

缺省情况下，未指定实体所属组织。

【举例】

配置实体所属组织名称。

```
[SecBlade_VPN-pki-entity-1] organization hua wei – 3com
```

5.2.7 organization-unit

【命令】

organization-unit *org-unit-str*

undo organization-unit

【视图】

PKI 实体视图

【参数】

org-unit-str：组织部门的名称。长度范围 1～31 字符。

【描述】

organization-unit 命令用来指定实体所属的组织部门的名称。**undo organization-unit** 命令用来删除实体所属的组织部门的名称。

缺省情况下，未指定实体所属部门。

【举例】

配置实体所属组织部门名称。

```
[SecBlade_VPN-pki-entity-1] organization-unit soft plat
```

5.2.8 state

【命令】

state *state-str*

undo state

【视图】

PKI 实体视图

【参数】

state-str：州或省的名称。长度范围 1～31 字符。

【描述】

state 命令指定实体所属的州或省的名称。**undo state** 命令用来

删除此配置。

缺省情况下，未指定实体所在州或省。

【举例】

配置实体所在省。

```
[SecBlade_VPN-pki-entity-1] state bei jing
```

5.2.9 pki entity

【命令】

pki entity *name-str*

undo pki entity *name-str*

【视图】

所有视图

【参数】

name-str：本设备唯一的标识字符串，用于被引用时指定。长度范围 1～15 字符。

【描述】

pki entity 命令用来指定 PKI 实体的名称并进入 PKI 实体视图，**undo pki entity** 命令用来删除此实体的名称及其名字空间下所有配置。

在 PKI 实体视图下可配置实体的各种属性值。*name-str* 只是用来方便被其它命令引用，不用于证书的相关字段。

缺省情况下，未指定实体名称。

【举例】

进入 PKI 实体视图。

```
[SecBlade_VPN] pki entity en
[SecBlade_VPN-pki-entity-en]
```

5.3 PKI 证书操作命令

5.3.1 pki delete-certificate

【命令】

pki delete-certificate { **local** | **ca** } **domain** *domain-name*

【视图】

系统视图

【参数】

local：表示删除存储在本地的所有本地证书。

ca：表示删除存储在本地的所有 CA 证书。

domain-name：指定待删除证书所在的 PKI 域。

【描述】

pki delete-certificate 命令用来删除本地存储的证书。

【举例】

删除 PKI 域“cer”中的本地证书。

```
[SecBlade_VPN] pki delete-certificate local domain cer
```

5.3.2 pki import-certificate

【命令】

pki import-certificate { **local** | **ca** } **domain** *domain-name* { **der** | **p12** | **pem** } [**filename** *filename*]

【视图】

系统视图

【参数】

local：表示本地证书。

ca：表示 CA 证书。

domain-name：证书所在的 PKI 域。

der：指定证书文件格式为 DER 编码。

p12：指定证书文件格式为 P12 编码。

pem：指定证书文件格式为 PEM 编码。

filename：证书的文件名，文件名长度为 1～127 个字符。

【描述】

pki import-certificate 命令用来导入已有的 CA 证书或本地证书。

相关命令请参考 **pki domain**。

【举例】

导入 CA 证书，证书文件格式为 PEM 编码。

```
[SecBlade_VPN] pki import-certificate ca domain cer pem
```

5.3.3 pki request-certificate

【命令】

pki request-certificate domain *domain-name* [*password*] [**pkcs10** [**filename** *filename*]]

【视图】

系统视图

【参数】

domain-name：是包含证书申请中 CA 或 RA 等信息的域名。该名字是使用 **pki domain** 命令配置的。

password：在证书撤销时需要提供的密码，可选，长度为 1～31 个字符。

pkcs10：在终端上显示出 BASE64 编码的 PKCS#10 证书请求，该信息可用于带外方式（如电话、磁盘、电子邮件等）的证书请求，可选。

filename：将 PKCS#10 证书请求保存到名为 *filename* 的文件。

【描述】

pki request-certificate 命令为已经生成的 RSA 密钥对通过 SCEP 协议向 CA 申请证书。当 SCEP 出现异常无法正常通信时，可以使用可选参数 pem 打印出本地的证书请求信息(base64 格式)，用户保存该信息，并通过带外方式将该信息发送给 CA 进行证书请求。

此命令不被保存在配置中。

相关命令请参考 **pki domain**。

【举例】

手工申请证书，并在终端上显示 PKCS#10 证书请求。

```
[SecBlade_VPN] pki request-certificate domain 1 pkcs10
```

5.3.4 pki retrieval-certificate

【命令】

pki retrieval-certificate { **local** | **ca** } **domain** *domain-name*

【视图】

系统视图

【参数】

local：表示下载本地证书。

ca：表示下载 CA 的证书。

domain-name：是包含证书申请中 CA 或 RA 等信息的域名。该域名是使用 **pki domain** 命令配置的。

【描述】

pki retrieval-certificate 命令用来从证书发布服务器上下载证书。

相关命令请参考 **pki domain**。

【举例】

获取证书。

```
[SecBlade_VPN] pki retrieval-certificate ca domain 1
```

5.3.5 pki retrieval-crl

【命令】

pki retrieval-crl domain *domain-name*

【视图】

系统视图

【参数】

domain-name：是包含证书申请中 CA 或 RA 等信息的域名。该域名是使用 **pki domain** 命令配置的。

【描述】

pki retrieval-crl 命令用来从 CRL 发布服务器上获取最新的 CRL。下载 CRL 目的是验证当前证书的合法性。

相关命令请参考 **pki domain**。

【举例】

获取 CRL。

```
[SecBlade_VPN] pki retrieval-crl domain 1
```

5.3.6 pki validate-certificate

【命令】

pki validate-certificate { **local** | **ca** } **domain** *domain-name*

【视图】

系统视图

【参数】

local：表示验证本地证书。

ca：表示验证 ca 的证书。

domain-name：指明待验证证书所在的域。该域名是使用 **pki domain** 命令配置的。

【描述】

pki validate-certificate 命令用来检查一个证书的有效性。证书验证的核心就是检查 ca 在证书上的签名，并确定证书仍在有效期内，而且未被废除。由于人们相信 ca 不会发行伪造证书，所以含有它的真实签名的任何证书都可通过验证。

相关命令请参考 **pki domain**。

【举例】

验证 CA 证书。

```
[SecBlade_VPN] pki validate-certificate ca domain 1
```

5.4 PKI 显示与调试命令

5.4.1 debugging pki

【命令】

debugging pki { **all** | **request** | **retrieval** | **verify** | **error** }

undo debugging pki { **all** | **request** | **retrieval** | **verify** | **error** }

【视图】

用户视图

【参数】

all：打开所有的调试开关。

request：证书申请过程的调试开关。

retrieval：证书获取过程的调试开关。

verify：证书验证过程的调试开关。

error：错误发生的调试开关。

【描述】

debugging pki 命令用来打开 PKI 调试信息开关。**undo debugging pki** 命令用来关闭 PKI 调试开关。

在设备使用过程中可能会出现意想不到的问题，所以采用调试命令可以进行有选择性的调试信息打印输出，为网络管理员和开发人员监控网络运行情况和诊断网络故障提供了强有力的支持。

缺省情况下，关闭所有 PKI 调试开关。

【举例】

打开 PKI 证书操作发生错误时的调试开关。

```
[SecBlade_VPN] debugging pki error
[SecBlade_VPN] pki delete-certificate ca domain 1
[SecBlade_VPN] pki request-certificate domain 1
Certificate enroll failed!
Cannot get the CA/RA certificate when creating the x509 Request
```

打开 PKI 证书获取过程的调试开关。

```
[SecBlade_VPN] debugging pki retrieval
[SecBlade_VPN] pki retrieval-certificate local domain 1
Retrievaling CA/RA certificates. Please wait a while......
We receive 3 certificates.
The trusted CA's finger print is:
    MD5  fingerprint:74C9 B71D 406B DDB3 F74A 96BC E05B 40E9
SHA1 fingerprint:770E 2937 4E32 ACD4 4ACC 7CF1 0FF0 6FB8 6C34 E24A
Is the finger print correct?(Y/N):y
Saving the CA/RA certificate to flash.....................Done!
```

打开 PKI 证书申请过程的调试开关。

```
[SecBlade_VPN] debugging pki request
[SecBlade_VPN] pki request-certificate 1
Create PKCS#10 request: token seen: CN=pki test
Create PKCS#10 request: CN=pki test added
Create PKCS#10 request: subject dn set to '/CN=pki test'

Certificate Request:
   …..

dir_name:certsrv/mscep/mscep.dll
host_name:169.254.0.100
SCEP transaction id: 58D41D0C5A7B1E21C5F4A008B580B1A1
PKCS#7 envelope: creating inner PKCS#7
PKCS#7 envelope: data payload size: 297 bytes

data payload:
….
```

```
PKCS#7 envelope: successfully encrypted payload
PKCS#7 envelope: size 667 bytes
PKCS#7 envelope: creating outer PKCS#7
PKCS#7 envelope: signature added successfully
PKCS#7 envelope: adding signed attributes
PKCS#7 envelope: adding string attribute transId
PKCS#7 envelope: adding string attribute messageType
PKCS#7 envelope: adding octet attribute senderNonce
PKCS#7 envelope: PKCS#7 data written successfully
PKCS#7 envelope: applying base64 encoding
PKCS#7 envelope: base64 encoded payload size: 2145 bytes
SCEP send message:IP = 0xa9fe0064
SCEP send message: Server returned status code
Valid response from server
PKCS#7 develope: reading outer PKCS#7
PKCS#7 develope: PKCS#7 payload size: 1872 bytes
PKCS#7 develope: PKCS#7 contains 1276 bytes of enveloped data
PKCS#7 develope: verifying signature
PKCS#7 develope: signature ok
PKCS#7 develope: finding signed attributes
PKCS#7 develope: finding attribute transId
PKCS#7 develope: allocating 32 bytes for attribute
PKCS#7 develope: reply transaction id: 58D41D0C5A7B1E21C5F4A008B580B1A1

PKCS#7 develope: finding attribute messageType
PKCS#7 develope: allocating 1 bytes for attribute
PKCS#7 develope: reply message type is good
PKCS#7 develope: finding attribute senderNonce
PKCS#7 develope: allocating 16 bytes for attribute

PKCS#7 develope: senderNonce in reply: :

a6341944 28d9b544 a4755d9a ba320d35
PKCS#7 develope: finding attribute recipientNonce
PKCS#7 develope: allocating 16 bytes for attribute

PKCS#7 develope: recipientNonce in reply: :

b98da9c3 20b638c5 634f4924 65f804d9
PKCS#7 develope: finding attribute pkiStatus
PKCS#7 develope: allocating 1 bytes for attribute
PKCS#7 develope: pkistatus SUCCESS
```

```
PKCS#7 develope: reading inner PKCS#7
PKCS#7 develope: decrypting inner PKCS#7
PKCS#7 develope: PKCS#7 payload size: 1003 bytes
PKI Get the Signed Certificates:
  subject: / CN=pki test
  issuer:
/emailAddress=myca@h3c.com/C=CN/ST=Beijing/L=Beijing/O=hw3c/OU=bjs/
CN=myca
Key usage: general purpose
```

打开 PKI 证书验证过程的调试开关。

```
[SecBlade_VPN] debugging pki verify
[SecBlade_VPN] pki validate-certificate local domain 1
Verify certificate......
        Serial Number:
            101E266A 00000000 006B
        Issuer:
            emailAddress=myca@h3c.com
            C=CN
            ST=Beijing
            L=Beijing
            O=hw3c
            OU=bjs
            CN=myca
        Subject:
            C=CN
            ST=bei jing
            O=hua wei - 3com
            CN=pki test
Verify result: ok
```

表5-1 debuging pki 调试信息的域描述

域	描述
Create PKCS#10 request	实体请求信息格式封装成 PKCS#10 格式
PKCS#7 envelope	数据封装为 PKCS#7 加密格式
inner PKCS#7	PKCS#7 数据报文的加密处理
outer PKCS#7	PKCS#7 数据报文的签名处理
PKCS#7 develope	PKCS#7 加密报文解包
host_name	注册服务器主机名称
dir_name	注册服务器 CGI 脚本目录

域	描述
data payload	数据载荷
token seen	实体 DN 信息
pkistatus	PKI 证书操作状态
SUCCESS	成功
FAILURE	失败
PENDING	等待处理
fingerprint	指纹，一般指 CA 的签名
base64 encoded	一种数据编码方式
x509 Request	X509 证书请求（证书格式为 X509 标准）
Key usage	密钥用途(一般为加密、签名和通用)
Issuer	证书颁发者
Subject	证书请求实体
SCEP send message	实体通过 SCEP 协议向 CA 发出证书操作报文
Signed Certificates	经 CA 签名的证书

5.4.2 display pki certificate

【命令】

display pki certificate { **local** | **ca** } **domain** *domain-name* | **request-status** }

【视图】

所有视图

【参数】

local：表示显示本地的证书。

ca：表示显示 ca 的证书。

request-status：表示显示证书申请后的状态。

domain-name：指明待验证证书所在的域。该域名是使用 **pki domain** 命令配置的，可选。

【描述】

display pki certificate 命令用来显示和查看证书的内容。

相关命令请参考 **pki retrieval-certificate**、**pki domain**、**certificate request polling**。

【举例】

显示本地证书。

```
[SecBlade_VPN] display pki certificate local domain 1
Data:
        Version: 3 (0x2)
        Serial Number:
            10B7D4E3 00010000 0086
        Signature Algorithm: md5WithRSAEncryption
        Issuer:
            emailAddress=myca@h3c.com
            C=CN
            ST=Beijing
            L=Beijing
            O=hw3c
            OU=bjs
            CN=new-ca
        Validity
            Not Before: Jan 13 08:57:21 2004 GMT
            Not After : Jan 20 09:07:21 2005 GMT
        Subject:
            C=CN
            ST=beijing
            L=beijing
            CN=pki test
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (512 bit)
                Modulus (512 bit):
                    00D41D1F …
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
            DNS:hyf.h3c.com
            …          …
    Signature Algorithm: md5WithRSAEncryption
        A3A5A447 4D08387D …
```

表5-2 证书显示的内容描述

域	描述
Version	证书版本号
Serial Number	证书序列号

域	描述
Signature Algorithm	签名算法
Issuer	证书颁发者
Validity	证书有效期
Subject	证书申请实体
Subject Public Key Info	申请实体公钥信息
X509v3 extensions	X509(版本 3)格式证书扩展属性
X509v3 CRL Distribution Points	X509(版本 3)格式 CRL 发布点

5.4.3 display pki crl

【命令】

display pki crl domain *domain-name*

【视图】

所有视图

【参数】

domain-name：指明待验证证书所在的域。该域名是使用 **pki domain** 命令配置的，可选。

【描述】

display pki crl 命令用来显示和查看存储在本地的 CRL。

相关命令请参考 **pki retrieval-crl**，**pki domain**。

【举例】

显示 CRL。

```
[SecBlade_VPN] display pki crl domain 1
 Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer:
            C=CN
            O=h3c
            OU=soft
            CN=A Test Root
        Last Update: Jan  5 08:44:19 2004 GMT
        Next Update: Jan  5 21:42:13 2004 GMT
```

```
CRL extensions:
    X509v3 CRL Number:            2
    X509v3 Authority Key Identifier:
    keyid:0F71448E E075CAB8 ADDB3A12 0B747387 45D612EC
    Revoked Certificates:
    Serial Number: 05a234448E…
    Revocation Date: Sep  6 12:33:22 2004 GMT
    CRL entry extensions:……
    Serial Number: 05a278445E…
    Revocation Date: Sep  7 12:33:22 2004 GMT
    CRL entry extensions:…
```

表5-3 CRL 显示的内容描述

域	描述
Version	CRL 版本号
Signature Algorithm	CRL 采用的签名算法
Issuer	颁发该 CRL 的 CA
Last Update	上次更新时间
Next Update	下次更新时间
CRL extensions	CRL 扩展属性
CRL Number	CRL 列表中撤消证书的数量
Authority Key Identifier	发布该无效证书(即 CRL)的 CA
Revoked Certificates	撤销的证书
Serial Number	撤销证书的序列号
Revocation Date	撤销日期

第6章 动态 VPN 配置命令

6.1 动态 VPN 配置命令

6.1.1 algorithm-suite

【命令】

algorithm-suite *suite-number*

undo algorithm-suite

【视图】

dvpn-class 视图

【参数】

suite-number：Client 注册过程中使用的算法套件，可取值范围 1～12，缺省值为 1。

1 DES_MD5_DHGROUP1

2 DES_MD5_DHGROUP2

3 DES_SHA1_DHGROUP1

4 DES_SHA1_DHGROUP2

5 3DES_MD5_DHGROUP1

6 3DES_MD5_DHGROUP2

7 3DES_SHA1_DHGROUP1

8 3DES_SHA1_DHGROUP2

9 AES128_MD5_DHGROUP1

10 AES128_MD5_DHGROUP2

11 AES128_SHA1_DHGROUP1

12 AES128_SHA1_DHGROUP2

【描述】

algorithm-suite 命令用来配置客户端注册过程使用的算法套件，**undo algorithm-suite** 命令用来恢复缺省的客户端注册使用的算法套件。

缺省情况下客户端使用的算法套件为 1，即加密算法为 des、验证算法为 MD5，使用 dh-gropp1 算法进行密钥协商。

【举例】

设置注册过程使用的加密算法为 aes，验证算法使用 sha1，使用 dh-gropp1 算法进行密钥协商。

```
[SecBlade_VPN-dvpn-class-abc] algorithm-suite 11
```

6.1.2 authentication-client method

【命令】

authentication-client method { **none** | { **chap** | **pap** } [**domain** *isp-name*] }

【视图】

dvpn-policy 视图

【参数】

pap：表示 server 使用 pap 对 Client 进行验证；

none：表示 server 不需要对 Client 进行验证；

chap：表示 server 使用 chap 对 Client 进行验证。

domain *isp-name*：表示 server 对 Client 采用域认证。

【描述】

authentication-client method 命令用来配置使用该策略的 Dvpn 服务器对客户端进行身份验证的方法。目前支持 none、chap、和 pap 三种认证方式。

缺省情况下，不对客户端进行验证。

【举例】

设置 dvpn 策略，Server 对 Client 进行 chap 验证。

```
[SecBlade_VPN-dvpn-policy-abc] authentication-client method chap
```

6.1.3 authentication-server method

【命令】

authentication-server method { **none** | **pre-share** }

【视图】

dvpn-class 视图

【参数】

none：表示 Client 不需要对 Server 进行验证；

pre-share：表示 Client 使用预共享密钥对 Server 进行验证。

【描述】

authentication-server method 命令用来配置客户端对其需要接入的服务器端进行身份验证。

缺省情况为客户端不要求对服务器进行身份验证。

【举例】

设置 Client 使用 pre-share 方式对 Server 进行验证。

```
[SecBlade_VPN-dvpn-class-abc] authentication-server method pre-share
```

6.1.4 data algorithm-suite

【命令】

data algorithm-suite *suite-number*

undo data algorithm-suite

【视图】

dvpn-policy 视图

【参数】

suite-number：会话数据加密使用的算法套件，即 IPSec SA 使用的算法套件，可取值范围 0～12，缺省值为 1。

0 Without protection

1 DES_MD5_DHGROUP1

2 DES_MD5_DHGROUP2

3 DES_SHA1_DHGROUP1

4 DES_SHA1_DHGROUP2

5 3DES_MD5_DHGROUP1

6 3DES_MD5_DHGROUP2

7 3DES_SHA1_DHGROUP1

8 3DES_SHA1_DHGROUP2

9 AES128_MD5_DHGROUP1

10 AES128_MD5_DHGROUP2

11 AES128_SHA1_DHGROUP1

12 AES128_SHA1_DHGROUP2

【描述】

data algorithm-suite 命令用来配置转发数据的 IPSec SA 使用的算法套件。 **undo data algorithm-suite** 命令用来恢复 IPSec SA 的算法套件为缺省值。

缺省情况下 IPSec SA 使用的算法套件为 1，即加密算法为 DES、验证算法为 MD5、使用 dh-gropp1 算法进行密钥协商。

【举例】

设置不对报文进行加密保护，即算法套件 0。

```
[SecBlade_VPN-dvpn-policy-abc] data algorithm-suite 0
```

6.1.5 data ipsec-sa duration

【命令】

data ipsec-sa duration time-based *time-interval*

undo data ipsec-sa duration time-based

【视图】

dvpn-policy 视图

【参数】

time-interval：Dvpn 数据加密的 IPSec SA 的重协商时间，可取值范围 180～604800 秒，缺省值为 3600 秒。

【描述】

data ipsec-sa duration time-based 命令用来配置 Dvpn 的数据通信使用的加密 IPSec SA 的密钥重新协商超时时间，**undo data ipsec-sa duration time-based** 命令用来恢复 IPSec SA 的重协商超时时间为缺省值。

缺省情况下 IPSec SA 密钥重新协商超时时间为 3600 秒。

【举例】

设置 IPSec SA 的重协商时间间隔为 86400 秒。

```
[SecBlade_VPN-dvpn-policy-abc] data ipsec-sa duration time-based 86400
```

6.1.6 debugging dvpn

【命令】

debugging dvpn { **all** | **error** | **event** { **all** | **misc** | **register** | **session** } | **hexadecimal** | **packet** { **all** | **control** | **data** | **ipsec** } }

undo debugging dvpn { **all** | **error** | **event** { **all** | **register** | **session** | **misc** } | **hexadecimal** | **packet** { **all** | **control** | **data** | **ipsec** } }

【视图】

用户视图

【参数】

all：打开所有调试信息；

error：打开 DVPN 错误调试信息；

event：打开 DVPN 的事件调试开关，包括 register、session、misc 事件；

hexadecimal：16 进制报文显示调试开关；

packet：打开 DVPN 的报文调试开关，包括 control 控制报文、data 数据报文及 ipsec 报文。

【描述】

debugging dvpn 命令用来打开 DVPN 的调试信息开关。**undo debugging dvpn** 命令用来关闭 DVPN 调试信息开关。

缺省情况下，DVPN 调试信息开关是关闭的。

【举例】

打开 DVPN 的注册事件调试开关。

```
<SecBlade_VPN> debugging dvpn event register
```

6.1.7 display dvpn ipsec-sa

【命令】

display dvpn ipsec-sa { **all** | **dvpn-id** *dvpn-id* [**private-ip** *private-ip*] }

【视图】

所有视图

【参数】

all：表示所有 ipsec-sa 的信息。

dvpn-id *dvpn-id*：指定 *dvpn-id*。取值范围为 1～65535。

private-ip *private-ip*：指定私网 IP 地址。

【描述】

display dvpn ipsec-sa 命令用来显示指定的 ipsec-sa 信息。

【举例】

显示 Dvpn 1 的 IPSec SA 信息。

```
<SecBlade_VPN> display dvpn ipsec-sa dvpn-id 1

  ---------------------------
  Session dvpn-id : 1
  Session local   : 10.0.0.3
  Session remote  : 10.0.0.2
  sa mode         : DVPN
  ---------------------------

  [Inbound ESP SAs]
   spi : 1549550209 (0x5c5c4281)
   authentication-algorithm : ESP-AUTH-MD5
   encryption-algorithm : ESP-ENCRYPT-3DES

   life duration(bytes/sec): 0/180
   remaining life duration(bytes/sec): 0/102

  [Outbound ESP SAs]
   spi : 2421434273 (0x905427a1)
   authentication-algorithm : ESP-AUTH-MD5
   encryption-algorithm : ESP-ENCRYPT-3DES

   life duration(bytes/sec): 0/180
   remaining life duration(bytes/sec): 0/102
```

6.1.8 display dvpn map

【命令】

display dvpn map { **all** | **dvpn-id** d*vpn-id* | **public-ip** *public-ip* }

【视图】

所有视图

【参数】

dvpn-id *dvpn-id*：指定 dvpn-id。取值范围为 1～65535。

public-ip *public-ip*：指定公网 IP 地址（即 Tunnel 口的 IP 地址）。

【描述】

display dvpn map 命令用来显示指定 DVPN 的 Map 信息。显示的信息包括私网地址、公网地址、端口号、DVPN 连接状态、DVPN 连接类型和控制标识。

【举例】

显示系统当前的所有 Map 信息。

```
[SecBlade_VPN] display dvpn map all
  vpn-id     private-ip    public-ip     port      state   type    control-id
-------------------------------------------------------------------------
       1     10.0.0.2      211.1.1.2     9876   SUCCESS  C->S     70433124
       2     11.0.0.2      211.1.1.2     9876   SUCCESS  C->S     70432548
```

6.1.9 display dvpn session

【命令】

display dvpn session { **all** | **dvpn-id** d*vpn-id* [**private-ip** *private-ip*] }

【视图】

所有视图

【参数】

dvpn-id：指定 dvpn-id。

private-IP：指定私网 IP 地址（指 Tunnel 口的 IP 地址）。

【描述】

display dvpn session 命令用来显示当前节点所拥有的全部 Session 信息。

【举例】

显示 Dvpn 2 的所有的 session 信息。

```
<SecBlade_VPN> display dvpn session dvpn-id 2
  vpn-id       private-ip        public-ip    port     state  type
 ------------------------------------------------------------------
       2         11.0.0.2        211.1.1.2    9876   SUCCESS   C->S
       2         11.0.0.4      211.1.1.100   12289   SUCCESS  C->C
```

6.1.10 display dvpn info

【命令】

display dvpn info { **dvpn-id** d*vpn-id* | **global** }

【视图】

所有视图

【参数】

dvpn-id：指定 dvpn-id。取值范围为 1～65535。

global：DVPN 全局配置信息。

【描述】

display dvpn info 命令用来显示指定 dvpn 的配置信息以及当前的运行信息。可以使用 **display dvpn info global** 显示系统当前 dvpn 的全局配置信息和运行信息。

【举例】

显示 Dvpn 1 的所有信息。

```
[SecBlade_VPN] display dvpn info dvpn-id 1
  ------------------------------------------------
  DVPN Domain 1 Information
  ------------------------------------------------
  type             : client
  register type  : Undistributed | Forward
  session number : 1

  server           : server0
    server state      : active
    server public IP  : 211.1.1.2
    algorithm suite   : DES_MD5_DHGROUP1

  session encryption flag        : Need encryption
  data encryption flag            : Need encryption
  authentication server method   : none

  session algorithm suite        : AES128_SHA1_DHGROUP1
  session setup time              : 10
  session idle time               : 300
  session keepalive time         : 10
  data algorithm suite            : 3DES_MD5_DHGROUP2
  data ipsecsa duration time     : 180
  data ipsecsa duration byte     : 0

  input packets                     : 17160
  input dropped packets           : 0
  output packets                    : 87
```

```
  output direct send packets      : 42
  output error dropped packets   : 3
  output send ipsec packets       : 42
  output send ipsec fail packets : 0
```

6.1.11 display dvpn online-user

【命令】

display dvpn online-user

【视图】

所有视图

【参数】

无

【描述】

display dvpn online-user 命令用来显示 DVPN 用户的在线信息。当 Server 对 Client 进行身份验证时，可以通过该命令查看目前已经通过 AAA 验证接入到 DVPN 域的用户信息。

【举例】

显示 DVPN 的在线用户信息。

```
<SecBlade_VPN> dis dvpn online-user
  username    : dvpnuser@dvpn
  authen-type : CHAP
  DVPN total online-user count : 1
```

6.1.12 dvpn class

【命令】

dvpn class *dvpn-class-name*

undo dvpn class *dvpn-class-name*

【视图】

系统视图

【参数】

dvpn-class-name：创建的 *dvpn-class* 的名称，以字符串方式表示，字符串的最大长度为 31 字节。

【描述】

dvpn class 命令用来创建一个 dvpn-class 视图，并进入该视图。**undo dvpn class** 命令用来删除 dvpn-class 视图。dvpn-class 视图可以配置目的 Server 的地址，注册使用的用户名、密码等。当该 dvpn-class 已经被接口应用，不能被直接删除。

缺省情况没有配置任何 dvpn-class。

【举例】

创建一个名为“abc”的 dvpn-class。

```
[SecBlade_VPN] dvpn class abc
```

6.1.13 dvpn client register-dumb

【命令】

dvpn client register-dumb *time*

undo dvpn client register-dumb

【视图】

系统视图

【参数】

time：客户端连续注册失败后的静默时间，可取值范围 60～3600 秒，缺省时间为 300 秒。

【描述】

dvpn client register-dumb 命令用来设置客户端连续注册失败达到最大次数时进入静默状态的时间，即多长时间后进行下一次注册。 **undo dvpn client register-dumb** 命令用来恢复客户端静默的时间间隔为缺省值。

【举例】

设置客户端进行注册失败后的静默时间为 600 秒。

```
[SecBlade_VPN] dvpn client register-dumb 600
```

6.1.14 dvpn client register-interval

【命令】

dvpn client register-interval *time-interval*

undo dvpn client register-interval

【视图】

系统视图

【参数】

time-interval：客户端进行注册的时间间隔，可取值范围 3～60 秒，缺省值为 10 秒。

【描述】

dvpn client register-interval 命令用来设置客户端进行注册的时间间隔。 **undo dvpn client register-interval** 命令用来恢复客户端进行注册的时间间隔为缺省值。

DVPN 客户端向服务器发起注册请求时，在一定的时间间隔内，若客户端注册不成功，客户端将重新发起注册请求，在达到失败的最大次数时，若仍不成功，DVPN 客户端将进入 dumb 状态。

缺省情况下客户端进行注册的时间间隔为 10 秒。

【举例】

设置客户端进行注册的时间间隔为 20 秒。

```
[SecBlade_VPN] dvpn client register-interval 20
```

6.1.15 dvpn client register-retry

【命令】

dvpn client register-retry *times*

undo dvpn client register-retry

【视图】

系统视图

【参数】

times：客户端连续进行注册的最大次数，可取值范围 1～6 次，缺省值为 3 次。

【描述】

dvpn client register-retry 命令用来设置客户端连续进行注册的最大次数； **undo dvpn client register-retry** 命令用来恢复客户端连续进行注册的最大次数为缺省值。

【举例】

设置客户端连续进行注册的最大次数为 6 次。

```
[SecBlade_VPN] dvpn client register-retry 6
```

6.1.16 dvpn dvpn-id

【命令】

dvpn dvpn-id d*vpn-id*

undo dvpn dvpn-id

【视图】

Tunnel 接口视图

【参数】

dvpn-id：接口所属的 DVPN 域编号，取值范围为 1～65535。

【描述】

dvpn dvpn-id 命令用来配置 Tunnel 接口所属的 DVPN 域，在 Tunnel 接口封装为 dvpn 时有效；**undo dvpn dvpn-id** 命令用来删除 Tunnel 接口指定的 DVPN 的标识。

缺省情况下 Tunnel 接口没有指定任何 DVPN 标识。

相关配置请参考命令 **tunnel-protocol udp dvpn**。

【举例】

设置 Tunnel 接口所属的 DVPN 域标示为 100。

```
[SecBlade_VPN] interface tunnel 0
[SecBlade_VPN-Tunnel0] dvpn-protocol udp dvpn
[SecBlade_VPN-Tunnel0] dvpn dvpn-id 100
```

6.1.17 dvpn interface-type

【命令】

dvpn interface-type { **client** | **server** }

undo dvpn interface-type

【视图】

Tunnel 接口视图

【参数】

client：表示接口类型为 client。

server：表示接口类型为 server。

【描述】

dvpn interface-type 命令用来指定了 Tunnel 接口的接口类型。**undo dvpn interface-type** 命令用来恢复 Tunnel 接口的缺省类型。

缺省情况下为 client 类型。

【举例】

设置 Tunnel 接口为 server 类型。

```
[SecBlade_VPN-Tunnel0] dvpn interface-type server
```

6.1.18 dvpn policy

【命令】

dvpn policy *dvpn-policy-name*

undo dvpn policy *dvpn-policy-name*

【视图】

系统视图

【参数】

dvpn-polciy-name：创建的 *dvpn-policy* 的名称，以字符串方式表示，字符串的最大长度为 31 字节。

【描述】

dvpn policy 命令用来创建一个 dvpn-policy 视图，并进入该视图。**undo dvpn policy** 命令用来删除 dvpn-policy 视图。dvpn-policy 视图用来配置对 client 的身份的认证方式，会话使用的加密算法套件、转发数据使用的算法套件、以及各种时间参数等各种 dvpn 策略。如果一个 dvpn-policy 已经被接口使用，则需要删除接口的应用才可以删除该 dvpn-policy。

缺省情况没有配置任何 dvpn-policy。

【举例】

创建一个名为“abc”的 dvpn-policy。

```
[SecBlade_VPN] dvpn policy abc
```

6.1.19 dvpn policy

【命令】

dvpn policy *dvpn-policy-name*

undo dvpn policy *dvpn-policy-name*

【视图】

Tunnel 接口视图

【参数】

policy-class-name：本接口使用的 dvpn-policy 的名称。dvpn-policy 是一个包含 Dvpn 会话使用的算法、以及各种时间定时器的时间设置等信息的数据结构，该结构通过系统视图下的 **dvpn policy** 命令创建。

【描述】

dvpn policy 命令用来配置作为 Server 端的 Tunnel 接口使用的 dvpn-policy 名称。**undo dvpn policy** 命令用来删除 Tunnel 接口使用的 dvpn-policy。

每个接口最多应用一个 dvpn-policy；如果需要应用新的 dvpn-policy，则必须删除原有的 dvpn-policy；另外一个 dvpn-Policy 可以被多个接口同时使用。

只有配置为 server 模式的 tunnel 接口才能够使用 **dvpn-policy**。

缺省情况 Tunnel 接口没有应用 dvpn policy。

相关配置请参考命令 **dvpn interface-type**。

【举例】

设置 Tunnel 接口应用的 policy“abc”。

```
[SecBlade_VPN-Tunnel0] dvpn interface-type server
[SecBlade_VPN-Tunnel0] dvpn policy abc
```

6.1.20 dvpn register-type

【命令】

dvpn register-type { **forward** | **undistributed** } *

undo dvpn register-type { **forward** | **undistributed** } *

【视图】

Tunnel 接口视图

【参数】

forward：DVPN 服务器转发从此客户端发送的数据包。

undistributed：不允许服务器向其它客户端发布本客户端的注册信息。

【描述】

dvpn register-type 命令用来配置 Client 向 Server 注册时的附加信息类型。**undo dvpn register-type** 命令用来取消所配置的 Client 向 Server 注册时的附加信息类型。Server 可以根据指定的类型确定是否发送重定向报文。

只有配置为 client 模式的 tunnle 接口才能够配置 **dvpn register-type** 命令。

相关配置请参考命令 **dvpn interface-type**。

在缺省情况下，系统没有设置这里两个标志。

【举例】

设置注册的类型为不允许 Server 向其他节点发布本 Client 的信息。

```
[SecBlade_VPN-tunnel0] dvpn register-type undistributed
```

6.1.21 dvpn security

【命令】

dvpn security acl *acl-number*

undo dvpn security acl

【视图】

Tunnel 接口视图

【参数】

acl-number：接口进行 IPSec 加密数据流判断的 acl 的编号，取值范围为 3000～3999。

【描述】

dvpn security acl 命令用来配置 Tunnel 接口的 IPSec 加密数据流匹配的 acl；**undo dvpn security acl** 命令用来删除 Tunnel 接口指定的 IPSec 加密数据流匹配的 acl。

Dvpn 进行数据转发时，需要进行相应的 Acl 的匹配判断，对于被 acl 拒绝的数据报文不进行 IPSec 处理，否则进行 IPSec 加密保护。

【举例】

设置 Tunnel 接口 IPSec 加密数据流的 acl 为 3100。

```
[SecBlade_VPN-Tunnel0] dvpn security acl 3100
```

6.1.22 dvpn server

【命令】

dvpn server *dvpn-class-name*

undo dvpn server *dvpn-class-name*

【视图】

Tunnel 接口视图

【参数】

dvpn-class-name：本接口使用的 dvpn-class 的名称。dvpn-class 是一个包含 Server 端公网 IP 地址、私网（Tunnel）IP 地址、注册用户名密码等信息的数据结构，该结构通过系统视图下的 **dvpn class** 命令创建。

【描述】

dvpn server 命令用来配置 Tunnel 接口使用的 dvpn-class 名称，**undo dvpn server** 命令用来删除 Tunnel 接口使用的 dvpn-class。

目前每个接口最多支持一个 dvpn server；同时一个 dvpn-class 只允许被一个接口使用。

缺省情况下 Tunnel 接口没有配置 dvpn-class。

【举例】

设置 Tunnel 接口使用的 server“abc”。

```
[SecBlade_VPN-Tunnel0] dvpn server abc
```

6.1.23 dvpn server authentication-client method

【命令】

dvpn server authentication-client method { **none** | { **chap** | **pap** } [**domain** *isp-name*] }

【视图】

系统视图

【参数】

none：表示 server 不需要对 Client 进行验证。

pap：表示 server 使用 pap 对 Client 进行验证。

chap：表示 server 使用 chap 对 Client 进行验证。

domain *isp-name*：表示 server 对 Client 采用域认证。

【描述】

dvpn server authentication-client method 命令用来设置服务器端默认对客户端的身份认证方式，如果客户端注册时不指定需要接入的 Dvpn，则会使用默认的身份认证方式对客户端进行认证。目前支持 none、chap、和 pap 三种认证方式。

Client 在 Server 进行注册过程中，会根据配置确定使用 DVPN 域的策略确定对 Client 使用的认证方式，如果没有对应的策略则使用全局配置的验证方式对 Client 进行身份验证。

缺省情况，服务器不对客户端进行验证。

【举例】

设置服务器端默认使用 chap 对客户端进行身份认证。

```
[SecBlade_VPN] dvpn server authentication-client method chap
```

6.1.24 dvpn server map age-time

【命令】

dvpn server map age-time *time*

undo dvpn server map age-time

【视图】

系统视图

【参数】

time：服务器 map 的超时时间，可取值范围 10～180 秒，缺省值为 30 秒。

【描述】

dvpn server map age-time 命令用来设置服务器端的注册不成功的 map 的超时时间。 **undo dvpn server map age-time** 命令用来设置服务器端 map 超时时间为缺省值。

当服务器端的 map 在指定的超时时间内仍注册不成功时，将删除该 map。

缺省的超时时间为 30 秒。

【举例】

设置服务器端 map 超时时间为 60 秒。

```
[SecBlade_VPN] dvpn server map age-time 60
```

6.1.25 dvpn server pre-shared-key

【命令】

dvpn server pre-shared-key *key*

undo dvpn server pre-shared-key

【视图】

系统视图

【参数】

key：设置的 server 的身份密钥信息，以字符串方式表示，字符串的最大长度为 127 字符。

【描述】

dvpn server pre-shared-key 命令用来设置服务器的身份标识的预共享密钥信息。**undo dvpn server pre-shared-key** 命令用来清除服务器的预共享密钥。

缺省情况服务器没有设置预共享密钥。

【举例】

设置服务器身份标示的密钥为“123”。

```
[SecBlade_VPN] dvpn server pre-shared-key 123
```

6.1.26 dvpn service enable

【命令】

dvpn service enable

undo dvpn service enable

【视图】

系统视图

【参数】

无

【描述】

dvpn service enable 命令用来使能设备的 DVPN 特性功能。undo **dvpn service** 命令用来禁止设备的 DVPN 特性功能。

设备缺省情况下，关闭 DVPN 特性功能。

【举例】

使能 DVPN 特性功能。

```
[SecBlade_VPN] dvpn service enable
```

6.1.27 local-user

【命令】

local-user *username* **password** { **simple** | **cipher** } *password*

undo local-user

【视图】

dvpn-class 视图

【参数】

username：Client 的用户名，长度为 1～80 个字符的字符串。

password：Client 的用户口令。

simple：表示不加密显示口令。

cipher：表示加密显示口令。

【描述】

local-user 命令用来配置 Client 的用户名和密码，**undo local-user** 命令用来取消已经配置的用户名和密码。

【举例】

设置 Client 进行身份认证的用户名 user、密码为 test。

```
[SecBlade_DVPN-class-abc] local-user user password simple test
```

6.1.28 public-ip

【命令】

public-ip *ip-address*

undo public-ip

【视图】

dvpn-class 视图

【参数】

ip-address：指定的 Server 的公网 IP 地址。

【描述】

public-ip 命令用来配置指定的 Server 端的公网 IP 地址，**undo public-ip** 命令用来删除指定的 Server 端的公网 IP 地址。

缺省情况下，没有配置指定 Server 端的公网 IP 地址。

【举例】

指定 Server 的公网 IP 地址为 61.18.3.66。

```
[SecBlade_VPN-dvpn-class-abc] public-ip 61.18.3.66
```

6.1.29 pre-shared-key

【命令】

pre-shared-key *key*

undo pre-shared-key

【视图】

dvpn-class 视图

【参数】

key：设置的 Server 的身份密钥信息，以字符串方式表示，字符串的最大长度为 127 字符。

【描述】

pre-shared-key 命令用来设置客户端需要对服务器进行身份认证的的预共享密钥信息，**undo pre-shared-key** 命令用来清除客户端设置的服务器的预共享密钥。

【举例】

设置客户端的服务器的共享密钥为“123”。

```
[SecBlade_VPN-dvpn-class-abc] pre-shared-key 123
```

6.1.30 private-ip

【命令】

private-ip *ip-address*

undo private-ip

【视图】

dvpn-class 视图

【参数】

ip-address：指定的 Server 端的私网 IP 地址（即 Tunnel 接口的 IP 地址）。

【描述】

private-ip 命令用来配置指定 Server 的私网 IP 地址，**undo private-ip** 命令用来删除指定 Server 的私网 IP 地址。

缺省情况下，没有配置 Server 端的私网 IP 地址。

【举例】

指定 Server 的私网（Tunnel）IP 地址为 192.168.0.1。

```
[SecBlade_VPN-Dvpn-class-abc] private-ip 192.168.0.1
```

6.1.31 reset dvpn all

【命令】

reset dvpn all *dvpn-id*

【视图】

用户视图

【参数】

dvpn-id：指定的 DVPN 的标识。

【描述】

reset dvpn all 命令用来清除指定 DVPN 的所有运行信息，对指定的 DVPN 进行初始化。

【举例】

重置 dvpn 2。

```
<SecBlade_VPN> reset dvpn all 2
```

6.1.32 reset dvpn map

【命令】

reset dvpn map *public-ip port* [*client-id*]

【视图】

用户视图

【参数】

public-ip：公网 IP 地址。

port：指定的端口号，取值范围为 1～65535。

client-id：client 端的 ID。取值范围为 1～4294967295。

【描述】

reset dvpn map 命令用来清除指定的 Map，如果已经建立了会话连接，则同时会清除相关的会话连接，如果该 Map 为 Client 注册使用的 Map，则会清除使用该 Map 进行注册的 DVPN client 的所有的会话。

【举例】

清除地址为 10.0.0.2，端口号位 9876，client-id 为 123456 的 Map。

```
<SecBlade_VPN> reset dvpn map 10.0.0.2 9876 123456
```

6.1.33 reset dvpn session

【命令】

reset dvpn session *dvpn-id private-ip*

【视图】

用户视图

【参数】

dvpn-id：指定的 DVPN 的标示 ID。取值范围为 1～65535。

private-ip：私网 IP 地址。

【描述】

reset dvpn session 命令用来清除指定的 session，如果该 session 为 Client 注册过程建立的 session，则会清除使用该 DVPN Client 的所有的 session。

【举例】

清除 dvpn 2 域中私网地址为 10.0.0.2 的 session。

```
<SecBlade_VPN> reset dvpn session 2 10.0.0.2
```

6.1.34 reset dvpn statistics

【命令】

reset dvpn statistics

【视图】

用户视图

【参数】

无

【描述】

reset dvpn statistics 命令用来清除 dvpn 模块的所有的统计信息。

【举例】

清除 dvpn 的统计信息。

```
<SecBlade_VPN> reset dvpn statistics
```

6.1.35 session algorithm-suite

【命令】

session algorithm-suite *suite-number*

undo session algorithm-suite

【视图】

dvpn-policy 视图

【参数】

suite-number：会话控制报文加密保护使用的算法套件，取值范围为 0～12。

0	Without protection
1	DES_MD5_DHGROUP1
2	DES_MD5_DHGROUP2
3	DES_SHA1_DHGROUP1
4	DES_SHA1_DHGROUP2
5	3DES_MD5_DHGROUP1
6	3DES_MD5_DHGROUP2
7	3DES_SHA1_DHGROUP1
8	3DES_SHA1_DHGROUP2
9	AES128_MD5_DHGROUP1
10	AES128_MD5_DHGROUP2
11	AES128_SHA1_DHGROUP1
12	AES128_SHA1_DHGROUP2NONE 0

【描述】

session algorithm-suite 命令用来配置会话使用的算法套件， **undo session algorithm-suite** 命令用来恢复算法套件的缺省设置。

缺省情况下，会话控制报文使用的算法套件为 1，即加密算法为 DES，验证算法为 MD5，密钥协商算法为 DHGROUP1。

【举例】

设置不对会话控制报文进行加密保护，即使用套件 0。

```
[SecBlade_VPN-dvpn-policy-abc] session algorithm-suite 0
```

6.1.36 session idle-time

【命令】

session idle-time *time*

undo session idle-time

【视图】

dvpn-policy 视图

【参数】

time：会话的空闲超时时间会话建立请求定时器的时间间隔，单位为秒，可取值范围为 60～86400。

【描述】

session idle-time 命令用来配置会话的空闲超时时间，**undo session idle-time** 命令用来恢复会话空闲超时时间的缺省设置。

如果会话在空闲超时时间内没有数据传输，该会话会被自动删除。

缺省情况下，空闲超时时间为 300 秒。

【举例】

设置会话空闲超时时间为 180 秒。

```
[SecBlade_VPN-dvpn-policy-abc] session idle-time 180
```

6.1.37 session keepalive-interval

【命令】

session keepalive-interval *time-interval*

undo session keepalive-interval

【视图】

dvpn-policy 视图

【参数】

time-interval：保持定时器的时间间隔，单位为秒，取值范围为 5～300 秒。

【描述】

session keepalive-interval 命令用来配置 DVPN 的会话 Session 状态的保持连接定时器的时间间隔，**undo session keepalive-interval** 命令用来恢复保持连接定时器的缺省设置。

Keepalive 用来保持会话的连接状态。当会话建立成功后，主动方会定时发送 Keepalive 报文，被动端接收到 Keepalive 报文会回应 Keepalive-ack 报文。被动端不会主动发送 Keepalive 报文。

缺省情况下，时间间隔为 10 秒。

【举例】

设置会话状态的保持连接时间间隔为 30 秒。

```
[SecBlade_VPN-dvpn-policy-abc] session keepalive-interval 30
```

6.1.38 session setup-interval

【命令】

session setup-interval *time-interval*

undo session setup-interval

【视图】

dvpn-policy 视图

【参数】

time-interval：会话建立请求定时器的时间间隔，单位为秒，取值范围为 5～60，缺省值为 10 秒。

【描述】

session setup-interval 命令用来配置会话建立请求（Setup Request）的时间间隔，每次超时将重新发送会话建立请求报文。**undo session setup-interval** 命令用来恢复会话建立请求定时器的缺省值。

当 Client 端发送一个会话建立请求之后，在没有收到对端的应答之前如果定时器超时则再向对端节点发送会话建立请求报文。

缺省情况下，时间间隔 10 秒。

【举例】

设置会话建立请求的时间间隔为 30 秒。

```
[SecBlade_VPN-dvpn-policy-abc] session setup-interval 30
```

6.1.39 tunnel-protocol udp dvpn

【命令】

tunnel-protocol udp dvpn

【视图】

Tunnel 接口视图

【参数】

udp dvpn：Tunnel 接口采用 UDP **DVPN** 封装格式建立 Tunnel。

【描述】

tunnel-protocol udp dvpn 命令用来配置 Tunnel 接口的封装格式，设置 Tunnel 接口采用 DVPN 方式，接口将变成 Multipoint 属性，NBMA 类型。

缺省情况下，Tunnel 接口封装为 GRE 模式。

【举例】

设置 Tunnel 接口为 UDP DVPN 封装格式。

```
[SecBlade_VPN-Tunnel0] tunnel-protocol udp dvpn
```

安全

目 录

第 1 章 AAA及RADIUS/HWTACACS协议配置命令 1-1
1.1 AAA配置命令 1-1
1.1.1 access-limit 1-1
1.1.2 accounting 1-2
1.1.3 accounting optional 1-2
1.1.4 authentication 1-3
1.1.5 authentication super hwtacacs-scheme 1-4
1.1.6 authorization 1-5
1.1.7 display connection 1-6
1.1.8 display domain 1-7
1.1.9 display local-user 1-8
1.1.10 domain 1-10
1.1.11 ip pool 1-11
1.1.12 level 1-12
1.1.13 local-user 1-13
1.1.14 local-user password-display-mode 1-14
1.1.15 password 1-14
1.1.16 scheme 1-15
1.1.17 service-type 1-16
1.1.18 service-type dvpn 1-17
1.1.19 service-type ftp 1-17
1.1.20 service-type ppp 1-18
1.1.21 state 1-19
1.1.22 super authentication-mode 1-19
1.2 RADIUS协议配置命令 1-20
1.2.1 accounting optional 1-20
1.2.2 data-flow-format 1-21
1.2.3 debugging local-server 1-22
1.2.4 debugging radius 1-22
1.2.5 display local-server statistics 1-23
1.2.6 display radius scheme 1-24
1.2.7 display radius statistics 1-25
1.2.8 display stop-accounting-buffer 1-29
1.2.9 key 1-30
1.2.10 local-server 1-31
1.2.11 nas-ip 1-32
1.2.12 primary accounting 1-32
1.2.13 primary authentication 1-33
1.2.14 radius scheme 1-34
1.2.15 radius nas-ip 1-35

1.2.16 radius trap 1-36
1.2.17 reset radius statistics 1-36
1.2.18 reset stop-accounting-buffer 1-37
1.2.19 retry 1-38
1.2.20 retry realtime-accounting 1-39
1.2.21 retry stop-accounting 1-39
1.2.22 secondary accounting 1-40
1.2.23 secondary authentication 1-41
1.2.24 server-type 1-42
1.2.25 state 1-42
1.2.26 stop-accounting-buffer enable 1-43
1.2.27 timer quiet 1-44
1.2.28 timer realtime-accounting 1-45
1.2.29 timer response-timeout 1-46
1.2.30 user-name-format 1-46
1.3 HWTACACS协议配置命令 1-47
1.3.1 data-flow-format 1-47
1.3.2 debugging hwtacacs 1-48
1.3.3 display hwtacacs scheme 1-49
1.3.4 display stop-accounting-buffer 1-51
1.3.5 hwtacacs nas-ip 1-52
1.3.6 hwtacacs scheme 1-53
1.3.7 key 1-53
1.3.8 nas-ip 1-54
1.3.9 primary accounting 1-55
1.3.10 primary authentication 1-56
1.3.11 primary authorization 1-56
1.3.12 reset hwtacacs statistics 1-57
1.3.13 reset stop-accounting-buffer 1-58
1.3.14 retry stop-accounting 1-58
1.3.15 secondary accounting 1-59
1.3.16 secondary authentication 1-60
1.3.17 secondary authorization 1-60
1.3.18 stop-accounting-buffer enable 1-61
1.3.19 timer quiet 1-62
1.3.20 timer realtime-accounting 1-62
1.3.21 timer response-timeout 1-63
1.3.22 user-name-format 1-64
第 2 章 访问控制列表配置命令 2-1
2.1 访问控制列表配置命令 2-1
2.1.1 acl 2-1
2.1.2 description 2-2
2.1.3 display acl 2-2
2.1.4 reset acl counter 2-3
2.1.5 rule 2-3

2.1.6 rule comment 2-7
2.2 时间段配置命令 2-8
2.2.1 display time-range 2-8
2.2.2 time-range 2-9
第 3 章 NAT配置命令 3-1
3.1 NAT配置命令 3-1
3.1.1 connection-limit default 3-1
3.1.2 connection-limit default amount 3-1
3.1.3 connection-limit enable 3-2
3.1.4 connection-limit policy 3-3
3.1.5 debugging connection-limit 3-3
3.1.6 debugging nat 3-4
3.1.7 display connection-limit policy 3-4
3.1.8 display connection-limit statistics 3-5
3.1.9 display nat 3-6
3.1.10 display nat connection-limit 3-8
3.1.11 limit 3-9
3.1.12 nat address-group 3-10
3.1.13 nat aging-time 3-11
3.1.14 nat alg 3-12
3.1.15 nat connection-limit-policy 3-13
3.1.16 nat dns-map 3-13
3.1.17 nat outbound 3-14
3.1.18 nat outbound interface 3-15
3.1.19 nat outbound static 3-16
3.1.20 nat overlapaddress 3-17
3.1.21 nat server 3-18
3.1.22 nat static 3-20
3.1.23 nat static inside 3-21
3.1.24 reset nat 3-22
第 4 章 防火墙配置命令 4-1
4.1 包过滤防火墙配置命令 4-1
4.1.1 debugging firewall packet-filter 4-1
4.1.2 debugging firewall packet-filter fragments-inspect events 4-2
4.1.3 display firewall fragment 4-2
4.1.4 display firewall packet-filter statistics 4-3
4.1.5 firewall packet-filter default 4-3
4.1.6 firewall packet-filter enable 4-4
4.1.7 firewall packet-filter fragments-inspect 4-4
4.1.8 firewall packet-filter fragments-inspect { high | low } 4-5
4.1.9 firewall packet-filter 4-6
4.1.10 reset firewall packet-filter statistics 4-7
4.2 状态防火墙配置命令 4-8
4.2.1 aging-time 4-8

4.2.2 aspf-policy 4-9
4.2.3 debugging aspf 4-9
4.2.4 debugging aspf http 4-10
4.2.5 detect 4-11
4.2.6 detect http 4-12
4.2.7 display aspf all 4-13
4.2.8 display aspf interface 4-14
4.2.9 display aspf policy 4-15
4.2.10 display aspf session 4-16
4.2.11 display aspf statistics 4-17
4.2.12 display firewall fragment 4-17
4.2.13 display firewall session aging-time 4-18
4.2.14 display firewall session table 4-19
4.2.15 display port-mapping 4-20
4.2.16 firewall aspf 4-21
4.2.17 firewall session aging-time 4-22
4.2.18 firewall session aging-time default 4-23
4.2.19 log enable 4-23
4.2.20 port-mapping 4-24
4.2.21 reset aspf session 4-25
4.2.22 reset aspf statistic http 4-25
4.2.23 reset firewall session table 4-26
4.3 VPN实例配置命令 4-26
4.3.1 firewall session limit 4-26
4.3.2 firewall fragment limit 4-27
4.3.3 aspf session limit 4-27
4.4 黑名单配置命令 4-28
4.4.1 debugging firewall blacklist 4-28
4.4.2 display firewall blacklist 4-28
4.4.3 firewall blacklist 4-29
4.5 MAC和IP地址绑定配置命令 4-30
4.5.1 debugging firewall mac-binding 4-30
4.5.2 display firewall mac-binding 4-31
4.5.3 firewall mac-binding 4-32
4.5.4 firewall mac-binding enable 4-33
4.5.5 reset firewall mac-binding 4-33
4.6 区域配置命令 4-34
4.6.1 add interface 4-34
4.6.2 display interzone 4-34
4.6.3 display zone 4-35
4.6.4 set priority 4-36
4.6.5 firewall interzone 4-36
4.6.6 firewall zone 4-37
4.6.7 firewall zone name 4-37

第 5 章 透明防火墙配置命令 5-1
5.1 透明防火墙配置命令 5-1
5.1.1 acl number 5-1
5.1.2 bridge vlanid-transparent-transmit enable 5-1
5.1.3 debugging firewall eff 5-2
5.1.4 debugging firewall transparent-mode eth-forwarding 5-4
5.1.5 debugging firewall transparent-mode ip-forwarding 5-5
5.1.6 display firewall ethernet-frame-filter 5-7
5.1.7 display firewall mode 5-8
5.1.8 display firewall transparent-mode address-table 5-8
5.1.9 display firewall transparent-mode config 5-9
5.1.10 display firewall transparent-mode traffic 5-10
5.1.11 firewall arp-learning enable 5-12
5.1.12 firewall ethernet-frame-filter 5-13
5.1.13 firewall mode 5-13
5.1.14 firewall system-ip 5-14
5.1.15 firewall transparent-mode aging-time 5-15
5.1.16 firewall transparent-mode transmit 5-16
5.1.17 firewall unknown-mac 5-16
5.1.18 firewall unknown-mac broadcast 5-17
5.1.19 firewall unknown-mac multicast 5-18
5.1.20 firewall unknown-mac unicast 5-18
5.1.21 reset firewall ethernet-frame-filter 5-19
5.1.22 reset firewall transparent-mode address-table 5-19
5.1.23 reset firewall transparent-mode traffic 5-20
5.1.24 rule 5-20
第 6 章 Web和邮件过滤配置命令 6-1
6.1 Web过滤配置命令 6-1
6.1.1 debugging firewall url-filter host 6-1
6.1.2 debugging firewall url-filter parameter 6-1
6.1.3 debugging firewall webdata-filter 6-2
6.1.4 display firewall url-filter host 6-3
6.1.5 display firewall url-filter parameter 6-4
6.1.6 display firewall url-filter parameter counter detail 6-4
6.1.7 display firewall webdata-filter 6-5
6.1.8 firewall url-filter host acl-number 6-6
6.1.9 firewall url-filter host add 6-6
6.1.10 firewall url-filter host clear 6-7
6.1.11 firewall url-filter host default 6-7
6.1.12 firewall url-filter host delete 6-8
6.1.13 firewall url-filter host enable 6-8
6.1.14 firewall url-filter host ip-address 6-9
6.1.15 firewall url-filter host save-file 6-9
6.1.16 firewall url-filter host load-file 6-10

6.1.17 firewall url-filter parameter add 6-10
6.1.18 firewall url-filter parameter add-default 6-11
6.1.19 firewall url-filter parameter clear 6-12
6.1.20 firewall url-filter parameter delete 6-12
6.1.21 firewall url-filter parameter enable 6-13
6.1.22 firewall url-filter parameter load-file 6-13
6.1.23 firewall url-filter parameter save-file 6-14
6.1.24 firewall webdata-filter add 6-14
6.1.25 firewall webdata-filter clear 6-15
6.1.26 firewall webdata-filter delete 6-16
6.1.27 firewall webdata-filter enable 6-16
6.1.28 firewall webdata-filter load-file 6-17
6.1.29 firewall webdata-filter save-file 6-18
6.1.30 reset firewall url-filter host counter 6-18
6.1.31 reset firewall url-filter parameter counter 6-18
6.1.32 reset firewall webdata-filter counter 6-19
6.2 邮件过滤配置命令 6-19
6.2.1 debugging firewall smtp-filter 6-19
6.2.2 display firewall smtp-filter 6-20
6.2.3 firewall smtp-filter attach add 6-21
6.2.4 firewall smtp-filter attach clear 6-22
6.2.5 firewall smtp-filter attach delete 6-22
6.2.6 firewall smtp-filter attach enable 6-23
6.2.7 firewall smtp-filter attach load-file 6-23
6.2.8 firewall smtp-filter attach save-file 6-24
6.2.9 firewall smtp-filter content add 6-24
6.2.10 firewall smtp-filter content clear 6-25
6.2.11 firewall smtp-filter content delete 6-25
6.2.12 firewall smtp-filter content enable 6-26
6.2.13 firewall smtp-filter content load-file 6-26
6.2.14 firewall smtp-filter content save-file 6-27
6.2.15 firewall smtp-filter rcptto add 6-27
6.2.16 firewall smtp-filter rcptto clear 6-28
6.2.17 firewall smtp-filter rcptto default 6-29
6.2.18 firewall smtp-filter rcptto delete 6-29
6.2.19 firewall smtp-filter rcptto enable 6-30
6.2.20 firewall smtp-filter rcptto load-file 6-30
6.2.21 firewall smtp-filter rcptto save-file 6-31
6.2.22 firewall smtp-filter subject add 6-31
6.2.23 firewall smtp-filter subject clear 6-32
6.2.24 firewall smtp-filter subject delete 6-32
6.2.25 firewall smtp-filter subject enable 6-33
6.2.26 firewall smtp-filter subject load-file 6-33
6.2.27 firewall smtp-filter subject save-file 6-34
6.2.28 reset firewall smtp-filter counter 6-34

第 7 章 攻击防范配置命令 7-1
7.1 攻击防范配置命令 7-1
7.1.1 debugging firewall defend 7-1
7.1.2 display firewall defend flag 7-1
7.1.3 display firewall tcp-proxy session 7-2
7.1.4 firewall defend all 7-4
7.1.5 firewall defend arp-flood 7-4
7.1.6 firewall defend arp-spoofing 7-5
7.1.7 firewall defend fraggle 7-6
7.1.8 firewall defend frag-flood 7-6
7.1.9 firewall defend icmp-flood 7-7
7.1.10 firewall defend icmp-flood enable 7-8
7.1.11 firewall defend icmp-redirect 7-9
7.1.12 firewall defend icmp-unreachable 7-9
7.1.13 firewall defend ip-fragment 7-10
7.1.14 firewall defend ip-spoofing 7-10
7.1.15 firewall defend ip-sweep 7-11
7.1.16 firewall defend land 7-12
7.1.17 firewall defend large-icmp 7-12
7.1.18 firewall defend ping-of-death 7-13
7.1.19 firewall defend port-scan 7-14
7.1.20 firewall defend route-record 7-14
7.1.21 firewall defend smurf 7-15
7.1.22 firewall defend source-route 7-16
7.1.23 firewall defend syn-flood 7-16
7.1.24 firewall defend syn-flood enable 7-17
7.1.25 firewall defend tcp-flag 7-18
7.1.26 firewall defend teardrop 7-18
7.1.27 firewall defend tracert 7-19
7.1.28 firewall defend udp-flood 7-19
7.1.29 firewall defend udp-flood enable 7-20
7.1.30 firewall defend winnuke 7-21
7.1.31 firewall tcp-proxy 7-22
第 8 章 IDS联动配置命令 8-1
8.1 IDS联动配置命令 8-1
8.1.1 Ids-acl enable 8-1
8.1.2 display ids 8-1
8.1.3 display ids-acl 8-2
8.1.4 debugging ids 8-3
第 9 章 报文统计与日志配置命令 9-1
9.1 报文统计配置命令 9-1
9.1.1 display firewall statistic 9-1
9.1.2 display firewall statistic system defend 9-3
9.1.3 display firewall statistic system flow-percent 9-4

9.1.4 firewall statistic system connect-number 9-5
9.1.5 firewall statistic system enable 9-6
9.1.6 firewall statistic system flow-percent 9-6
9.1.7 firewall statistic warning-level drop 9-7
9.1.8 reset firewall statistic ip 9-8
9.1.9 reset firewall statistic system 9-8
9.1.10 reset firewall statistic zone 9-9
9.1.11 statistic connect-number ip 9-10
9.1.12 statistic connect-number zone 9-11
9.1.13 statistic connect-speed ip 9-12
9.1.14 statistic connect-speed zone 9-13
9.1.15 statistic enable 9-14
9.2 SMTP客户端配置命令 9-15
9.2.1 debugging smtpc 9-15
9.2.2 display smtpc 9-15
9.2.3 smtpc administrator mail 9-16
9.2.4 smtpc trigger time 9-17
9.3 DNS客户端配置命令 9-17
9.3.1 debugging dnsc 9-17
9.3.2 display dnsc 9-18
9.3.3 dnsc server 9-18
9.3.4 dnsc cache 9-19
9.4 日志配置命令 9-20
9.4.1 firewall session log-type 9-20
9.4.2 firewall log-time 9-20
9.4.3 reset firewall log-buf 9-21

第1章 AAA 及 RADIUS/HWTACACS 协议配置命令

📖 **说明：**

以下内容都是针对 SecBlade 单板的，所以文中的命令所在的视图也都是在 SecBlade 的相应视图下，而不是其它的视图。

1.1 AAA 配置命令

1.1.1 access-limit

【命令】

access-limit { **disable** | **enable** *max-user-number* }

undo access-limit

【视图】

ISP 域视图

【参数】

disable：表示不对当前 ISP 域可容纳的接入用户数作限制。

enable *max-user-number*：表示当前 ISP 域可容纳接入用户数的最大值，取值范围为 1～1048。

【描述】

access-limit 命令用来指定当前 ISP 域可容纳接入用户数的最大值。**undo access-limit** 命令用来恢复缺省设置。

缺省情况下，不对当前 ISP 域可容纳的接入用户数作限制。

由于接入用户之间会发生资源的争用，因此适当地配置该值可以使属于当前 ISP 域的用户获得可靠的性能保障。

【举例】

指定 ISP 域“test163.net”最多可容纳 500 个接入用户。

```
[SecBlade_FW-isp-test163.net] access-limit enable 500
```

1.1.2 accounting

【命令】

accounting { **hwtacacs-scheme** *hwtacacs-scheme-name* | **radius-scheme** *radius-scheme-name* | **none** }

undo accounting

【视图】

ISP 域视图

【参数】

hwtacacs-scheme *hwtacacs-scheme-name*：指定计费使用 HWTACACS 方案。

radius-scheme *radius-scheme-name*：指定计费使用 RADIUS 方案。

none：不计费。

【描述】

accounting 命令用来配置当前 ISP 域使用的计费方案。**undo accounting** 命令用来删除 ISP 域使用的计费方案。

缺省情况下，系统没有配置计费方案。

accounting 命令为当前 ISP 域指定引用的 RADIUS/HWTACACS 方案时，所引用的 RADIUS/HWTACACS 方案必须是已经设置好的。

在域视图下，如果配置了 **accounting** 命令，则采用该命令中引用的计费方案进行计费；否则使用 **scheme** 命令中引用的方案进行计费。

相关配置可参考命令 **scheme**，**radius scheme**，**hwtacacs scheme**。

【举例】

指定当前 ISP 域 h3c163.net 引用的 RADIUS 计费方案为 **radius**。

```
[SecBlade_FW-isp-h3c163.net] accounting radius-scheme radius
```

设置 ISP 域 h3c 引用的为 HWTACACS 计费方案为 hwtac。

```
[SecBlade_FW-isp-h3c] accounting hwtacacs-scheme hwtac
```

1.1.3 accounting optional

【命令】

accounting optional

undo accounting optional

【视图】

ISP 域视图

【参数】

无

【描述】

accounting optional 命令用来打开计费可选开关，**undo accounting optional** 命令用来关闭计费可选开关。

系统缺省为关闭计费可选开关。

当没有可用的计费服务器或与计费服务器通信失败时，若配置了 **accounting optional** 命令，则用户可以继续使用网络资源，否则用户将被切断。这个命令经常被用于只认证不计费的情况。

【举例】

打开名为 test163.net 的域用户的计费可选开关。

```
[SecBlade_FW] domain test163.net
[SecBlade_FW-isp-test163.net] accounting optional
```

1.1.4 authentication

【命令】

authentication { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **radius-scheme** *radius-scheme-name* [**local**] | **local** | **none** }

undo authentication

【视图】

ISP 域视图

【参数】

hwtacacs-scheme *hwtacacs-scheme-name*：指定认证使用的 HWTACACS 方案。

radius-scheme *radius-scheme-name*：指定认证使用的 RADIUS 方案。

local：指定认证使用本地认证方案。

none：不认证。

【描述】

authentication 命令用来配置当前 ISP 域使用的认证方案。**undo authentication** 命令用来恢复域缺省的认证方案。

缺省情况下，系统认证方案为 local。

当使用 **authentication** 命令为当前 ISP 域指定引用的 RADIUS/HWTACACS 方案时，所引用的 RADIUS/HWTACACS 方案必须是已经设置好的。

如果配置了 **authentication radius-scheme** *radius-scheme-name* **local** 或 **authentication hwtacacs-scheme** *hwtacacs-scheme-name* **local**，则 **local** 为 RADIUS 服务器或 TACACS 服务器没有正常响应后的备选认证方案。即当 RADIUS 服务器或 TACACS 服务器有效时，不使用本地认证；当 RADIUS 服务器或 TACACS 服务器无效时，使用本地认证。

如果 **local** 作为第一方案，那么只能采用本地认证，不能再同时采用 RADIUS 或 HWTACACS 方案。**none** 与 **local** 的使用情况相同。

在域视图下，如果配置了 **authentication** 命令，则采用该命令中引用的认证方案进行认证；否则使用 **scheme** 命令中引用的方案进行认证。

相关配置可参考命令 **scheme**，**radius scheme**，**hwtacacs scheme**。

【举例】

指定当前 ISP 域 h3c163.net 引用的 RADIUS 认证方案为 **radius** 。

```
[SecBlade_FW-isp-h3c163.net] authentication radius-scheme  radius
```

设置 ISP 域 h3c 引用的 RADIUS 认证方案为 rd，并采用 local 作为备选认证方案。

```
[SecBlade_FW-isp-h3c] authentication radius-scheme rd local
```

设置 ISP 域 h3c 引用的 HWTACACS 认证方案为 hwtac，并采用 local 作为备选认证方案。

```
[SecBlade_FW-isp-h3c] authentication hwtacacs-scheme hwtac local
```

1.1.5 authentication super hwtacacs-scheme

【命令】

authentication super hwtacacs-scheme *hwtacacs-scheme-name*

undo authentication super hwtacacs-scheme

【视图】

ISP 域视图

【参数】

hwtacacs-scheme-name：指定 HWTACACS 方案名称。

【描述】

authentication super hwtacacs-scheme 命令用来设置域的 super 认证方案。

undo authentication super 命令用来取消域的 super 认证方案。

缺省情况下，未配置 super 认证方案。

【举例】

配置 system 域的 super 认证方案为 sup。

```
[SecBlade_FW] domain system
[SecBlade_FW-isp-system] authentication super hwtacacs-scheme sup
```

1.1.6 authorization

【命令】

authorization { **hwtacacs-scheme** *hwtacacs-scheme-name* | **none** }

undo authorization

【视图】

ISP 域视图

【参数】

hwtacacs-scheme *hwtacacs-scheme-name*：指定授权使用的 HWTACACS 方案。

none：不需要授权，即不需要授权也可以提供服务。

【描述】

authorization 命令用来配置当前 ISP 域使用的授权方案。**undo authorization** 命令用来恢复域缺省的授权方案。

缺省情况下，系统授权方案为 local。

当使用 **authorization** 命令为当前 ISP 域指定引用的 RADIUS/HWTACACS 方案时，所引用的 RADIUS/HWTACACS 方案必须是已经设置好的。

在域视图下，如果配置了 **authorization** 命令，则采用该命令中引用的授权方案进行授权；否则使用 **scheme** 命令中引用方案进行授权。

相关配置可参考命令 **scheme**，**radius scheme**，**hwtacacs scheme**。

【举例】

设置 ISP 域 h3c 引用的 HWTACACS 授权方案为 hwtac。

```
[SecBlade_FW-isp-h3c] authorization hwtacacs-scheme hwtac
```

1.1.7 display connection

【命令】

display connection [**domain** *isp-name* | **ip** *ip-address* | **mac** *mac-address* | **radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name* | **ucibindex** *ucib-index* | **user-name** *user-name*]

【视图】

所有视图

【参数】

domain *isp-name*：显示某个 ISP 域下的全部用户连接。其中，*isp-name* 为 ISP 域名，为不超过 24 个字符的字符串。指定的 ISP 域必须已经存在。

ip *ip-address*：显示某个 IP 地址为 *ip-address* 的所有用户连接。

mac *mac-address*：显示某个 MAC 地址为 *mac-address* 的用户连接。其中，*mac-address* 为点分十六进制格式（即形如 X-X-X 的样式）。

radius-scheme *radius-scheme-name*：显示名称为 *radius-scheme-name* 的 RADIUS 方案的所有用户连接。*radius-scheme-name* 为不超过 32 个字符的字符串。

hwtacacs-scheme *hwtacacs-scheme-name*：显示名称为 *hwtacacs-scheme-name* 的 HWTACACS 方案的所有用户连接。*hwtacacs-scheme-name* 为不超过 32 个字符的字符串。

ucibindex *ucib-index*：显示某个连接索引号为 *ucib-index* 的用户连接。其中，*ucib-index* 的取值范围为 0～7071。

user-name *user-name*：显示某个用户名为 *user-name* 的用户连接。其中，用户名的格式为 *pure-username@domain*。*pure-username* 为纯用户名，不超过 55 个字符；*domain* 为域名，不超过 24 个字符。

【描述】

display connection 命令用来显示所有或指定的用户连接的相关信息。根据输出的信息，可以帮助诊断与排除用户连接方面的故障。

缺省情况下，显示所有用户连接的相关信息。

【举例】

显示所有用户 system 连接的相关信息。

```
<SecBlade_FW> display connection domain system
Index=0   ,Username=hfx@system
 IP=188.188.188.3
```

```
Total 1 connections matched, 1 listed.
```

表1-1 display connection 显示信息描述表

域名	解释
Index	索引号
Username	用户名
IP	该用户的 IP 地址

1.1.8 display domain

【命令】

display domain [*isp-name*]

【视图】

所有视图

【参数】

isp-name：ISP 域名。为不超过 24 个字符的字符串。所指定的 ISP 域必须已经存在。

【描述】

display domain 命令用来显示指定 ISP 域的配置信息或所有 ISP 域的概要信息。

若不指定域名，则显示系统中所有 ISP 域的概要信息。

display domain 命令可以输出指定 ISP 域的配置信息或所有 ISP 域的概要信息。在指定显示某个 ISP 域的配置信息时，输出内容和格式与 **display domain** 命令的输出完全一致。根据输出的信息，可以帮助诊断与排除与 ISP 域有关的故障。

相关配置可参考命令 **access-limit**，**domain**，**scheme**，**state**，**display domain**。

【举例】

显示系统中所有 ISP 域的概要信息。

```
<SecBlade_FW> display domain
0  Domain = system
   State = Active
   Scheme = LOCAL
   Access-limit = Disable
   Domain User Template:
Default Domain Name: system
Total 1 domain(s).1 listed.
```

表1-2 display domain 显示信息描述表

域名	解释
Domain	域名及序号
State	该域用户的状态（Active/Block）
Scheme	该域用户的认证方案（Local/Radius/Tacacs）
Access-limit	对该域用户能够同时接入用户的数量是否进行限制（Disable/Enable）

1.1.9 display local-user

【命令】

display local-user [**domain** *isp-name* | **service-type** { **telnet** | **ssh** | **terminal** | **dvpn** | **ftp** | **ppp** } | **state** { **active** | **block** } | **user-name** *user-name*]

【视图】

所有视图

【参数】

domain *isp-name*：显示属于某个 ISP 域的全部本地用户。其中，*isp-name* 为 ISP 域名，为不超过 24 个字符的字符串。指定的 ISP 域必须已经存在。

service-type：根据用户类型显示本地用户。其中，**telent** 为 telnet 用户；**ssh** 为 SSH 用户；**terminal** 为从 Console 口、AUX 口登录的终端用户；**ftp** 指定用户为 FTP 类型；**ppp** 为 PPP 用户；**dvpn** 为 DVPN 用户。

state { **active** | **block** }：显示处于某种状态的本地用户。其中，**active** 表示系统允许用户请求网络服务；**block** 表示系统不允许用户请求网络服务。

user-name *user-name*：显示用户名为 *user-name* 的本地用户。其中，*user-name* 为用户名，为不超过 80 个字符的字符串，字符串中不能包括“/”、“:”、“*”、“?”、“<”以及“>”等字符，并且“@”出现的次数不能多于 1 次，纯用户名（“@”以前部分，即用户标识）不能超过 55 个字符。

【描述】

display local-user 命令用来显示所有或指定的本地用户的相关信息。根据输出的信息，可以帮助诊断和排除与本地用户有关的故障。

缺省情况下，显示所有本地用户的相关信息。

相关配置可参考命令 **local-user**。

【举例】

显示所有本地用户的相关信息。

```
<SecBlade_FW> display local-user
The contents of local user admin:
 State:          Active            ServiceType Mask: T
 Idle-cut:       Disable
 Access-limit:   Disable           Current AccessNum: 0
 Bind location:  Disable
 Vlan ID:        Disable
 IP address:     Disable
 MAC address:    Disable
 User Privilege: 3

The contents of local user ftpuser:
 State:          Active            ServiceType Mask: F
 Idle-cut:       Disable
 Access-limit:   Disable           Current AccessNum: 0
 Bind location:  Disable
 Vlan ID:        Disable
 IP address:     Disable
 MAC address:    Disable
 FTP Directory:  flash:

Total 2 local user(s) Matched, 2 listed.
ServiceType Mask Meaning: A--PAD  C--Terminal  D--DVPN  F--FTP  P--PPP  S--SSH
T--Telnet
```

对上述显示信息的各项解释如下表所示。

表1-3 display local-user 显示信息描述表

域名	解释
State	该用户的状态（active/block）
ServiceType Mask	服务类型的缩写
Idle-cut	闲置切断开关
Access-Limit	接入用户连接数限制
Current AccessNum	当前接入用户的数量
Bind location	是否与端口捆绑
VLAN ID	用户所属的 VLAN
IP address	用户的 IP 地址
MAC address	用户的 MAC 地址

域名	解释
FTP Directory	授权给 FTP 用户的路径
User Privilege	用户级别

1.1.10 domain

【命令】

domain { *isp-name* | **default** { **disable** | **enable** *isp-name* } }

undo domain *isp-name*

【视图】

系统视图

【参数】

isp-name：ISP 域名。为不超过 24 个字符的字符串，且不能包括“/”、“:”、“*”、“?”、“<”以及“>”等字符。

default：配置缺省的 ISP 域。系统缺省的 ISP 域为 system，用户可以使用该命令手工配置缺省域。系统缺省的 ISP 域为 system。

disable：禁止配置的缺省 ISP 域，此时不带域的用户将被拒绝。如果配置了发送给 RADIUS 服务器的用户不携带域名，此时就不会被拒绝。

enable：使能配置的缺省 ISP 域，此时不带域的用户名在发往 AAA 服务器前将被加上缺省的 ISP 域名。如果配置了发送给 RADIUS 服务器的用户不携带域名，此时不带域的用户名也不会加上缺省的域名。

【描述】

domain 命令用来创建一个 ISP 域，或者进入已创建 ISP 域的视图，**undo domain** 命令用来删除指定的 ISP 域。

缺省情况下，系统中使用的域为“system”，该域不可以删除，但是可以修改其属性。通过 **display domain** 命令可以查看缺省域 system 的设置。

ISP 域即 ISP 用户群，一个 ISP 域即是由同属于一个 ISP 的用户构成的用户群。一般说来，在“userid@isp-name”形式（例如 gw20010608@test163.net）的用户名中，“@”后的“isp-name”（如例中的“test163.net”）即为 ISP 域的域名。在 AAA 服务器对用户进行接入控制时，对于用户名为“userid@isp-name”形式的 ISP 用户，系统就将把“userid”作为用于身份认证的用户名，把“isp-name”作为域名。

引入 ISP 域的设置是为了支持多 ISP 的应用环境：在这种环境中，同一个接入设备

接入的有可能是不同 ISP 的用户。由于各 ISP 用户的用户属性（例如用户名及密码构成、服务类型/权限等）有可能各不相同，因此有必要通过设置 ISP 域的方法把它们区别开。在 ISP 域视图下，可以为每个 ISP 域配置包括 AAA 方案（使用的 RADIUS 方案等）在内的一整套单独的 ISP 域属性。

对于 SecBlade 来说，每个接入用户都属于一个 ISP 域。系统中最多可以配置 16 个 ISP 域。

使用此命令时，如果指定的 ISP 域不存在，系统将会创建一个新的 ISP 域，所有的 ISP 域在创建后即处于 **active** 状态。

相关配置可参考命令 **access-limit**，**scheme**，**state**，**display domain**。

【举例】

创建一个新的 ISP 域“test163.net”，并进入其视图。

```
[SecBlade_FW] domain test163.net
```

New Domain added.

```
[SecBlade_FW-isp-test163.net]
```

1.1.11 ip pool

【命令】

ip pool *pool-number low-ip-address* [*high-ip-address*]

undo ip pool *pool-number*

【视图】

系统视图、ISP 域视图

【参数】

pool-number：地址池编号，取值范围为 0～99。

low-ip-address 和 *high-ip-address*：分别为地址池的起始和结束 IP 地址。一个地址池中起始 IP 和结束 IP 地址之间的地址数不能超过 1024。如果在定义 IP 地址池时不指定结束 IP 地址，则该地址池中只有一个 IP 地址，即起始 IP 地址。

【描述】

命令 **ip pool** 用来定义为 PPP 用户分配 IP 地址的本地地址池，命令 **undo ip pool** 用来删除指定的本地地址池。

缺省情况下，没有配置本地 IP 地址池。

在系统视图下，配置 IP 地址池，通过在接口视图下使用命令 **remote address** 为 PPP 用户分配 IP 地址。

在 ISP 域视图下，配置的 IP 地址池用于为相应的 ISP 域所属的 PPP 用户分配 IP 地

址。这主要用于通过某接口接入的 PPP 用户较多，而接口所能分配的地址不够用的情况。例如，运行 PPPoE 协议的 Ethernet 接口，最多可以接入 4095 个用户，但在该 Ethernet 接口的 Virtual Template 上，只能配置一个地址池，而一个地址池最多只有 1024 个地址，这显然不能满足要求。通过配置 ISP 域的地址池，可以为 ISP 的 PPP 用户分配地址，从而解决接口地址池中地址不够的问题。

相关配置可参考命令 **remote address**。

【举例】

配置本地 IP 地址池 0，地址范围为 129.102.0.1 到 129.102.0.10。

```
[SecBlade_FW] domain test163.net
[SecBlade_FW-isp-test163.net] ip pool 0 129.102.0.1 129.102.0.10
```

1.1.12 level

【命令】

level *level*

undo level

【视图】

本地用户视图

【参数】

level：指定用户的优先级。*level* 为整数，取值范围 0~3。

【描述】

level 命令用来设置用户的优先级，**undo level** 命令用来恢复用户缺省的优先级。

缺省情况下，用户的优先级为 0。

相关配置可参考命令 **local user**。

📖 **说明：**

如果配置的认证方式为不认证或采用 password 认证，则用户登录到系统后所能访问的命令级别由用户界面的优先级确定。对于使用 RSA 认证的用户，其所能访问的命令级别由用户界面的优先级确定。如果配置的认证方式需要用户名和口令，则用户登录系统后所能访问的命令级别由用户的优先级确定。

【举例】

设置用户 test 的级别为 3。

```
[SecBlade_FW-luser-test] level 3
```

1.1.13 local-user

【命令】

local-user *user-name*

undo local-user *user-name* [**service-type** | **level**]

undo local-user all [**service-type** { **ftp** | **ppp** | **ssh** | **telnet** | **terminal** }]

【视图】

系统视图

【参数】

user-name：本地用户名。为不超过 80 个字符的字符串，字符串中不能包括“/”、“:”、“*”、“?”、“<”以及“>”等字符，并且“@”出现的次数不能多于 1 次，纯用户名（“@”以前部分，即用户标识）不能超过 55 个字符。用户名不区分大小写，输入 UserA 和 usera，系统视为同一用户。

service-type：服务类型。

all：所有的用户。

ftp：服务类型为 FTP。

ppp：服务类型为 PPP。

ssh：服务类型为 SSH。

telnet：服务类型为 Telnet。

terminal：终端服务类型。

【描述】

local-user 命令用来添加本地用户并进入本地用户视图，**undo local-user** *user-name* 命令用来删除本地用户或本地用户的相关属性，**undo local-user all** 命令用来删除所有本地用户或指定类型的本地用户。

缺省情况下，无本地用户。

相关配置可参考命令 **display local-user**。

【举例】

添加名称为 test1 的本地用户。

```
[SecBlade_FW] local-user test1
[SecBlade_FW-luser-test1]
```

1.1.14 local-user password-display-mode

【命令】

local-user password-display-mode { **cipher-force** | **auto** }

undo local-user password-display-mode

【视图】

系统视图

【参数】

cipher-force：强制 cipher 方式，即所有接入用户的密码显示方式必须采用密文方式。

auto：自动方式，即接入用户的密码显示方式可以由用户自己通过 **password** 命令来设置。

【描述】

local-user password-display-mode 命令用来设置所有本地用户密码的显示方式，**undo local-user password-display-mode** 命令用来恢复缺省的本地用户密码显示方式。

当采用 **cipher-force** 方式后，即使用户通过 **password** 命令指定密码显示方式为明文显示（即 **simple** 方式）后，也不起作用。

缺省情况下，所有接入用户的密码显示方式 **auto**。

相关配置可参考命令 **display local-user， password**。

【举例】

强制所有接入用户采用密码密文方式显示。

```
[SecBlade_FW] local-user password-display-mode cipher-force
```

1.1.15 password

【命令】

password { **simple** | **cipher** } *password*

undo password

【视图】

本地用户视图

【参数】

simple：表示密码为明文。

cipher：表示密码为密文。

password：表示设置的密码。

当采用 **simple** 明文密码时，*password* 为明文验证字，长度为 1～16 个字符。

当采用 **cipher** 密文密码时，*password* 为密文验证字。如果以明文形式输入，长度为 1～16 个字符，如：1234567；如果以密文形式输入，长度必须为 24，并且必须是密文形式，如：_(TT8F]Y\5SQ=^Q`MAF4<1!!。

【描述】

password 命令用来设置本地用户的密码，**undo password** 命令用来取消本地用户的密码。

需要注意的是，当采用 **local-user password-display-mode cipher-force** 命令后，即使用户通过 **password** 命令指定密码显示方式为明文显示（即 **simple** 方式）后，也不起作用。

相关配置可参考命令 **display local-user**。

【举例】

设置名称为 test1 的用户采用明文加密方式，密码为 20030422。

```
[SecBlade_FW-luser-test1] password simple 20030422
```

1.1.16 scheme

【命令】

scheme { **radius-scheme** *radius-scheme-name* [**local**] | **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** }

undo scheme [**radius-scheme** | **hwtacacs-scheme** | **none**]

【视图】

ISP 域视图

【参数】

radius-scheme-name：RADIUS 方案名，为不超过 32 个字符的字符串。

hwtacacs-scheme-name：HWTACACS 方案名，为不超过 32 个字符的字符串。

local：本地认证。

none：不进行认证。

【描述】

scheme 命令用来配置当前 ISP 域使用的 AAA 方案。**undo scheme** 命令用来恢复域缺省的 AAA 方案。

系统缺省使用的 AAA 方案为 **local**。

scheme 命令为当前 ISP 域指定引用的 RADIUS/HWTACACS 方案。所指定引用的 RADIUS/**HWTACACS** 方案必须是已经设置好的。

如果配置了 **radius-scheme** *radius-scheme-name* **local** 或 **hwtacacs-scheme** *hwtacacs-scheme-name* **local**，则 **local** 为 **radius server** 或 **tacacs server** 没有正常响应后的备选认证方案。即当 RADIUS 服务器或 TACACS 服务器有效时，不使用本地认证；当 RADIUS 服务器或 TACACS 服务器无效时，使用本地认证。

如果 **local** 作为第一方案，那么只能采用本地认证，不能再同时采用 RADIUS 或 HWTACACS 方案。

如果 **none** 作为第一方案，那么将不采用认证，且不能再同时采用 RADIUS 或 HWTACACS 方案。

当对 FTP 用户进行验证时，不能使用 none 认证，因为 CMW 实现的 FTP 服务器不支持匿名用户登录。

如果配置 **scheme none**，则用户登录到系统后所拥有的级别为 level 0。

相关配置可参考命令 **radius scheme**，**hwtacacs scheme**。

【举例】

指定当前 ISP 域“test163.net”引用的 RADIUS 方案为“test”。

```
[SecBlade_FW-isp-test163.net] scheme radius Test
```

设置 ISP 域 test 引用的方案为 RADIUS 方案“rd”，并采用 local 作为备选认证 scheme。

```
[SecBlade_FW-isp-test] scheme radius-scheme rd local
```

设置 ISP 域 test 引用的方案为 HWTACACS 方案“hwtac”，并采用 local 作为备选认证 scheme。

```
[SecBlade_FW-isp-test] scheme hwtacacs-scheme hwtac local
```

1.1.17 service-type

【命令】

service-type { **telnet** | **ssh** | **terminal** }* [**level** *level*]

undo service-type { **telnet** | **ssh** | **terminal** }*

【视图】

本地用户视图

【参数】

telnet：授权用户可以使用 Telnet 服务。

ssh：授权用户可以使用 SSH 服务。

terminal：授权用户可以使用 terminal 服务（即从 Console 口、AUX 口登录）。

level *level*：指定用户的优先级。*level* 为整数，取值范围 0～3。

【描述】

service-type 命令用来设置用户可以使用的服务类型，**undo service-type** 命令用来删除用户可以使用的服务类型。

缺省情况下，系统不对用户授权任何服务。

相关配置可参考命令 **service-type ppp**，**service-type ftp**。

【举例】

设置用户可以使用 Telnet 服务。

```
[SecBlade_FW-luser-test1] service-type telnet
```

1.1.18 service-type dvpn

【命令】

service-type dvpn

undo service-type dvpn

【视图】

本地用户视图

【参数】

无

【描述】

service-type dvpn 命令用来授权用户可以使用 DVPN 服务，**undo service-type dvpn** 命令用来取消用户可以使用 DVPN 服务。

缺省情况下，用户未被授权使用 DVPN 服务。

【举例】

授权用户可以使用 DVPN 服务。

```
[SecBlade_FW-luser-test1] service-type dvpn
```

1.1.19 service-type ftp

【命令】

service-type ftp [**ftp-directory** *directory*]

undo service-type ftp [**ftp-directory**]

【视图】

本地用户视图

【参数】

ftp-directory *directory*：授权 FTP 用户可以访问的目录。

【描述】

service-type ftp 命令用来授权用户可以使用 FTP 服务和 FTP 用户可以访问的目录，**undo service-type ftp** 命令用来取消用户可以使用 FTP 服务和恢复对 FTP 用户授权的缺省目录。

缺省情况下，系统不对用户授权任何服务；若授权 FTP 服务，缺省授权使用根目录 flash:/。缺省情况下，系统不支持 FTP 匿名用户访问。

【举例】

授权用户可以使用 FTP。

```
[SecBlade_FW-luser-test1] service-type ftp
```

1.1.20 service-type ppp

【命令】

service-type ppp

undo service-type ppp

【视图】

本地用户视图

【参数】

无

【描述】

service-type 命令用来授权用户可以使用 PPP 服务，**undo service-type** 命令用来取消用户可以使用 PPP 服务。

缺省情况下，系统不对用户授权任何服务。

【举例】

设置用户可以使用 PPP 服务。

```
[SecBlade_FW-luser-test1] service-type ppp
```

1.1.21 state

【命令】

state { **active** | **block** }

【视图】

ISP 域视图，本地用户视图

【参数】

active：指定当前 ISP 域（ISP 域视图）/当前本地用户（本地用户视图）处于“活动”状态，即系统允许该域下的用户（ISP 域视图）/当前本地用户（本地用户视图）请求网络服务。

block：指定当前 ISP 域（ISP 域视图）/当前本地用户（本地用户视图）处于“挂起”状态，即系统不允许该域下的用户（ISP 域视图）/当前本地用户（本地用户视图）请求网络服务。

【描述】

state 命令用来设置当前 ISP 域/当前本地用户的状态。

缺省情况下，当一个 ISP 域被创建以后，其状态为 **active**（ISP 域视图）。

当一个本地用户被创建以后，其状态为 **active**（本地用户视图）。

在 ISP 域视图下，每个 ISP 域有两个状态：active 或 block。当指示某个 ISP 域处于 active 状态时，允许该域下的用户请求网络服务；当指示某个 ISP 域处于 block 状态时，不允许该域下的用户请求网络服务，但是不影响已经在线的用户。本地用户视图下同理。

相关配置可参考命令 **domain**。

【举例】

设置当前 ISP 域“test163.net”处于“挂起”状态，其下的接入用户不能再请求网络服务。

```
[SecBlade_FW-isp-test163.net] state block
```

设置用户 test1 处于“挂起”状态。

```
[SecBlade_FW-user-test1] state block
```

1.1.22 super authentication-mode

【命令】

super authentication-mode { **super-password** | **scheme** }*

undo super authentication-mode

【视图】

用户界面视图

【参数】

super-password：采用 super-password 进行认证。

scheme：采用用户配置方案进行认证。

【描述】

super authentication-mode 命令用来配置 super 认证方式，**undo super authentication-mode** 命令用来恢复 super 认证方式为缺省值。

缺省情况下，采用 super-password 认证。

【举例】

配置 console 用户采用 scheme 认证方式。

```
<SecBlade_FW> system-view
[SecBlade_FW] user-interface console 0
[SecBlade_FW-ui-con0] super authentication-mode scheme
```

1.2 RADIUS 协议配置命令

1.2.1 accounting optional

【命令】

accounting optional

undo accounting optional

【视图】

RADIUS 域视图

【参数】

无

【描述】

accounting optional 命令用来打开计费可选开关，**undo accounting optional** 命令用来关闭计费可选开关。

系统缺省为关闭计费可选开关。

当没有可用的计费服务器或与计费服务器通信失败时，若配置了 **accounting optional** 命令，则用户可以继续使用网络资源，否则用户将被切断。这个命令经常被用于只认证不计费的情况。

【举例】

打开 RADIUS 方案“test”的计费可选开关。

```
[SecBlade_FW-radius-test] accounting optional
```

1.2.2 data-flow-format

【命令】

data-flow-format data { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** }

undo data-flow-format

【视图】

RADIUS 视图

【参数】

data：设置数据的单位。

byte：数据单位为字节。

giga-byte：数据单位千兆字节。

kilo-byte：数据单位为千字节。

mega-byte：数据单位为兆字节。

packet：设置数据包的单位。

giga-packet：数据包的单位为“giga-packet”。

kilo-packet：数据包的单位为“kilo-packet”。

mega-packet：数据包的单位为“mega -packet”。

one-packet：数据包的单位为“one-packet”。

【描述】

data-flow-format 命令用来配置发送到 RADIUS 服务器的数据流的单位。**undo data-flow-format** 命令用来恢复发送到 RADIUS 服务器的数据流的单位为缺省设置。

缺省情况下，数据的单位为 byte，数据包的单位为 one-packet。

相关配置可参考命令 **display radius**。

【举例】

设置发往服务器 test 的数据流的单位为千字节，数据包的单位为 kilo-packet

```
[SecBlade_FW-radius-test] data-flow-format data kilo-byte packet kilo-packet
```

1.2.3 debugging local-server

【命令】

debugging local-server { **all** | **error** | **event** | **packet** }

undo debugging local-server { **all** | **error** | **event** | **packet** }

【视图】

用户视图

【参数】

all：所有调试开关。

error：错误调试开关。

event：事件调试开关。

packet：报文调试开关。

【描述】

debugging local-server 命令用来打开本地 RADIUS 认证服务器的调试开关，**undo debugging local-server** 命令用来关闭本地 RADIUS 认证服务器的调试开关。

缺省情况下，关闭本地 RADIUS 认证服务器的调试开关。

【举例】

打开本地 RADIUS 认证服务器的调试开关

```
[SecBlade_FW] debugging local-server all
*0.9045238 SecBlade_FW LS/8/EVENT-MSG:Message  received. MessageType = 1
*0.9045238 SecBlade_FW LS/8/PACKET:Packet Received,Code = 1
*0.9045239 SecBlade_FW LS/8/PACKET:Packet Send auth pkt ,Code = 2
```

1.2.4 debugging radius

【命令】

debugging radius packet

undo debugging radius packet

【视图】

用户视图

【参数】

packet：打开报文调试开关。

【描述】

debugging radius 命令用来使能 RADIUS 协议的调试功能。**undo debugging radius** 命令用来禁止 RADIUS 协议的调试功能。

缺省情况下，禁止 RADIUS 协议的调试功能。

【举例】

使能 RADIUS 协议的报文调试功能。

```
<SecBlade_FW> debugging radius packet
```

1.2.5 display local-server statistics

【命令】

display local-server statistics

【视图】

所有视图

【参数】

无

【描述】

display local-server statistics 命令用来显示本地 RADIUS 认证服务器的统计信息。

相关配置可参考命令 **local-server**。

【举例】

显示本地 RADIUS 认证服务器的统计信息。

```
<SecBlade_FW> display local-server statistics
The localserver packet statistics:
Receive:                  82          Send:                     61
Discard:                  21          Receive Packet Error:     0
Auth Receive:             82          Auth Send:                61
Acct Receive:             0           Acct Send:                0
```

1.2.6 display radius scheme

【命令】

display radius scheme [*radius-scheme-name*]

【视图】

所有视图

【参数】

radius-scheme-name：RADIUS 方案名，为不超过 32 个字符的字符串。此项如果为空，则显示所有 RADIUS 方案的配置信息。

【描述】

display radius scheme 命令用来显示所有或指定 RADIUS 方案的配置信息或统计信息。

缺省情况下，显示所有 RADIUS 方案的配置信息。

相关配置可参考命令 **radius scheme**。

【举例】

显示所有 RADIUS 方案的配置信息。

```
<SecBlade_FW> display radius scheme
------------------------------------------------------------------------
SchemeName  = system                    Index=0    Type=extended
Primary Auth IP  =127.0.0.1        Port=1645   State=active
Primary Acct IP  =127.0.0.1        Port=1646   State=active
Second  Auth IP  =0.0.0.0          Port=1812   State=block
Second  Acct IP  =0.0.0.0          Port=1813   State=block
Auth Server Encryption Key= Not configured
Acct Server Encryption Key= Not configured
Accounting method = required
TimeOutValue(in second)=3 RetryTimes=3 RealtimeACCT(in minute)=12
Permitted send realtime PKT failed counts       =5
Retry sending times of noresponse acct-stop-PKT =500
Quiet-interval(min)                             =5
Username format                                 =without-domain
Data flow unit                                  =Byte
Packet unit                                     =One Packet

------------------------------------------------------------------------
Total 1 RADIUS scheme(s). 1 listed
```

表1-4 Radius 服务器配置信息描述表

域名	描述
SchemeName	RADIUS 方案的名称
Index	RADIUS 方案的索引号
Type	RADIUS 服务器的类型
Primary Auth IP/ Port/ State	主认证服务器 IP 地址/接入端口号/该服务器目前状态
Primary Acct IP/ Port/ State	主计费服务器 IP 地址/接入端口号/该服务器目前状态
Second Auth IP/ Port/ State	备认证服务器 IP 地址/接入端口号/该服务器目前状态
Second Acct IP/ Port/ State	备计费服务器 IP 地址/接入端口号/该服务器目前状态
Auth Server Encryption Key	认证服务器的共享密钥
Acct Server Encryption Key	计费服务器的共享密钥
TimeOutValue (seconds)	RADIUS 服务器响应超时定时器时长
Permitted send realtime PKT failed counts	允许发送的实时计费请求无响应报文的最大次数
Retry sending times of noresponse acct-stop-PKT	缓存的停止计费请求报文的最大重发次数
Quiet-interval(min)	主服务器恢复激活状态的时间
Username format	用户名的格式
Data flow unit	数据流的单位
Packet unit	数据包的单位

1.2.7 display radius statistics

【命令】

display radius statistics

【视图】

所有视图

【参数】

无

【描述】

display radius statistics 命令用来显示 RADIUS 报文的统计信息。根据显示的信息，可以帮助诊断与排除 RADIUS 相关故障。

相关配置可参考命令 **radius scheme**。

【举例】

显示 RADIUS 报文的统计信息。

```
<SecBlade_FW> display radius statistics
state statistic(total=1048):
     DEAD=1047     AuthProc=0        AuthSucc=0
AcctStart=0         RLTSend=0         RLTWait=1
 AcctStop=0          OnLine=1             Stop=0
 StateErr=0

Received and Sent packets statistic:
Sent PKT total  :38       Received PKT total:2
Resend Times     Resend total
1                12
2                12
Total            24
RADIUS received packets statistic:
Code= 2,Num=1       ,Err=0
Code= 3,Num=0       ,Err=0
Code= 5,Num=1       ,Err=0
Code=11,Num=0       ,Err=0

Running statistic:
RADIUS received messages statistic:
Normal auth request             , Num=13      , Err=0       , Succ=13
EAP auth request                , Num=0       , Err=0       , Succ=0
Account request                 , Num=1       , Err=0       , Succ=1
Account off request             , Num=0       , Err=0       , Succ=0
PKT auth timeout                , Num=36      , Err=12      , Succ=24
PKT acct_timeout                , Num=0       , Err=0       , Succ=0
Realtime Account timer          , Num=0       , Err=0       , Succ=0
PKT response                    , Num=2       , Err=0       , Succ=2
EAP reauth_request              , Num=0       , Err=0       , Succ=0
PORTAL access                   , Num=0       , Err=0       , Succ=0
Update ack                      , Num=0       , Err=0       , Succ=0
PORTAL access ack               , Num=0       , Err=0       , Succ=0
Session ctrl pkt                , Num=0       , Err=0       , Succ=0
RADIUS sent messages statistic:
Auth accept                     , Num=0
Auth reject                     , Num=0
EAP auth replying               , Num=0
Account success                 , Num=0
```

```
Account failure                , Num=0
Cut req                        , Num=0
RecError_MSG_sum:0        SndMSG_Fail_sum :0
Timer_Err        :0       Alloc_Mem_Err   :0
State Mismatch   :0       Other_Error     :0

No-response-acct-stop packet =0
Discarded No-response-acct-stop packet for buffer overflow =0
```

表1-5 display radius statistics 显示信息描述表

域名	描述
state statistic(total=1048) DEAD=1047 AuthProc=0 AuthSucc=0 AcctStart=0 RLTSend=0 RLTWait=1 AcctStop=0 OnLine=1 Stop=0 StateErr=0	状态统计信息
Received and Sent packets statistic: Sent PKT total :38 Received PKT total:2 Resend Times Resend total 1 12 2 12 Total 24 RADIUS received packets statistic: Code= 2,Num=1 ,Err=0 Code= 3,Num=0 ,Err=0 Code= 5,Num=1 ,Err=0 Code=11,Num=0 ,Err=0	收发包统计信息： 共发送包数：38 共接收包数：2 重发次数： 重发包总数： 1 12 2 12 总共 24 RADIUS 接收报文统计信息： Code= 2,Num=1 ,Err=0 收到 1 个认证回应包，没有错误包 Code= 3,Num=0 ,Err=0 收到 1 个认证拒绝包，没有错误包 Code= 5,Num=1 ,Err=0 收到 1 个计费回应包，没有错误包 Code=11,Num=0 ,Err=0 收到一个 Access-Challenge（EAP 认证）包，没有错误包

域名	描述
Running statistic: RADIUS received messages statistic: Normal auth request , Num=13 , Err=0 , Succ=13 EAP auth request , Num=0 , Err=0 , Succ=0 Account request , Num=1 , Err=0 , Succ=1 Account off request , Num=0 , Err=0 , Succ=0 PKT auth timeout , Num=36 , Err=12 , Succ=24 PKT acct_timeout , Num=0 , Err=0 , Succ=0 Realtime Account timer , Num=0 , Err=0 , Succ=0 PKT response , Num=2 , Err=0 , Succ=2 EAP reauth_request , Num=0 , Err=0 , Succ=0 PORTAL access , Num=0 , Err=0 , Succ=0 Update ack , Num=0 , Err=0 , Succ=0 PORTAL access ack , Num=0 , Err=0 , Succ=0 Session ctrl pkt , Num=0 , Err=0 , Succ=0 RADIUS sent messages statistic: Auth accept , Num=0 Auth reject , Num=0 EAP auth replying , Num=0 Account success , Num=0 Account failure , Num=0 Cut req , Num=0 RecError_MSG_sum:0 SndMSG_Fail_sum :0 Timer_Err :0 Alloc_Mem_Err :0 State Mismatch :0 Other_Error :0	- RADIUS 接收信息统计： 正常认证请求 数目＝13，错误＝0，成功＝0 EAP 认证请求 数目＝0，错误＝0，成功＝0 计费请求 数目＝0，错误＝0，成功＝0 计费停止请求 数目＝0，错误＝0，成功＝0 认证超时 数目＝36，错误＝0，成功＝0 计费超时 数目＝0，错误＝0，成功＝0 实时计费次数 数目＝0，错误＝0，成功＝0 回复包 数目＝2，错误＝0，成功＝2 EAP 重认证请求 数目＝0，错误＝0，成功＝0 PORTAL 接入认证请求 数目＝13，错误＝0，成功＝0 升级包 数目＝0，错误＝0，成功＝0 会话控制包 认证请求 数目＝0，错误＝0，成功＝0 RADIUS 发送信息统计 认证通过，数目＝0 认证拒绝，数目＝0 计费成功，数目＝0 计费失败，数目＝0 EAP 认证回应，数目＝0 计费成功，数目＝0 计费失败，数目＝0 删除请求，数目＝0 接收错误信息数：0 发送信息失败数：0 时间错误 ：0 分配内存错误：0 状态不匹配：0 其他错误：0

域名	描述
No-response-acct-stop packet =0	无响应的停止计费报文数为 0
Discarded No-response-acct-stop packet for buffer overflow =0	由于缓存溢出而丢弃的无响应停止计费报文数为 0

1.2.8 display stop-accounting-buffer

【命令】

display stop-accounting-buffer { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }

【视图】

所有视图

【参数】

radius-scheme *radius-scheme-name*：根据 RADIUS 方案名显示暂存的停止计费请求报文。其中，*radius-scheme-name* 为 RADIUS 方案名，为不超过 32 个字符的字符串，且不能包括“/”、“:”、“*”、“?”、“<”以及“>”等字符。

session-id *session-id*：根据会话 ID 显示暂存的停止计费请求报文。其中，*session-id* 为会话 ID，为不超过 50 个字符的字符串。

time-range *start-time stop-time*：根据停止计费请求时刻显示暂存的停止计费请求报文。其中，*start-time* 为请求时间段的起始时间；*stop-time* 为请求时间段的结束时间，格式为 hh:mm:ss- mm/dd/yyyy（时:分:秒-月/日/年）或 *hh:mm:ss-yyyy/mm/dd*（时:分:秒-年/月/日）。

user-name *user-name*：根据用户名显示暂存的停止计费请求报文。

【描述】

display stop-accounting-buffer 命令用来显示缓存在 SecBlade 中的停止计费请求报文。可以选择显示发往某个 RADIUS 方案的报文；也可以根据用户会话的 session-id 或用户名来显示报文；还可以指定一个时间段，显示那些发起停止计费请求的时刻处于指定时间段内的报文。根据显示的报文信息，可以帮助诊断与排除 RADIUS 相关故障。

在发送停止计费请求报文而 RADIUS 服务器没有响应时，SecBlade 会缓存该报文，然后以一定的次数重新发送，具体发送的次数由 **retry stop-accounting** 命令设置。

相关配置可参考命令 **reset stop-accounting-buffer**，**stop-accounting-buffer enable**， **retry stop-accounting**。

【举例】

显示从 2002 年 8 月 31 日 0 点 0 分 0 秒到 2002 年 8 月 31 日 23 点 59 分 59 秒期间内系统缓存的停止计费请求报文。

```
<SecBlade_FW> display stop-accounting-buffer time-range 0:0:0-08/31/2002
23:59:59-08/31/2002
Total find    0 record
```

1.2.9 key

【命令】

key { **accounting** | **authentication** } *string*

undo key { **accounting** | **authentication** }

【视图】

RADIUS 视图

【参数】

accounting：设置/删除 RADIUS 计费报文的共享密钥。

authentication：设置/删除 RADIUS 认证/授权报文的共享密钥。

string：密钥。为不超过 16 个字符的字符串。

【描述】

key 命令用来设置 RADIUS 认证/授权或计费报文的共享密钥，**undo key** 命令用来恢复相应的共享密钥为缺省设置。

RADIUS 客户端（即 SecBlade）与 RADIUS 服务器使用 MD5 算法来加密交互的 RADIUS 报文，双方通过设置共享密钥来验证报文的合法性。只有在密钥一致的情况下，双方才能彼此接收对方发来的报文并作出响应。因此，必须保证：SecBlade 上设置的共享密钥与 RADIUS 服务器上的完全一样。在认证/授权服务器与计费服务器不相同且这两台服务器中的共享密钥也不同时，必须分别设置认证/授权报文和计费报文的共享密钥。

缺省情况下，认证/授权报文和计费报文的密钥为为空。

相关配置可参考命令 **primary accounting**， **primary authentication**， **radius scheme**。

【举例】

将 RADIUS 方案“test”的认证/授权报文的共享密钥设置为“hello”。

```
[SecBlade_FW-radius-test] key authentication hello
```

将 RADIUS 方案“test”的计费报文的共享密钥设置为“ok”。

```
[SecBlade_FW-radius-test] key accounting ok
```

1.2.10 local-server

【命令】

local-server nas-ip *ip-address* **key** *password*

undo local-server nas-ip *ip-address*

【视图】

系统视图

【参数】

nas-ip *ip-address*：设置接入服务器的 NAS-IP 地址，地址采用点分十进制格式。

key *password*：设置本地服务器的共享密钥，*password* 为密钥，为不超过 16 个字符的字符串。

【描述】

local-server 命令用来设置本地 RADIUS 认证服务器的相关参数，**undo local-server** 命令用来删除设置的本地 RADIUS 认证服务器。

缺省情况下，系统创建了一个 NAS-IP 为 127.0.0.1、密钥为空的本地 RADIUS 认证服务器。

需要注意以下几点：

- 设备除了支持传统的作为 RADIUS 客户端的服务——即分别采用认证/授权服务器、计费服务器的方式进行用户的认证管理外，还提供了本地简单 RADIUS 服务器端功能（包括认证和授权），称之为本地 RADIUS 认证服务器功能。
- 采用本地 RADIUS 认证服务器功能时，其认证/授权服务的 UDP 端口号必须为 1645，计费服务的 UDP 端口号为 1646。
- 用此命令配置的报文加密密钥（key password）必须和在 RADIUS 方案视图下用命令 key authentication 配置的认证/授权报文加密密钥一致。
- 包括系统缺省创建的本地 RADIUS 认证服务器在内，设备最多支持 16 个本地 RADIUS 认证服务器。

相关配置可参考命令 **radius scheme**，**state**。

【举例】

设置本地 RADIUS 认证服务器的 IP 地址为 10.110.1.2、登录密码为 aabbcc。

```
[SecBlade_FW] local-server nas-ip 10.110.1.2 key aabbcc
```

1.2.11 nas-ip

【命令】

nas-ip *ip-address*

undo nas-ip

【视图】

RADIUS 视图

【参数】

ip-address：IP 地址，点分十进制形式。

【描述】

nas-ip 命令用来设置 NAS（SecBlade）发送 RADIUS 报文使用的源 IP 地址，这样发送到 RADIUS 服务器的所有报文携带相同的源 IP 地址。**undo nas-ip** 命令用来删除配置。

指定发送 RADIUS 报文使用的源地址，可以避免物理接口故障时从服务器返回的报文不可达。一般推荐使用 loopback 接口地址。

缺省情况下，报文的源 IP 地址是发送端口的 IP 地址。

相关配置可参考命令 **display radius**。

【举例】

配置 NAS（SecBlade）发送 RADIUS 报文使用的源 IP 地址为 10.1.1.1。

```
[SecBlade_FW] radius scheme test1
[SecBlade_FW-radius-test1] nas-ip 10.1.1.1
```

1.2.12 primary accounting

【命令】

primary accounting *ip-address* [*port-number*]

undo primary accounting

【视图】

RADIUS 视图

【参数】

ip-address：IP 地址，为点分十进制格式。缺省情况下，在 system 方案中，主计费服务器的 IP 地址为 127.0.0.1，新创建的 RADIUS 方案中的主计费服务器的 IP 地址均为 0.0.0.0。

port-number：UDP 端口号。取值范围为 1～65535。缺省情况下，在 system 方案中，主计费服务的 UDP 端口号为 1646，新创建的 RADIUS 方案中的主计费服务的 UDP 端口号为 1813。

【描述】

primary accounting 命令用来设置主 RADIUS 计费服务器的 IP 地址和端口号，**undo primary accounting** 命令用来将主 RADIUS 计费服务器的 IP 地址和端口号恢复为缺省值。

当创建一个新的 RADIUS 方案之后，需要对属于此方案的 RADIUS 服务器的 IP 地址和 UDP 端口号进行设置，这些服务器包括认证/授权和计费服务器，而每种服务器又有主服务器和备服务器的区别。在实际组网环境中，上述参数的设置需要根据具体需求来决定。但是必须至少设置一个认证/授权服务器和一个计费服务器。同时在配置过程中，请保证 SecBlade 上的 RADIUS 服务端口设置与 RADIUS 服务器上的端口设置保持一致。

在计费成功后，计费更新以及计费停止报文都会发往计费成功时使用的服务器上，即使此服务器不可用，也不会发生主备切换。只有在最开始的认证、授权、计费过程中才会发生切换，成功后将不再切换。

相关配置可参考命令 **key**，**radius scheme**，**state**。

【举例】

设置 RADIUS 方案“test”的主计费服务器的 IP 地址为 10.110.1.2，使用 UDP 端口 1813 提供 RADIUS 计费服务。

```
[SecBlade_FW-radius-test] primary accounting 10.110.1.2 1813
```

1.2.13 primary authentication

【命令】

primary authentication *ip-address* [*port-number*]

undo primary authentication

【视图】

RADIUS 视图

【参数】

ip-address：IP 地址，为点分十进制格式。缺省情况下，在 system 方案中，主认证/授权服务器的 IP 地址为 127.0.0.1，新创建的 RADIUS 方案中的主认证/授权服务器的 IP 地址均为 0.0.0.0。

port-number：UDP 端口号。取值范围为 1～65535。缺省情况下，在 system 方案中，主认证/授权服务的 UDP 端口号为 1645，新创建的 RADIUS 方案中的主认证/授权服务的 UDP 端口号为 1812。

【描述】

primary authentication 命令用来设置主 RADIUS 认证/授权的 IP 地址和端口号，**undo primary authentication** 命令用来将主 RADIUS 认证/授权的 IP 地址和端口号恢复为缺省值。

当创建一个新的 RADIUS 方案之后，需要对属于此方案的 RADIUS 服务器的 IP 地址和 UDP 端口号进行设置，这些服务器包括认证/授权和计费服务器，而每种服务器又有主服务器和备服务器的区别。在实际组网环境中，上述参数的设置需要根据具体需求来决定。但是必须至少设置一个认证/授权服务器和一个计费服务器。同时在配置过程中，请保证 SecBlade 上的 RADIUS 服务端口设置与 RADIUS 服务器上的端口设置保持一致。

相关配置可参考命令 **key**，**radius scheme**，**state**。

【举例】

设置 RADIUS 方案“test”的主认证/授权服务器的 IP 地址为 10.110.1.1、使用 UDP 端口 1812 提供 RADIUS 认证/授权服务。

```
[SecBlade_FW-radius-test] primary authentication 10.110.1.1 1812
```

1.2.14 radius scheme

【命令】

radius scheme *radius-scheme-name*

undo radius scheme *radius-scheme-name*

【视图】

系统视图

【参数】

radius-scheme-name：RADIUS 方案名，为不超过 32 个字符的字符串。

【描述】

radius scheme 命令用来创建 RADIUS 方案并进入其视图，**undo radius scheme** 命令用来删除指定的 RADIUS 方案。

缺省情况下，系统中已创建了一个名为“system”的 RADIUS 方案，其各项属性均为缺省值，该方案不可以修改。可以用 **display radius** 命令来查看缺省 RADIUS 方案 system 的设置。

RADIUS 协议的配置是以 RADIUS 方案为单位进行的。每个 RADIUS 方案至少须指明 RADIUS 认证/授权/计费服务器的 IP 地址、UDP 端口号以及 RADIUS 客户端（SecBlade）与之交互所需的一些参数。因此，在进行其它 RADIUS 协议配置之前，必须先创建 RADIUS 方案并进入其视图。

一个 RADIUS 方案可以同时被多个 ISP 域引用。

undo radius scheme 命令虽然可以用来删除指定的 RADIUS 方案，但是不能删除缺省的 RADIUS 方案。注意：当有使用 RADIUS 方案的用户在线时不允许删除。

相关配置可参考命令 **key**，**retry realtime-accounting**，**scheme**，**timer realtime-accounting**，**stop-accounting-buffer enable**，**retry stop-accounting**，**server-type**，**state**，**user-name-format**，**retry**，**display radius**，**display radius statistics**。

【举例】

创建名为“test”的 RADIUS 方案并进入其视图。

```
[SecBlade_FW] radius scheme test
[SecBlade_FW-radius-test]
```

1.2.15 radius nas-ip

【命令】

radius nas-ip *ip-address*

undo radius nas-ip

【视图】

系统视图

【参数】

ip-address：指定的源 IP 地址，应该为本机的地址，禁止配置全 0 地址、D 类地址、网络地址、以及 127 网段地址。

【描述】

radius nas-ip 命令用来指定 NAS 发送 RADIUS 报文使用的源地址。**undo radius nas-ip** 命令用来恢复缺省状态。

指定发送 RADIUS 报文使用的源地址，可以避免物理接口故障时从服务器返回的报文不可达。一般推荐使用 loopback 接口地址。

缺省情况下，不指定源地址，即以发送报文的接口地址作为源地址。

本命令只能指定一个源地址，新配置的源地址会覆盖原有的源地址。

相关配置可参考命令 **nas-ip**。

【举例】

配置 SecBlade 发送 RADIUS 报文使用的源地址为 129.10.10.1。

```
[SecBlade_FW] radius nas-ip 129.10.10.1
```

1.2.16 radius trap

【命令】

radius trap { **authentication-server-down** | **accounting-server-down** }

undo radius trap { **authentication-server-down** | **accounting-server-down** }

【视图】

系统视图

【参数】

authentication-server-down：RADIUS 认证服务器状态变为 down；

accounting-server-down：RADIUS 计费服务器状态变为 down。

【描述】

radius trap 命令用来使能 RADIUS 服务器状态变为 down 时发送 trap 报文的功能，**undo radius trap** 用来关闭 RADIUS 服务器状态变为 down 时发送 trap 报文的功能。

缺省情况下，关闭该功能。

【举例】

使能 RADIUS 认证服务器状态变为 down 时发送 trap 报文的功能。

```
[SecBlade_FW] radius trap authentication-server-down
```

1.2.17 reset radius statistics

【命令】

reset radius statistics

【视图】

用户视图

【参数】

无

【描述】

reset radius statistics 命令用来清除 RADIUS 协议的统计信息。

相关配置请参考命令 **display radius**。

【举例】

清除 RADIUS 协议的统计信息。

```
<SecBlade_FW> reset radius statistics
```

1.2.18 reset stop-accounting-buffer

【命令】

reset stop-accounting-buffer { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }

【视图】

用户视图

【参数】

radius-scheme *radius-scheme-name*：根据 RADIUS 方案名删除暂存的停止计费请求报文。其中，*radius-scheme-name* 为 RADIUS 方案名，为不超过 32 个字符的字符串。

session-id *session-id*：根据会话 ID 删除暂存的停止计费请求报文。其中，*session-id* 为会话 ID，为不超过 50 个字符的字符串。

time-range *start-time stop-time*：根据停止计费请求时刻删除暂存的停止计费请求报文。其中，*start-time* 为请求时间段的起始时间；*stop-time* 为请求时间段的结束时间，格式为 *hh:mm:ss-mm/dd/yyyy*（时:分:秒-月/日/年）或 *hh:mm:ss-yyyy/mm/dd*（时:分:秒-年/月/日）。

user-name *user-name*：根据用户名删除暂存的停止计费请求报文。

【描述】

reset stop-accounting-buffer 命令用来删除那些缓存的、没有得到响应的停止计费请求报文。在发送停止计费请求报文而 RADIUS 服务器没有响应时，SecBlade 会缓存该报文，然后以一定的次数重新发送，具体发送的次数由 **retry stop-accounting** 命令设置。

可以选择删除某个 RADIUS 方案的报文；也可以根据用户会话的 session-id 或用户名来删除报文；还可以指定一个时间段，删除那些发起停止计费请求的时刻处于指定时间段内的报文。

相关配置可参考命令 **stop-accounting-buffer enable,retry stop-accounting**，**display stop-accounting-buffer**。

【举例】

删除用户“user0001@test163.net”缓存在系统中的停止计费请求报文。

```
<SecBlade_FW> reset stop-accounting-buffer user-name user0001@test163.net
```

删除从 2002 年 8 月 31 日 0 点 0 分 0 秒到 2002 年 8 月 31 日 23 点 59 分 59 秒期间内系统缓存的停止计费请求报文。

```
<SecBlade_FW> reset stop-accounting-buffer time-range 0:0:0-08/31/2002 23:59:59-08/31/2002
```

1.2.19 retry

【命令】

retry *retry-times*

undo retry

【视图】

RADIUS 视图

【参数】

retry-times：最大传送次数，取值范围为 1～20。缺省情况下，RADIUS 请求报文的最大传送次数为 3 次。

【描述】

retry 命令用来设置 RAIUDS 请求报文的最大传送次数，**undo retry** 命令用来将 RAIUDS 请求报文的最大传送次数恢复为缺省值。

由于 RADIUS 协议采用 UDP 报文来承载数据，因此其通信过程是不可靠的。如果 RADIUS 服务器在响应超时定时器规定的时长内没有响应 NAS，则 NAS 有必要向 RADIUS 服务器重传 RADIUS 请求报文。假设最大传送次数为 N，则如果累计的传送次数超过（N-[N/2]）次而主 RADIUS 服务器仍旧没有响应，则 NAS 将认为其与当前 RADIUS 服务器的通信已经中断，并将转而向其它的 RADIUS 服务器发送请求报文。

根据网络状况合理的设置重发次数可以提高系统的响应速度。

相关配置可参考命令 **radius scheme**。

【举例】

设置在 RADIUS 方案“test”下，RAIUDS 请求报文的最大传送次数为 5 次。

```
[SecBlade_FW-radius-test] retry 5
```

1.2.20 retry realtime-accounting

【命令】

retry realtime-accounting *retry-times*

undo retry realtime-accounting

【视图】

RADIUS 视图

【参数】

retry-times：允许实时计费请求无响应的最大次数，取值范围为 1～255。缺省情况下，最多允许 5 次实时计费请求无响应。

【描述】

retry realtime-accounting 命令用来设置允许实时计费请求无响应的最大次数。**undo retry realtime-accounting** 命令用来恢复允许实时计费请求无响应的最大次数为缺省值。

RADIUS 服务器通常通过连接超时定时器来判断用户是否在线。如果 RADIUS 服务器长时间收不到 NAS 传来的实时计费报文，它会认为线路或设备故障并停止对用户记帐。为了配合 RADIUS 服务器的这种特性，有必要在不可预见的故障条件下在 NAS 端尽量与 RADIUS 服务器同步切断用户连接。SecBlade 提供对连续实时计费请求无响应次数限制的设置——在 NAS 向 RADIUS 服务器发出的实时计费请求没有得到响应的次数超过所设定的限度时，NAS 将切断用户连接。

假设 RADIUS 服务器的应答超时时长为 T（假设定义为 3 秒），NAS 的实时计费间隔为 t（假设定义为 12 分钟），则 NAS 的实时计费请求无响应的最大次数为 *retry-times*（假设定义为 5 次），则其含义为：NAS 每隔 12 分钟发起一次记费请求，如果 3 秒钟得不到回应就重新发起一次请求，如果 5 次发送都没有回应就认为该次实时记费失败。一般情况下，T 乘以 *retry-times* 应该小于 t。

相关配置可参考命令 **radius scheme**，**timer realtime-accounting**。

【举例】

设置 RADIUS 方案“test”最多允许 10 次实时计费请求无响应。

```
[SecBlade_FW -radius-test] retry realtime-accounting 10
```

1.2.21 retry stop-accounting

【命令】

retry stop-accounting *retry-times*

undo retry stop-accounting

【视图】

RADIUS 视图

【参数】

retry-times：缓存的停止计费请求报文的最大重发次数，取值范围为 10～65535。缺省情况下，取值为 500。

【描述】

retry stop-accounting 命令用来指示当出现没有得到响应的停止计费请求时，将该报文存入 SecBlade 缓存后，停止计费请求报文的最大重发次数。**undo retry stop-accounting** 命令用来恢复停止计费请求报文的最大重发次数为缺省值。

由于停止计费请求报文涉及到话单结算，并最终影响收费多少，对用户和 ISP 都有比较重要的影响，因此 NAS 应该尽最大努力把它发送给 RADIUS 计费服务器。所以，如果 RADIUS 计费服务器对 SecBlade 发出的停止计费请求报文没有响应，SecBlade 应将其缓存在本机上，然后重新发送直到 RADIUS 计费服务器产生响应，或者在重新发送的次数达到指定的次数限制后将其丢弃。

相关配置可参考命令 **reset stop-accounting-buffer**，**radius scheme** ，**display stop-accounting-buffer**。

【举例】

指示对于 RADIUS 方案“test”中的服务器，SecBlade 最多可以将缓存的停止计费请求报文重发 1000 次。

```
[SecBlade_FW-radius-test] retry stop-accounting 1000
```

1.2.22 secondary accounting

【命令】

secondary accounting *ip-address* [*port-number*]

undo secondary accounting

【视图】

RADIUS 视图

【参数】

ip-address：IP 地址，为点分十进制格式。缺省情况下，备计费服务器的 IP 地址均为 0.0.0.0。

port-number：UDP 端口号。取值范围为 1～65535。缺省情况下，计费服务的 UDP 端口号为 1813。

【描述】

secondary accounting 命令用来设置备 RADIUS 计费服务器的 IP 地址和端口号，**undo secondary accounting** 命令用来将备 RADIUS 计费服务器的 IP 地址和端口号恢复为缺省值。

具体的描述请参见 **primary accounting** 命令的描述部分。

相关配置可参考命令 **key**，**radius scheme**，**state**。

【举例】

设置 RADIUS 方案“test”的备计费服务器的 IP 地址为 10.110.1.1、使用 UDP 端口 1813 提供 RADIUS 计费服务。

```
[SecBlade_FW-radius-test] secondary accounting 10.110.1.1 1813
```

1.2.23 secondary authentication

【命令】

secondary authentication *ip-address* [*port-number*]

undo secondary authentication

【视图】

RADIUS 视图

【参数】

ip-address：IP 地址，为点分十进制格式。缺省情况下，备认证/授权的 IP 地址均为 0.0.0.0。

port-number：UDP 端口号。取值范围为 1～65535。缺省情况下，认证/授权服务的 UDP 端口号为 1812。

【描述】

secondary authentication 命令用来设置备 RADIUS 认证/授权或计费服务器的 IP 地址和端口号，**undo secondary authentication** 命令用来将备 RADIUS 认证/授权或计费服务器的 IP 地址和端口号恢复为缺省值。

具体的描述请参见 **primary authentication** 命令的描述部分。

相关配置可参考命令 **key**，**radius scheme**，**state**。

【举例】

设置 RADIUS 方案“test”的备认证/授权服务器的 IP 地址为 10.110.1.2、使用 UDP 端口 1812 提供 RADIUS 认证/授权服务。

```
[SecBlade_FW-radius-test] secondary authentication 10.110.1.2 1812
```

1.2.24 server-type

【命令】

server-type { **extended** | **standard** }

undo server-type

【视图】

RADIUS 视图

【参数】

extended：指定 Extended 的 RADIUS 服务器（一般为 CAMS），即要求 RADIUS 客户端（SecBlade）和 RADIUS 服务器按照华为公司私有 RADIUS 协议的规程和报文格式进行交互。

standard：指定 Standard 类型的 RADIUS 服务器，即要求 RADIUS 客户端（SecBlade）和 RADIUS 服务器按照标准 RADIUS 协议（RFC 2138/2139 或更新）的规程和报文格式进行交互。

【描述】

server-type 命令用来指定 SecBlade 支持的 RADIUS 服务器类型。**undo server-type** 命令用来恢复 RADIUS 服务器类型的缺省值。

缺省情况下，system 方案中的 RADIUS 服务器的类型为 **extended**，新创建的 RADIUS 方案中的 RADIUS 服务器的类型为 **standard**。

相关配置可参考命令 **radius scheme**。

【举例】

将 RADIUS 方案“test”的 RADIUS 服务器类型设置为 extended。

```
[SecBlade_FW-radius-test] server-type extended
```

1.2.25 state

【命令】

state { **primary** | **secondary** } { **accounting** | **authentication** } { **block** | **active** }

【视图】

RADIUS 视图

【参数】

primary：指示设置主 RADIUS 服务器的状态。

secondary：指示设置备 RADIUS 服务器的状态。

accounting：指示设置 RADIUS 计费服务器的状态。

authentication：指示设置 RADIUS 认证/授权服务器的状态。

block：指示 RADIUS 服务器的状态为 **block**，即处于宕机状态。

active：指示 RADIUS 服务器的状态为 **active**，即处于正常工作状态。

【描述】

state 命令用来设置 RADIUS 服务器的状态。

缺省情况下，system 方案中的主认证/授权服务器和主计费服务器的状态为 **active**，备认证/授权服务器和备计费服务器的状态为 **block**；新创建的 RADIUS 方案中各 RADIUS 服务器的状态均为 **block**。

对于某个 RADIUS 方案中的主、备服务器（无论是认证/授权服务器还是计费服务器），当主服务器因故障而导致其与 NAS 的通信中断时，NAS 会主动地转而与备服务器交互报文。当主服务器恢复正常后，NAS 却不会立即恢复与其通信，而是继续与备服务器通信；直到备服务器也出现故障后，NAS 才能再转而恢复与主服务器交互报文。为了使 NAS 在主服务器故障排除后迅速恢复与其通信，需要通过 **state** 命令手工将主服务器的状态设为 **active**。

当主服务器与备服务器的状态都为 **active** 或都为 **block** 时，NAS 将只把报文发送到主服务器上。

相关配置可参考命令 **radius scheme**，**primary authentication**，**secondary authentication**，**primary accounting**，**secondary accounting**。

【举例】

将 RADIUS 方案“test”的备认证服务器的状态设置为 active。

```
[SecBlade_FW-radius-test] state secondary authenticaiton active
```

1.2.26 stop-accounting-buffer enable

【命令】

stop-accounting-buffer enable

undo stop-accounting-buffer enable

【视图】

RADIUS 视图

【参数】

无

【描述】

stop-accounting-buffer enable 命令用来允许在 SecBlade 上缓存没有得到响应的停止计费请求报文。**undo stop-accounting-buffer enable** 命令用来禁止在 SecBlade 上缓存没有得到响应的停止计费请求报文。

缺省情况下，允许 SecBlade 缓存没有得到响应的停止计费请求报文。

由于停止计费请求报文涉及到话单结算、并最终影响收费多少，对用户和 ISP 都有比较重要的影响，因此 NAS 应该尽最大努力把它发送给 RADIUS 计费服务器。所以，如果 RADIUS 计费服务器对 SecBlade 发出的停止计费请求报文没有响应，SecBlade 应将其缓存在本机上，然后重新发送直到 RADIUS 计费服务器产生响应，或者在重新发送的次数达到指定的次数限制后将其丢弃。

相关配置可参考命令 **reset stop-accounting-buffer**，**radius scheme** ，**display stop-accounting-buffer**。

【举例】

指示对于 RADIUS 方案“test”中的服务器，SecBlade 能够缓存没有得到响应的停止计费请求报文。

```
[SecBlade_FW-radius-test] stop-accounting-buffer enable
```

1.2.27 timer quiet

【命令】

timer quiet *minutes*

undo timer quiet

【视图】

RADIUS 视图

【参数】

minutes：取值范围为 1～255，单位为分钟。缺省情况下，主服务器恢复激活状态前需要等待 5 分钟。

【描述】

timer quiet 命令用来设置主服务器恢复激活状态的时间。**undo timer quiet** 命令用来恢复缺省配置。

相关配置可参考命令 **display radius**。

【举例】

设置主服务器恢复激活状态的时间为 10 分钟。

```
[SecBlade_FW] radius scheme test1
[SecBlade_FW-radius-test1] timer quiet  10
```

1.2.28 timer realtime-accounting

【命令】

timer realtime-accounting *minutes*

undo timer realtime-accounting

【视图】

RADIUS 视图

【参数】

minutes：实时计费的时间间隔，单位为分钟，取值范围为 3～60，必须为 3 的倍数。

【描述】

timer realtime-accounting 命令用来设置实时计费的时间间隔，**undo timer realtime-accounting** 命令用来将实时计费的时间间隔恢复为缺省值。

为了对用户实施实时计费，有必要设置实时计费的时间间隔。在设置了该属性以后，每隔设定的时间，NAS 会向 RADIUS 服务器发送一次在线用户的计费信息。

实时计费间隔的取值对 NAS 和 RADIUS 服务器的性能有一定的相关性要求——取值越小，对 NAS 和 RADIUS 服务器的性能要求越高。建议当用户量比较大（≥1000）时，尽量把该间隔的值设置得大一些。以下是实时计费间隔与用户量之间的推荐比例关系：

表1-6 实时计费间隔与用户量之间的推荐比例关系

用户数	实时计费间隔（分钟）
1～99	3
100～499	6
500～999	12
≥1000	≥15

缺省情况下，实时计费的时间间隔为 12 分钟。

相关配置可参考命令 **retry realtime-accounting**，**radius scheme**。

【举例】

将 RADIUS 方案“test”的实时计费的时间间隔设置为 51 分钟。

```
[SecBlade_FW-radius-test] timer realtime-accounting 51
```

1.2.29 timer response-timeout

【命令】

timer *seconds*

undo timer

timer response-timeout *seconds*

undo timer response-timeout

【视图】

RADIUS 视图

【参数】

seconds：RADIUS 服务器应答超时时间，单位为秒，取值范围为 1～10。

【描述】

timer 和 timer response-timeout 命令用来设置 RADIUS 服务器应答超时时间，**undo timer 和 undo timer response-timeout** 命令用来将 RADIUS 服务器应答超时时间恢复为缺省值。

如果在 RADIUS 请求报文（认证/授权请求或计费请求）传送出去一段时间后，NAS 还没有得到 RADIUS 服务器的响应，则有必要重传 RADIUS 请求报文，以保证用户确实能够得到 RADIUS 服务，这段时间被称为 RADIUS 服务器响应超时时长，SecBlade 中用于控制这个时长的定时器就被称为 RADIUS 服务器响应超时定时器，**timer 和 timer response-timeout** 命令就是用来设置这个定时器时长的。

根据网络状况，合理地设置这个定时器的时长，有利于提高系统性能。

缺省情况下，RADIUS 服务器应答超时时间为 3 秒。

相关配置可参考命令 **radius scheme**，**retry**。

【举例】

将 RADIUS 方案“test”的响应超时定时器设置为 5 秒。

```
[SecBlade_FW-radius-test] timer response-timeout 5
```

1.2.30 user-name-format

【命令】

user-name-format { **with-domain** | **without-domain** }

【视图】

RADIUS 视图

【参数】

with-domain：指定发送给 RADIUS 服务器的用户名带域名。

without-domain：指定发送给 RADIUS 服务器的用户名不带域名。

【描述】

user-name-format 命令用来设置发送给 RADIUS 服务器的用户名格式。

缺省情况下，在 system 方案中，NAS 发送给 RADIUS 服务器的用户名不携带 ISP 域名；在新创建的 RADIUS 方案中，NAS 发送给 RADIUS 服务器的用户名携带有 ISP 域名。

接入用户通常以“userid@isp-name”的格式命名，“@”后面的部分为 ISP 域名，SecBlade 就是通过该域名来决定将用户归于哪个 ISP 域的。但是，有些较早期的 RADIUS 服务器不能接受携带有 ISP 域名的用户名，在这种情况下，有必要将用户名中携带的域名去除后再传送给 RADIUS 服务器。因此，SecBlade 提供此命令以指定发送给 RADIUS 服务器的用户名是否携带有 ISP 域名。

🕮 **说明：**

如果指定某个 RADIUS 方案不允许用户名中携带有 ISP 域名，那么请不要在两个乃至两个以上的 ISP 域中同时设置使用该 RADIUS 方案，否则，会出现虽然实际用户不同（在不同的 ISP 域中）、但 RADIUS 服务器认为用户相同（因为传送到它的用户名相同）的错误。

相关配置可参考命令 **radius scheme**。

【举例】

指定发送给 RADIUS 方案“test”中 RADIUS 服务器的用户名不得携带域名。

```
[SecBlade_FW-radius-test] user-name-format without-domain
```

1.3 HWTACACS 协议配置命令

1.3.1 data-flow-format

【命令】

data-flow-format data { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** }

data-flow-format packet { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** }

undo data-flow-format { **data** | **packet** }

【视图】

HWTACACS 视图

【参数】

data：设置数据的单位。

byte：数据单位为比特。

giga-byte：数据单位千兆字节。

kilo-byte：数据单位为千字节。

mega-byte：数据单位为兆字节。

packet：设置数据包的单位。

giga-packet：数据包的单位为“giga-packet”。

kilo-packet：数据包的单位为“kilo-packet”。

mega-packet：数据包的单位为“mega-packet”。

one-packet：数据包的单位为“one-packet”。

【描述】

data-flow-format 命令用来配置发送到 TACACS 服务器的数据流的单位。**undo data-flow-format** 命令用来恢复发送到 TACACS 服务器的数据流的单位为缺省设置。

缺省情况下，数据的单位为 byte，数据包的单位为 one-packet。

相关配置可参考命令 **display hwtacacs**。

【举例】

设置发往服务器 test 的数据流的单位为千比特，数据包的单位为 kilo-packet。

```
[SecBlade_FW-hwtacacs-test] data-flow-format data kilo-byte packet kilo-packet
```

1.3.2 debugging hwtacacs

【命令】

debugging hwtacacs { **all** | **error** | **event** | **message** | **receive-packet** | **send-packet** }

undo debugging hwtacacs { **all** | **error** | **event** | **message** | **receive-packet** | **send-packet** }

【视图】

用户视图

【参数】

all：HWTACACS 协议的所有调试功能。

error：错误调试功能。

event：事件调试功能。

message：消息调试功能。

receive-packet：对接收到的报文的调试功能。

send-packet：对发送报文的调试功能。

【描述】

debugging hwtacacs 命令用来使能 HWTACACS 协议的调试功能。**undo debugging hwtacacs** 命令用来禁止 HWTACACS 协议的调试功能。

缺省情况下，禁止 HWTACACS 协议的调试功能。

【举例】

使能 HWTACACS 协议的事件调试功能。

```
<SecBlade_FW> debugging hwtacacs event
```

1.3.3 display hwtacacs scheme

【命令】

display hwtacacs scheme [*hwtacacs-scheme-name* [**statistics**]]

【视图】

所有视图

【参数】

hwtacacs-scheme-name：HWTACACS 方案名，字符串形式，长度为 1～32，不区分大小写。此项如果为空，则显示所有 HWTACACS 方案的配置信息。

statistics：显示 HWTACACS 报文的详细统计信息。

【描述】

display hwtacacs scheme 命令用来查看所有或指定 HWTACACS 方案的配置信息。

不带任何参数的情况下，显示所有 HWTACACS 方案的配置信息。

相关配置请参考命令 **hwtacacs scheme**。

【举例】

查看所有 HWTACACS 方案 gy 的配置情况。

```
<SecBlade_FW> display hwtacacs scheme gy
-------------------------------------------------------------------------
HWTACACS-server template name   : gy
  Primary-authentication-server   : 172.31.1.11:49
  Primary-authorization-server    : 172.31.1.11:49
  Primary-accounting-server       : 172.31.1.11:49
  Secondary-authentication-server : 0.0.0.0:0
  Secondary-authorization-server  : 0.0.0.0:0
  Secondary-accounting-server     : 0.0.0.0:0
  Current-authentication-server   : 172.31.1.11:49
  Current-authorization-server    : 172.31.1.11:49
  Current-accounting-server       : 172.31.1.11:49
  Source-IP-address               : 0.0.0.0
  key authentication              : 790131
  key authorization               : 790131
  key accounting                  : 790131
  Quiet-interval(min)             : 5
  Response-timeout-Interval(sec)  : 5
  Domain-included                 : No
  Traffic-unit                    : B
  Packet traffic-unit             : one-packet
```

表1-7 display hwtacacs scheme 显示信息描述表

域名	描述
HWTACACS-server template name	HWTACACS 服务器组名（即 HWTACACS 方案名）
Primary-authentication-server	主认证服务器 IP 地址及端口号
Primary-authorization-server	主授权服务器 IP 地址及端口号
Primary-accounting-server	主计费服务器 IP 地址及端口号
Secondary-authentication-server	备认证服务器 IP 地址及端口号
Secondary-authorization-server	备授权服务器 IP 地址及端口号
Secondary-accounting-server	备计费服务器 IP 地址及端口号
Current-authentication-server	当前认证服务器 IP 地址及端口号
Current-authorization-server	当前授权服务器 IP 地址及端口号
Current-accounting-server	当前计费服务器 IP 地址及端口号
Source-IP-address	路由器发送 HWTACACS 报文使用的源 IP 地址
key authentication	HWTACACS 认证服务器共享密钥

域名	描述
key authorization	HWTACACS 授权服务器共享密钥
key accounting	HWTACACS 计费服务器共享密钥
Quiet-interval(min)	主服务器恢复激活状态的等待时间
Response-timeout-Interval(sec)	TACACS 服务器应答超时时间
Domain-included	发送给 TACACS 服务器的用户名为含域名的格式
Traffic-unit	流量单位： B：数据单位为字节。 GB：数据单位千兆字节。 KB：数据单位为千字节。 MB：数据单位为兆字节。
Packet traffic-unit	数据包的单位： **giga-packet**：数据包的单位为千兆“giga-packet”。 **kilo-packet**：数据包的单位为千“kilo-packet”。 **mega-packet**：数据包的单位为兆“mega -packet”。 **one-packet**：数据包的单位为 1 包“one -packet”。

1.3.4 display stop-accounting-buffer

【命令】

display stop-accounting-buffer hwtacacs-scheme *hwtacacs-scheme-name*

【视图】

所有视图

【参数】

hwtacacs-scheme *hwtacacs-scheme-name*：根据 HWTACACS 方案名显示暂存的停止计费请求报文。其中，*hwtacacs-scheme-name* 为 HWTACACS 方案名，为不超过 32 个字符的字符串。

【描述】

display stop-accounting-buffer 命令用来显示缓存在 SecBlade 上的停止计费请求报文。

相关配置可参考命令 **reset stop-accounting-buffer**，**stop-accounting-buffer enable**，**retry stop-accounting**。

【举例】

显示为 HWTACACS 方案“huwei”缓存的停止计费请求报文。

```
<SecBlade_FW> display stop-accounting-buffer hwtacacs-scheme test
----------------------------------------------------------
NO. SendTime      IP Address                        Template
  1       10              172.31.1.27                          test
----------------------------------------------------------
Whole accounting stop packet to resend:1
```

表1-8 display stop-accounting-buffer 显示信息描述表

域名	描述
NO.	停止计费请求报文的序号
SendTime	停止计费报文已发送次数
IP Address	TACACS 服务器 IP 地址
Template	hwtacacs 认证方案名

1.3.5 hwtacacs nas-ip

【命令】

hwtacacs nas-ip *ip-address*

undo hwtacacs nas-ip

【视图】

系统视图

【参数】

ip-address：指定的源 IP 地址，应该为本机的地址，禁止配置全 0 地址、D 类地址、网络地址、以及 127 网段地址。

【描述】

hwtacacs nas-ip 命令用来指定 NAS 发送 HWTACACS 报文使用的源地址。**undo hwtacacs nas-ip** 命令用来恢复缺省状态。

指定发送 HWTACACS 报文使用的源地址，可以避免物理接口故障时从服务器返回的报文不可达。一般推荐使用 loopback 接口地址。

缺省情况下，不指定源地址，即以发送报文的接口地址作为源地址。

本命令只能指定一个源地址，新配置的源地址会覆盖原有的源地址。

【举例】

配置 SecBlade 发送 HWTACACS 报文使用的源地址为 129.10.10.1。

```
[SecBlade_FW] hwtacacs nas-ip 129.10.10.1
```

1.3.6 hwtacacs scheme

【命令】

hwtacacs scheme *hwtacacs-scheme-name*

undo hwtacacs scheme *hwtacacs-scheme-name*

【视图】

系统视图

【参数】

hwtacacs-scheme-name：HWTACACS 方案名称，字符串形式，长度为 1～32。

【描述】

hwtacacs scheme 命令用来进入 HWTACACS 视图，如果指定的 HWTACACS 方案名不存在，则同时创建一个新的 HWTACACS 方案。**undo hwtacacs scheme** 命令用来删除一个 HWTACACS 方案。

【举例】

创建名为 test1 的 HWTACACS 方案并进入相应的 HWTACACS 方案视图。

```
[SecBlade_FW] hwtacacs scheme test1
[SecBlade_FW-hwtacacs-test1]
```

1.3.7 key

【命令】

key { **accounting** | **authentication** | **authorzation** } *string*

undo key { **accounting** | **authentication** | **authorzation** }

【视图】

HWTACACS 视图

【参数】

accounting：计费服务器的共享密钥。

authentication：认证服务器的共享密钥。

authorzation：授权服务器的共享密钥。

string：密钥。为不超过 16 个字符的字符串。

【描述】

key 命令用来设置 HWTACACS 认证、授权、计费服务器的共享密钥。**undo key** 命令用来删除配置。

缺省情况下，TACACS 服务器没有密钥。

TACACS 客户端（即 SecBlade）与 TACACS 服务器使用 MD5 算法来加密交互的 HWTACACS 报文，双方通过设置共享密钥来验证报文的合法性。只有在密钥一致的情况下，双方才能彼此接收对方发来的报文并作出响应。因此，必须保证 SecBlade 上设置的共享密钥与 TACACS 服务器上的完全一样。在认证/授权服务器与计费服务器不相同且这两台服务器中的共享密钥也不同时，必须分别设置认证/授权报文和计费报文的共享密钥。

相关配置可参考命令 **display hwtacacs**。

【举例】

配置 HWTACACS 计费服务器共享密钥为 hello。

```
[SecBlade_FW] hwtacacs scheme test1
[SecBlade_FW-hwtacacs-test1] key accounting hello
```

1.3.8 nas-ip

【命令】

nas-ip *ip-address*

undo nas-ip

【视图】

HWTACACS 视图

【参数】

ip-address：IP 地址，点分十进制形式。

【描述】

nas-ip 命令用来设置 NAS（SecBlade）发送 HWTACACS 报文使用的源 IP 地址，这样发送到 TACACS 服务器的所有报文携带相同的源 IP 地址。**undo nas-ip** 命令用来删除配置。

指定发送 HWTACACS 报文使用的源地址，可以避免物理接口故障时从服务器返回的报文不可达。一般推荐使用 loopback 接口地址。

缺省情况下，报文的源 IP 地址是发送端口的 IP 地址。

相关配置可参考命令 **display hwtacacs**。

【举例】

配置 NAS（SecBlade）发送 HWTACACS 报文使用的源 IP 地址为 10.1.1.1。

```
[SecBlade_FW] hwtacacs scheme test1
[SecBlade_FW-hwtacacs-test1] nas-ip 10.1.1.1
```

1.3.9 primary accounting

【命令】

primary accounting *ip-address* [*port*]

undo primary accounting

【视图】

HWTACACS 视图

【参数】

ip-address：服务器的 IP 地址，点分十进制格式。必须是合法的单播地址。

port：服务器的端口号，取值范围为 1～65535，缺省端口号为 49。

【描述】

primary accounting 命令用来配置 HWTACACS 主计费服务器。**undo primary accounting** 命令用来删除配置的 HWTACACS 主计费服务器。

缺省情况下，HWTACACS 计费服务器的 IP 地址为 0.0.0.0。

主计费服务器和备用计费服务器的 IP 地址不能相同，否则将提示配置不成功。

如果多次执行此命令，新的配置将覆盖原来的配置。

只有当没有活跃的、用于发送计费报文的 TCP 连接使用该计费服务器时，才允许删除该服务器。删除服务器只对之后的报文有效。

在计费成功后，计费更新以及计费停止报文都会发往计费成功时使用的服务器上，即使此服务器不可用，也不会发生主备切换。只有在最开始的认证、授权、计费过程中才会发生切换，成功后将不再切换。

【举例】

配置主计费服务器。

```
[SecBlade_FW] hwtacacs scheme test1
[SecBlade_FW-hwtacacs-test1] primary accouting 10.163.155.12 49
```

1.3.10 primary authentication

【命令】

primary authentication *ip-address* [*port*]

undo primary authentication

【视图】

HWTACACS 视图

【参数】

ip-address：服务器的 IP 地址，点分十进制格式。必须是合法的单播地址。

port：服务器的端口号，取值范围为 1～65535，缺省端口号为 49。

【描述】

primary authentication 命令用来配置 HWTACACS 认证服务器。**undo primary authentication** 命令用来删除配置的认证服务器。

缺省情况下，HWTACACS 认证服务器的 IP 地址为 0.0.0.0。

主认证服务器和备用认证服务器的 IP 地址不能相同，否则将提示配置不成功。

如果多次执行此命令，新的配置将覆盖原来的配置。

只有当没有活跃的、用于发送认证报文的 TCP 连接使用该认证服务器时，才允许删除该服务器。删除服务器只对之后的报文有效。

相关配置可参考命令 **display hwtacacs**。

【举例】

配置主认证服务器。

```
[SecBlade_FW] hwtacacs scheme test1
[SecBlade_FW-hwtacacs-test1] primary authentication 10.163.155.13 49
```

1.3.11 primary authorization

【命令】

primary authorization *ip-address* [*port*]

undo primary authorization

【视图】

HWTACACS 视图

【参数】

ip-address：服务器的 IP 地址，点分十进制格式。必须是合法的单播地址。

port：服务器的端口号，取值范围为 1～65535，缺省端口号为 49。

【描述】

primary authorization 命令用来配置 HWTACACS 主授权服务器。**undo primary authorization** 命令用来删除配置的主授权服务器。

缺省情况下，HWTACACS 授权服务器的 IP 地址为 0.0.0.0。

对于所有类型的用户，如果配置了 TACACS 认证，但没有配置 TACACS 授权服务器，则用户无法登录。

主授权服务器和备用授权服务器的 IP 地址不能相同，否则将提示配置不成功。

如果多次执行此命令，新的配置将覆盖原来的配置。

只有当没有活跃的、用于发送授权报文的 TCP 连接使用该授权服务器，才允许删除该服务器。删除服务器只对之后的报文有效。

相关配置可参考命令 **display hwtacacs**。

【举例】

配置主授权服务器。

```
[SecBlade_FW] hwtacacs scheme test1
[SecBlade_FW-hwtacacs-test1] primary authorization 10.163.155.13 49
```

1.3.12 reset hwtacacs statistics

【命令】

reset hwtacacs statistics{ **accounting** | **authentication** | **authorization** | **all** }

【视图】

用户视图

【参数】

accounting：清除所有 HWTACACS 协议关于计费的统计信息。

authentication：清除所有 HWTACACS 协议关于认证的统计信息。

authorization：清除所有 HWTACACS 协议关于授权的统计信息。

all：清除所有统计信息。

【描述】

reset hwtacacs statistics 命令用来清除 HWTACACS 协议的统计信息。

相关配置请参考命令 **display hwtacacs**。

【举例】

清除所有 HWTACACS 协议的统计信息。

```
<SecBlade_FW> reset hwtacacs statistics all
```

1.3.13 reset stop-accounting-buffer

【命令】

reset stop-accounting-buffer hwtacacs-scheme *hwtacacs-scheme-name*

【视图】

用户视图

【参数】

hwtacacs-scheme *hwtacacs-scheme-name*：根据 HWTACACS 方案名删除暂存的停止计费请求报文。其中，*hwtacacs-scheme-name* 为 HWTACACS 方案名，为不超过 32 个字符的字符串。

【描述】

reset stop-accounting-buffer 命令用来清除那些在 SecBlade 上缓存的、没有得到响应的停止计费请求报文。

相关配置可参考命令 **stop-accounting-buffer enable**， **retry stop-accounting**，**display stop-accounting-buffer**。

【举例】

删除 HWTACACS 方案“test”缓存在系统中的停止计费请求报文。

```
<SecBlade_FW> reset stop-accounting-buffer hwtacacs-scheme test
```

1.3.14 retry stop-accounting

【命令】

retry stop-accounting *retry-times*

undo retry stop-accounting

【视图】

HWTACACS 视图

【参数】

retry-times：停止计费报文传送的最大次数，取值范围为 1～300。

【描述】

retry stop-accounting 命令用来使能停止计费报文重传功能，并配置停止计费报文传送的最大次数。**undo retry stop-accounting** 命令用来恢复停止计费报文传送次数为缺省值。

缺省情况下，使能停止计费报文重传功能，可传送报文的最大次数为 100。

相关配置可参考命令 **reset stop-accounting-buffer**，**hwtacacs scheme**，**display stop-accounting-buffer**。

【举例】

使能停止计费报文重发功能，每次可重发 50 个报文。

```
[SecBlade_FW-hwtacacs-test] retry stop-accounting 50
```

1.3.15 secondary accounting

【命令】

secondary accounting *ip-address* [*port*]

undo secondary accounting

【视图】

HWTACACS 视图

【参数】

ip-address：服务器的 IP 地址，点分十进制格式，必须是合法的单播地址。

port：服务器的端口号，取值范围为 1～65535，缺省端口号为 49。

【描述】

secondary accounting 命令用来配置 HWTACACS 备计费服务器。**undo secondary accounting** 命令用来删除配置的 HWTACACS 备计费服务器。

缺省情况下，HWTACACS 计费服务器的 IP 地址为 0.0.0.0。

主计费服务器和备用计费服务器的 IP 地址不能相同，否则将提示配置不成功。

如果多次执行此命令，新的配置将覆盖原来的配置。

只有当没有活跃的、用于发送计费报文的 TCP 连接使用该计费服务器时，才允许删除该服务器。

【举例】

配置备计费服务器。

```
[SecBlade_FW] hwtacacs scheme test1
[SecBlade_FW-hwtacacs-test1] secondary accouting 10.163.155.12 49
```

1.3.16 secondary authentication

【命令】

secondary authentication *ip-address* [*port*]

undo secondary authentication

【视图】

HWTACACS 视图

【参数】

ip-address：服务器的 IP 地址，点分十进制格式。必须是合法的单播地址。

port：服务器的端口号，取值范围为 1～65535，缺省端口号为 49。

【描述】

secondary authentication 命令用来配置 HWTACACS 备认证服务器。**undo secondary authentication** 命令用来删除配置的备认证服务器。

缺省情况下，HWTACACS 认证服务器的 IP 地址为 0.0.0.0。

主认证服务器和备用认证服务器的 IP 地址不能相同，否则将提示配置不成功。

如果多次执行此命令，新的配置将覆盖原来的配置。

只有当没有活跃的、用于发送认证报文的 TCP 连接使用该认证服务器时，才允许删除该服务器。

相关配置可参考命令 **display hwtacacs**。

【举例】

配置备认证服务器。

```
[SecBlade_FW] hwtacacs scheme test1
[SecBlade_FW-hwtacacs-test1] secondary authentication 10.163.155.13 49
```

1.3.17 secondary authorization

【命令】

secondary authorization *ip-address* [*port*]

undo secondary authorization

【视图】

HWTACACS 视图

【参数】

ip-address：服务器的 IP 地址，点分十进制格式。必须是合法的单播地址。

port：服务器的端口号，取值范围为 1～65535，缺省端口号为 49。

【描述】

secondary authorization 命令用来配置 HWTACACS 备授权服务器。**undo secondary authorization** 命令用来删除配置的备授权服务器。

缺省情况下，HWTACACS 授权服务器的 IP 地址为 0.0.0.0。

主授权服务器和备用授权服务器的 IP 地址不能相同，否则将提示配置不成功。

如果多次执行此命令，新的配置将覆盖原来的配置。

只有当没有活跃的、用于发送授权报文的 TCP 连接使用该授权服务器，才允许删除该服务器。

相关配置可参考命令 **display hwtacacs**。

【举例】

配置备授权服务器。

```
[SecBlade_FW] hwtacacs scheme test1
[SecBlade_FW-hwtacacs-test1] secondary authorization 10.163.155.13 49
```

1.3.18 stop-accounting-buffer enable

【命令】

stop-accounting-buffer enable

undo stop-accounting-buffer enable

【视图】

HWTACACS 视图

【参数】

无

【描述】

stop-accounting-buffer enable 命令用来允许在 SecBlade 上缓存没有得到响应的停止计费请求报文。**undo stop-accounting-buffer enable** 命令用来禁止在 SecBlade 上缓存没有得到响应的停止计费请求报文。

缺省情况下，允许 SecBlade 缓存没有得到响应的停止计费请求报文。

此命令的具体描述请参见 RADIUS 方案中的 **stop-accounting-buffer enable** 命令。

【举例】

指示对于 HWTACACS 方案“test”中的服务器，SecBlade 系统能够缓存没有得到响应的停止计费请求报文。

```
[SecBlade_FW-hwtacacs-test] stop-accounting-buffer enable
```

1.3.19 timer quiet

【命令】

timer quiet *minutes*

undo timer quiet

【视图】

HWTACACS 视图

【参数】

minutes：取值范围为 1～255，单位为分钟。缺省情况下，主服务器恢复激活状态前需要等待 5 分钟。

【描述】

timer quiet 命令用来设置主服务器恢复激活状态的时间。**undo timer quiet** 命令用来恢复缺省配置。

相关配置可参考命令 **display hwtacacs**。

【举例】

设置主服务器恢复激活状态的时间为 10 分钟。

```
[SecBlade_FW] hwtacacs scheme test1
[SecBlade_FW-hwtacacs-test1] timer quiet 10
```

1.3.20 timer realtime-accounting

【命令】

timer realtime-accounting *minutes*

undo timer realtime-accounting

【视图】

HWTACACS 视图

【参数】

minutes：实时计费的时间间隔，单位为分钟，取值范围为 3～60，必须为 3 的倍数。

【描述】

timer realtime-accounting 命令用来设置实时计费的时间间隔，**undo timer realtime-accounting** 命令用来将实时计费的时间间隔恢复为缺省值。

为了对用户实施实时计费，有必要设置实时计费的时间间隔。在设置了该属性以后，每隔设定的时间，NAS 会向 TACACS 服务器发送一次在线用户的计费信息。

实时计费间隔的取值对 NAS 和 TACACS 服务器的性能有一定的相关性要求——取值越小，对 NAS 和 TACACS 服务器的性能要求越高。建议当用户量比较大（≥1000）时，尽量把该间隔的值设置得大一些。以下是实时计费间隔与用户量之间的推荐比例关系：

表1-9 实时计费间隔与用户量之间的推荐比例关系

用户数	实时计费间隔（分钟）
1～99	3
100～499	6
500～999	12
≥1000	≥15

缺省情况下，实时计费的时间间隔为 12 分钟。

【举例】

将 HWTACACS 方案“test”的实时计费的时间间隔设置为 51 分钟。

```
[SecBlade_FW-hwtacacs-test] timer realtime-accounting 51
```

1.3.21 timer response-timeout

【命令】

timer response-timeout *seconds*

undo timer response-timeout

【视图】

HWTACACS 视图

【参数】

seconds：取值范围为 1～300，单位为秒。

【描述】

timer response-timeout 命令用来设置 TACACS 服务器应答超时时间。**undo timer response-timeout** 命令用来恢复缺省配置。

缺省情况下，TACACS 服务器应答超时时间为 5 秒。

📖 **说明：**

由于 HWTACACS 是基于 TCP 实现的，因此，服务器应答超时或 TCP 超时都可能导致与 TACACS 服务器的连接断开。

相关配置可参考命令 **display hwtacacs**。

【举例】

配置 TACACS 服务器应答超时时间为 30 秒。

```
[SecBlade_FW] hwtacacs scheme test1
[SecBlade_FW-hwtacacs-test1] timer response-timeout 30
```

1.3.22 user-name-format

【命令】

user-name-format { **with-domain** | **without-domain** }

【视图】

HWTACACS 视图

【参数】

with-domain：指定发送给 TACACS 服务器的用户名带域名。

without-domain：指定发送给 TACACS 服务器的用户名不带域名。

【描述】

user-name-format 命令用来设置发送给 TACACS 服务器的用户名格式。

缺省情况下，HWTACACS 方案默认发送给 TACACS 服务器的用户名携带有 ISP 域名。

接入用户通常以“userid@isp-name”的格式命名，“@”后面的部分为 ISP 域名，SecBlade 就是通过该域名来决定将用户归于哪个 ISP 域的。但是，有些较早期的 TACACS 服务器不能接受携带有 ISP 域名的用户名，在这种情况下，有必要将用户名中携带的域名去除后再传送给 TACACS 服务器。因此，SecBlade 提供此命令以指定发送给 TACACS 服务器的用户名是否携带有 ISP 域名。

📖 **说明：**

如果指定某个 HWTACACS 方案不允许用户名中携带有 ISP 域名，那么请不要在两个乃至两个以上的 ISP 域中同时设置使用该 HWTACACS 方案，否则，会出现虽然实际用户不同（在不同的 ISP 域中）、但 TACACS 服务器认为用户相同（因为传送到它的用户名相同）的错误。

相关配置可参考命令 **hwtacacs scheme**。

【举例】

指定发送给 HWTACACS 方案“test”的用户不得携带域名。

```
[SecBlade_FW-hwtacacs-test] user-name-format without-domain
```

第2章 访问控制列表配置命令

2.1 访问控制列表配置命令

2.1.1 acl

【命令】

acl number *acl-number* [**match-order** { **config** | **auto** }]

undo acl { **number** *acl-number* | **all** }

【视图】

系统视图

【参数】

number *acl-number*：定义一个数字型的访问控制列表，访问控制列表的序号。1000～1999 为基于接口的访问控制列表，2000～2999 为基本访问控制列表（basic），3000～3999 为高级访问控制列表（advanced），4000～4999 为基于 MAC 地址访问控制列表。

match-order：指定规则的配置顺序。

config：指定匹配该规则时按用户的配置顺序。

auto：指定匹配该规则时系统自动排序（按“深度优先”的顺序）。

all：所有的 ACL。

【描述】

命令 **acl** 用于创建一个访问控制列表并进入 ACL 视图，命令 **undo acl** 用于删除访问控制列表。

一个访问控制列表是由 **permit** 和 **deny** 语句组成的一系列的规则列表，若干个规则构成一个访问控制列表。在配置访问控制列表的规则之前，首先需要创建一个访问控制列表。

【举例】

创建一个序号为 2000 的基本 ACL。

```
[SecBlade_FW] acl number 2000
[SecBlade_FW-acl-basic-2000]
```

2.1.2 description

【命令】

description *text*

undo description

【视图】

ACL 视图

【参数】

text：ACL 的描述，描述内容最长为 127 个字符。

【描述】

description 命令用来为 ACL 添加描述，**undo description** 命令用来删除 ACL 的描述。

【举例】

为编号为 2001 的基本 ACL 添加描述。

```
[SecBlade_FW-acl-basic-2001] description Deny HTTP from host 10.0.0.1
```

2.1.3 display acl

【命令】

display acl { **all** | *acl-number* }

【视图】

所有视图。

【参数】

all：所有的 ACL。

acl-number：特定编号的 ACL。

【描述】

命令 **display acl** 用来显示配置的访问控制列表的规则。

默认情况下，规则的匹配顺序为 **config**（配置顺序），**display** 命令将不会显示该匹配顺序；而如果匹配顺序为 **auto** 时，**display** 命令则会显示出该顺序。

【举例】

显示 ACL 2000 的规则的内容。

```
[SecBlade_FW-acl-basic-2000] display acl 2000
```

```
Basic ACL  2000, 2 rules
Acl's step is 1
 rule 1 permit (0 times matched)
 rule 2 permit source 1.1.1.1 0 (0 times matched)
```

2.1.4 reset acl counter

【命令】

reset acl counter { **all** | *acl-number* }

【视图】

用户视图

【参数】

acl-number：特定编号的 ACL。

all：所有的 ACL。

【描述】

命令 **reset acl counter** 用来清除访问控制列表的统计信息。

【举例】

清除访问控制列表 1000 的统计信息。

```
<SecBlade_FW> reset acl counter 1000
```

2.1.5 rule

【命令】

(1) 增加/删除一个基本访问控制列表的规则

rule [*rule-id*] { **permit** | **deny** } [**source** { *sour-addr sour-wildcard* | **any** }] [**time-range** *time-name*] [**logging**] [**fragment**]

undo rule *rule-id* [**source**] [**time-range**] [**logging**] [**fragment**]

(2) 增加/删除一个高级访问控制列表的规则

rule [*rule-id*] { **permit** | **deny** } *protocol* [**source** { *sour-addr sour-wildcard* | **any** }] [**destination** { *dest-addr dest-wildcard* | **any** }] [**source-port** *operator port1* [*port2*]] [**destination-port** *operator port1* [*port2*]] [**icmp-type** { *icmp-message* |*icmp-type icmp-code*}] [**dscp** *dscp*] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**time-range** *time-name*] [**logging**] [**fragment**]

undo rule *rule-id* [**source**] [**destination**] [**source-port**] [**destination-port**] [**icmp-type**] [**dscp**] [**precedence**] [**tos**] [**time-range**] [**logging**] [**fragment**]

(3) 增加/删除一个基于接口的访问控制列表的规则

rule [*rule-id*] { **permit** | **deny** } **interface** { *interface-type interface-number* | **any** } [**time-range** *time-name*] [**logging**]

undo rule *rule-id* [**time-range**] [**logging**]

(4) 增加/删除一个以太网 MAC 地址的访问控制列表的规则

rule [*rule-id*] { **deny** | **permit** } [**type** *type-code type-mask* | **lsap** *lsap-code lsap-mask*] [**source-mac** *sour-addr sour-mask*] [**dest-mac** *dest-addr dest-mask*] [**time-range** *time-name*] [**logging**]

undo rule *rule-id* [**time-range**] [**logging**]

【视图】

ACL 视图

【参数】

使用命令 **rule** 为 ACL 增加一个规则的时候，参数说明如下：

rule-id：可选参数，ACL 的规则编号，范围为 0～65534。当指定了编号，如果与编号对应的规则已经存在，则会部分覆盖旧的规则，相当于编辑一个已经存在的 ACL 规则。故建议用户当编辑一个已存在编号的规则时，先将旧的规则删除，再创建新的规则，否则配置结果可能与预期的效果不同。如果与编号对应的规则不存在，则使用指定的编号创建一个新的规则。如果不指定编号，表示增加一个新规则，系统自动会为这个规则分配一个编号。

deny：表示拒绝符合条件的数据包。

permit：表示允许符合条件的数据包。

protocol：用名字或数字表示的 IP 承载的协议类型。数字范围为 1～255；用名字表示时，可以选取：gre、icmp、igmp、ip、ipinip、ospf、tcp、udp。

source：可选参数，指定 ACL 规则的源地址信息。如果不配置，表示报文的任何源地址都匹配。

sour-addr：数据包的源地址，点分十进制表示。

sour-wildcard：源地址通配符，点分十进制表示。

destination：可选参数，指定 ACL 规则的目的地址信息。如果不配置，表示报文的任何目的地址都匹配。

dest-addr：数据包的目的地址，点分十进制表示。

dest-wildcard：目的地址通配符，点分十进制表示。

any：表示所有源地址或目的地址，作用与源或目的地址是 0.0.0.0，通配符是 255.255.255.255 相同。

icmp-type：可选参数，指定 ICMP 报文的类型和消息码信息，仅仅在报文协议是 ICMP 的情况下有效。如果不配置，表示任何 ICMP 类型的报文都匹配。

icmp-type：ICMP 包可以依据 ICMP 的消息类型进行过滤。取值为 0～255 的数字。

icmp-code：依据 ICMP 的消息类型进行过滤的 ICMP 包也可以依据消息码进行过滤。取值为 0～255 的数字。

icmp-message：ICMP 包可以依据 ICMP 消息类型名字或 ICMP 消息类型和码的名字进行过滤。

source-port：可选参数，指定 UDP 或者 TCP 报文的源端口信息，仅仅在规则指定的协议号是 TCP 或者 UDP 有效。如果不指定，表示 TCP/UDP 报文的任何源端口信息都匹配。

destination-port：可选参数，指定 UDP 或者 TCP 报文的目的端口信息，仅仅在规则指定的协议号是 TCP 或者 UDP 时有效。如果不指定，表示 TCP/UDP 报文的任何目的端口信息都匹配。

operator：可选参数。比较源或者目的地址的端口号的操作符，名字及意义如下：lt（小于），gt（大于），eq（等于），neq（不等于），range（在范围内）。只有 range 需要两个端口号做操作数，其他的只需要一个端口号做操作数。

port1、*port2*：可选参数。TCP 或 UDP 的端口号，用名字或数字表示，数字的取值范围为 0～65535。

dscp *dscp*：指定 DSCP 字段（IP 报文中的 DS 字节）。

established：匹配所有标志为 ACK 和 RST 的 TCP 报文（特征是 ACK 或者 RST 标志已置位）。包括 SYN+ACK、ACK、FIN+ACK、RST、RST+ACK 等几种报文。此选项可以匹配那些已经建立的 TCP 会话的流量，即过滤掉始发的 TCP 会话请求。

precedence：可选参数，数据包可以依据优先级字段进行过滤。取值为 0～7 的数字，或名字。

tos *tos*：可选参数，数据包可以依据服务类型字段进行过滤。取值为 0～15 的数字，或名字。

logging：可选参数，是否对符合条件的数据包做日志。日志内容包括访问控制列表规则的序号、数据包通过或被丢弃、IP 承载的上层协议类型、源/目的地址、源/目的端口号、数据包的数目。仅当 ACL 被用作包过滤防火墙时，系统将记录日志。

time-range *time-name*：配置这条访问控制规则生效的时间段。

fragment：指定该规则是否仅对非首片分片报文有效。当包含此参数时，表示该规则仅对非首片分片报文有效。

interface *interface-type interface-number*：指定数据包的接口信息，即对从此接口接收到的报文进行过滤。**any** 代表所有的接口。

使用命令 **undo rule** 删除规则的时候，参数说明如下：

rule-id：ACL 规则编号，必须是一个已经存在的 ACL 规则编号。如果 *rule-id* 后面不指定参数，则将这个 ACL 规则完全删除。否则，只是删除对应 ACL 规则的部分信息。

source：可选参数，仅仅删除编号对应的 ACL 规则的源地址部分的信息设置。

destination：可选参数，仅仅删除编号对应的 ACL 规则的目的地址部分的信息设置。

source-port：可选参数，仅仅删除编号对应的 ACL 规则的源端口部分的信息设置，仅仅在规则的协议号是 TCP 或者 UDP 的情况下有效。

destination-port：可选参数，仅仅删除编号对应的 ACL 规则的目的端口部分的信息设置，仅仅在规则的协议号是 TCP 或者 UDP 的情况下有效。

icmp-type：可选参数，仅仅删除编号对应的 ACL 规则 ICMP 类型和消息码部分的信息设置，仅仅在规则的协议号是 ICMP 的情况下有效。

precedence：可选参数，仅仅删除编号对应的 ACL 规则的 precedence 的相关设置。

tos *tos*：可选参数，仅仅删除编号对应的 ACL 规则的 tos 的相关设置。

time-range *time-name*：配置这条访问控制规则生效的时间段。

logging：可选参数，仅仅删除编号对应的 ACL 规则对符合条件的数据包做日志的设置。

fragment：可选参数，仅仅删除编号对应的 ACL 规则仅对非首片分片报文有效的设置。

type-code：数据帧的类型，一个 16 比特的十六进制数，对应Ethernet_II类型和Ethernet_SNAP类型帧中的type-code域。关于*type-code*的值请参考 表 5-1。

type-mask：类型掩码，是一个 16 比特的十六进制数，用于指定屏蔽位。

lsap-code：数据帧的封装格式的值，是一个 16 比特的十六进制数。

lsap-mask：Lsap 值的掩码，是一个 16 比特的十六进制数，用于指定屏蔽位。

sour-addr：源 MAC 地址，格式为 xxxx-xxxx-xxxx，用来匹配一个分组的源地址。

sour-mask：源 MAC 地址的掩码。

dest-addr：目的 MAC 地址，格式为 xxxx-xxxx-xxxx，用来匹配一个分组的源地址。

dest-mask：目的 MAC 地址的掩码。

【描述】

命令 **rule** 用来在对应的 ACL 视图下，增加一个规则。命令 **undo rule** 用来删除一个规则。

在删除一条规则时，需要指定规则的编号，如果不知道规则的编号，可以使用命令 **display acl** 来查看。

【举例】

创建 ACL 3001，增加一条规则，禁止接收和发送 RIP 报文。

```
[SecBlade_FW] acl number 3001
[SecBlade_FW-acl-adv-3001] rule deny udp destination-port eq rip
```

增加一条规则，允许从 129.9.0.0 网段的主机向 202.38.160.0 网段的主机发送 WWW 报文。

```
[SecBlade_FW-acl-adv-3001] rule permit tcp source 129.9.0.0 0.0.255.255 destination 202.38.160.0 0.0.0.255 destination-port eq www
```

增加一条规则，禁止从 129.9.0.0 网段内的主机建立与 202.38.160.0 网段内的主机的 WWW 端口（80）的连接，并对违反此规则的事件作日志。

```
[SecBlade_FW-acl-adv-3001] rule deny tcp source 129.9.0.0 0.0.255.255 destination 202.38.160.0 0.0.0.255 eq www logging
```

增加一条规则，允许从 129.9.8.0 网段内的主机建立与 202.38.160.0 网段内的主机的 WWW 端口（80）的连接。

```
[SecBlade_FW-acl-adv-3001] rule permit tcp source 129.9.8.0 0.0.0.255 destination 202.38.160.0 0.0.0.255 destination-port eq www
```

增加一条规则，禁止从一切主机建立与 IP 地址为 202.38.160.1 的主机的 Telnet（23）的连接。

```
[SecBlade_FW-acl-adv-3001] rule deny tcp destination 202.38.160.1 0 destination-port eq telnet
```

增加一条规则，禁止从 129.9.8.0 网段内的主机建立与 202.38.160.0 网段内的主机的端口号大于 128 的 UDP（用户数据报协议）连接。

```
[SecBlade_FW-acl-adv-3001] rule deny udp source 129.9.8.0 0.0.0.255 destination 202.38.160.0 0.0.0.255 destination-port gt 128
```

2.1.6 rule comment

【命令】

rule *rule-id* **comment** *text*

undo rule *rule-id* **comment**

【视图】

ACL 视图

【参数】

rule-id：已创建的 ACL 规则的编号。

comment *text*：ACL 规则的注释，注释内容最长为 128 个字符。

【描述】

rule comment 命令用来为 ACL 规则添加注释，**undo rule comment** 命令用来删除 ACL 规则的描述。

【举例】

为编号为 7 的 ACL 规则添加注释。

```
[SecBlade_FW-acl-adv-3001] rule 7 comment Allow FTP from any source to host
172.16.0.1
```

2.2 时间段配置命令

2.2.1 display time-range

【命令】

display time-range { **all** | *time-name* }

【视图】

所有视图

【参数】

time-name：时间段的名称。

all：所有配置的时间段。

【描述】

命令 **display time-range** 用来显示当前时间段的配置和状态，对于当前处在激活状态的时间段将显示 active，对于非激活状态显示 inactive。

注意，由于系统更新 ACL 状态有一个误差，大约 1 分钟，而 **display time-range** 会采用当前时间对其进行判断，所以有可能出现 **display time-range** 看到一个时间段已经激活，而引用它的 ACL 没有激活，这种情况是正常的。

【举例】

显示所有时间段。

```
[SecBlade_FW] display time-range all
```

显示名字为 trname 的时间段。

```
[SecBlade_FW] display time-range trname
Current time is 02:49:36 2/15/2003 Saturday
Time-range : trname ( Inactive )
 14:00 to 16:00 off-day from 00:00 12/1/2002 to 00:00 12/1/2003
```

2.2.2 time-range

【命令】

time-range *time-name* { *start-time* **to** *end-time days-of-the-week* [**from** *start-time start-date*] [**to** *end-time end-date*] | **from** *start-time start-date* [**to** *end-time end-date*] | **to** *end-time end-date* }

undo time-range *time-name* [*start-time* **to** *end-time days-of-the-week* [**from** *start-time start-date*] [**to** *end-time end-date*] | **from** *start-time start-date* [**to** *end-time end-date*] | **to** *end-time end-date*]

【视图】

系统视图

【参数】

time-name：时间段的名字，不能大于 32 个字符，且必须以字母 a-z，A-Z 开头。

start-time：一个时间范围的开始时间，格式为 hh:mm，小时和分钟之间使用“:”分隔，hh 的范围为 0～23，mm 的范围为 0～59。

end-time：一个时间范围的结束时间，格式为 hh:mm，小时和分钟之间使用“:”分隔，hh 的范围为 0～23（绝对时间段）或 0～24（周期时间段），mm 的范围为 0～59。

days-of-the-week：表示配置的时间范围在每周几有效，可以输入如下参数：

数字（0～6）；

星期日到星期六（Sunday，Monday，Tuesday，Wednesday，Thursday，Friday，Saturday）；

工作日（Working-day），包括从星期一到星期五五天；

休息日（Off-day），包括星期六和星期天；

所有日子（Daily)，包括一周七天。

start-date：表示起始日期，输入格式为 MM/DD/YYYY。DD 可以输入 1～31 之间的数字，MM 需要输入 1～12 之间的数字，YYYY 使用 4 位输入，范围为 1970～2100。

end-date：表示结束日期，输入格式为 MM/DD/YYYY。DD 可以输入 1～31 之间的数字，MM 需要输入 1～12 之间的数字，YYYY 使用 4 位输入，范围为 1970～2100。

【描述】

命令 **time-range** 用来定义一个时间段，描述一个特殊的时间范围。命令 **undo time-range** 用来删除一个时间段。

时间段可以分为如下几种：

- 绝对时间段

例如：

配置时间段，从 2003 年 4 月 1 日 20:00 起，到 2003 年 12 月 10 日 20:00 之间有效。

```
[SecBlade_FW] time-range test from 20:00 04/01/2003 to 20:00 12/10/2003
```

此时查看配置只有一条单独的绝对时间段：

```
[SecBlade_FW] display time-range test
Current time is 19:41:22 Jan/1/2000 Saturday

Time-range : test ( Inactive )
From 20:00 Apr/1/2003 to 20:00 Dec/10/2003
```

- 周期时间段

例如：

配置时间段，在每天的 12:00 到 17:00 之间有效。

```
[SecBlade_FW] time-range  test 12:00 to 17:00 daily
```

此时查看配置只有一条周期时间段：

```
[SecBlade_FW] display time-range test
Current time is 19:44:25 Jan/1/2000 Saturday

Time-range : test ( Inactive )
12:00 to 17:00 daily
```

- 在绝对时间段内生效的周期时间段

例如：

配置时间段，从 2003 年 4 月 1 日 20:00 起，到 2003 年 12 月 10 日 20:00 之间，在每个周末的下午 14:00 到 16:00 之间有效。

```
[SecBlade_FW] time-range test 14:00 to 16:00 off-day from 20:00 04/01/2003 to
20:00 12/10/2003
```

此时查看配置其实是由一条单独的周期时间段和一条单独的绝对时间段组成的：

```
[SecBlade_FW] display time-range test
Current time is 18:39:49 Jan/1/2000 Saturday

Time-range : test ( Inactive )
 14:00 to 16:00 off-day
 From 20:00 Apr/1/2003 to 20:00 Dec/10/2003
```

- 复合时间段

复合时间段是由若干条周期时间段和（或）绝对时间段组成，比如：

```
[SecBlade_FW] time test 16:30 to 18:00 daily from 01:00 01/01/2000 to 23:00
```

```
01/10/2000
[SecBlade_FW] time test 18:00 to 21:30 daily from 23:00 01/10/2000 to 23:00
02/01/2000
[SecBlade_FW] display time-range test
Current time is 18:29:37 Jan/1/2000 Saturday

Time-range : test ( Active )
 16:30 to 18:00 daily
 18:00 to 21:30 daily
 From 01:00 Jan/1/2000 to 23:00 Jan/10/2000
 From 23:00 Jan/10/2000 to 23:00 Feb/1/2000
```

实际的有效时间是从 2000 年 1 月 1 日 01:00 到 2000 年 2 月 1 日 23:00 期间每天的 16:30 到 21:30。而不只是从 2000 年 1 月 1 日 01:00 到 2000 年 1 月 10 日 23:00 期间的 16:30 到 18:00，和从 2000 年 1 月 10 日 23:00 到 2000 年 2 月 1 日 23:00 期间的 18:00 到 21:30 有效。

总之，复合时间段与各子时间段之间的关系是：如果没有周期时间段，则为所有的绝对时间段的并集；如果有周期时间段，则为所有的绝对时间段的并集与所有周期时间段的并集的交集。

【举例】

配置时间段，在 2003 年 1 月 1 日 0:0 生效，并永远有效。

```
[SecBlade_FW] time-range test from 0:0 1/1/2003
```

配置时间段，从 2003 年 4 月 1 日 20:00 起，到 2003 年 12 月 10 日 20:00 之间，在每个周末的下午 14:00 到 16:00 之间有效。

```
[SecBlade_FW] time-range test 14:00 to 16:00 off-day from 20:00 04/01/2003 to
20:00 12/10/2003
```

配置时间段，在周一到周五每天 8:00 到 18:00 生效。

```
[SecBlade_FW] time-range test 8:00 to 18:00 working-day
```

配置时间段，在周末下午 14:00 到 18:00 生效。

```
[SecBlade_FW] time-range test 14:00 to 18:00 off-day
```

第3章 NAT 配置命令

3.1 NAT 配置命令

3.1.1 connection-limit default

【命令】

connection-limit default { **permit** | **deny** }

undo connection-limit default { **permit** | **deny** }

【视图】

系统视图

【参数】

permit：进行限制，上下限使用系统默认值。

deny：不进行限制。

【描述】

connection-limit default 命令用来设置在查不到限制策略时的动作。

undo connection-limit default 命令用来取消设置的动作。

connection-limit default 命令可重复配置，后一个配置将覆盖前一个配置。

【举例】

设置在查不到限制策略时进行连接数限制。

```
[SecBlade_FW] connection-limit default permit
```

3.1.2 connection-limit default amount

【命令】

connection-limit default amount { **upper-limit** *upper-limit* | **lower-limit** *lower-limit* }*

undo connection-limit default amount { **upper-limit** | **lower-limit** }*

【视图】

系统视图

【参数】

upper-limit：设置缺省上限。

upper-limit：缺省上限值，取值范围是 1～4294967295。

lower-limit：设置缺省下限。

lower-limit：缺省下限值，取值范围是 0～4294967295。

【描述】

connection-limit default amount 命令用来设置连接数限制的缺省阈值。

undo connection-limit default amount 命令用来取消设置的阈值。

缺省情况下，上限为 50，下限为 20。

【举例】

设置连接数限制的缺省阈值，上限为 100，下限为 20。

```
[SecBlade_FW] connection-limit default amount upper-limit 100 lower-limit 20
```

3.1.3 connection-limit enable

【命令】

connection-limit enable

undo connection-limit enable

【视图】

系统视图

【参数】

无

【描述】

connection-limit enable 命令用来使能连接数限制功能。

undo connection-limit enable 命令用来关闭连接数限制功能。

缺省情况下，连接数限制功能处于关闭状态。

【举例】

使能连接数限制功能。

```
[SecBlade_FW] connection-limit enable
```

3.1.4 connection-limit policy

【命令】

connection-limit policy *policy-number*

undo connection-limit policy { *policy-number* | **all** }

【视图】

系统视图

【参数】

policy-number：连接数限制策略编号，范围为 0～19。

all：删除策略时使用，删除所有策略。

【描述】

connection-limit policy 命令用来创建连接数限制策略并进入策略视图。

undo connection-limit policy 命令用来删除连接数限制策略。

【举例】

创建一个编号为 10 的连接数限制策略。

```
[SecBlade_FW] connection-limit policy 10
```

3.1.5 debugging connection-limit

【命令】

debugging connection-limit

undo debugging connection-limit

【视图】

用户视图

【参数】

无

【描述】

debugging connection-limit 命令用来打开连接数限制的调试功能。

undo debugging connection-limit 命令用来关闭连接数限制的调试功能。

缺省情况下，关闭连接数限制的调试功能。

【举例】

打开连接数限制的调试功能。

```
<SecBlade_FW> debugging connection-limit
```

3.1.6 debugging nat

【命令】

debugging nat { **alg** | **event** | **packet** } [**interface** *interface-type interface-number*]

undo debugging nat { **alg** | **event** | **packet** } [**interface** *interface-type interface-number*]

【视图】

用户视图

【参数】

alg：打开应用协议地址转换信息开关。

event：打开地址转换事件调试信息开关。

packet：打开地址转换数据包调试信息开关。

interface：打开指定接口的地址转换数据包调试信息开关。

【描述】

debugging nat 命令用来打开 NAT 信息调试开关，**undo debugging nat** 命令用来关闭 NAT 信息调试开关。

【举例】

打开地址转换的事件调试信息开关。

```
<SecBlade_FW> debugging nat event
```

3.1.7 display connection-limit policy

【命令】

display connection-limit policy { *policy-number* | **all** }

【视图】

任意视图

【参数】

policy-number：要显示的策略编号，范围为 0~255。

all：显示所有的策略。

【描述】

display connection-limit policy 命令用来显示连接数限制策略。

【举例】

显示编号为 1 的策略。

```
[SecBlade_FW] display connection-limit policy 1
```

3.1.8 display connection-limit statistics

【命令】

display connection-limit statistics [**source** *source-addr source-mask*] [**destination** *destination-addr destination-mask*] [**destination-port** { { **eq** | **neq** | **gt** | **lt** } *destination-port* | **range** *destination-port1 destination-port2* }]

【视图】

任意视图

【参数】

source：指定源 IP 地址。

source-addr：源 IP 地址。

source-mask：源 IP 地址的掩码。

destination：指定目的 IP 地址。

destination-addr：目的 IP 地址。

destination-mask：目的 IP 地址掩码。

destination-port：指定目的端口号。

eq：显示目的端口号等于指定端口号的服务的连接数。

neq：显示目的端口号不等于指定端口号的服务的所有连接数。

gt：显示目的端口号大于指定端口号的服务的所有连接数。

lt：显示目的端口号小于指定端口号的服务的所有连接数。

range：显示目的端口号在指定范围内的服务的所有连接数。

destination-port：目的端口号。

destination-port1、*destination-port2*：按端口范围显示时的参数，分别表示服务端口的上下限。

【描述】

display connection-limit statistics 命令用来显示连接数限制信息。

用户可以通过此命令，灵活的查看所关心的连接数信息。当该命令后面不接其他参数时，将显示所有的连接数信息。

【举例】

显示所有的连接数限制信息。

```
[SecBlade_FW] display connection-limit statistics
```

3.1.9 display nat

【命令】

display nat { **address-group** | **aging-time** | **all** | **outbound** | **server** | **statistics** | **static | dns-map** | **session** [**vpn-instance** *vpn-instance-name*] [**source** { **global** *global-addr* | **inside** *inside-addr* }] }

【视图】

所有视图

【参数】

address-group：表示显示地址池的信息。

aging-time：显示地址转换连接的有效时间。

all：表示显示所有的关于地址转换的信息。

outbound：表示显示配置的地址转换的信息。

server：表示显示内部服务器的信息。

statistics：显示当前的地址转换记录统计数据。

static：显示静态地址转换信息。

dns-map: 表示显示配置的域名映射信息。

session：表示显示当前激活的连接信息。

vpn-instance *vpn-instance-name*：只显示指定 VPN 内的 NAT 转换表项。若没有该值，将显示所有私网内的 NAT 转换表项。

source global *global-addr*：只显示 NAT 转换后地址为 *global-addr* 的转换表项。

source inside *inside-addr*：只显示内部地址为 *inside-addr* 的 NAT 转换表项。

【描述】

display nat 命令显示用户对地址转换的配置，用户可以根据该命令的输出信息验证地址转换的配置是否正确。

【举例】

显示所有的关于地址转换的信息。

```
<SecBlade_FW> display nat all
NAT address-group Information:
    1: from 11.1.1.1      to  11.1.1.20
    2: from 22.1.1.1      to  22.1.1.20
NAT outbound information:
   GigabitEthernet0/0.1: acl(2011)-NAT address-group(1) [no-pat]
   GigabitEthernet0/0.1: acl(2022)-NAT address-group(2) [no-pat]
Server in private network information:
Interface GlobalAddr   GlobalPort  InsideAddr  InsidePort Pro
GigabitEthernet0/0.1  201.119.11.3     8080     5.5.5.5      80(www) 6(tcp)
GigabitEthernet0/0.1  201.119.11.3     2121     5.5.5.5      21(ftp) 6(tcp)
NAT dns-map information:
  There are currently 2 dns-map
    nat dns-map www.sina.com 1.1.1.1 80 tcp
    nat dns-map www.aaaaaaaaaaaaaaaaaaaaa.com 2.2.2.2 80 tcp
NAT aging-time value information:
       tcp ---- aging-time value is  86400 (seconds)
       udp ---- aging-time value is    300 (seconds)
      icmp ---- aging-time value is     60 (seconds)
      pptp ---- aging-time value is  86400 (seconds)
       dns ---- aging-time value is     60 (seconds)
   tcp-fin ---- aging-time value is     60 (seconds)
   tcp-syn ---- aging-time value is     60 (seconds)
  ftp-ctrl ---- aging-time value is   7200 (seconds)
  ftp-data ---- aging-time value is    300 (seconds)
```

如上信息表示：

配置了两个地址池：1、2 地址范围分别是 11.1.1.1 到 11.1.1.20 和 22.1.1.1 到 22.1.1.20。

在 GigabitEthernet0/0.1 配置了 2 个地址转换关联：ACL 规则 2011 与地址池 1 关联，进行一对一方式的地址转换；ACL 规则 2022 与地址池 2 关联，进行一对一方式的地址转换。

在 GigabitEthernet0/0.1 配置了 2 个内部服务器。http://202.119.11.3:8080 的 www 服务器，内部地址是 5.5.5.5。ftp://202.119.11.3:2121 的 ftp 服务器，内部的地址是 5.5.5.5。

配置了两条域名映射信息：域名 www.sina.com 映射为公网地址 1.1.1.1，公网端口为 80，协议为 TCP；域名 www.aaaaaaaaaaaaaaaaaaaaa.com 映射为公网地址 2.2.2.2，公网端口为 80，协议为 UDP。

显示 NAT 的转换信息。

```
<SecBlade_FW> display nat session
There are currently 40001 NAT sessions:

Protocol      GlobalAddr  Port      InsideAddr  Port        DestAddr  Port
       -  192.168.100.10   ---     192.168.1.5   ---             ---   ---
                 status: NOPAT,        TTL: 00:04:00,       Left: 00:04:00
       6  192.168.100.10  1024     192.168.1.5  1024   192.168.100.1  1025
                 status: NOPAT,        TTL: 00:01:00,       Left: 00:00:59
       6  192.168.100.10  2048     192.168.1.5  2048   192.168.100.1  2049
                 status: NOPAT,        TTL: 00:01:00,       Left: 00:01:00
       6  192.168.100.10  1025     192.168.1.5  1025   192.168.100.1  1026
                 status: NOPAT,        TTL: 00:01:00,       Left: 00:00:59
```

📖 **说明：**

当使用 No-PAT 转换方式时，通过 **display nat session** 命令查看 NAT 表项时，针对每个内网地址发起的多个连接转换，相应的会有多个 No-PAT 表项，如以上显示信息所示。这样保证了只有从内网向外网发起的连接才会被转换，对于由外网发起的连接将不被转换，提高了网络安全性。

3.1.10 display nat connection-limit

【命令】

display nat connection-limit [**source** *source-addr source-wildcard*] [**destination** *destination-addr destination-wildcard*] [**destination-port** { { **eq** | **neq** | **gt** | **lt** } *destination-port* | **range** *destination-port1 destination-port2* }]

【视图】

任意视图

【参数】

nat：显示 NAT 创建的连接数信息。

source：指定源 IP 地址。

source-addr：源 IP 地址。

source-wildcard：源 IP 地址的掩码。

destination：指定目的 IP 地址。

destination-addr：目的 IP 地址。

destination-wildcard：目的 IP 地址掩码。

destination-port：指定目的端口号。

eq：显示目的端口号等于指定端口号的服务的连接数。

neq：显示目的端口号不等于指定端口号的服务的所有连接数。

gt：显示目的端口号大于指定端口号的服务的所有连接数。

lt：显示目的端口号小于指定端口号的服务的所有连接数。

range：显示目的端口号在指定范围内的服务的所有连接数。

destination-port：目的端口号。

destination-port1、*destination-port2*：按端口范围显示时的参数，分别表示服务端口的上下限。

【描述】

display nat connection-limit 命令用来显示与 NAT 相关的连接数限制信息。

用户可以通过此命令，灵活的查看所关心的连接数信息。当该命令后面没有接任何参数时，将显示所有与 NAT 相关的连接数限制信息。

【举例】

显示所有与 NAT 相关的连接数限制信息。

```
[SecBlade_FW] display nat connection-limit
```

3.1.11 limit

【命令】

limit *limit-id* **acl** *acl-number* [{ **per-source** | **per-destination** | **per-service** }* **amount** *upper-limit lower-limit*]

undo limit *limit-id*

【视图】

连接数限制策略视图

【参数】

limit-id：连接数限制策略的子规则编号，范围为 0～255。

acl：指定 ACL。连接数限制策略使用 ACL 来指定需要进行限制的连接的特征。使用 ACL 能够指定几乎所有特征的连接。

acl-number：指定的 ACL 编号，范围为 2000～3999。

per-source：指定按每个源地址方式分别进行限制。

per-destination：指定按每个目的地址方式分别进行限制。

per-service：指定按每个服务（目的端口）方式分别进行限制。

amount：标识配置的是连接数的限制，而非速率的限制。以后增加速率限制时方便添加速率标识。

upper-limit、*lower-limit*：指定此子规则的连接数上下限。此参数的作用是，当连接特征符合指定的规则时，使用这两个值对连接的建立进行限制。*upper-limit* 的取值范围是 1～4294967295，*lower-limit* 的取值范围是 0～4294967295。当连接数到达上限时，禁止新连接建立。此时，只有当连接数降低到小于等于下限时，才允许建立新连接。

【描述】

limit 命令用来在对应的连接数限制策略下创建规则。

undo limit 命令用来在对应的连接数限制策略下删除规则。

当某条规则已经与 NAT 绑定时，用户不能对该规则进行修改和删除，如果用户需要修改或删除该规则，必须先解除该规则与 NAT 的绑定。

通过定义连接限制策略规则的 ACL，不但可以限制 TCP 连接数量，也可以限制非 TCP 流量（如：UDP、ICMP）。如果只对 TCP 连接进行限制，需要在 ACL 中明确指定。

【举例】

在策略 1 下创建一个规则，使用 ACL3000，连接数上限为 100，下限为 10，对源地址进行限制。

```
[SecBlade_FW] connection-limit policy 1
[SecBlade_FW-connection-limit-policy-1] limit 0 acl 3000 per-source 100 10
```

3.1.12 nat address-group

【命令】

nat address-group *group-number start-addr end-addr*

undo nat address-group *group-number*

【视图】

系统视图

【参数】

group-number：地址池的编号，范围为 0～31 的整数。

start-addr：地址池的开始 IP 地址。

end-addr：地址池的结束 IP 地址。

【描述】

nat address-group 命令用来配置地址池，**undo nat address-group** 命令用来删除地址池。

地址池表示了一些外部 IP 地址的集合，如果 *start-addr* 和 *end-addr* 相同，表示只有一个地址。

⚠ 注意：

- 地址池长度（地址池中包含的所有地址个数）不能超过 255 个地址。
- 当某个地址池已经和某个访问控制列表关联进行地址转换，是不允许删除这个地址池的。

【举例】

配置一个从 202.110.10.10 到 202.110.10.15 的地址池，地址池号为 1。

```
[SecBlade_FW] nat address-group 1 202.110.10.10 202.110.10.15
```

3.1.13 nat aging-time

【命令】

nat aging-time { **default** | { **dns** | **ftp-ctrl** | **ftp-data** | **icmp** | **pptp** | **tcp** | **tcp-fin** | **tcp-syn** | **udp** } *seconds* }

【视图】

系统视图

【参数】

default：设置地址转换有效时间为系统缺省默认值。

dns：DNS 协议地址转换有效时间 ，缺省为 60 秒。

ftp-ctrl：FTP 协议控制链路地址转换有效时间，缺省为 7200 秒。

ftp-data：FTP 协议数据链路地址转换有效时间，缺省为 300 秒。

icmp：ICMP 协议地址转换有效时间，缺省为 60 秒。

pptp：PPTP 协议地址转换有效时间，缺省为 86400 秒。

tcp：TCP 协议地址转换有效时间，缺省为 86400 秒。

tcp-fin：TCP 协议 FIN 或 RST 连接地址转换有效时间，缺省为 60 秒。

tcp-syn：TCP 协议 SYN 连接地址转换有效时间，缺省为 60 秒。

udp：UDP 地址转换有效时间，缺省为 300 秒。

seconds：为一个时间值，单位为秒，取值范围为 10～86400（即 24 小时）。

【描述】

nat aging-time 命令用来设置地址转换连接的有效时间。

该命令设置地址转换连接的有效时间，针对不同的协议类型设定不同的时间。单位为秒。ALG 的默认老化时间和对应的应用有关，同时为防止攻击，首包老化时间设置为 5 秒。

【举例】

设定 TCP 协议的连接有效时间为 240 秒。

```
[SecBlade_FW] nat aging-time tcp 240
```

3.1.14 nat alg

【命令】

nat alg { **dns** | **ftp** | **h323** | **ils** | **msn** | **nbt** | **pptp** }

undo nat alg { **dns** | **ftp** | **h323** | **ils** | **msn** | **nbt** | **pptp** }

【视图】

系统视图

【参数】

dns：支持 DNS 协议。

ftp：支持 FTP 协议。

h323：支持 H.323 协议。

ils：支持 ILS 协议。

msn：支持 MSN 协议。

nbt：支持 NBT 协议。

pptp：支持 PPTP 协议。

【描述】

nat alg 命令用来使能地址转换应用层网关功能，**undo nat alg** 命令用来禁用地址转换应用层网关功能。

缺省情况下，使能地址转换应用层网关功能。

【举例】

使能地址转换应用层网关功能，使 NAT 支持 FTP 应用。

```
[SecBlade_FW] nat alg ftp
```

3.1.15 nat connection-limit-policy

【命令】

nat connection-limit-policy *policy-number*

undo nat connection-limit-policy *policy-number*

【视图】

系统视图

【参数】

policy-number：与 NAT 绑定的连接数限制策略编号，范围为 0～19。

【描述】

nat connection-limit-policy 命令用来指定与 NAT 绑定的连接数限制策略。

undo nat connection-limit-policy 命令用来取消与 NAT 绑定的连接数限制策略。

缺省情况下，策略和 NAT 未进行绑定。

nat connection-limit-policy 命令可重复配置，后面的配置将覆盖前面的配置。

【举例】

将策略 1 与 NAT 绑定。

```
[SecBlade_FW] nat connection-limit-policy 1
```

3.1.16 nat dns-map

【命令】

nat dns-map *domain-name global-addr global-port* [**tcp** | **udp**]

undo nat dns-map *domain-name*

【视图】

系统视图

【参数】

domain-name：可被外部 DNS 服务器正确解析的合法域名。

global-addr：提供给外部网络访问的 IP 地址（一个合法的 IP 地址）。

global-port：提供给外部网络访问的服务的端口号。

tcp：表示 IP 协议承载的协议类型是 TCP。

udp：表示 IP 协议承载的协议类型是 UDP。

【描述】

nat dns-map 命令用来配置一条域名到外部 IP 地址、端口号、协议类型的映射，**undo nat dns-map** 命令用来删除一条域名到外部 IP 地址、端口号、协议类型的映射。

此命令用于配置内部服务器的“域名-外部 IP 地址、端口、协议类型”的映射，使内部主机在内部无 DNS 服务器的情况下，可以使用不同的域名区别并访问对应的内部服务器。

缺省情况下，未配置此类映射，此时内部主机的域名请求被外部 DNS 服务器解析得到外部 IP 地址后，只能映射到一台内部服务器上，无法实现内部主机使用不同的域名区别并访问其对应的内部服务器的功能。

最多允许配置 16 条映射。

【举例】

配置一条域名到外部 IP 地址、端口号、协议类型的映射。

```
[SecBlade_FW] nat dns-map www.abc.com 202.112.0.1 80 tcp
```

3.1.17 nat outbound

【命令】

nat outbound *acl-number* [**address-group** *group-number* [**no-pat**]]

undo nat outbound *acl-number* [**address-group** *group-number* [**no-pat**]]

【视图】

接口视图

【参数】

address-group：表示使用地址池的方式配置地址转换，如果不指定地址池，则直接使用该接口的 IP 地址作为转换后的地址，即 easy-ip 特性。

no-pat：表示使用多对多的地址转换，只转换数据包的地址而不转换端口信息。

acl-number：访问控制列表的索引值，范围为 2000～3999（可以使用高级 ACL）。

group-number：一个已经定义的地址池的编号。

【描述】

nat outbound 命令用来将一个访问控制列表 ACL 和一个地址池关联起来，表示 *acl-number* 中规定的地址可以使用地址池 *group-number* 进行地址转换，**undo nat outbound** 命令用来删除相应的地址转换。

通过配置访问控制列表和地址池的关联，将符合访问控制列表中的数据报文的源地址进行地址转换，选用地址池中的某个地址或者直接使用接口的 IP 地址进行转换。

可以在同一个接口上配置不同的地址转换关联。使用对应的 **undo** 命令可以将相应的地址转换关联删除。该接口一般情况应该是和 ISP 连接，是内部网络的出口。

该命令如果不带 **address-group** 参数，即使用 **nat outbound** *acl-number* 命令，则实现了 easy-ip 的特性，地址转换时，使用接口的 IP 地址作为转换后的地址，利用访问控制列表控制哪些地址可以进行地址转换。

【举例】

允许 10.110.10.0/24 网段的主机进行地址转换，选用 202.110.10.10 到 202.110.10.12 之间的地址作为转换后的地址。假设 GigabitEthernet0/0.1 口连接 ISP。

```
[SecBlade_FW] acl number 2001
[SecBlade_FW-acl-basic-2001] rule permit source 10.110.10.0 0.0.0.255
[SecBlade_FW-acl-basic-2001] rule deny
```

配置地址池。

```
[SecBlade_FW] nat address-group 1 202.110.10.10 202.110.10.12
```

允许地址转换，使用地址池 1 中的地址进行地址转换。在转换的时候使用 TCP/UDP 的端口信息，使用如下配置。

```
[SecBlade_FW-GigabitEthernet0/0.1] nat outbound 2001 address-group 1
```

删除对应配置。

```
[SecBlade_FW-GigabitEthernet0/0.1] undo nat outbound 2001 address-group 1
```

如果使用一对一的地址转换（不使用 TCP/UDP 的端口信息进行地址转换），可以使用如下配置。

```
[SecBlade_FW-GigabitEthernet0/0.1] nat outbound 2001 address-group 1 no-pat
```

删除对应配置。

```
[SecBlade_FW-GigabitEthernet0/0.1] undo nat outbound 2001 address-group 1
no-pat
```

如果直接使用 GigabitEthernet0/0.1 口的 IP 地址，可以使用如下的配置。

```
[SecBlade_FW-GigabitEthernet0/0.1] nat outbound 2001
```

删除对应配置。

```
[SecBlade_FW-GigabitEthernet0/0.1] undo nat outbound 2001
```

3.1.18 nat outbound interface

【命令】

nat outbound *acl-number* **interface** *interface-type interface-number*

undo nat outbound *acl-number* **interface** *interface-type interface-number*

【视图】

接口视图

【参数】

acl-number：访问控制列表的索引值，范围为 2000～3999。

interface *interface-type interface-number*：指定接口类型及接口号，目前只支持指定 Loopback 接口。

【描述】

nat outbound interface 命令将一个访问控制列表 ACL 和一个指定接口关联起来，并用使用指定接口地址作为转换后的地址，即将匹配访问控制列表的数据报文的源地址转换为指定接口的 IP 地址。**undo nat outbound interface** 命令用来删除访问控制列表和其他接口地址关联，即取消地址转换。

目前仅支持使用指定的 loopback 接口地址作为转换后的地址。

【举例】

使用 loopback0 接口地址作为转换后地址

```
[SecBlade_FW] interface loopback0
[SecBlade_FW-LoopBack0] ip address 202.38.160.106
[SecBlade_FW-LoopBack0] quit
[SecBlade_FW] acl number 2000
[SecBlade_FW-acl-basic-2000] rule permit source 10.110.12.0 0.0.0.255
[SecBlade_FW-acl-basic-2000] quit
[SecBlade_FW] interface GigabitEthernet0/0.3
[SecBlade_FW- GigabitEthernet0/0.3] nat outbound 2000 interface loopback 0
```

3.1.19 nat outbound static

【命令】

nat outbound static

undo nat outbound static

【视图】

接口视图

【参数】

无

【描述】

nat outbound static 命令用来使 **nat static** 命令配置的 NAT 静态转换表项在接口上生效。**undo nat outbound static** 命令用来禁止在接口上配置的 NAT 静态转换表项生效。

【举例】

配置使 GigabitEthernet0/0.1 接口上的 NAT 静态转换表项。

```
[SecBlade_FW-GigabitEthernet0/0.1] nat outbound static
```

3.1.20 nat overlapaddress

【命令】

nat overlapaddress *number overlappool-startaddress temppool-startaddress* { **pool-length** *pool-length* | **address-mask** *mask* }

undo nat overlapaddress *number*

【视图】

系统视图

【参数】

number：地址池对编号，取值范围为 0～7。

overlappool-startaddress：重叠地址池起始地址，各重叠地址池的地址不能有交集。

temppool-startaddress：临时地址池起始地址，各临时地址池的地址不能有交集。临时地址池里面的地址应该与内网及外网地址都不重叠。建议选择私网地址段，避免与公网地址重叠。

pool-length：地址池长度，以十进制表示。相互关联的重叠地址池与临时地址池长度相等，地址一一对应。

mask：地址池对应的子网掩码。

【描述】

nat overlapaddress 命令用于配置一个重叠地址池到一个临时地址池的映射。**undo nat overlapaddress** 命令用于取消已配置的映射。

📖 说明：

重叠地址池与临时地址池一一对应，转换规则为：

临时地址 = 临时地址池首地址 + （重叠地址 – 重叠地址池首地址）

重叠地址 = 重叠地址池首地址 + （临时地址 – 临时地址池首地址）

【举例】

配置一个从 171.69.100.0 到 192.168.0.0 的映射，地址池对编号为 0。

```
[SecBlade_FW] nat overlapaddress 0 171.69.100.0 192.168.0.0 address-mask 24
```

3.1.21 nat server

【命令】

nat server [*acl-number*] **protocol** *pro-type* **global** { *global-addr global-port1 global-port2* | **current-interface** | **interface** *type number* } **inside** *host-addr1 host-addr2 host-port*

nat server [*acl-number*] **protocol** *pro-type* **global** { *global-addr* [*global-port*] | **current-interface** | **interface** *type number* } **inside** *host-addr* [*host-port*]

undo nat server [*acl-number*] **protocol** *pro-type* **global** { *global-addr global-port1 global-port2* | **current-interface** | **interface** *type number* } **inside** *host-addr1 host-addr2 host-port*

undo nat server [*acl-number*] **protocol** *pro-type* **global** { *global-addr* [*global-port*] | **current-interface** | **interface** *type number* } **inside** *host-addr* [*host-port*]

【视图】

接口视图

【参数】

acl-number：基本访问列表或高级访问列表的编号，范围为 2000～3999。指定的访问控制列表只对内部到外部的报文生效，即控制其是否进行地址转换处理，对外部到内部的报文不生效。

global-addr：提供给外部访问的 IP 地址（一个合法的 IP 地址）。

global-port：提供给外部访问的服务的端口号。若忽略的话，将和 *host-port* 的值一致。

current-interface：使用 SecBlade 当前公网接口的地址作为 NAT Server 的公网地址。

interface *type number*：指定使用其他接口的地址作为 NAT Server 的公网地址。目前仅支持 LoopBack 接口，且必须已在 SecBlade 中配置。

host-addr：服务器在内部局域网的 IP 地址。

host-port：服务器提供的服务端口号，范围为 0～65535，常用的端口号可以用关键字代替。如：www 服务端口为 80，同时可以使用 **www** 代替。FTP 服务端口号为 21，同时可以使用 **ftp** 代替。如果为零，表示任何类型的服务都提供，可以用 **any** 关键字代替。如果没有配置这个参数，则表示是 **any** 的情况，相当于 *global-addr*

和 *host-addr* 之间有一个静态的连接。当 *host-port* 是 **any** 时候，*global-port* 也必须是 **any**，否则是非法配置。

global-port1、*global-port2*：通过两个端口指定一个端口范围，和内部的主机的地址范围构成一种对应关系。*global-port2* 必须大于 *global-port1*。

host-addr1、*host-addr2*：定义一组连续的地址范围，和前面定义的端口范围构成一一对应的关系。*host-addr2* 必须大于 *host-addr1*。该地址范围的数量必须和 *global-port1*、*global-port2* 定义的端口数量相同。

pro-type：表示 IP 协议承载的协议类型，可以使用协议号，也可用关键字代替。如：**icmp**（协议号为 1）、**tcp**（协议号为 6）、**udp**（协议号为 7）。

【描述】

nat server 命令用来定义一个内部服务器的映射表，用户可以通过 *global-addr* 和 *global-port* 定义的地址端口来访问地址和端口分别为 *host-addr* 和 *host-port* 的内部服务器。**undo nat server** 命令用来取消映射表。

通过该命令可以配置一些内部网络提供给外部使用的服务器，内部服务器可以位于普通的私网内。例如 www、ftp、telnet、pop3、dns 等等。

在一个接口下最多可以配置 256 条内部服务器转换命令，一个接口下最多可以配置 4096 个内部服务器，系统一共可以最多配置 1024 个内部服务器转换命令。如果配置端口范围的 nat server（即通过配置 *global-port1*、*global-port2* 指定一个端口范围，和内部主机的地址范围构成一种对应关系），则对应配置多少端口，即为多少个内部服务器。

如果 *global-port* 和 *inside-port* 都为 0、any 或未配置的话，则内网服务器可以通过该配置访问公网，但发起访问的协议必须与配置的协议相同。

当使用端口范围配置 FTP 服务器的 NAT Server 时，内部端口号不能配置为 20 和 21；当不使用端口范围配置 FTP 服务器的 NAT Server 时，内部端口号不能配置为 20。

由于 TFTP 协议的特殊性，当配置 TFTP 服务器的 NAT Server 时，还应对内部的 TFTP 服务器配置相应的 **nat outbound** 命令。

配置该命令的接口应该是和 ISP 连接的，是内部网络的出口。

【举例】

指定局域网内部的 WWW 服务器的 IP 地址是 10.110.10.10，内部的 FTP 服务器的 IP 地址是 10.110.10.11，希望外部通过 http:// 202.110.10.10:8080 可以访问 web，通过 ftp://202.110.10.10 可以连接 FTP 站点。假设 GigabitEthernet0/0.1 和 ISP 连接。

```
[SecBlade_FW-GigabitEthernet0/0.1] nat server protocol tcp global
202.110.10.10 8080 inside 10.110.10.10 www
```

```
[SecBlade_FW-GigabitEthernet0/0.1] nat server protocol tcp global
202.110.10.10 inside 10.110.10.11 ftp
```

指定一个内部的主机 10.110.10.12，希望外部网络的主机可以利用 ping 202.110.10.11 命令 ping 通它。

```
[SecBlade_FW-GigabitEthernet0/0.1] nat server protocol icmp global
202.110.10.11 inside 10.110.10.12
```

用以下面命令可以删除 WWW 服务器。

```
[SecBlade_FW-GigabitEthernet0/0.1] undo nat server protocol tcp global
202.110.10.10 8080 inside 10.110.10.10 www
```

用以下面命令可以删除内部的 FTP 服务器。

```
[SecBlade_FW-GigabitEthernet0/0.1] undo nat server protocol tcp global
202.110.10.11 8080 inside 10.110.10.11 ftp
```

指定一个外部地址 202.110.10.10，从端口 1001～1100 分别映射主机 10.110.10.1～10.110.10.100 的 telnet 服务。202.110.10.10:1001 访问 10.110.10.1，202.110.10:1002 访问 10.110.10.2。

```
[SecBlade_FW-GigabitEthernet0/0.1] nat server protocol tcp global
202.110.10.10 1001 1100 inside 10.110.10.1 10.110.10.100 telnet
```

指定使用 Dialer 0 接口获取的 IP 地址作为 NAT Server 的公网地址。

```
[SecBlade_FW-Dialer0] nat server protocol tcp global current-interface 5000
inside 10.0.0.10 5000
```

3.1.22 nat static

【命令】

nat static *ip-addr1 ip-addr2*

undo nat static *ip-addr1 ip-addr2*

【视图】

系统视图

【参数】

ip-addr1：内部主机私有 IP 地址。

ip-addr2：全局 IP 地址。

【描述】

nat static 命令用来配置从内部地址到外部地址的一对一转换。**undo nat static** 命令用来删除已经配置的 NAT 一对一转换。

【举例】

配置内部私有 IP 地址到外部全局 IP 地址的一对一转换。

```
[SecBlade_FW] nat static 192.168.1.1 2.2.2.2
```

3.1.23 nat static inside

【命令】

nat static inside ip *inside-address* **global ip** *global-address*

nat static inside ip *inside-start-address inside-end-address* **global ip** *global-address* { *mask* | *mask-length* }

undo nat static inside ip *inside-address*

undo nat static inside ip *inside-address* **global ip** *global-address*

undo nat static inside ip *inside-start-address inside-end-address* [**global ip** *global-address* { *mask* | *mask-length* }]

【视图】

系统视图

【参数】

inside-address：指定的静态表项需要转换的内网的地址。

inside-start-address：指定的静态表项需要转换的内网的起始地址。

inside-end-address：指定的静态表项需要转换的内网的结束地址。

global-address：指定的静态表项转化后的公网的网段地址。

mask：公网网段地址对应的子网掩码。

mask-length：公网网段地址对应的子网掩码长度。

【描述】

nat static inside 命令用来配置网段转换静态表项的信息，使用该静态表项进行 NAT 转换时，只进行网段地址的转换，而保持主机地址不变。**undo nat static inside** 命令用来删除已经配置的静态表项。

其中 *global-address* 可以输入任何的地址，配置的 *global-address* 结果会根据输入的 *mask* 和掩码的长度对输入的 *global-address* 进行计算。

nat static inside 和 **nat static** 配置会创建两种不同的 NAT 静态表项，在具体的配置中，两种 NAT 静态表项不存在冲突即可。

缺省情况为没有配置任何静态表项。

【举例】

指定静态表项，将 10.1.1.1 到 10.1.1.100 保持主机地址不变 NAT 转换为 211.1.1.0 网段地址。

```
[SecBlade_FW] nat static inside ip 10.1.1.1 10.1.1.100 global ip 211.1.1.0
255.255.255.0
```

3.1.24 reset nat

【命令】

reset nat { **log-entry** | **session** }

【视图】

用户视图

【参数】

log-entry：清除 NAT 日志缓冲区。

session：清除地址转换表信息。

【描述】

reset nat 命令用来清除内存中地址转换的映射表，释放动态分配的用于存放映射表的内存。

【举例】

清除 NAT 日志缓冲区。

```
<SecBlade_FW> reset nat log-entry
```

清除地址转换表信息。

```
<SecBlade_FW> reset nat session
```

第4章 防火墙配置命令

4.1 包过滤防火墙配置命令

4.1.1 debugging firewall packet-filter

【命令】

debugging firewall packet-filter { { **all** | **icmp** | **tcp** | **udp** | **fragments-inspect** | **others** } [**interface** *type number*] | **denied** | **permitted** }

undo debugging firewall packet-filter { { **all** | **icmp** | **tcp** | **udp** | **fragments-inspect** | **others** } [**interface** *type number*] | **denied** | **permitted** }

【视图】

用户视图

【参数】

all：有关全部的调试信息。

icmp：有关 ICMP 包过滤的调试信息。

tcp：有关 TCP 包过滤的调试信息。

udp：有关 UDP 包过滤的调试信息。

others：除了 ICMP、TCP、UDP 外其它所有类型的报文调试信息。

fragments-inspect：有关分片报文调试信息。

interface *type number*：经过该接口的相应数据包的调试信息，没有这个参数时，表示显示所有接口的调试信息。

denied：有关被禁止的数据包的调试信息。

permitted：有关被允许的数据包的调试信息。

【描述】

debugging firewall packet-filter 命令用来打开防火墙包过滤调试信息开关，**undo debugging firewall packet-filter** 命令用来关闭防火墙包过滤调试信息开关。

缺省设置是关闭包过滤防火墙全部调试信息开关。

相关配置可参考命令 **display debugging**。

【举例】

打开有关 UDP 包过滤的调试信息。

```
<SecBlade_FW> debugging firewall packet-filter udp
```

4.1.2 debugging firewall packet-filter fragments-inspect events

【命令】

debugging firewall packet-filter fragments-inspect events

undo debugging firewall packet-filter fragments-inspect events

【视图】

用户视图

【参数】

无

【描述】

debugging firewall packet-filter fragments-inspect events 命令用来打开分片报文的检测事件信息的调试开关，**undo debugging firewall packet-filter fragments-inspect events** 命令用来关闭分片报文的检测事件信息的调试开关。

缺省情况下，关闭分片报文的检测事件信息的调试开关。

【举例】

打开分片报文的检测事件信息的调试开关。

```
<SecBlade_FW> debugging firewall packet-filter fragments-inspect events
```

4.1.3 display firewall fragment

【命令】

display firewall fragment

【视图】

所有视图

【参数】

无

【描述】

display firewall fragment 命令用来显示防火墙的分片表。

【举例】

显示防火墙的分片表。

```
<SecBlade_FW> display firewall fragment
```

4.1.4 display firewall packet-filter statistics

【命令】

display firewall packet-filter statistics { **all** | **interface** *type number* | **fragments-inspect** }

【视图】

所有视图

【参数】

all：表示显示所有接口的过滤报文统计信息。

interface *type number*：接口类型及接口号，表示显示某接口的过滤报文统计信息。

fragments-inspect：显示分片报文检测统计信息。

【描述】

display firewall packet-filter statistics 命令用来显示包过滤防火墙的统计信息。

【举例】

显示分片报文检测信息。

```
[SecBlade_FW] display firewall packet-filter statistics fragments-inspect
  Fragments inspection is enabled.
  The high-watermark for clamping is 10000.
  The low-watermark for clamping is 1000.
  Current records for fragments inspection is 0.
```

4.1.5 firewall packet-filter default

【命令】

firewall packet-filter default { **permit** | **deny** }

【视图】

系统视图

【参数】

permit：默认过滤规则为允许。

deny：默认过滤规则为禁止。

【描述】

firewall packet-filter default 命令用来设置包过滤防火墙的缺省过滤方式为“允许”或“禁止”。

当防火墙工作在透明模式下，若缺省过滤方式为 deny，除了绑定编号为 4000～4999 的以太帧 ACL 外，还需要绑定编号为 1000～1999 的接口 ACL，才能正常转发报文。

系统缺省为拒绝任何报文通过。

【举例】

设置防火墙缺省过滤规则为允许。

```
[SecBlade_FW] firewall packet-filter default permit
```

4.1.6 firewall packet-filter enable

【命令】

firewall packet-filter enable

undo firewall packet-filter enable

【视图】

系统视图

【参数】

无

【描述】

firewall packet-filter enable 命令用来启用包过滤防火墙功能，命令 **undo firewall packet-filter enable** 用来关闭包过滤防火墙功能。

缺省情况下，启用包过滤防火墙功能。

【举例】

禁止防火墙包过滤防火墙功能

```
[SecBlade_FW] undo firewall packet-filter enable
```

4.1.7 firewall packet-filter fragments-inspect

【命令】

firewall packet-filter fragments-inspect

undo firewall packet-filter fragments-inspect

【视图】

系统视图

【参数】

无

【描述】

firewall packet-filter fragments-inspect 命令用来打开分片报文检测开关， **undo firewall packet-filter fragments-inspect** 命令用来关闭分片报文检测开关。

缺省情况下，分片检测开关为关闭。

此命令是实现精确匹配的前提。只有打开分片检测开关，才能进行分片报文的精确匹配。这时，包过滤防火墙将记录分片报文的状态，根据高级 ACL 规则对三层（IP 层）以外的信息进行精确匹配。

包过滤防火墙对分片报文的状态记录需要消耗系统资源。如果不使用精确匹配模式，则可以关闭此功能，以提高系统运行效率，减小系统开销。

只有打开了分片报文检测开关，精确匹配模式才能真正有效。

相关配置可参考命令 **firewall packet-filter**（接口视图）。

【举例】

打开分片检测开关。

```
[SecBlade_FW] firewall packet-filter fragments-inspect
```

4.1.8 firewall packet-filter fragments-inspect { high | low }

【命令】

firewall packet-filter fragments-inspect { **high** | **low** } { **default** | *number* }

undo firewall packet-filter fragments-inspect { **high** | **low** }

【视图】

系统视图

【参数】

high *number*：指定上限分片状态记录数目，取值范围是 100～10000。

low *number*：指定下限分片状态记录数目，取值范围是 100～10000。

default：记录分片状态的缺省数目。上限分片状态记录数目（**high**）缺省值为 2000。下限分片状态记录数目（**low**）缺省值为 1500。

【描述】

firewall packet-filter fragments-inspect { **high** | **low** } 命令用来配置分片报文检测的上、下门限值， **undo firewall packet-filter fragments-inspect** { **high** | **low** } 命令用来恢复上、下门限值为缺省值。

如果打开分片检测开关，应用精确匹配过滤后，包过滤的执行效率会略微降低，配置的匹配项目越多，效率降低越多。因此，需要设定门限值（最大允许上、下限域值）。当记录状态数达到上限时，将删除最先保存的状态项直至下限值。

下限值必须小于或等于上限值。

相关配置可参考命令 **display firewall packet-filter statistics fragments-inspect**，**firewall packet-filter fragments-inspect**。

【举例】

配置检测上限 3000，下限为缺省值。

```
[SecBlade_FW] firewall packet-filter fragments-inspect high 3000
[SecBlade_FW] firewall packet-filter fragments-inspect low default
```

4.1.9 firewall packet-filter

【命令】

firewall packet-filter *acl-number* { **inbound** | **outbound** } [**match-fragments** { **normally** | **exactly** }]

undo firewall packet-filter *acl-number* { **inbound** | **outbound** }

【视图】

接口视图

【参数】

acl-number：ACL 的序号。

inbound：过滤从接口收到的数据包。

outbound：过滤从接口发送的数据包。

match-fragments：指定分片的匹配模式，只有高级访问控制列表有此参数。

normally：标准匹配模式，此模式为缺省模式，只有高级访问控制列表有此参数。

exactly：精确匹配模式，只有高级访问控制列表有此参数。

【描述】

firewall packet-filter 命令用来将访问控制列表应用到相应的接口上， **undo firewall packet-filter** 命令用来删除相应的设置。

基于接口的访问控制列表（即序号为 1000 到 1999 的 ACL）只能用参数 **outbound**。接口访问控制列表用来匹配从特定接口接收到的报文，然后允许或拒绝匹配的报文从某接口（包括接收报文的接口）发送出去。

CMW 平台的包过滤提供了对分片报文过滤的功能，可以对所有的分片报文进行三层（IP 层）的匹配过滤（例如基于源、目的 IP 地址）；同时，对于包含扩展信息的高级 ACL 规则（例如包含 TCP/UDP 端口号，ICMP 类型等），提供标准匹配和精确匹配两种匹配方式。标准匹配即三层信息的匹配，匹配将忽略三层以外的信息；精确匹配则对所有的高级 ACL 的过滤规则进行匹配，这就要求防火墙必须记录首片分片报文的状态以获得完整的后续分片的匹配信息。

缺省的模式为标准匹配方式。

只有在启用包过滤防火墙功能后，在接口上应用的访问控制列表才能生效。

相关配置可参考命令 **acl**，**display acl**，**firewall packet-filter enable**，**firewall packet-filter fragments-inspect**。

【举例】

在接口 GigabitEthernet0/0.2 应用访问控制列表 3001，过滤接口发送的报文。

```
[SecBlade_FW-GigabitEthernet0/0.2] firewall packet-filter 3001 outbound
```

4.1.10 reset firewall packet-filter statistics

【命令】

reset firewall packet-filter statistics { **all** | **interface** *type number* }

【视图】

用户视图

【参数】

all：表示清除所有接口的过滤报文统计信息。

interface：表示清除某接口的过滤报文统计信息。

type number：为接口类型及接口号。

【描述】

reset firewall packet-filter statistics 命令用来清除包过滤防火墙的统计信息。

【举例】

清除接口 GigabitEthernet0/0.2 的接口过滤报文统计信息。

```
<SecBlade_FW> reset firewall packet-filter statistics interface
GigabitEthernet0/0.2
```

4.2 状态防火墙配置命令

4.2.1 aging-time

【命令】

aging-time { **syn** | **fin** | **tcp** | **udp** } *seconds*

undo aging-time { **syn** | **fin** | **tcp** | **udp** }

【视图】

ASPF 策略视图

【参数】

seconds：用于指定在检测到 SYN 和 FIN 报文或者 TCP 和 UDP 协议时，会话表项的空闲超时时间。

【描述】

aging-time 命令用来配置 TCP 的 SYN 状态等待超时值、FIN 状态等待超时值，以及 TCP 和 UDP 会话表项空闲状态超时值， **undo aging-time** 命令用来恢复超时缺省值。

在超时时间以内，系统会保留所建立的连接和会话。

缺省情况下，SYN、FIN、TCP、UDP 的超时时间分别为 30s、30s、3600s 和 30s。

相关配置可参考命令 **display aspf all**，**display aspf policy**，**display aspf session**，**display aspf interface**。

【举例】

配置 TCP 的 SYN 状态等待时间超时值为 20 秒。

```
[SecBlade_FW-aspf-policy-1] aging-time syn 20
```

配置 TCP 的 FIN 状态等待时间超时值为 10 秒。

```
[SecBlade_FW-aspf-policy-1] aging-time fin 10
```

配置 TCP 空闲时间超时值为 3000 秒。

```
[SecBlade_FW-aspf-policy-1] aging-time tcp 3000
```

设置 UDP 空闲超时值为 110 秒。

```
[SecBlade_FW-aspf-policy-1] aging-time udp 110
```

4.2.2 aspf-policy

【命令】

aspf-policy *aspf-policy-number*

undo aspf-policy *aspf-policy-number*

【视图】

系统视图

【参数】

aspf-policy-number：ASPF 策略号，范围为 1～99。

【描述】

命令 **aspf-policy** 用来定义一个 ASPF 策略。对于一个已定义的 ASPF 策略，可通过策略号对该策略进行引用。

【举例】

定义一个 ASPF 策略，并进入该 ASPF 策略视图。

```
[SecBlade_FW] aspf-policy 1
[SecBlade_FW-aspf-policy-1]
```

4.2.3 debugging aspf

【命令】

debugging aspf { **all** | **verbose** | **events** | **ftp** | **h323** | **rtsp** | **session** | **smtp** | **tcp** | **timers** | **udp** }

undo debugging aspf { **all** | **verbose** | **events** | **ftp** | **h323** | **rtsp** | **session** | **smtp** | **tcp** | **timers** | **udp** }

【视图】

用户视图

【参数】

all：所有 ASPF 调试开关。

verbose：详细功能调试开关。

events：事件调试开关。

ftp：FTP 检测信息调试开关。

h323：H.323 检测信息调试开关。

rtsp：RTSP 检测信息调试开关。

session：会话信息调试开关。

smtp：SMTP 检测信息调试开关。

tcp：TCP 检测信息调试开关。

timers：计时器信息调试开关。

udp：UDP 检测信息调试开关。

【描述】

debugging aspf 命令用来打开 ASPF 调试信息开关，**undo debugging aspf** 命令用来关闭 ASPF 调试信息开关。

缺省情况下，关闭 ASPF 全部调试信息开关。

相关配置可参考命令 **display aspf all**，**display aspf policy**，**display aspf session**，**display aspf interface**。

【举例】

打开 ASPF 所有的调试开关。

```
<SecBlade_FW> debugging aspf all
```

4.2.4 debugging aspf http

【命令】

debugging aspf http { **java-blocking** | **activex-blocking** } { **all** | **error** | **event** | **filter** | **packet** }

undo debugging aspf http { **java-blocking** | **activex-blocking** } { **all** | **error** | **event** | **filter** | **packet** }

【视图】

用户视图

【参数】

java-blocking：Java Applet 阻断调试开关。

activex-blocking：ActiveX 控件阻断调试开关。

all：所有调试功能。

error：错误调试功能。

event：事件调试功能。

filter：过滤调试功能。

packet：报文调试功能。

【描述】

debugging aspf http java-blocking 命令用来打开 HTTP 检测的 Java Applet 阻断调试开关，**undo debugging aspf http java-blocking** 命令用来关闭 HTTP 检测的 Java Applet 阻断调试开关。

debugging aspf http activex-blocking 命令用来打开 HTTP 检测的 ActiveX 控件阻断调试开关，**undo debugging aspf http activex-blocking** 命令用来关闭 HTTP 检测的 ActiveX 控件阻断调试开关。

缺省情况下，未打开 HTTP 检测的 Java Applet 阻断和 ActiveX 控件阻断调试开关。

【举例】

打开 Java Applet 阻断功能的所有调试开关。

```
<SecBlade_FW> debugging aspf http java-blocking all
```

4.2.5 detect

【命令】

detect *protocol* [**aging-time** *seconds*]

undo detect *protocol*

【视图】

ASPF 策略视图

【参数】

protocol：ASPF 支持的协议名称。应用层协议包括：FTP、HTTP、H323、SMTP、RTSP；传输层协议包括：TCP、UDP。

seconds：配置协议空闲的超时时间，取值范围是 5～43200 秒，应用层协议的超时时间缺省值为 3600 秒。基于 TCP 协议的超时时间缺省值为 3600 秒；基于 UDP 协议的超时时间缺省值为 30 秒。

【描述】

detect 命令用来为应用层协议指定 ASPF 策略，**undo detect** 命令用来取消所做的配置。

当协议类型为 HTTP 时，允许 Java Applet 阻断和 ActiveX 控件阻断。

如果同时配置了应用层协议检测和通用 TCP/UDP 检测，应用层协议检测优先于通用 TCP/UDP 检测。

ASPF 使用超时时间去管理协议的会话状态信息，以便决定何时终结一个会话状态信息的管理或删除一个不能正常建立的会话。设置超时时间是一个全局的配置，适用于所有的会话，可以保护系统资源不被恶意占用。

相关配置可参考命令 **display aspf all**，**display aspf policy**，**display aspf session**，**display aspf interface**。

【举例】

配置对 FTP 协议指定 ASPF 策略，策略号为 1。

```
[SecBlade_FW] aspf-policy 1
[SecBlade_FW-aspf-policy-1] detect ftp
```

4.2.6 detect http

【命令】

detect http [**java-blocking** [*acl-number1*] | **activex-blocking** [*acl-number2*]]* [**aging-time** *seconds*]

undo detect http [**java-blocking** | **activex-blocking**]*

【视图】

ASPF 策略视图

【参数】

java-blocking：阻断 Java Applet。

acl-number1：基本访问控制列表（ACL）号，取值范围是 2000～2999。若不指定，则表示阻断所有的 Jave Applet。

activex-blocking：阻断 ActiveX 控件。

acl-number2：基本访问控制列表（ACL）号，取值范围是 2000～2999。若不指定，则表示阻断所有的 ActiveX 控件。

seconds：配置协议空闲的超时时间，取值范围是 5～43200 秒，应用层协议的超时时间缺省值为 3600 秒。基于 TCP 协议的超时时间缺省值为 3600 秒；基于 UDP 协议的超时时间缺省值为 30 秒。

【描述】

detect http 命令用来配置检测 HTTP 协议，并且可以配置对 Jave Applet 和 ActiveX 控件进行阻断，**undo detect http** 命令用来取消检测 HTTP。

目前 Java 阻断功能只能过滤 HTTP 请求中以“.class”为后缀的 Java 请求。

缺省情况下，不对 HTTP 进行检测。

【举例】

配置 ASPF 策略，检测 HTTP，并阻断所有的 ActiveX 控件和来自服务器 10.1.1.1 的 Java Applet。

```
[SecBlade_FW] acl number 2000
[SecBlade_FW-acl-basic-2000] rule permit source 10.1.1.1 0
[SecBlade_FW-acl-basic-2000] rule deny source any
[SecBlade_FW-acl-basic-2000] quit
[SecBlade_FW] aspf-policy 1
[SecBlade_FW-aspf-policy-1] detect http activex-blocking java-blocking 2000
```

4.2.7 display aspf all

【命令】

display aspf all

【视图】

所有视图

【参数】

无

【描述】

display aspf all 命令用来显示所有的 ASPF 策略和会话信息。

【举例】

下面是 **display aspf all** 命令的输出信息。

```
[SecBlade_FW] display aspf all
[ASPF Policy Configuration]
  Policy Number 1:
    Log:                 disable
    SYN timeout:         30    s
    FIN timeout:         30    s
    TCP timeout:         3600  s
    UDP timeout:         30    s
    Detect Protocols:
      h323 timeout 3600
      rtsp timeout 3600
      http  timeout 3600
      smtp timeout 3600
      ftp  timeout 3600
      tcp  timeout 3600
      udp  timeout 30

[Interface Configuration]
   Interface                     InboundPolicy   OutboundPolicy
```

```
-------------------------------------------------------------
GigabitEthernet0/0.1                  none            1
```

表4-1 ASPF 配置信息显示描述表

域名	描述
Log	表示是否开会话日志功能
SYN timeout	TCP 连接的 SYN 状态超时值为 30 秒
FIN timeout	TCP 连接的 FIN 状态超时值为 5 秒
TCP timeout	TCP 会话的空闲时间超时值为 3600 秒
UDP timeout	UDP 会话的空闲时间超时值为 30 秒
Detect Protocols	ASPF 策略所检测的协议
InboundPolicy	入方向的 ASPF 策略
OutboundPolicy	出方向的 ASPF 策略

4.2.8 display aspf interface

【命令】

display aspf interface

【视图】

所有视图

【参数】

无

【描述】

display aspf interface 命令用来显示接口上配置的 ASPF 策略。

【举例】

下面是 **display aspf interface** 的输出。

```
[SecBlade_FW] display aspf interface
[Interface Configuration]
  Interface                      InboundPolicy   OutboundPolicy
 -------------------------------------------------------------
  GigabitEthernet0/0.1                 none            1
```

表4-2 ASPF 接口配置信息显示描述表

域名	描述
InboundPolicy	入方向的 ASPF 策略
OutboundPolicy	出方向的 ASPF 策略

4.2.9 display aspf policy

【命令】

display aspf policy *aspf-policy-number*

【视图】

所有视图

【参数】

aspf-policy-number：ASPF 策略号，范围为 1～99。

【描述】

display aspf policy 命令用来显示一个特定 ASPF 策略。

【举例】

显示策略号为 1 的 ASPF 策略的配置信息。

```
[SecBlade_FW] display aspf policy 1
[ASPF Policy Configuration]
  Policy Number 1:
    Log:                 disable
    SYN timeout:         30    s
    FIN timeout:         30    s
    TCP timeout:         3600  s
    UDP timeout:         30    s
    Detect Protocols:
      h323 timeout 3600
      rtsp timeout 3600
      http  timeout 3600
      smtp timeout 3600
      ftp  timeout 3600
      tcp  timeout 3600
      udp  timeout 30
```

以上显示信息中的描述请参见 表 4-1

4.2.10 display aspf session

【命令】

display aspf session [**verbose**] [**vpn-instance** *vpn-instance-name*]

【视图】

所有视图

【参数】

verbose：显示会话表项的详细信息。

vpn-instance-name：显示使用的 vpn-instance 名字。

【描述】

display aspf session 命令用来显示 ASPF 的会话表，可指定 vpn-instance 用于显示属于指定 VPN 实例的会话表，若不指定 vpn-instance，则显示所有的会话表。

display aspf session 命令和 **display firewall session table** 命令显示的是两个会话表，这两个会话表的默认老化时间是不同的。对于同一条数据流，有可能在 ASPF 会话表中仍然存在，而在防火墙会话表中已经老化不存在，反之亦然。

【举例】

显示 VPN 实例 vpntest 的当前 ASPF 会话的相关信息。

```
[FireWall] display aspf session vpn-instance vpntest
Total session number:2
Syn-list session number:0
Fin-list session munber:0
[Established Sessions]
VPN-instance  Session Initiator            Responder      Application Status
vpntest       212BA84 169.254.1.121:1427 169.254.1.52:0 ftp-data    TCP_DOWN
vpntest       2B738C4 169.254.1.121:1426 169.254.1.52:21 ftp    FTP_CONXN_UP
```

显示 VPN 实例 vpntest 的当前 ASPF 会话的详细信息。

```
[FireWall] display aspf session verbose vpn-instance vpntest
[Session 0x256E5B24]
Total session number:1
Syn-list session number:0
Fin-list session munber:0
VPN-Instance: vpntest
Initiator: 1.1.1.4:1024           Responder: 2.1.1.2:1719
Application protocol: unknown     Status: UDP_OPENING
Transport protocol: 17            Port: 1719
Child: 0x0                        Parent: 0x0
```

```
Interface: GigabitEthernet0/0     Direction: inbound
Timeout 00:00:30                  Time left 00:00:10
Initiator Bytes/Packets sent: 110/1
Responder Bytes/Packets sent: 0/0
Initiator tcp SeqNumber/AckNumber: 0/0
Responder tcp SeqNumber/AckNumber: 0/0
```

4.2.11 display aspf statistics

【命令】

display aspf statistics

【视图】

任意视图

【参数】

无

【描述】

display aspf statistics 命令用来显示 ASPF 的统计信息。

【举例】

显示 ASPF 的统计信息。

```
<SecBlade_FW> display aspf statistics
ASPF Syn list full occur times:0
ASPF Hash list full occur times:0
ASPF Tacl list full occur times:0
ASPF Session table full occur times:0
ASPF Fin list error occur times:0
```

4.2.12 display firewall fragment

【命令】

display firewall fragment [**vpn-instance** *VPN-Instance name*]

【视图】

所有视图

【参数】

vpn-instance-name：显示使用的 vpn-instance 名字。

【描述】

display firewall fragment 命令用来显示防火墙的分片表，可指定 vpn-instance 用于显示属于指定 VPN 实例的分片表，若不指定 vpn-instance，则显示所有的分片表。

【举例】

显示 VPN 实例 vpntest 的当前防火墙会话的分片表。

```
[FireWall] display firewall fragment vpn-instance vpntest
172.31.48.45<--222.1.1.2
vpn-instance: vpntest : PacID: 758,    ttl:  00:00:05    left:  00:00:01
172.31.48.45-->222.1.1.2
vpn-instance: vpntest : PacID: 755,    ttl:  00:00:05    left:  00:00:01
172.31.48.45-->222.1.1.2
vpn-instance: vpntest : PacID: 756,    ttl:  00:00:05    left:  00:00:01
172.31.48.45-->222.1.1.2
vpn-instance: vpntest : PacID: 757,    ttl:  00:00:05    left:  00:00:01
172.31.48.45-->222.1.1.2
vpn-instance: vpntest : PacID: 758,    ttl:  00:00:05    left:  00:00:01
172.31.48.45-->222.1.1.2
vpn-instance: vpntest : PacID: 759,    ttl:  00:00:05    left:  00:00:01
```

4.2.13 display firewall session aging-time

【命令】

display firewall session aging-time

【视图】

所有视图

【参数】

无

【描述】

display firewall session aging-time 命令用来显示所有协议的会话超时时间。

相关配置命令请参考 **firewall session aging-time**，**firewall session aging-time default**。

【举例】

显示所有协议的会话超时时间。

```
[SecBlade_FW] display firewall session aging-time
Firewall aging-time value information:
```

```
      tcp ---- aging-time value is    240 (seconds)
      udp ---- aging-time value is     40 (seconds)
     icmp ---- aging-time value is     20 (seconds)
   finrst ---- aging-time value is     10 (seconds)
      syn ---- aging-time value is      5 (seconds)
 fragment ---- aging-time value is      5 (seconds)
    h.323 ---- aging-time value is    600 (seconds)
      ftp ---- aging-time value is    600 (seconds)
      ras ---- aging-time value is    600 (seconds)
     http ---- aging-time value is    240 (seconds)
     smtp ---- aging-time value is     40 (seconds)
     rtsp ---- aging-time value is    240 (seconds)
   telnet ---- aging-time value is    240 (seconds)
  netbios ---- aging-time value is    240 (seconds)
```

4.2.14 display firewall session table

【命令】

display firewall session table [**verbose**] [**vpn-instance** *VPN-Instance name*] [**source** *ip-address*] [**destination** *ip-address*]

【视图】

所有视图

【参数】

verbose：显示详细信息。

source *ip-address*：会话的源 IP 地址。

destination *ip-address*：会话的目的 IP 地址。

vpn-instance-name：显示使用的 vpn-instance 名字。

【描述】

display firewall session table 命令用来显示防火墙的会话表，可指定 vpn-instance 用于显示属于指定 VPN 实例的会话表，若不指定 vpn-instance，则显示所有的会话表。

display firewall session table 命令和 **display aspf session** 命令显示的是两个会话表，这两个会话表的默认老化时间是不同的。对于同一条数据流，有可能在 ASPF 会话表中仍然存在，而在防火墙会话表中已经老化不存在，反之亦然。

防火墙会话老化后将会有一个 timeout 状态，从 timeout 状态到会话被删除会有一定的时间间隔，该时间间隔因实际组网应用而异。

【举例】

显示 VPN 实例 vpntest 的当前防火墙会话的相关信息。

```
[FireWall] display firewall session table vpn-instance vpntest
vpn-instance: vpntest Total session number: 8
vpn-instance: vpntest
HTTP:192.168.4.1:80<--192.168.4.8:3391
vpn-instance: vpntest
HTTP:192.168.4.1:80<--192.168.4.8:3392
vpn-instance: vpntest
HTTP:192.168.4.1:80<--192.168.4.8:3387
vpn-instance: vpntest
NBT datagram:192.168.4.255:138<--192.168.4.8:138
vpn-instance: vpntest
HTTP:192.168.4.1:80<--192.168.4.8:3396
vpn-instance: vpntest
NBT name:192.168.4.255:137<--192.168.4.8:137
vpn-instance: vpntest
HTTP:192.168.4.1:80<--192.168.4.8:3389
vpn-instance: vpntest
HTTP:192.168.4.1:80<--192.168.4.8:3398
```

显示 VPN 实例 vpntest 的当前防火墙会话的详细信息。

```
[FireWall] display firewall session table vpn-instance vpntest verbose
vpn-instance: vpntest Total session number: 1
tcp, FTP,
172.31.48.45:21<--222.1.1.2:1033
tag: 0,    ttl:  01:00:00    left:  00:59:59
```

4.2.15 display port-mapping

【命令】

display port-mapping [*application-name* | **port** *port-number*]

【视图】

所有视图

【参数】

application-name：指定用于端口映射的应用的名称。可选的应用有：FTP、HTTP、H323、SMTP、RTSP。

port-number：端口号，范围为 0～65535。

【描述】

display port-mapping 命令用来显示用户定义的端口映射情况。

相关配置可参考命令 **port-mapping**。

【举例】

显示端口映射的所有信息。

```
[SecBlade_FW] display port-mapping
  SERVICE    PORT       ACL        TYPE
 ------------------------------------------------
  ftp          21                   system defined
  smtp         25                   system defined
  http         80                   system defined
  rtsp        554                   system defined
  h323       1720                   system defined
```

4.2.16 firewall aspf

【命令】

firewall aspf *aspf-policy-number* { **inbound** | **outbound** } [**vpn-instance** *vpn-instance-name*]

undo firewall aspf *aspf-policy-number* { **inbound** | **outbound** } [**vpn-instance** *vpn-instance-name*]

【视图】

接口视图

【参数】

aspf-policy-number：在接口上使用的 ASPF 策略号。

inbound：对接口的入方向的报文应用 ASPF 策略。

outbound：对接口的出方向的报文应用 ASPF 策略。

vpn-instance-name：在接口上使用的 vpn-instance 名字。

【描述】

firewall aspf 命令用来在一个接口的指定方向上应用 ASPF 策略，**undo firewall aspf** 命令用来删除该接口的指定方向上应用的 ASPF 策略。

对 ASPF 策略，有两个概念：内部接口和外部接口。如果安全网关连接了内部网和 Internet，并且安全网关要通过部署 ASPF 来保护内部网的服务器，则安全网关上与内部网连接的接口就是内部接口，与 Internet 相连的接口就是外部接口。

vpn-instance 表明 aspf policy 作用的 VPN 实例，该策略只在所指定名字的 VPN 实例中起作用。

【举例】

接口 GigabitEthernet0/0.300 的出方向上配置针对 VPN 实例 vpntest 的 ASPF 防火墙功能。

```
[FireWall- GigabitEthernet0/0.300] firewall aspf 1 outbound vpn-instance vpntest
```

4.2.17 firewall session aging-time

【命令】

firewall session aging-time { **fin-rst** | **fragment** | **ftp** | **h323** | **http** | **icmp** | **netbios** | **ras** | **rtsp** | **smtp** | **syn** | **tcp** | **telnet** | **udp** } { **default** | *seconds* }

【视图】

系统视图

【参数】

default：设置协议的超时时间为缺省值。

seconds：协议的超时时间，单位为“秒”。

各种协议的缺省超时时间如下：

fin-rst：10 秒

fragment：5 秒

ftp：600 秒

h323：600 秒

http：240 秒

icmp：20 秒

netbios：240 秒

ras：600 秒

rtsp：240 秒

smtp：40 秒

syn：5 秒

tcp：240 秒

telnet：240 秒

udp：40 秒

【描述】

firewall session aging-time 命令用来设置各种协议的会话表的超时时间。

相关配置命令请参考 **firewall session aging-time default**，**display firewall session aging-time**。

【举例】

设置 http 协议的超时时间为 1200 秒。

```
[SecBlade_FW] firewall session aging-time http 1200
```

4.2.18 firewall session aging-time default

【命令】

firewall session aging-time default

【视图】

系统视图

【参数】

无

【描述】

firewall session aging-time default 命令用来将所有协议的超时时间恢复到缺省值。

相关配置命令请参考 **firewall session aging-time**，**display firewall session aging-time**。

【举例】

设置所有协议的超时时间为缺省值。

```
[SecBlade_FW] firewall session aging-time default
```

4.2.19 log enable

【命令】

log enable

undo log enable

【视图】

ASPF 策略视图

【描述】

log enable 命令用来使能 ASPF 的会话日志功能， **undo log enable** 命令用来关闭日志功能。

缺省情况下，关闭会话日志功能。

ASPF 提供了增强的会话日志功能。可以对所有的连接进行记录，记录包括：记录连接的时间、源地址、目的地址、使用的端口和传输的字节数。

相关配置可参考命令 **display aspf all**，**display aspf policy**，**display aspf session**，**display aspf interface**。

【举例】

使能 ASPF 会话日志功能。

```
[SecBlade_FW-aspf-policy-1] log enable
```

4.2.20 port-mapping

【命令】

port-mapping *application-name* **port** *port-number* [**acl** *acl-number*]

undo port-mapping [*application-name* **port** *port-number* [**acl** *acl-number*]]

【视图】

系统视图

【参数】

application-name：应用协议的名称。可选的应用协议有：FTP、HTTP、H323、SMTP、RTSP。

port-number：端口号范围为 0～65535。

acl-number：基本访问列表号，范围为 2000～2999。

【描述】

port-mapping 命令用来建立端口到应用层协议的映射，**undo port-mapping** 命令用来删除端口映射项。

有两类映射机制：通用端口映射和基于基本访问控制列表（ACL）的主机端口映射。通用端口映射是将用户自定义端口号和应用层协议建立映射关系；例如：将 8080 端口映射为 HTTP 协议，这样所有目标端口是 8080 的 TCP 报文被认为是 HTTP 报文。基于基本访问控制列表（ACL）的主机端口映射是对来自某些特定主机的报文建立自定义端口号和应用协议的映射，例如：将去往 1.1.0.0 网段的使用 8080 端口的 TCP 报文映射为 HTTP 报文。主机的范围由基本的 ACL 指定。

相关配置可参考命令 **display port-mapping**。

【举例】

设置 FTP 协议使用端口 3456。

```
[SecBlade_FW] port-mapping ftp port 3456
```

4.2.21 reset aspf session

【命令】

reset aspf session

【视图】

用户视图

【参数】

无

【描述】

reset aspf session 命令用来清除 ASPF 的会话信息。

【举例】

#清除 ASPF 的会话信息。

```
<SecBlade_FW> reset aspf session
```

4.2.22 reset aspf statistic http

【命令】

reset aspf statistic http [**java-blocking** | **activex-blocking**]

【视图】

用户视图

【参数】

java-blocking：清除 HTTP 的 Java 阻断的统计信息。

activex-blocking：清除 HTTP 的 ActiveX 阻断的统计信息。

【描述】

reset aspf statistic http 命令用来清除 HTTP 的 Java 阻断和 ActiveX 阻断的统计信息。

若不指定参数，则同时清除 Java 阻断和 ActiveX 阻断的统计信息。

【举例】

清除 Java 阻断的统计信息。

```
<SecBlade_FW> reset aspf statistic http java-blocking
```

4.2.23 reset firewall session table

【命令】

reset firewall session table [**vpn-instance** *VPN-Instance name*]

【视图】

用户视图

【参数】

vpn-instance-name：清除操作使用的 vpn-instance 名字。

【描述】

reset firewall session table 命令用来清除防火墙的会话表信息，可指定 vpn-instance 用于清除属于指定 VPN 实例的会话表，若不指定 vpn-instance，则清除所有的会话表。

【举例】

清除防火墙的会话表信息。

```
<FireWall> reset firewall session table vpn-instance vpntest
```

4.3 VPN 实例配置命令

4.3.1 firewall session limit

【命令】

firewall session limit *percentage*

undo firewall session limit

【视图】

vpn-instance 视图

【参数】

percentage：指定 VPN 实例的防火墙 Session 数量百分比。

【描述】

firewall session limit 用来指定 VPN 实例对应的防火墙 session 的限制百分比。
undo firewall session limit 用来取消此限制。默认情况下不进行限制。

【举例】

配置使 VPN 实例 fw1 的防火墙 Session 的数量限制为系统总数的 30%。

```
[Firewall-vpn-fw1] firewall session limit 30
```

4.3.2 firewall fragment limit

【命令】

firewall fragment limit *percentage*
undo firewall fragment limit

【视图】

vpn-instance 视图

【参数】

percentage：指定 VPN 实例的防火墙分片表数量百分比。

【描述】

firewall fragment limit 用来指定 VPN 实例对应的防火墙分片表的限制百分比。
undo firewall fragment limit 用来取消此限制。默认情况下不进行限制。

【举例】

配置使 VPN 实例 fw1 的 防火墙分片表的数量限制为系统总数的 30%。

```
[Firewall-vpn-fw1] firewall fragment limit 30
```

4.3.3 aspf session limit

【命令】

aspf session limit *percentage*
undo aspf session limit

【视图】

vpn-instance 视图

【参数】

percentage：指定 VPN 实例的 ASPF Session 数量百分比。

【描述】

aspf session limit 用来指定 VPN 实例对应的防火墙分片表的限制百分比。**undo aspf session limit** 用来取消此限制。默认情况下不进行限制。

【举例】

配置使 VPN 实例 fw1 的 ASPF Session 的数量限制为系统总数的 30%。

```
[Firewall-vpn-fw1] aspf session limit 30
```

4.4 黑名单配置命令

4.4.1 debugging firewall blacklist

【命令】

debugging firewall blacklist { **all** | **item** | **packet** }

undo debugging firewall blacklist { **all** | **item** | **packet** }

【视图】

用户视图

【参数】

all：显示全部调试信息。

item：显示黑名单表项变化调试信息。

packet：显示报文中黑名单表项调试信息。

【描述】

debugging firewall blacklist 命令用来打开 SecBlade 黑名单功能调试开关，**undo debugging firewall blacklist** 命令用来关闭 SecBlade 黑名单功能调试信息开关。

缺省情况关闭调试信息开关。

相关配置可参考命令 **display debugging**。

【举例】

打开黑名单表项的全部调试信息。

```
<SecBlade_FW> debugging firewall blacklist all
```

4.4.2 display firewall blacklist

【命令】

display firewall blacklist { **enable** | **item** [*sour-addr*] }

【视图】

所有视图

【参数】

enable：显示黑名单功能运行状况。

item *sour-addr*：显示黑名单表项内容。*sour-addr* 为表项的 IP 地址。

【描述】

display firewall blacklist 命令用来显示 SecBlade 黑名单功能的运行状况和黑名单表项信息。参数 **item** [*sour-addr*]显示黑名单表项信息。如果不指定 IP 地址，显示当前全部黑名单表项的概要信息。如果指定了要显示的 IP 地址，显示特定黑名单表项的详细信息。

【举例】

显示全部黑名单表项概要信息。

```
<SecBlade_FW> display firewall blacklist item
Firewall blacklist items :
Current manual insert items:2
Current automatic insert items:0
Need aging items:1
 192.168.1.1
 20.202.16.5
```

显示特定黑名单表项详细信息。

```
<SecBlade_FW> display firewall blacklist item 192.168.1.1
Firewall blacklist items : 192.168.1.1
 Insert reason : Manual
 Insert time : 2003/06/11 08:04:56
 Age action : Aging
 Age time : 100 minutes
```

显示黑名单表项的运行状况。

```
<SecBlade_FW> display firewall blacklist enable
Blacklist is Disabled
```

4.4.3 firewall blacklist

【命令】

firewall blacklist { **enable** | *sour-addr* [**timeout** *minutes*] }

undo firewall blacklist [**enable** | *sour-addr*]

【视图】

系统视图

【参数】

enable：使能黑名单功能。

sour-addr：指定添加到黑名单的 IP 地址。

timeout *minutes*：指定超时时间。*minutes* 取值范围为 1～1000，以分钟为单位。

【描述】

firewall blacklist 命令用来添加黑名单表项内容，也可以用来使能黑名单功能。**undo firewall blacklist** 命令用来删除黑名单表项内容，也可以用来禁止黑名单功能。

【举例】

在黑名单表项中插入一条 IP 地址为 192.168.10.10 的黑名单表项，老化时间为 100 分钟。

```
[SecBlade_FW] firewall blacklist 192.168.10.10 timeout 100
```

使能黑名单功能。

```
[SecBlade_FW] firewall blacklist enable
```

4.5 MAC 和 IP 地址绑定配置命令

4.5.1 debugging firewall mac-binding

【命令】

debugging firewall mac-binding { **all** | **item** | **packet** }

undo debugging firewall mac-binding { **all** | **item** | **packet** }

【视图】

用户视图

【参数】

all：显示全部调试信息。

item：显示地址绑定表项变化调试信息。

packet：显示报文中地址绑定表项调试信息。

【描述】

debugging firewall mac-binding 命令用来打开 SecBlade 地址绑定功能调试开关，**undo debugging firewall mac-binding** 命令用来关闭 SecBlade 地址绑定功能调试信息开关。

缺省情况关闭调试信息开关。

相关配置可参考命令 **display debugging**。

【举例】

打开地址绑定表项全部调试信息。

```
<SecBlade_FW> debugging firewall mac-binding all
```

4.5.2 display firewall mac-binding

【命令】

display firewall mac-binding { **enable** | **item** [*ip-addr*] [**statistic**] }

【视图】

所有视图

【参数】

enable：显示地址绑定功能运行状况。

item：显示地址绑定表项内容。

ip-addr：显示指定 IP 地址的表项内容。

statistic：显示地址绑定功能的统计信息。

【描述】

display firewall mac-binding 命令用来显示 SecBlade 地址绑定功能的运行状况和地址绑定表项信息。参数 **item** [*ip-addr*]显示地址绑定表项信息，如果不指定 IP 地址，显示当前全部地址绑定表项的概要信息，如果指定了要显示的 IP 地址，显示特定地址绑定表项的详细信息。参数 **enable** 显示地址绑定功能的运行状况。

【举例】

显示全部地址绑定表项概要信息。

```
<SecBlade_FW> display firewall mac-binding item
Firewall mac-binding items :
Current items:2
 192.168.1.1      00e0-0f0c-1149
 20.202.16.5      0adc-0e0f-23ed
```

显示特定地址绑定表项详细信息。

```
<SecBlade_FW> display firewall mac-binding item 192.168.1.1
Firewall mac-binding items :
 192.168.1.1      00e0-0f0c-1149
```

显示地址绑定表项的运行状况。

```
<SecBlade_FW> display firewall mac-binding enable
Mac-binding is Disabled
```

显示地址绑定功能的统计信息。

```
<SecBlade_FW> display firewall mac-binding item statistic
Firewall Mac-binding item(s) :
Current items : 1
      IP Address       Mac                 True Pkts          False Pkts
     192.168.1.2  000f-1f73-fec5                   0                  57
```

4.5.3 firewall mac-binding

【命令】

firewall mac-binding *ip-addr mac-addr*

undo firewall mac-binding [*ip-addr*]

【视图】

系统视图

【参数】

ip-addr：指定地址绑定对的 IP 地址。

mac-addr：指定地址绑定对的 MAC 地址。

【描述】

firewall mac-binding 命令用来添加 MAC 地址绑定条目。**undo firewall mac-binding** 命令用来删除 MAC 地址绑定条目，若 **undo firewall mac-binding** 命令使用 *ip-addr* 参数，表示删除特定的绑定条目，否则将删除所有绑定条目。

【举例】

在地址绑定表项中插入一条 IP 地址为 192.168.10.10，MAC 地址为 00e0-0000-0001 的地址绑定条目。

```
[SecBlade_FW] firewall mac-binding 192.168.10.10 00e0-0000-0001
```

使能地址绑定功能。

```
[SecBlade_FW] firewall mac-binding enable
```

4.5.4 firewall mac-binding enable

【命令】

firewall mac-binding enable

undo firewall mac-binding enable

【视图】

系统视图

【参数】

enable：使能地址绑定功能。

【描述】

firewall mac-binding enable 命令用来使能 MAC 地址绑定功能，**undo firewall mac-binding enable** 命令用来关闭 MAC 地址绑定功能。

【举例】

使能 MAC 地址绑定功能。

```
[SecBlade_FW] firewall mac-binding enable
```

4.5.5 reset firewall mac-binding

【命令】

reset firewall mac-binding item [*ip-addr*] **statistic**

【视图】

用户视图

【参数】

item：MAC 和 IP 地址绑定表项。

ip-addr：清除指定 IP 地址的绑定信息。

statistic：MAC 和 IP 地址绑定的统计信息。

【描述】

reset firewall mac-binding 命令用来清除 MAC 和 IP 地址绑定的统计信息。

【举例】

清除所有 MAC 和 IP 地址绑定的统计信息。

```
<SecBlade_FW> reset firewall mac-binding item statistic
```

4.6 区域配置命令

4.6.1 add interface

【命令】

add interface *interface-type interface-number*

undo add interface *interface-type interface-number*

【视图】

区域视图

【参数】

interface-type interface-number：指定接口类型及接口号。

【描述】

add interface 命令用来将接口加入到安全区域，**undo add interface** 命令用来将接口从安全区域中删除。

将接口加入到一个安全区域中前，这个接口不能已经属于其它的区域，否则需要先将此接口从其它区域中删除，即一个接口只能属于一个安全区域。

缺省情况下，所有安全区域中未添加任何接口。

若要实现 SecBlade 和其它设备的互通，必须将相应的接口添加到某一安全区域中。

【举例】

将 Trust 区域接口 GigabitEthernet0/0.1 加入到 DMZ 区域。

```
[SecBlade_FW] firewall zone trust
[SecBlade_FW-zone-trust] undo add interface GigabitEthernet0/0.1
[SecBlade_FW-zone-trust] quit
[SecBlade_FW] firewall zone DMZ
[SecBlade_FW-zone-DMZ] add interface GigabitEthernet0/0.1
```

4.6.2 display interzone

【命令】

display interzone [*zone1 zone2*]

【视图】

任意视图

【参数】

zone1 zone2：指定两个安全区域名称，即显示安全区域 *zone1* 和 *zone2* 的区域间配置。

【描述】

display interzone 命令用来显示安全区域间的配置信息。

若不指定参数，则显示所有区域间的配置信息。

【举例】

显示安全区域 trust 和 untrust 的区域间配置信息。

```
<SecBlade_FW> display interzone trust untrust
```

4.6.3 display zone

【命令】

display zone [*zone-name*] [**interface** | **priority**]

【视图】

所有视图

【参数】

zone-name：安全区域的名称。系统预先定义了 4 个安全区域：Trust、Untrust、DMZ 和 Local。

interface：显示安全区域所包含的接口。

priority：显示安全区域的优先级。

【描述】

display zone 命令用来显示安全区域所包含的接口以及安全区域的优先级。

【举例】

显示所有安全区域的优先级。

```
<SecBlade_FW> display zone priority
local
 priority is 100
#
trust
 priority is 85
#
untrust
```

```
 priority is 5
#
DMZ
 priority is 50
#
```

4.6.4 set priority

【命令】

set priority *number*

【视图】

区域视图

【参数】

number：区域的优先级数值，范围为 1～100。

【描述】

set priority 命令用来设置安全区域的优先级，优先级数值越高，表示此区域的安全性越高。

系统预定义了 4 个安全区域：Local、Trust、Untrust 和 DMZ。这些区域的优先级是不能被更改的。**set priorit** 命令只能用来设置和修改新建的区域的优先级。

不同安全区域之间没有访问限制，且安全区域不支持策略配置，若需要访问控制，请在安全区域中的相应接口进行配置。

缺省情况下，Local 区域的优先级为 100，Trust 区域的优先级为 85，Untrust 区域的优先级为 5，DMZ 区域的优先级为 50。

【举例】

设置区域 newzone 的优先级为 70。

```
[SecBlade_FW] firewall zone newzone
[SecBlade_FW-zone-newzone] set priority 70
```

4.6.5 firewall interzone

【命令】

firewall interzone *zone1 zone2*

【视图】

系统视图

【参数】

zone1：安全区域名。

zone2：安全区域名。

【描述】

firewall interzone 命令用来进入区域间视图。

【举例】

进入 Trust 区域和 Untrust 区域的区域间视图。

```
[SecBlade_FW] firewall interzone trust untrust
[SecBlade_FW-interzone-trust-untrust]
```

4.6.6 firewall zone

【命令】

firewall zone *zonename*

【视图】

系统视图

【参数】

zonename：安全区域名。

【描述】

firewall zone 命令用来进入安全区域视图。

【举例】

进入 DMZ 区域视图。

```
[SecBlade_FW] firewall zone DMZ
[SecBlade_FW-zone-DMZ]
```

4.6.7 firewall zone name

【命令】

firewall zone name *zonename*

undo firewall zone name *zonename*

【视图】

系统视图

【参数】

zonename：安全区域名。

【描述】

firewall zone name 命令用来创建新的安全区域，**undo firewall zone name** 命令用来删除新建的安全区域。

缺省情况下，系统预先定义了 4 个安全区域：Trust、Untrust、DMZ 和 Local，这些安全区域是不能被删除的。

【举例】

创建一个新的名为 newzone 的安全区域。

```
[SecBlade_FW] firewall zone name newzone
[SecBlade_FW-zone-newzone]
```

第5章 透明防火墙配置命令

5.1 透明防火墙配置命令

5.1.1 acl number

【命令】

acl number *acl-number*

undo acl { **number** *acl-number* | **all** }

【视图】

系统视图

【参数】

number *acl-number*：基于 MAC 地址的访问控制列表的序号，范围为 4000～4999。

all：删除所有的 ACL，包括那些基于接口的访问控制列表，基本访问控制列表和高级访问控制列表。

【描述】

acl number 命令用来创建访问控制列表，**undo acl** 命令用来删除一个已经存在的访问控制列表。

缺省情况下，系统未定义任何基于 MAC 地址的访问控制列表。

关于访问控制列表的其它命令请参考 2.1.1 和 2.1.5 。

【举例】

创建一个编号为 4009 的基于 MAC 地址的访问控制列表。

```
[SecBlade_FW] acl number 4009
```

5.1.2 bridge vlanid-transparent-transmit enable

【命令】

bridge vlanid-transparent-transmit enable

undo bridge vlanid-transparent-transmit enable

【视图】

接口视图

【参数】

无

【描述】

bridge vlanid-transparent-transmit enable 命令用来使能 VLAN ID 透传功能。**undo bridge vlanid-transparent-transmit enable** 命令用来关闭 VLAN ID 透传功能。

VLAN ID 透传是指接口直接转发报文，不对该报文中的 VLAN ID 做任何处理。即使出接口上有 VLAN ID 的情况下，也不会改变报文原有的 VLAN ID。

当以太网子接口配置 VLAN ID 后，该子接口只会接收这个 VLAN 的数据，这就决定了该桥组负责传输哪些 VLAN 的数据。

在使能 VLAN ID 透传功能以后，系统不对报文的 VLAN ID 做任何处理，两端相连的交换机可以看成是直接相连的。为了正常通信，用户需要给两端交换机的 trunk 口配置相同的 VLAN ID。

⚠ 注意：

如果某个接口启用 VLAN 透传，那么这个接口对应的物理接口和相应的子接口必须配置基于接口的访问控制列表以过滤从本接口收到的报文，防止报文又被转发回去。

缺省情况下，关闭 VLAN ID 透传功能。

【举例】

在 GigabitEthernet 0/0 接口上使能 VLAN ID 透传功能。

```
[SecBlade_FW] interface GigabitEthernet 0/0
[SecBlade_FW-GigabitEthernet0/0] bridge vlanid-transparent-transmit enable
```

5.1.3 debugging firewall eff

【命令】

debugging firewall eff [**interface** *interface-type interface-number*]

undo debugging firewall eff [**interface** *interface-type interface-number*]

【视图】

用户视图

【参数】

interface *interface-type interface-number*：特定接口的调试信息。

【描述】

debugging firewall eff 命令用来打开以太帧过滤的调试开关，**undo debugging firewall eff** 命令用来关闭以太帧过滤的调试开关。

缺省情况下，关闭以太帧过滤的调试开关。

【举例】

打开以太帧过滤的调试开关。

```
<SecBlade_FW> debugging firewall eff
 Ethernet-frame-filter's debugging is on
<SecBlade_FW>
*0.1350738 SecBlade_FW EFF/8/DEBUGGING:
 OutBound List 4001, deny the frame with the following head :
 dest-mac is 000f-1f7e-fec5,sour-mac is 00e0-fc36-a7a9, type is 0800
*0.1350739 SecBlade_FW BRIDGE/8/DEBUGGING:
Discard a frame for the filter on outport ; received from interface GigabitEther
net0/1;and try to send to interface GigabitEthernet0/0, with following frame
head :
00 0f 1f 7e fe c5 00 e0 fc 36 a7 a9 08 00
*0.1352740 SecBlade_FW EFF/8/DEBUGGING:
 OutBound List 4001, deny the frame with the following head :
 dest-mac is 000f-1f7e-fec5,sour-mac is 00e0-fc36-a7a9, type is 0800
*0.1352740 SecBlade_FW BRIDGE/8/DEBUGGING:
Discard a frame for the filter on outport ; received from interface GigabitEther
net0/1;and try to send to interface GigabitEthernet0/0, with following frame
head :
00 0f 1f 7e fe c5 00 e0 fc 36 a7 a9 08 00
*0.1352925 SecBlade_FW EFF/8/DEBUGGING:
 InBound List 4001, deny the frame with the following head :
 dest-mac is ffff-ffff-ffff,sour-mac is 000f-1f7e-fec5, type is 0806
*0.1352925 SecBlade_FW BRIDGE/8/DEBUGGING:
Discard a frame for the filter on inport ; received from interface GigabitEthern
et0/0, with following frame head :
ff ff ff ff ff ff 00 0f 1f 7e fe c5 08 06
*0.1354741 SecBlade_FW EFF/8/DEBUGGING:
 OutBound List 4001, deny the frame with the following head :
 dest-mac is 000f-1f7e-fec5,sour-mac is 00e0-fc36-a7a9, type is 0800
*0.1354741 SecBlade_FW BRIDGE/8/DEBUGGING:
Discard a frame for the filter on outport ; received from interface GigabitEther
net0/1;and try to send to interface GigabitEthernet0/0, with following frame
head :
00 0f 1f 7e fe c5 00 e0 fc 36 a7 a9 08 00
```

```
*0.1356742 SecBlade_FW EFF/8/DEBUGGING:
 OutBound List 4001, deny the frame with the following head :
 dest-mac is 000f-1f7e-fec5,sour-mac is 00e0-fc36-a7a9, type is 0800
*0.1356742 SecBlade_FW BRIDGE/8/DEBUGGING:
Discard a frame for the filter on outport ; received from interface GigabitEther
net0/1;and try to send to interface GigabitEthernet0/0, with following frame
head :
00 0f 1f 7e fe c5 00 e0 fc 36 a7 a9 08 00
```

5.1.4 debugging firewall transparent-mode eth-forwarding

【命令】

debugging firewall transparent-mode eth-forwarding [**interface** *interface-type interface-number*]

undo debugging firewall transparent-mode eth-forwarding [**interface** *interface-type interface-number*]

【视图】

用户视图

【参数】

interface *interface-type interface-number*：特定接口的调试信息。

【描述】

debugging firewall transparent-mode eth-forwarding 命令用来打开透明防火墙的以太帧转发调试开关，**undo debugging firewall transparent-mode eth-forwarding** 命令用来关闭透明防火墙的以太帧转发调试开关。

当不指定接口时，则打开或关闭所有接口的以太帧转发调试开关。

缺省情况下，关闭透明防火墙的以太帧转发调试开关。

【举例】

打开透明防火墙的以太帧转发调试开关。

```
<SecBlade_FW> debugging firewall transparent-mode eth-forwarding
The Transparent-mode eth-forwarding Debugging  is on
*0.695514 SecBlade_FW BRIDGE/8/DEBUGGING:
Forward a frame; received from interface GigabitEthernet0/0;and try to send
to interface GigabitEthernet0/1, with following frame head :
00 e0 fc 36 a7 a9 00 0f 1f 7e fe c5 08 00
*0.695514 SecBlade_FW BRIDGE/8/DEBUGGING:
Forward a frame; received from interface GigabitEthernet0/1;and try to send
to interface GigabitEthernet0/0, with following frame head :
```

```
00 0f 1f 7e fe c5 00 e0 fc 36 a7 a9 08 00
*0.696515 SecBlade_FW BRIDGE/8/DEBUGGING:
Forward a frame; received from interface GigabitEthernet0/0;and try to send
to interface GigabitEthernet0/1, with following frame head :
00 e0 fc 36 a7 a9 00 0f 1f 7e fe c5 08 00
*0.696515 SecBlade_FW BRIDGE/8/DEBUGGING:
Forward a frame; received from interface GigabitEthernet0/1;and try to send
to interface GigabitEthernet0/0, with following frame head :
00 0f 1f 7e fe c5 00 e0 fc 36 a7 a9 08 00
*0.696582 SecBlade_FW BRIDGE/8/DEBUGGING:
Forward a frame; received from interface GigabitEthernet0/1;and try to send
to interface GigabitEthernet0/0, with following frame head :
00 0f 1f 7e fe c5 00 e0 fc 36 a7 a9 08 00
*0.696582 SecBlade_FW BRIDGE/8/DEBUGGING:
Forward a frame; received from interface GigabitEthernet0/0;and try to send
to interface GigabitEthernet0/1, with following frame head :
00 e0 fc 36 a7 a9 00 0f 1f 7e fe c5 08 00
*0.696584 SecBlade_FW BRIDGE/8/DEBUGGING:
Forward a frame; received from interface GigabitEthernet0/1;and try to send
to interface GigabitEthernet0/0, with following frame head :
00 0f 1f 7e fe c5 00 e0 fc 36 a7 a9 08 00
*0.696584 SecBlade_FW BRIDGE/8/DEBUGGING:
Forward a frame; received from interface GigabitEthernet0/0;and try to send
to interface GigabitEthernet0/1, with following frame head :
00 e0 fc 36 a7 a9 00 0f 1f 7e fe c5 08 00
```

5.1.5 debugging firewall transparent-mode ip-forwarding

【命令】

debugging firewall transparent-mode ip-forwarding

undo debugging firewall transparent-mode ip-forwarding

【视图】

用户视图

【参数】

无

【描述】

debugging firewall transparent-mode ip-forwarding 命令用来打开透明防火墙的 IP 报文转发调试开关，**undo debugging firewall transparent-mode ip-forwarding** 命令用来关闭透明防火墙的 IP 报文转发调试开关。

缺省情况下，关闭透明防火墙的 IP 报文转发调试开关。

【举例】

打开透明防火墙的 IP 报文转发调试开关。

```
<SecBlade_FW> debugging firewall transparent-mode ip-forwarding
 The Transparent-mode Ip-forwarding Debugging  is on
<SecBlade_FW>
*0.11355193 SecBlade_FW FWTP/8/rcv_ip:Receive an IP packet
    interface: GigabitEthernet0/0
    source_ip_addr : 192.168.3.6
    source_port : 33073
    destination_ip_addr : 192.168.3.8
    destination_port : 52128
    protocol : 1

*0.11355193 SecBlade_FW FWTP/8/sndto_secur:Send an IP packet to security
module
    source_ip_addr : 192.168.3.6
    source_port : 17664
    destination_ip_addr : 192.168.3.8
    destination_port : 60
    protocol : 1
    return value:0

*0.11355193 SecBlade_FW FWTP/8/snd_ip:Send an IP packet
    interface: GigabitEthernet0/1
    source_ip_addr : 192.168.3.6
    source_port : 0
    destination_ip_addr : 192.168.3.8
    destination_port : 1
    protocol : 1

*0.11355193 SecBlade_FW FWTP/8/rcv_ip:Receive an IP packet
    interface: GigabitEthernet0/1
    source_ip_addr : 192.168.3.8
    source_port : 33073
    destination_ip_addr : 192.168.3.6
    destination_port : 52128
    protocol : 1
*0.11355193 SecBlade_FW FWTP/8/sndto_secur:Send an IP packet to security
module
    source_ip_addr : 192.168.3.8
```

```
    source_port : 17664
    destination_ip_addr : 192.168.3.6
    destination_port : 60
    protocol : 1
    return value:0

*0.11355193 SecBlade_FW FWTP/8/snd_ip:Send an IP packet
    interface: GigabitEthernet0/0
    source_ip_addr : 192.168.3.8
    source_port : 0
    destination_ip_addr : 192.168.3.6
    destination_port : 1
    protocol : 1
```

5.1.6 display firewall ethernet-frame-filter

【命令】

display firewall ethernet-frame-filter { **all** | **interface** *interface-type interface-number* }

【视图】

所有视图

【参数】

all：所有接口的以太帧过滤的统计信息。

interface *interface-type interface-number*：特定接口的以太帧过滤的统计信息。

【描述】

display firewall ethernet-frame-filter 命令用来显示以太帧过滤的统计信息。

【举例】

显示所有接口的以太帧过滤的统计信息。

```
<SecBlade_FW> display firewall ethernet-frame-filter all
  Interface: GigabitEthernet0/1
  In-bound Policy: acl 4000
  From 2099-08-02 5:55:05  to 2099-08-02 5:55:41
     11 packets, 668 bytes, 100% permitted,
     0 packets, 0 bytes, 0% denied,
     0 packets, 0 bytes, 0% permitted default,
     0 packets, 0 bytes, 0% denied default,
  Totally 11 packets, 668 bytes, 100% permitted,
```

```
  Totally 0 packets, 0 bytes, 0% denied.
  Out-bound Policy: acl 4000
  From 2099-08-02 5:55:07  to 2099-08-02 5:55:41
     0 packets, 0 bytes, 0% permitted,
     0 packets, 0 bytes, 0% denied,
     0 packets, 0 bytes, 0% permitted default,
     0 packets, 0 bytes, 100% denied default,
  Totally 0 packets, 0 bytes, 0% permitted,
  Totally 0 packets, 0 bytes, 100% denied.
```

5.1.7 display firewall mode

【命令】

display firewall mode

【视图】

所有视图

【参数】

无

【描述】

display firewall mode 命令用来显示当前 SecBlade 的工作模式。

【举例】

显示当前 SecBlade 的工作模式。

```
<SecBlade_FW> display firewall mode
 Firewall mode: transparent
```

5.1.8 display firewall transparent-mode address-table

【命令】

display firewall transparent-mode address-table [**interface** *interface-type interface-number* | **mac** *mac-address*]

【视图】

所有视图

【参数】

interface *interface-type interface-number*：与指定接口相关联的 MAC 地址信息。

mac *mac-address*：特定 MAC 地址条目的信息。

【描述】

display firewall transparent-mode address-table 命令用来显示透明防火墙的 MAC 地址表信息。

【举例】

显示透明防火墙的 MAC 地址表信息。

```
<SecBlade_FW> display firewall transparent-mode address-table
 The total of the address-items is 2
 Mac-address    Flag   Aging-time   Receive       Send Interface-name
 00e0-fc36-a7a9  PD    00:01:41         23         13  GigabitEthernet0/0.1
 000f-1f7e-fec5  PD    00:03:28        121         12  GigabitEthernet0/0.2
Flag meaning:  P--PERMIT   N--DENY  D--DYNAMIC  S--STATIC
```

5.1.9 display firewall transparent-mode config

【命令】

display firewall transparent-mode config

【视图】

所有视图

【参数】

无

【描述】

display firewall transparent-mode config 命令用来显示透明防火墙的配置信息。

【举例】

显示透明防火墙的配置信息。

```
<SecBlade_FW> display firewall transparent-mode config
 Firewall transparent-info:
  ARP learning     : enable
  System IP address: 169.0.0.1
  System IP mask   : 255.0.0.0
  Unknown-mac:
    Unicast IP packet  : arp
    broadcast IP packet: drop
    Multicast IP packet: drop
```

5.1.10 display firewall transparent-mode traffic

【命令】

display firewall transparent-mode traffic [**interface** *interface-type interface-number*]

【视图】

所有视图

【参数】

interface *interface-type interface-number*：特定接口的流量信息。

【描述】

display firewall transparent-mode traffic 命令用来显示透明防火墙的流量信息。

【举例】

显示透明防火墙的流量信息。

```
<SecBlade_FW> display firewall transparent-mode traffic
 system error  is 0,inport error  is 0,
 outport error is 0 ,other error is 0

the total statistic :
 Input:
         860 total, 0 bpdu, 750 single,
         0 multi, 110 broadcast;
         860 ip,0 ipx, 0 other protocol;
         860 eth2, 0 snap,
         0 dlsw, 0 other,
         0 vlan;
 Output:
         747 total, 0 bpdu, 747 single,
         0 multi, 0 broadcast;
         747 ip, 0 ipx, 0 other protocol;
         747 eth2, 0 snap,
         0 dlsw, 0 other,
         0 vlan;
 Send way:
         0 broadcast, 0 fast, 747 other
 Discard:
         0 by inport state,
         0 for local frame ,
         0 by mac table,
```

```
        0 by inport filter,
        0 by outport filter,
        113 by ip filter ,
        0 other

the statistic of interface GigabitEthernet0/1
 Input:
        376 total, 0 bpdu, 375 single,
        0 multi, 1 broadcast;
        376 ip,0 ipx, 0 other protocol;
        376 eth2, 0 snap,
        0 dlsw, 0 other,
        0 vlan;
 Output:
        374 total, 0 bpdu, 374 single,
        0 multi, 0 broadcast;
        374 ip, 0 ipx, 0 other protocol;
        374 eth2, 0 snap,
        0 dlsw, 0 other,
        0 vlan;
 Send way:
        0 broadcast, 0 fast, 374 other
 Discard:
        0 by inport state,
        0 for local frame ,
        0 by mac table,
        0 by inport filter,
        0 by outport filter,
        3 by ip filter ,
        0 other

the statistic of interface GigabitEthernet0/0
 Input:
        484 total, 0 bpdu, 375 single,
        0 multi, 109 broadcast;
        484 ip,0 ipx, 0 other protocol;
        484 eth2, 0 snap,
        0 dlsw, 0 other,
        0 vlan;
 Output:
        373 total, 0 bpdu, 373 single,
        0 multi, 0 broadcast;
```

```
        373 ip, 0 ipx, 0 other protocol;
        373 eth2, 0 snap,
        0 dlsw, 0 other,
        0 vlan;
Send way:
        0 broadcast, 0 fast, 373 other
Discard:
        0 by inport state,
        0 for local frame ,
        0 by mac table,
        0 by inport filter,
        0 by outport filter,
        110 by ip filter ,
        0 other
```

5.1.11 firewall arp-learning enable

【命令】

firewall arp-learning enable

undo firewall arp-learning enable

【视图】

系统视图

【参数】

无

【描述】

firewall arp-learning enable 命令用来启用工作在透明模式下的 SecBlade 的动态 ARP 表项学习功能，**undo firewall arp-learning enable** 命令用来关闭透明防火墙的 ARP 学习功能。

缺省情况下，当 SecBlade 工作在透明模式下时，SecBlade 自动启用动态 ARP 表项学习功能。

【举例】

启用 SecBlade 的 ARP 学习功能。

```
[SecBlade_FW] firewall arp-learning enable
```

5.1.12 firewall ethernet-frame-filter

【命令】

firewall ethernet-frame-filter *acl-number* { **inbound** | **outbound** }

undo firewall ethernet-frame-filter { **inbound** | **outbound** }

【视图】

以太网接口视图

【参数】

acl-number：基于 MAC 地址的 ACL 编号，范围为 4000～4999。

inbound：过滤从接口接收的帧。

outbound：过滤从接口发送的帧。

【描述】

firewall ethernet-frame-filter 命令用来将基于 MAC 地址的 ACL 应用到接口上，**undo firewall ethernet-frame-filter** 命令用来从接口上删除基于 MAC 地址的 ACL。

要将基于 MAC 地址的访问控制列表应用到接口上，防火墙必须工作在透明模式下，否则系统会提示错误信息。

当防火墙处于混杂和透明模式的时候，报文过滤的处理过程是先检查二层的过滤规则，然后检查三层的过滤规则。

缺省情况下，未在接口上应用任何基于 MAC 地址的 ACL。

【举例】

在以太网接口 GigabitEthernet0/0.1 的入方向上应用编号为 4009 的基于 MAC 地址的 ACL。

```
[SecBlade_FW-GigabitEthernet0/0.1] firewall ethernet-frame-filter 4009 inbound
```

5.1.13 firewall mode

【命令】

firewall mode { **route** | **transparent** }

undo firewall mode

【视图】

系统视图

【参数】

route：配置 SecBlade 工作在路由模式下。

transparent：配置 SecBlade 工作在透明模式下。

【描述】

firewall mode 命令用来配置 SecBlade 的工作模式，**undo firewall mode** 命令用来将 SecBlade 恢复到工作在缺省模式下。

缺省情况下，SecBlade 工作在路由模式。

当 SecBlade 工作在路由模式下时，其所有接口都工作在第三层，即可以为接口配置 IP 地址等第三层属性。当 SecBlade 工作在透明模式下时，其所有接口都将工作在第二层，即转换为交换端口，且不能为接口配置 IP 地址等第三层属性。

【举例】

配置 SecBlade 工作在透明模式。

```
[SecBlade_FW] firewall mode transparent
 Set system ip address successfully.
All the Interfaces's ips have been deleted.
 The mode is set successfully.
```

从以上显示的系统提示信息可以看出，SecBlade 已经工作在透明模式下，且所有接口上的 IP 地址已经被删除。

5.1.14 firewall system-ip

【命令】

firewall system-ip *ip-address* [*mask*]

undo firewall system-ip

【视图】

系统视图

【参数】

ip-address：SecBlade 的系统 IP 地址。

mask：系统 IP 地址的子网掩码。若不指定掩码，系统则使用默认的分类子网掩码。

【描述】

firewall system-ip 命令用来配置 SecBlade 的系统 IP 地址，**undo firewall system-ip** 命令用来将系统 IP 地址设置为 SecBlade 缺省的系统 IP 地址。

缺省情况下，SecBlade 的系统 IP 地址为 169.0.0.1/8。

当 SecBlade 工作在透明模式下时，若系统中不存在 Loopback0 接口，则系统会为 SecBlade 创建一个地址为 169.0.0.1/8 的 Loopback0 接口，此地址将为缺省的系统 IP 地址；若系统中已存在 Loopback0 接口，Loopback0 接口的地址将被设为系统 IP 地址。当修改 Loopback0 接口的地址或删除 Loopback0 接口时，系统 IP 地址也会被修改或删除，可以使用此命令修改系统 IP 地址。

当 SecBlade 工作在路由模式下时，不能配置系统 IP 地址。

【举例】

配置 SecBlade 的系统 IP 地址

```
[SecBlade_FW] firewall mode transparent
 Set system ip address successfully.
All the Interfaces's ip addresses have been deleted.
 The mode is set successfully.
[SecBlade_FW] firewall system-ip 10.1.1.5 255.255.255.0
 Set system ip address successfully.
```

5.1.15 firewall transparent-mode aging-time

【命令】

firewall transparent-mode aging-time *seconds*

undo firewall transparent-mode aging-time

【视图】

系统视图

【参数】

seconds：MAC 地址转发表的老化时间，范围为 10～1000000，单位为“秒”。

【描述】

firewall transparent-mode aging-time 命令用来配置 MAC 地址转发表的老化时间，**undo firewall transparent-mode aging-time** 命令用来恢复 MAC 地址转发表的老化时间为缺省值。

缺省情况下，MAC 地址转发表的老化时间为 300 秒。

【举例】

配置 MAC 地址转发表的老化时间为 1800 秒。

```
[SecBlade_FW] firewall transparent-mode aging-time 1800
```

5.1.16 firewall transparent-mode transmit

【命令】

firewall transparent-mode transmit { **bpdu** | **dlsw** | **ipx** }

undo firewall transparent-mode transmit { **bpdu** | **dlsw** | **ipx** }

【视图】

系统视图

【参数】

bpdu：Bridge Protocol Data Unit，桥协议数据单元。

dlsw：Data Link Switching，数据链路交换。

ipx：Internetwork Packet Exchange，网际报文交换。

【描述】

firewall transparent-mode transmit 命令用来配置允许通过的报文类型，**undo firewall transparent-mode transmit** 命令用来配置拒绝通过的报文类型。

缺省情况下，SecBlade 不允许这些类型的报文通过。

【举例】

配置允许 BPDU 通过透明防火墙。

```
[SecBlade_FW] firewall transparent-mode transmit bpdu
```

5.1.17 firewall unknown-mac

【命令】

firewall unknown-mac { **drop** | **flood** }

undo firewall unknown-mac

【视图】

系统视图

【参数】

drop：直接丢弃该未知目的 MAC 地址的 IP 单播、组播和广播报文。

flood：将此未知目的 MAC 地址的 IP 单播、组播和广播报文在除接收接口外的其它所有接口（接口必须属于某一安全区域）上泛洪。待收到响应报文后，则保存其 MAC 地址信息，后续报文将使用该 MAC 地址进行转发。

【描述】

firewall unknown-mac 命令用来配置 SecBlade 对未知目的 MAC 地址的单播、组播和广播报文的处理方式，**undo firewall unknown-mac** 命令用来恢复缺省处理方式。

缺省情况下，SecBlade 对单播 IP 报文按照 **arp** 方式进行处理，而对广播和组播报文按照 **drop** 的方式进行处理。

相关配置请参考命令 **firewall unknown-mac unicast**，**firewall unknown-mac multicast**，**firewall unknown-mac broadcast**。

【举例】

配置 SecBlade 泛洪未知目的 MAC 地址的 IP 报文。

```
[SecBlade_FW] firewall unknown-mac flood
```

5.1.18 firewall unknown-mac broadcast

【命令】

firewall unknown-mac broadcast { **drop** | **flood** }

undo firewall unknown-mac broadcast

【视图】

系统视图

【参数】

drop：直接丢弃广播 IP 报文。

flood：将广播 IP 报文在除接收接口外的其它所有接口（接口必须属于某一安全区域）上泛洪。待收到响应报文后，保存其 MAC 地址信息。

【描述】

firewall unknown-mac broadcast 命令用来配置 SecBlade 对广播 IP 报文的处理方式，**undo firewall unknown-mac broadcast** 命令用来恢复对广播 IP 报文的缺省处理方式。

缺省情况下，SecBlade 丢弃广播 IP 报文，即按照 **drop** 的方式进行处理。

【举例】

配置 SecBlade 泛洪广播 IP 报文。

```
[SecBlade_FW] firewall unknown-mac broadcast flood
```

5.1.19 firewall unknown-mac multicast

【命令】

firewall unknown-mac multicast { **drop** | **flood** }

undo firewall unknown-mac multicast

【视图】

系统视图

【参数】

drop：直接丢弃组播 IP 报文。

flood：将组播 IP 报文在除接收接口外的其它所有接口（接口必须属于某一安全区域）上泛洪。待收到响应报文后，保存其 MAC 地址信息。

【描述】

firewall unknown-mac multicast 命令用来配置 SecBlade 对组播 IP 报文的处理方式，**undo firewall unknown-mac multicast** 命令用来恢复对组播 IP 报文的缺省处理方式。

缺省情况下，SecBlade 丢弃组播 IP 报文，即按照 **drop** 的方式进行处理。

【举例】

配置 SecBlade 泛洪组播 IP 报文。

```
[SecBlade_FW] firewall unknown-mac multicast flood
```

5.1.20 firewall unknown-mac unicast

【命令】

firewall unknown-mac unicast { **drop** | **arp** | **flood** }

undo firewall unknown-mac unicast

【视图】

系统视图

【参数】

drop：直接丢弃该未知目的 MAC 地址的 IP 报文。

arp：在除接收到该报文的接口外的其它所有接口（接口必须属于某一安全区域）上广播 ARP 请求报文，并且丢弃原来的未知 MAC 地址的 IP 报文。收到 ARP 响应报文后，保存 MAC 地址和接口的对应关系。

flood：将此未知目的 MAC 地址的 IP 报文在除接收接口外的其它所有接口（接口必须属于某一安全区域）上泛洪。待收到响应报文后，则保存其 MAC 地址信息，后续报文将使用该 MAC 地址进行转发。

【描述】

firewall unknown-mac unicast 命令用来配置 SecBlade 对未知目的 MAC 地址的 IP 单播报文的处理方式，**undo firewall unknown-mac unicast** 命令用来恢复对未知目的 MAC 地址的 IP 单播报文的缺省处理方式。

缺省情况下，SecBlade 对未知目的 MAC 地址的单播 IP 报文按照 **arp** 方式进行处理。

【举例】

配置 SecBlade 丢弃未知目的 MAC 地址的 IP 单播报文。

```
[SecBlade_FW] firewall unknown-mac unicast drop
```

5.1.21 reset firewall ethernet-frame-filter

【命令】

reset firewall ethernet-frame-filter { **all** | **interface** *interface-type interface-number* }

【视图】

用户视图

【参数】

all：所有接口上的以太帧的过滤信息。

interface *interface-type interface-number*：特定接口上的以太帧的过滤信息。

【描述】

reset firewall ethernet-frame-filter 命令用来清除以太帧的过滤信息。

【举例】

清除所有接口上的以太帧过滤信息。

```
<SecBlade_FW> reset firewall ethernet-frame-filter all
```

5.1.22 reset firewall transparent-mode address-table

【命令】

reset firewall transparent-mode address-table [**interface** *interface-type interface-number*]

【视图】

用户视图

【参数】

interface *interface-type interface-number*：与特定接口关联的 MAC 地址信息。

【描述】

reset firewall transparent-mode address-table 命令用来清除 MAC 地址表中的信息。

【举例】

清除与接口 GigabitEthernet 0/1 相关联的 MAC 地址信息。

```
<SecBlade_FW> reset firewall transparent-mode address-table interface GigabitEthernet0/1
```

5.1.23 reset firewall transparent-mode traffic

【命令】

reset firewall transparent-mode traffic [**interface** *interface-type interface-number*]

【视图】

用户视图

【参数】

interface *interface-type interface-number*：特定接口的流量统计信息。

【描述】

reset firewall transparent-mode traffic 命令用来清除透明防火墙的流量统计信息。

【举例】

清除透明防火墙的流量统计信息。

```
<SecBlade_FW> reset firewall transparent-mode traffic
```

5.1.24 rule

【命令】

rule [*rule-id*] { **permit** | **deny** } [**type** *type-code type-wildcard* | **lsap** *lsap-code lsap-wildcard*] [**source-mac** *sour-addr source-wildcard*] [**dest-mac** *dest-addr*

dest-wildcard] [**time-range** *time-name*] [**logging**]

undo rule *rule-id* [**time-range**] [**logging**]

【视图】

基于 MAC 地址的 ACL 视图

【参数】

rule-id：ACL 的规则编号，范围为 0～65534。当指定了编号，如果与编号对应的规则已经存在，则会部分覆盖旧的规则，相当于编辑一个已经存在的 ACL 规则。故建议用户当编辑一个已存在编号的规则时，先将旧的规则删除，再创建新的规则，否则配置结果可能与预期的效果不同。如果与编号对应的规则不存在，则使用指定的编号创建一个新的规则。如果不指定编号，表示增加一个新规则，系统自动会为这个规则分配一个编号。

permit：表示允许符合条件的数据包。

deny：表示拒绝符合条件的数据包。

type：数据帧的类型。

type-code：数据帧的类型，一个 16 比特的十六进制数，对应Ethernet_II类型和Ethernet_SNAP类型帧中的type-code域。关于*type-code*的值请参考 表 5-1。

type-mask：类型掩码，是一个 16 比特的十六进制数，用于指定屏蔽位。

lsap：数据帧的封装格式。

lsap-code：数据帧的封装格式的值，是一个 16 比特的十六进制数。

lsap-mask：lsap 值的掩码，是一个 16 比特的十六进制数，用于指定屏蔽位。

source-mac：源 MAC 地址。

sour-addr：源 MAC 地址，格式为 xxxx-xxxx-xxxx，用来匹配一个分组的源地址。

sour-mask：源 MAC 地址的掩码。

dest-mac：目的 MAC 地址。

dest-addr：目的 MAC 地址，格式为 xxxx-xxxx-xxxx，用来匹配一个分组的源地址。

dest-mask：目的 MAC 地址的掩码。

logging：对符合条件的数据包记录日志。

time-range *time-name*：配置这条访问控制规则生效的时间段。

【描述】

rule 命令用来添加一个 ACL 规则，**undo rule** 命令用来删除 ACL 规则。

缺省情况下，未创建任何 ACL 规则。

【举例】

配置一条拒绝任何以太网帧的规则。

```
[SecBlade_FW] acl number 4009
[SecBlade_FW-acl-ethernetframe-4009] rule deny
```

表5-1 以太网类型域值表

以太网类型域值（16 进制值）	描述
0000-05DC	IEEE802.3 Length Field
0101-01FF	Experimental
200	XEROX PUP (see 0A00)
201	PUP Addr Trans (see 0A01)
400	Nixdorf
600	XEROX NS IDP
660	DLOG
661	DLOG
800	Internet IP (IPv4)
801	X.75 Internet
802	NBS Internet
803	ECMA Internet
804	Chaosnet
805	X.25 Level 3
806	ARP
807	XNS Compatability
081C	Symbolics Private
0888-088A	Xyplex
900	Ungermann-Bass net debugr
0A00	Xerox IEEE802.3 PUP
0A01	PUP Addr Trans
0BAD	Banyan Systems
1000	Berkeley Trailer nego
1001-100F	Berkeley Trailer encap/IP
1600	Valid Systems
4242	PCS Basic Block Protocol
5208	BBN Simnet
6000	DEC Unassigned (Exp.)

以太网类型域值（16 进制值）	描述
6001	DEC MOP Dump/Load
6002	DEC MOP Remote Console
6003	DEC DECNET Phase IV Route
6004	DEC LAT
6005	DEC Diagnostic Protocol
6006	DEC Customer Protocol
6007	DEC LAVC, SCA
6008-6009	DEC Unassigned
6010-6014	3Com Corporation
7000	Ungermann-Bass download
7002	Ungermann-Bass dia/loop
7020-7029	LRT
7030	Proteon
7034	Cabletron
8003	Cronus VLN
8004	Cronus Direct
8005	HP Probe
8006	Nestar
8008	AT&T
8010	Excelan
8013	SGI diagnostics
8014	SGI network games
8015	SGI reserved
8016	SGI bounce server
8019	Apollo Computers
802E	Tymshare
802F	Tigan, Inc.
8035	Reverse ARP
8036	Aeonic Systems
8038	DEC LANBridge
8039-803C	DEC Unassigned
803D	DEC Ethernet Encryption
803E	DEC Unassigned
803F	DEC LAN Traffic Monitor

以太网类型域值（16 进制值）	描述
8040-8042	DEC Unassigned
8044	Planning Research Corp.
8046	AT&T
8047	AT&T
8049	ExperData
805B	Stanford V Kernel exp.
805C	Stanford V Kernel prod.
805D	Evans & Sutherland
8060	Little Machines
8062	Counterpoint Computers
8065	Univ. of Mass. @ Amherst
8066	Univ. of Mass. @ Amherst
8067	Veeco Integrated Auto.
8068	General Dynamics
8069	AT&T
806A	Autophon
806C	ComDesign
806D	Computgraphic Corp.
806E-8077	Landmark Graphics Corp.
807A	Matra
807B	Dansk Data Elektronik
807C	Merit Internodal
807D-807F	Vitalink Communications
8080	Vitalink TransLAN III
8081-8083	Counterpoint Computers
809B	Appletalk
809C-809E	Datability
809F	Spider Systems Ltd.
80A3	Nixdorf Computers
80A4-80B3	Siemens Gammasonics Inc.
80C0-80C3	DCA Data Exchange Cluster
80C4	Banyan Systems
80C5	Banyan Systems
80C6	Pacer Software

以太网类型域值（16 进制值）	描述
80C7	Applitek Corporation
80C8-80CC	Intergraph Corporation
80CD-80CE	Harris Corporation
80CF-80D2	Taylor Instrument
80D3-80D4	Rosemount Corporation
80D5	IBM SNA Service on Ether
80DD	Varian Associates
80DE-80DF	Integrated Solutions TRFS
80E0-80E3	Allen-Bradley
80E4-80F0	Datability
80F2	Retix
80F3	AppleTalk AARP (Kinetics)
80F4-80F5	Kinetics
80F7	Apollo Computer
80FF-8103	Wellfleet Communications
8107-8109	Symbolics Private
8130	Hayes Microcomputers
8131	VG Laboratory Systems
8132-8136	Bridge Communications
8137-8138	Novell, Inc.
8139-813D	KTI
8148	Logicraft
8149	Network Computing Devices
814A	Alpha Micro
814C	SNMP
814D	BIIN
814E	BIIN
814F	Technically Elite Concept
8150	Rational Corp
8151-8153	Qualcomm
815C-815E	Computer Protocol Pty Ltd
8164-8166	Charles River Data System
817D-818C	Protocol Engines
818D	Motorola Computer

以太网类型域值（16 进制值）	描述
819A-81A3	Qualcomm
81A4	ARAI Bunkichi
81A5-81AE	RAD Network Devices
81B7-81B9	Xyplex
81CC-81D5	Apricot Computers
81D6-81DD	Artisoft
81E6-81EF	Polygon
81F0-81F2	Comsat Labs
81F3-81F5	SAIC
81F6-81F8	VG Analytical
8203-8205	Quantum Software
8221-8222	Ascom Banking Systems
823E-8240	Advanced Encryption Syste
827F-8282	Athena Programming
8263-826A	Charles River Data System
829A-829B	Inst Ind Info Tech
829C-82AB	Taurus Controls
82AC-8693	Walker Richer & Quinn
8694-869D	Idea Courier
869E-86A1	Computer Network Tech
86A3-86AC	Gateway Communications
86DB	SECTRA
86DE	Delta Controls
86DF	ATOMIC
86E0-86EF	Landis & Gyr Powers
8700-8710	Motorola
8A96-8A97	Invisible Software
9000	Loopback
9001	3Com(Bridge) XNS Sys Mgmt
9002	3Com(Bridge) TCP-IP Sys
9003	3Com(Bridge) loop detect
FF00	BBN VITAL-LanBridge cache
FF00-FF0F	ISC Bunker Ramo

第6章 Web 和邮件过滤配置命令

6.1 Web 过滤配置命令

6.1.1 debugging firewall url-filter host

【命令】

debugging firewall url-filter host { **all** | **filter** | **packet** | **event** | **error** }

undo debugging firewall url-filter host { **all** | **filter** | **packet** | **event** | **error** }

【视图】

用户视图

【参数】

all：所有调试功能。

filter：过滤包调试功能。

packet：报文调试功能。

event：事件调试功能。

error：错误调试功能。

【描述】

debugging firewall url-filter host 命令用来打开 Web 地址过滤的调试功能，**undo debugging firewall url-filter host** 命令用来关闭调试功能。

缺省情况下，关闭调试功能。

【举例】

打开 Web 地址过滤的所有调试功能。

```
<SecBlade_FW> debugging firewall url-filter host all
```

6.1.2 debugging firewall url-filter parameter

【命令】

debugging firewall url-filter parameter { **all** | **error** | **event** | **filter** | **packet** }

undo debugging firewall url-filter parameter { **all** | **error** | **event** | **filter** | **packet** }

【视图】

用户视图

【参数】

all：所有调试功能。

filter：过滤包调试功能。

packet：报文调试功能。

event：事件调试功能。

error：错误调试功能。

【描述】

debugging firewall url-filter parameter 命令用来打开 SQL 注入攻击防范的调试功能，**undo debugging firewall url-filter parameter** 命令用来关闭 SQL 注入攻击防范的调试功能。

缺省情况下，关闭调试功能。

【举例】

打开 SQL 注入攻击防范的错误调试功能。

```
<SecBlade_FW> debugging firewall url-filter parameter error
```

6.1.3 debugging firewall webdata-filter

【命令】

debugging firewall webdata-filter { **all** | **filter** | **packet** | **event** | **error** }

undo debugging firewall webdata-filter { **all** | **filter** | **packet** | **event** | **error** }

【视图】

用户视图

【参数】

all：所有调试功能。

filter：过滤包调试功能。

packet：报文调试功能。

event：事件调试功能。

error：错误调试功能。

【描述】

debugging firewall webdata-filter 命令用来打开 Web 内容过滤的调试功能，**undo debugging firewall webdata-filter** 命令用来关闭调试功能。

缺省情况下，关闭调试功能。

【举例】

打开 Web 内容过滤的所有调试功能。

```
<SecBlade_FW> debugging firewall webdata-filter all
```

6.1.4 display firewall url-filter host

【命令】

display firewall url-filter host { **enable** | **all** | **item** *url-address* | **item-all** }

【视图】

所有视图

【参数】

enable：显示 Web 地址过滤的使能信息。

all：显示所有的 Web 地址过滤信息。

item *url-address*：显示具体的过滤地址条目的统计信息。

Item-all：显示所有过滤地址条目的统计信息。

【描述】

display firewall url-filter host 命令用来显示 Web 地址过滤的信息。

【举例】

显示 Web 地址过滤的信息。

```
[SecBlade_FW] display firewall url-filter host all
URL-filter is enabled.
Default method : permit.
No ACL configed to be Matched
Deny http requeset when the URL is ip address ,No acl selected to be Matched
Url host filter has loaded file "flash:/urlfilter" , there are 2 item(s) in
filter now( 2 Added,0 Loaded).
Packet(s) blocked.
Packet(s) allowed.
```

6.1.5 display firewall url-filter parameter

【命令】

display firewall url-filter parameter { **enable** | **all** | **item** *keywords* | **item-all** }

【视图】

所有视图

【参数】

enable：显示 SQL 注入攻击防范的使能信息。

all：显示所有的 SQL 注入攻击防范的过滤信息。

item *keywords*：显示具体的过滤关键字条目的统计信息。

Item-all：显示所有的过滤关键字条目的统计信息。

【描述】

display firewall url-filter parameter 命令用来显示 SQL 注入攻击的过滤信息。

【举例】

显示所有 SQL 注入攻击的过滤信息。

```
[SecBlade_FW] display firewall url-filter parameter all
Url parameter filter is enabled.
 Url parameter filter has loaded file "flash:/SQLfilter" , there are 9 item(s)
in filter now( 9 Added,0 Loaded).
Packet(s) blocked    :0.
 Packet(s) allowed    :0.
```

6.1.6 display firewall url-filter parameter counter detail

【命令】

display firewall url-filter parameter counter detail

【视图】

所有视图

【参数】

无

【描述】

display firewall url-filter parameter counter detail 命令用来详细显示每个关键字所匹配的次数。

【举例】

显示每个关键字所匹配的次数。

```
[SecBlade_FW] display firewall url-filter parameter counter detail
 ----------------------------------------
 ^select^            0
 ^insert^            0
 ^update^            0
 ^delete^            0
 ^drop^              0
 --                  0
 '                   0
 ^exec^              0
 %27                 0
```

6.1.7 display firewall webdata-filter

【命令】

display firewall webdata-filter { **enable** | **all** | **item** *keywords* | **item-all** }

【视图】

所有视图

【参数】

enable：显示 Web 内容过滤的使能信息。

all：显示所有的 Web 内容过滤信息。

item *keywords*：显示具体的过滤关键字条目的统计信息。

Item-all：显示所有的过滤关键字条目的统计信息。

【描述】

display firewall webdata-filter 命令用来显示 Web 内容过滤的信息。

【举例】

显示 Web 内容过滤的信息。

```
[SecBlade_FW] display firewall webdata-filter all
 Webdata-filter is enabled.
 Webdata-filter has loaded file "flash:/webdatafilter" , there are 1 item(s)
in
filter now ( 1 Added,0 Loaded).
 Packet(s) blocked.
 Packet(s) allowed.
```

6.1.8 firewall url-filter host acl-number

【命令】

firewall url-filter host acl-number *number*

undo firewall url-filter host acl-number

【视图】

系统视图

【参数】

number：基本访问控制列表的编号，范围为 2000～2999。

【描述】

firewall url-filter host acl-number 命令用来配置 SecBlade 通过使用 ACL 对目标 URL 为 IP 地址的 Web 请求进行过滤，**undo firewall url-filter host acl-number** 命令用来取消配置的过滤规则。

使用此命令只能引用一个 ACL 规则，随后配置的规则将覆盖原先的配置。

缺省情况下，未配置任何过滤规则。

【举例】

配置仅允许目标 IP 地址为符合编号 2001 的 ACL 规则的 Web 请求通过。

```
[SecBlade_FW] acl number 2001
[SecBlade_FW-acl-basic-2001] rule deny source 200.1.1.0 0.0.0.255
[SecBlade_FW-acl-basic-2001] rule permit
[SecBlade_FW-acl-basic-2001] quit
[SecBlade_FW] firewall url-filter host acl-number 2001
```

6.1.9 firewall url-filter host add

【命令】

firewall url-filter host add { **permit** | **deny** } *url-address*

【视图】

系统视图

【参数】

permit：表示操作行为为允许。

deny：表示操作行为为拒绝。

url-address：添加的 URL 过滤地址。

【描述】

firewall url-filter add 命令用来添加 Web 过滤地址，并设置对其的过滤行为。

用户添加的网址地址最长允许 128 个字符，否则视为非法地址，不予添加。如果输入*.sina.com 为匹配网址，则系统将匹配 www.sina.com、news.sina.com 等匹配掉，而不匹配 www.sina.com.cn。不支持以下的地址格式：*.*.com.cn、news.*.com、sina.com.*。

缺省情况下，未添加任何过滤地址。

【举例】

添加允许地址为 www.163.com 的过滤条目。

```
[SecBlade_FW] firewall url-filter host add permit www.163.com
```

6.1.10 firewall url-filter host clear

【命令】

firewall url-filter host clear

【视图】

系统视图

【参数】

无

【描述】

firewall url-filter host clear 命令用来清除所有过滤地址条目。

【举例】

清除所有过滤地址条目。

```
[SecBlade_FW] firewall url-filter host clear
```

6.1.11 firewall url-filter host default

【命令】

firewall url-filter host default { **permit** | **deny** }

【视图】

系统视图

【参数】

permit：配置默认过滤操作为允许。

deny：配置默认过滤操作为拒绝。

【描述】

firewall url-filter host default 命令用来允许或者拒绝未与管理员配置的网址发生匹配的数据报通过。

缺省情况下，允许未发生匹配的数据报通过。

【举例】

配置默认过滤行为为允许。

```
[SecBlade_FW] firewall url-filter host default permit
```

6.1.12 firewall url-filter host delete

【命令】

firewall url-filter host delete *url-address*

【视图】

系统视图

【参数】

url-address：删除的过滤地址。

【描述】

firewall url-filter host delete 命令用来删除 Web 过滤地址。

【举例】

删除地址为 www.163.com 的过滤条目。

```
[SecBlade_FW] firewall url-filter host delete www.163.com
```

6.1.13 firewall url-filter host enable

【命令】

firewall url-filter host enable

undo firewall url-filter host enable

【视图】

系统视图

【参数】

无

【描述】

firewall url-filter host enable 命令用来使能 Web 地址过滤功能，**undo firewall url-filter host enable** 命令用来关闭 Web 地址过滤功能。

缺省情况下，关闭 Web 地址过滤功能。

开启Web地址过滤功能之前要先配置ASPF策略，**detect http**，**detect tcp**，才能使Web地址过滤功能生效。有关ASPF配置命令请参见 4.2 状态防火墙配置命令。

【举例】

使能 Web 地址过滤功能。

```
[SecBlade_FW] firewall url-filter host enable
```

6.1.14 firewall url-filter host ip-address

【命令】

firewall url-filter host ip-address { **permit** | **deny** }

【视图】

系统视图

【参数】

permit：允许目标 URL 为 IP 地址的 Web 请求通过。

deny：拒绝目标 URL 为 IP 地址的 Web 请求通过

【描述】

firewall url-filter host ip-address 命令用来配置 SecBlade 是否允许目标 URL 为 IP 地址的 Web 请求通过。

缺省情况下，SecBlade 将阻止目标 URL 为 IP 地址的 Web 请求通过。

【举例】

配置允许目标 URL 为 IP 地址的 Web 请求通过。

```
[SecBlade_FW] firewall url-filter host ip-address permit
```

6.1.15 firewall url-filter host save-file

【命令】

firewall url-filter host save-file *file-name*

【视图】

系统视图

【参数】

file-name：保存的过滤文件名。

【描述】

firewall url-filter host save-file 命令用来保存 Web 地址过滤文件。

【举例】

保存名为 urlfilter 的 Web 地址过滤文件。

```
[SecBlade_FW] firewall url-filter host save-file urlfilter
```

6.1.16 firewall url-filter host load-file

【命令】

firewall url-filter host load-file *file-name*

undo firewall url-filter host load-file

【视图】

系统视图

【参数】

file-name：装载的过滤文件名。

【描述】

firewall url-filter host load-file 命令用来装载 Web 地址过滤文件，**undo firewall url-filter host load-file** 命令用来卸载 Web 地址过滤文件。

如果要使 Web 地址过滤文件中的条目生效并对地址进行过滤，必须将其装载。

【举例】

装载名为 urlfilter 的 Web 地址过滤文件。

```
[SecBlade_FW] firewall url-filter host load-file urlfilter
```

6.1.17 firewall url-filter parameter add

【命令】

firewall url-filter parameter add *keywords*

undo firewall url-filter parameter add *keywords*

【视图】

系统视图

【参数】

keywords：出现在 HTTP 命令中的关键字。

【描述】

firewall url-filter parameter add 命令用来添加 SQL 注入攻击过滤的关键字。若指定的关键字出现在 HTTP 命令中，SecBlade 将阻止此 HTTP 请求。

用户可以根据自己的需要，将一些表名、字段、以及一些系统的和自定义的存储过程名作为关键字。

缺省情况下，未添加任何关键字。

过滤关键字最长支持 128 字节。关键字过滤支持模糊查找，即允许向过滤关键字文件中添加带“*”、“^”、“?”和“ ”（空格）的关键字。“?”和“ ”（空格）可以通过文件进行加载或以 Web 管理方式输入，不能通过命令行输入。

“*”表示最少 0 个到最多 2 个任意中文字符或最少 0 个到最多 4 个任意英文字符。其不能出现在开头和结尾的位置，不能和“^”以及“?”相邻。为避免“*”带来的误判断，管理员应谨慎添加带“*”的过滤关键字。不允许一个关键字中出现两个以上的“*”。过滤词汇文件格式如：test1、te*st2；不允许：te**st、t*es*t、*test。

“^”只能出现在关键字的开头和结尾的位置，最多允许出现两个。例如：^hello，它可以匹配以 hello 开头的字符串，如 helloworld、hello，但其不匹配 ahelloworld；you^可以匹配以 you 结尾的字符串，如 thankyou、you，但其不匹配 thankyour、your。

“?”代表一个字符，如果是汉字这要用“??”。“?”可以出现多个，并可以连续出现。其可以出现在随意的位置，但不能和“*”相邻。如果出现在开始和结尾的位置，则一定要和“^”相邻。“?”只能通过文件加载，不能通过命令行输入。

用户可以通过命令行和文件的形式加载带空格“ ”的关键字。空格的个数和位置没有限制，一个空格可以匹配连续的几个空格。

相关配置命令请参考 **firewall url-filter parameter add-default**。

【举例】

若数据库中含有一个用户自定义的存储过程“sp_additem”，若要阻止对此存储过程的操作，可以将含有此存储过程名的 HTTP 命令进行阻止。

```
[SecBlade_FW] firewall url-filter parameter add sp_additem
```

6.1.18 firewall url-filter parameter add-default

【命令】

firewall url-filter parameter add-default

【视图】

系统视图

【参数】

无

【描述】

firewall url-filter parameter add-default 命令用来添加系统缺省的过滤关键字：^select^、^insert^、^update^、^delete^、^drop^、--、'、^exec^和%27，方便了用户的输入，也防止用户无意中删除了某些关键字，或者不恰当地使用了 **firewall url-filter parameter clear** 命令时可以很快地恢复缺省配置。

缺省情况下，未添加任何过滤关键字。

【举例】

添加系统缺省的过滤关键字。

```
[SecBlade_FW] firewall url-filter parameter add-default
 Success to add 9 keys!
```

6.1.19 firewall url-filter parameter clear

【命令】

firewall url-filter parameter clear

【视图】

系统视图

【参数】

无

【描述】

firewall url-filter parameter clear 命令用来清除所有过滤关键字。

【举例】

清除所有过滤关键字。

```
[SecBlade_FW] firewall url-filter parameter clear
```

6.1.20 firewall url-filter parameter delete

【命令】

firewall url-filter parameter delete *keywords*

【视图】

系统视图

【参数】

keywords：删除的过滤关键字。

【描述】

firewall url-filter parameter delete 命令用来删除一个以添加的过滤关键字。

【举例】

删除过滤关键字“select”

```
[SecBlade_FW] firewall url-filter parameter delete select
```

6.1.21 firewall url-filter parameter enable

【命令】

firewall url-filter parameter enable

undo firewall url-filter parameter enable

【视图】

系统视图

【参数】

无

【描述】

firewall url-filter parameter enable 命令用来使能 SQL 注入攻击防范功能，**undo** 命令用来关闭 SQL 注入攻击防范功能。

缺省情况下，关闭 SQL 注入攻击防范功能。

【举例】

使能 SQL 注入攻击防范功能。

```
[SecBlade_FW] firewall url-filter parameter enable
```

6.1.22 firewall url-filter parameter load-file

【命令】

firewall url-filter parameter load-file *file-name*

undo firewall url-filter parameter load-file

【视图】

系统视图

【参数】

file-name：装载的过滤文件名。

【描述】

firewall url-filter parameter load-file 命令用来装载 SQL 注入攻击过滤文件，**undo firewall url-filter parameter load-file** 命令用来卸载 SQL 注入攻击过滤文件。

【举例】

装载名为 sqlfilter 的 SQL 注入攻击过滤文件。

```
[SecBlade_FW] firewall url-filter parameter load-file sqlfilter
```

6.1.23 firewall url-filter parameter save-file

【命令】

firewall url-filter parameter save-file *file-name*

【视图】

系统视图

【参数】

file-name：保存的过滤文件名。

【描述】

firewall url-filter parameter save-file 命令用来保存 SQL 注入攻击过滤文件。

【举例】

保存名为 sqlfilter 的 SQL 注入攻击过滤文件。

```
[SecBlade_FW] firewall url-filter parameter save-file sqlfilter
```

6.1.24 firewall webdata-filter add

【命令】

firewall webdata-filter add *keywords*

【视图】

系统视图

【参数】

keywords：添加的过滤关键字。

【描述】

firewall webdata-filter add 命令用来添加 Web 内容过滤关键字。

过滤关键字最长支持 64 字节。关键字过滤支持模糊查找，即允许向过滤关键字文件中添加带“*”、“^”、“?”和“ ”（空格）的关键字。“?”和“ ”（空格）可以通过文件进行加载或以 Web 管理方式输入，不能通过命令行输入。

“*”表示最少 0 个到最多 2 个任意中文字符或最少 0 个到最多 4 个任意英文字符。其不能出现在开头和结尾的位置，不能和“^”以及“?”相邻。为避免“*”带来的误判断，管理员应谨慎添加带“*”的过滤关键字。不允许一个关键字中出现两个以上的“*”。过滤词汇文件格式如：test1、te*st2；不允许：te**st、t*es*t、*test。

“^”只能出现在关键字的开头和结尾的位置，最多允许出现两个。例如：^hello，它可以匹配以 hello 开头的字符串，如 helloworld、hello，但其不匹配 ahelloworld；you^可以匹配以 you 结尾的字符串，如 thankyou、you，但其不匹配 thankyour、your。

“?”代表一个字符，如果是汉字这要用“??”。“?”可以出现多个，并可以连续出现。其可以出现在随意的位置，但不能和“*”相邻。如果出现在开始和结尾的位置，则一定要和“^”相邻。“?”只能通过文件加载，不能通过命令行输入。

用户可以通过命令行和文件的形式加载带空格“ ”的关键字。空格的个数和位置没有限制，一个空格可以匹配连续的几个空格。

缺省情况下，未添加任何过滤关键字。

⚠ 注意：

添加的 Web 内容过滤关键字不能为 HTML 语言的标记，例如<head>、<html>、<title>、<script>等等，否则合法的网页可能会被过滤掉。

【举例】

添加包含关键字“music”的过滤条目。

```
[SecBlade_FW] firewall webdata-filter add music
```

6.1.25 firewall webdata-filter clear

【命令】

firewall webdata-filter clear

【视图】

系统视图

【参数】

无

【描述】

firewall webdata-filter clear 命令用来清除所有内容关键字条目。

【举例】

清除所有内容关键字条目。

```
[SecBlade_FW] firewall webdata-filter clear
```

6.1.26 firewall webdata-filter delete

【命令】

firewall webdata-filter delete *keywords*

【视图】

系统视图

【参数】

keywords：删除的过滤关键字。

【描述】

firewall webdata-filter delete 命令用来删除 Web 内容过滤关键字。

【举例】

删除包含关键字“music”的过滤条目。

```
[SecBlade_FW] firewall webdata-filter delete music
```

6.1.27 firewall webdata-filter enable

【命令】

firewall webdata-filter enable

undo firewall webdata-filter enable

【视图】

系统视图

【参数】

无

【描述】

firewall webdata-filter enable 命令用来使能 Web 内容过滤功能， **undo firewall webdata-filter enable** 命令用来关闭 Web 内容过滤功能。

缺省情况下，关闭 Web 内容过滤功能。

开启Web内容过滤功能之前要先配置ASPF策略，**detect http**，**detect tcp**，才能使Web内容过滤功能生效。有关ASPF配置命令请参见 4.2 状态防火墙配置命令。

【举例】

使能 Web 内容过滤功能。

```
[SecBlade_FW] firewall webdata-filter enable
```

6.1.28 firewall webdata-filter load-file

【命令】

firewall webdata-filter load-file *file-name*

undo firewall webdata-filter load-file

【视图】

系统视图

【参数】

file-name：装载的过滤文件名。

【描述】

firewall webdata-filter load-file 命令用来装载 Web 内容过滤文件，**undo firewall webdata-filter load-file** 命令用来卸载 Web 内容过滤文件。

如果要使 Web 内容过滤文件中的条目生效并对内容进行过滤，必须将其装载。

Web 内容过滤的真正目的是过滤掉包含非法内容的 HTTP 回应报文。一旦 HTTP 回应报文包含需要过滤的内容，则报文将被过滤。

【举例】

装载名为 webdatafilter 的 Web 内容过滤文件。

```
[SecBlade_FW] firewall webdata-filter load-file webdatafilter
```

6.1.29 firewall webdata-filter save-file

【命令】

firewall webdata-filter save-file *file-name*

【视图】

系统视图

【参数】

file-name：保存的过滤文件名。

【描述】

firewall webdata-filter save-file 命令用来保存 Web 内容过滤文件。

【举例】

保存名为 webdatafilter 的 Web 内容过滤文件。

```
[SecBlade_FW] firewall webdata-filter save-file webdatafilter
```

6.1.30 reset firewall url-filter host counter

【命令】

reset firewall url-filter host counter

【视图】

用户视图

【参数】

无

【描述】

reset firewall url-filter host counter 命令用来清除 Web 地址过滤的统计信息。

【举例】

清除 Web 地址过滤的统计信息。

```
<SecBlade_FW> reset firewall url-filter host counter
```

6.1.31 reset firewall url-filter parameter counter

【命令】

reset firewall url-filter parameter counter

【视图】

用户视图

【参数】

无

【描述】

reset firewall url-filter parameter counter 命令用来清除 SQL 注入攻击防范的统计信息。

【举例】

清除 SQL 注入攻击防范的统计信息。

```
<SecBlade_FW> reset firewall url-filter parameter counter
```

6.1.32 reset firewall webdata-filter counter

【命令】

reset firewall webdata-filter counter

【视图】

用户视图

【参数】

无

【描述】

reset firewall webdata-filter counter 命令用来清除 Web 内容过滤的统计信息。

【举例】

清除 Web 内容过滤的统计信息。

```
<SecBlade_FW> reset firewall webdata-filter counter
```

6.2 邮件过滤配置命令

6.2.1 debugging firewall smtp-filter

【命令】

debugging firewall smtp-filter

undo debugging firewall smtp-filter

【视图】

用户视图

【参数】

无

【描述】

debugging firewall smtp-filter 命令用来打开邮件过滤的调试功能，**undo debugging firewall smtp-filter** 命令用来关闭调试功能。

缺省情况下，关闭调试功能。

【举例】

打开邮件过滤的调试功能。

```
<SecBlade_FW> debugging firewall smtp-filter
```

6.2.2 display firewall smtp-filter

【命令】

display firewall smtp-filter { **all** | { **rcptto** | **subject** | **content** | **attach** } { **item** *string* | **item-all** } }

【视图】

所有视图

【参数】

all：显示所有的邮件过滤信息。

rcptto：显示邮件地址过滤信息。

subject：显示邮件主题过滤信息。

content：显示邮件内容过滤信息

attach：显示邮件附件过滤信息。

item *string*：显示具体的过滤关键字条目的统计信息。

Item-all：显示所有的过滤关键字条目的统计信息。

【描述】

display firewall smtp-filter 命令用来显示邮件过滤信息。

【举例】

显示所有邮件过滤的信息。

```
[SecBlade_FW] display firewall smtp-filter all
Smtp-filter rcptto is enabled.
 Default method: deny.
 Rcptto has Loaded file "flash:/rcpttofilter", there are 1 item(s) in filter
now( 5 Added,0 Loaded).
Packet(s) blocked    :0.

 Packet(s) allowed    :0.

 Smtp-filter subject is enabled.
 Subject has Loaded file "flash:/subjectfilter", there are 1 item(s) in filter
now( 7 Added,0 Loaded).
Packet(s) blocked    :0.

 Smtp-filter content is enabled.
 Content has Loaded file "flash:/contentfilter", there are 1 item(s) in filter
now( 5 Added,0 Loaded).
Packet(s) blocked    :0.

 Smtp-filter attach is enabled.
 Attach has Loaded file "flash:/attachfilter", there are 1 item(s) in filter
now( 6 Added,0 Loaded).
Packet(s) blocked    :0.
```

6.2.3 firewall smtp-filter attach add

【命令】

firewall smtp-filter attach add *file-name*

【视图】

系统视图

【参数】

file-name：添加的附件文件名。

【描述】

firewall smtp-filter attach add 命令用来添加过滤附件名。

过滤附件名最长支持 128 个字符。系统允许用户添加两种形式的过滤附件名，一种是完全的文件名，另外一种是“*.ext”形式的文件名。对于第二种则只过滤附件扩展名而不比较扩展名前的文件名。允许过滤文件中同时存在*.exe 和 abc.exe 这样的文件名，当用户取消*.exe 格式的文件名过滤后，abc.exe 过滤继续起作用。

缺省情况下，未添加过滤附件名。

【举例】

添加包含附件名为“virus.exe”的过滤条目。

```
[SecBlade_FW] firewall smtp-filter attach add virus.exe
```

6.2.4 firewall smtp-filter attach clear

【命令】

firewall smtp-filter attach clear

【视图】

系统视图

【参数】

无

【描述】

firewall smtp-filter attach clear 命令用来清除所有过滤附件名。

【举例】

清除所有过滤附件名条目。

```
[SecBlade_FW] firewall smtp-filter attach clear
```

6.2.5 firewall smtp-filter attach delete

【命令】

firewall smtp-filter attach delete *file-name*

【视图】

系统视图

【参数】

file-name：删除的附件文件名。

【描述】

firewall smtp-filter attach delete 命令用来删除过滤附件名。

【举例】

删除附件名为“virus.exe”的过滤条目。

```
[SecBlade_FW] firewall smtp-filter attach delete virus.exe
```

6.2.6 firewall smtp-filter attach enable

【命令】

firewall smtp-filter attach enable

undo firewall smtp-filter attach enable

【视图】

系统视图

【参数】

无

【描述】

firewall smtp-filter attach enable 命令用来使能邮件附件过滤功能，**undo firewall smtp-filter attach enable** 命令用来关闭邮件附件过滤功能。

当使用邮件附件过滤时，被过滤的邮件的附件名长度不能超过 128 个字符。

缺省情况下，关闭邮件附件过滤功能。

开启邮件附件过滤功能之前要先配置ASPF策略，**detect smtp**，**detect tcp**，才能使邮件附件过滤功能生效。有关ASPF配置命令请参见 4.2 状态防火墙配置命令。

【举例】

使能邮件附件过滤功能。

```
[SecBlade_FW] firewall smtp-filter attach enable
```

6.2.7 firewall smtp-filter attach load-file

【命令】

firewall smtp-filter attach load-file *file-name*

undo firewall smtp-filter attach load-file

【视图】

系统视图

【参数】

file-name：装载的过滤文件名。

【描述】

firewall smtp-filter attach load-file 命令用来装载邮件附件过滤文件，**undo firewall smtp-filter attach load-file** 命令用来卸载邮件附件过滤文件。

如果要使邮件附件过滤文件中的条目生效并对附件进行过滤，必须将其装载。

【举例】

装载名为 attachfilter 的邮件附件过滤文件。

```
[SecBlade_FW] firewall smtp-filter attach load-file attachfilter
```

6.2.8 firewall smtp-filter attach save-file

【命令】

firewall smtp-filter attach save-file *file-name*

【视图】

系统视图

【参数】

file-name：保存的过滤文件名。

【描述】

firewall smtp-filter attach save-file 命令用来保存邮件附件过滤文件。

【举例】

保存名为 attachfilter 的邮件附件过滤文件。

```
[SecBlade_FW] firewall smtp-filter attach save-file attachfilter
```

6.2.9 firewall smtp-filter content add

【命令】

firewall smtp-filter content add *content-keywords*

【视图】

系统视图

【参数】

content-keywords：添加的内容过滤关键字。

【描述】

firewall smtp-filter content add 命令用来添加内容过滤关键字。

过滤关键字最长支持 64 字节。关键字过滤支持模糊查找，即允许向过滤关键字文件中添加带“*”的关键字，“*”表示最少 0 个到最多 2 个任意中文字符或最少 0 个到最多 4 个任意英文字符。为避免“*”带来的误判断，管理员应谨慎添加带“*”

的过滤关键字。*只允许出现在关键字的中间。不允许一个关键字中出现两个以上的“*”。过滤词汇文件格式如：test1、te*st2；不允许：te**st、t*es*t。

缺省情况下，未添加内容过滤关键字。

【举例】

添加包含内容关键字“abcde”的过滤条目。

```
[SecBlade_FW] firewall smtp-filter content add abcde
```

6.2.10 firewall smtp-filter content clear

【命令】

firewall smtp-filter content clear

【视图】

系统视图

【参数】

无

【描述】

firewall smtp-filter content clear 命令用来清除所有内容过滤关键字条目。

【举例】

清除所有过滤关键字条目。

```
[SecBlade_FW] firewall smtp-filter content clear
```

6.2.11 firewall smtp-filter content delete

【命令】

firewall smtp-filter content delete *content-keywords*

【视图】

系统视图

【参数】

content-keywords：删除的内容过滤关键字。

【描述】

firewall smtp-filter content delete 命令用来删除邮件内容过滤关键字。

【举例】

删除内容关键字为“abcde”的过滤条目。

```
[SecBlade_FW] firewall smtp-filter content delete abcde
```

6.2.12 firewall smtp-filter content enable

【命令】

firewall smtp-filter content enable

undo firewall smtp-filter content enable

【视图】

系统视图

【参数】

无

【描述】

firewall smtp-filter content enable 命令用来使能邮件内容过滤功能，**undo firewall smtp-filter content enable** 命令用来关闭邮件内容过滤功能。

缺省情况下，关闭邮件内容过滤功能。

开启邮件内容过滤功能之前要先配置ASPF策略，**detect smtp**，**detect tcp**，才能使邮件内容过滤功能生效。有关ASPF配置命令请参见 4.2 状态防火墙配置命令。

【举例】

使能邮件内容过滤功能。

```
[SecBlade_FW] firewall smtp-filter content enable
```

6.2.13 firewall smtp-filter content load-file

【命令】

firewall smtp-filter content load-file *file-name*

undo firewall smtp-filter content load-file

【视图】

系统视图

【参数】

file-name：装载的过滤文件名。

【描述】

firewall smtp-filter content load-file 命令用来装载邮件内容过滤文件，**undo firewall smtp-filter content load-file** 命令用来卸载邮件内容过滤文件。

如果要使邮件内容过滤文件中的条目生效并对内容进行过滤，必须将其装载。

【举例】

装载名为 subjectfilter 的邮件地址过滤文件。

```
[SecBlade_FW] firewall smtp-filter content load-file contentfilter
```

6.2.14 firewall smtp-filter content save-file

【命令】

firewall smtp-filter content save-file *file-name*

【视图】

系统视图

【参数】

file-name：保存的过滤文件名。

【描述】

firewall smtp-filter content save-file 命令用来保存邮件内容过滤文件。

【举例】

保存名为 contentfilter 的邮件内容过滤文件。

```
[SecBlade_FW] firewall smtp-filter content save-file contentfilter
```

6.2.15 firewall smtp-filter rcptto add

【命令】

firewall smtp-filter rcptto add { **permit** | **deny** } *mail-address*

【视图】

系统视图

【参数】

permit：表示操作行为为允许。

deny：表示操作行为为拒绝。

mail-address：添加的过滤地址。

【描述】

firewall smtp-filter rcptto add 命令用来添加邮件过滤地址，并设置对其的过滤行为。

邮件地址最长允许 255 字节（含 用户名、@符和其后主机名）。电子邮件地址用户名部分要么是完整的用户名称，要么是*，不允许出现用户名称和*同时出现的邮件地址。

邮件地址可以是下面几种格式：

test@163.com：表示该地址需要进行精确匹配

*@163.com：表示只匹配@后面的主机名部分，忽略前面的用户名

@.sina.com：表示将类似 mail.sina.com 和 smtp.sina.com 的主机名都匹配，而不匹配 sina.com 和 smtp.sina.com.cn

不支持以下的地址格式：*@*.*.com.cn、*@news.*.com、*@163.*，即“*”只能出现在@前后。

系统对邮件地址进行检查时，先检查域名部分，找到与当前域名最匹配的一项或几项，然后按照配置的先后顺序对用户名进行检查。当找到一个匹配项后即按照设定的操作进行处理。

缺省情况下，未添加邮件过滤地址。

【举例】

添加允许收件人地址为 163.com 域中的所有地址“*@163.com”的过滤条目。

```
[SecBlade_FW] firewall smtp-filter rcptto add permit *@163.com
```

6.2.16 firewall smtp-filter rcptto clear

【命令】

firewall smtp-filter rcptto clear

【视图】

系统视图

【参数】

无

【描述】

firewall smtp-filter rcptto clear 命令用来清除所有邮件过滤地址条目。

【举例】

清除所有邮件过滤地址条目。

```
[SecBlade_FW] firewall smtp-filter rcptto clear
```

6.2.17 firewall smtp-filter rcptto default

【命令】

firewall smtp-filter rcptto default { **permit** | **deny** }

【视图】

系统视图

【参数】

permit：配置默认过滤操作为允许。

deny：配置默认过滤操作为拒绝。

【描述】

firewall smtp-filter rcptto default 命令用来允许或者拒绝未与管理员配置的邮件地址发生匹配的数据报通过。

缺省情况下，允许未发生匹配的数据报通过。

【举例】

配置默认过滤行为为允许。

```
[SecBlade_FW] firewall smtp-filter rcptto default permit
```

6.2.18 firewall smtp-filter rcptto delete

【命令】

firewall smtp-filter rcptto delete *mail-address*

【视图】

系统视图

【参数】

mail-address：删除的邮件过滤地址。

【描述】

firewall smtp-filter rcptto delete 命令用来删除邮件过滤地址。

【举例】

删除地址为“*@163.com”的过滤条目。

```
[SecBlade_FW] firewall smtp-filter rcptto delete *@163.com
```

6.2.19 firewall smtp-filter rcptto enable

【命令】

firewall smtp-filter rcptto enable

undo firewall smtp-filter rcptto enable

【视图】

系统视图

【参数】

无

【描述】

firewall smtp-filter rcptto enable 命令用来使能邮件地址过滤功能，**undo firewall smtp-filter rcptto enable** 命令用来关闭邮件地址过滤功能。

缺省情况下，关闭邮件地址过滤功能。

开启邮件地址过滤功能之前要先配置ASPF策略，**detect smtp**，**detect tcp**，才能使邮件地址过滤功能生效。有关ASPF配置命令请参见 4.2 状态防火墙配置命令。

【举例】

使能邮件地址过滤功能。

```
[SecBlade_FW] firewall smtp-filter rcptto enable
```

6.2.20 firewall smtp-filter rcptto load-file

【命令】

firewall smtp-filter rcptto load-file *file-name*

undo firewall smtp-filter rcptto load-file

【视图】

系统视图

【参数】

file-name：装载的过滤文件名。

【描述】

firewall smtp-filter rcptto load-file 命令用来装载邮件地址过滤文件，**undo firewall smtp-filter rcptto load-file** 命令用来卸载邮件地址过滤文件。

如果要使邮件地址过滤文件中的条目生效并对地址进行过滤，必须将其装载。

【举例】

装载名为 rcpttofilter 的邮件地址过滤文件。

```
[SecBlade_FW] firewall smtp-filter rcptto load-file rcpttofilter
```

6.2.21 firewall smtp-filter rcptto save-file

【命令】

firewall smtp-filter rcptto save-file *file-name*

【视图】

系统视图

【参数】

file-name：保存的过滤文件名。

【描述】

firewall smtp-filter rcptto save-file 命令用来保存邮件地址过滤文件。

【举例】

保存名为 rcpttofilter 的邮件地址过滤文件。

```
[SecBlade_FW] firewall smtp-filter rcptto save-file rcpttofilter
```

6.2.22 firewall smtp-filter subject add

【命令】

firewall smtp-filter subject add *mail-subject*

【视图】

系统视图

【参数】

mail-subject：添加的过滤主题。

【描述】

firewall smtp-filter subject add 命令用来添加邮件过滤主题。

过滤关键字最长支持 128 个字符。关键字过滤支持模糊查找，即允许向过滤关键字文件中添加带“*”的关键字，“*”表示最少 0 个到最多 2 个任意中文字符或最少 0 个到最多 4 个任意英文字符。为避免“*”带来的误判断，管理员应谨慎添加带“*”的过滤关键字。*只允许出现在关键字的中间。不允许一个关键字中出现两个以上的“*”。过滤词汇文件格式如：test1、te*st2；不允许：te**st、t*es*t。

缺省情况下，未添加过滤主题。

【举例】

添加包含主题“Hi”的过滤条目。

```
[SecBlade_FW] firewall smtp-filter subject add Hi
```

6.2.23 firewall smtp-filter subject clear

【命令】

firewall smtp-filter subject clear

【视图】

系统视图

【参数】

无

【描述】

firewall smtp-filter subject clear 命令用来清除所有过滤主题条目。

【举例】

清除所有过滤主题条目。

```
[SecBlade_FW] firewall smtp-filter subject clear
```

6.2.24 firewall smtp-filter subject delete

【命令】

firewall smtp-filter subject delete *mail-subject*

【视图】

系统视图

【参数】

mail-subject：删除的过滤主题。

【描述】

firewall smtp-filter subject delete 命令用来删除邮件过滤主题。

【举例】

删除主题为“Hi”的过滤条目。

```
[SecBlade_FW] firewall smtp-filter subject delete Hi
```

6.2.25 firewall smtp-filter subject enable

【命令】

firewall smtp-filter subject enable

undo firewall smtp-filter subject enable

【视图】

系统视图

【参数】

无

【描述】

firewall smtp-filter subject enable 命令用来使能邮件主题过滤功能，**undo firewall smtp-filter subject enable** 命令用来关闭邮件主题过滤功能。

当使用邮件主题过滤时，被过滤的邮件的主题长度不能超过 512 个字符。

缺省情况下，关闭邮件主题过滤功能。

开启邮件主题过滤功能之前要先配置ASPF策略，**detect smtp**，**detect tcp**，才能使邮件主题过滤功能生效。有关ASPF配置命令请参见 4.2 状态防火墙配置命令。

【举例】

使能邮件主题过滤功能。

```
[SecBlade_FW] firewall smtp-filter subject enable
```

6.2.26 firewall smtp-filter subject load-file

【命令】

firewall smtp-filter subject load-file *file-name*

undo firewall smtp-filter subject load-file

【视图】

系统视图

【参数】

file-name：装载的过滤文件名。

【描述】

firewall smtp-filter subject load-file 命令用来装载邮件主题过滤文件，**undo firewall smtp-filter subject load-file** 命令用来卸载邮件主题过滤文件。

如果要使邮件主题过滤文件中的条目生效并对主题进行过滤，必须将其装载。

【举例】

装载名为 subjectfilter 的邮件主题过滤文件。

```
[SecBlade_FW] firewall smtp-filter subject load-file subjectfilter
```

6.2.27 firewall smtp-filter subject save-file

【命令】

firewall smtp-filter subject save-file *file-name*

【视图】

系统视图

【参数】

file-name：保存的过滤文件名。

【描述】

firewall smtp-filter subject save-file 命令用来保存邮件主题过滤文件。

【举例】

保存名为 subjectfilter 的邮件主题过滤文件。

```
[SecBlade_FW] firewall smtp-filter subject save-file subjectfilter
```

6.2.28 reset firewall smtp-filter counter

【命令】

reset firewall smtp-filter [**rcptto** | **subject** | **content** | **attach**] **counter**

【视图】

用户视图

【参数】

rcptto：邮件地址过滤。

subject：邮件主题过滤。

content：邮件内容过滤。

attach：邮件附件过滤。

【描述】

reset firewall smtp-filter counter 命令用来清除邮件过滤的统计信息。

【举例】

清除邮件地址过滤的统计信息。

```
<SecBlade_FW> reset firewall smtp-filter rcptto counter
```

第7章 攻击防范配置命令

7.1 攻击防范配置命令

7.1.1 debugging firewall defend

【命令】

debugging firewall defend { **all** | **arp-flood** | **arp-spoofing** | **ip-spoofing** | **land** | **smurf** | **fraggle** | **frag-flood** | **winnuke** | **syn-flood** | **icmp-flood** | **udp-flood** | **icmp-redirect** | **icmp-unreachable** | **ip-sweep** | **port-scan** | **source-route** | **route-record** | **tracert** | **ping-of-death** | **teardrop** | **tcp-flag** | **ip-fragment** | **large-icmp** }

undo debugging firewall defend { **all** | **arp-flood** | **arp-reverse-query** | **arp-spoofing** | **ip-spoofing** | **land** | **smurf** | **fraggle** | **frag-flood** | **winnuke** | **syn-flood** | **icmp-flood** | **udp-flood** | **icmp-redirect** | **icmp-unreachable** | **ip-sweep** | **port-scan** | **source-route** | **route-record** | **tracert** | **ping-of-death** | **teardrop** | **tcp-flag** | **ip-fragment** | **large-icmp** }

【视图】

用户视图

【参数】

各参数：表示启动或关闭指定攻击防范功能的调试开关。

【描述】

debugging firewall defend 命令用来打开攻击防范功能的调试开关，**undo debugging firewall defend** 命令用来关闭攻击防范功能的调试开关。

系统缺省为关闭各攻击防范功能的调试开关。

相关配置可参考命令 **display debugging**。

【举例】

对 SYN Flood 攻击防范功能进行调试。

```
<SecBlade_FW> debugging firewall defend syn-flood
```

7.1.2 display firewall defend flag

【命令】

display firewall defend flag

【视图】

所有视图

【参数】

无

【描述】

display firewall defend flag 命令用来显示 SecBlade 上已启用的攻击防范的类型。

【举例】

显示 SecBlade 采用的攻击防范的类型信息。

```
<SecBlade_FW> display firewall defend flag
The attack defend flag is:
 ip-spoofing        land               smurf              fraggle
 winnuke            icmp-redirect      icmp-unreachable   source-route
 route-record       tracert            ping-of-death      tcp-flag
 ip-fragment        large-icmp         teardrop           ip-sweep
 port-scan          syn-flood          udp-flood          icmp-flood
 arp-spoofing        arp-flood          frag-flood
```

7.1.3 display firewall tcp-proxy session

【命令】

display firewall tcp-proxy session [**zone** *zone-name* **| ip** *ip-address*]

【视图】

所有视图

【参数】

zone *zone-name*：显示指定目的安全区域的 TCP 代理的会话信息。

ip *ip-address*：显示指定目的 IP 地址的 TCP 代理的会话信息。

【描述】

display firewall tcp-proxy session 命令用来显示 TCP 代理的会话信息，若不指定参数，则显示所有的 TCP 代理会话信息。

【举例】

显示所有的 TCP-Proxy 会话信息。

```
<SecBlade_FW> display firewall tcp-proxy session
Firewall Tcp-proxy session table information:
```

```
  Source zone: trust
  Source IP address: 172.16.1.254          Source port: 4638
  Destination zone: untrust
  Destination IP address: 2.2.2.1          Destination port: 80
  State:6

  Source zone: trust
  Source IP address: 172.16.1.254          Source port: 4637
  Destination zone: untrust
  Destination IP address: 2.2.2.2          Destination port: 80
  State:6

  Source zone: trust
  Source IP address: 172.16.1.254          Source port: 4635
  Destination zone: DMZ
  Destination IP address: 1.1.1.1          Destination port: 80
  State:6
```

显示指定目的安全区域的 TCP-Proxy 会话信息。

```
<SecBlade_FW> display firewall tcp-proxy session zone untrust
Firewall Tcp-proxy session table information for destination zone trust:

  Source zone: trust
  Source IP address: 172.16.1.254          Source port: 4638
  Destination zone: untrust
  Destination IP address: 2.2.2.1          Destination port: 80
  State:6

  Source zone: trust
  Source IP address: 172.16.1.254          Source port: 4637
  Destination zone: untrust
  Destination IP address: 2.2.2.2          Destination port: 80
  State:6
```

显示指定目的 IP 的 TCP-Proxy 会话信息。

```
<SecBlade_FW> display firewall tcp-proxy session ip 2.2.2.1
Firewall Tcp-proxy session table information for destination IP 2.2.2.1:

  Source zone: trust
  Source IP address: 172.16.1.254          Source port: 4638
  Destination zone: untrust
  Destination IP address: 2.2.2.1          Destination port: 80
```

```
State:6
```

表7-1 display firewall tcp-proxy session 命令显示信息描述表

字段	描述
SrcZone	源安全区域名
SrcIP	源 IP 地址
SrcPort	源端口号
DestZone	目的安全区域名
DestIP	目的 IP 地址
DestPort	目的端口号
State	TCP-Proxy 会话状态值

7.1.4 firewall defend all

【命令】

firewall defend all

undo firewall defend all

【视图】

系统视图

【参数】

无

【描述】

firewall defend all 命令用来打开所有的攻击防范功能，**undo firewall defend all** 命令用来关闭所有的攻击防范功能。

缺省情况下，关闭任何攻击防范功能。

【举例】

打开所有攻击防范功能。

```
[SecBlade_FW] firewall defend all
```

7.1.5 firewall defend arp-flood

【命令】

firewall defend arp-flood [**max-rate** *rate-number*]

undo firewall defend arp-flood [**max-rate**]

【视图】

系统视图

【参数】

max-rate *rate-number*：设定收到的 ARP 包速率的阈值，即一秒钟出现 ARP 包的总数，超过该阈值将视为攻击，*rate-number* 的默认值为 100 包/秒，取值范围为 1～1,000,000 包/秒。

【描述】

firewall defend arp-flood 命令用来打开 ARP Flood 攻击防范功能开关，**undo firewall defend arp-flood** 命令用来关闭 ARP Flood 攻击防范功能开关。

缺省情况下，关闭 ARP Flood 攻击防范功能开关。

【举例】

打开 ARP Flood 攻击防范功能开关。

```
[SecBlade_FW] firewall defend arp-flood
```

7.1.6 firewall defend arp-spoofing

【命令】

firewall defend arp-spoofing [**loose**]

undo firewall defend arp-spoofing [**loose**]

【视图】

系统视图

【参数】

loose：使用宽松检测模式。

【描述】

firewall defend arp-spoofing 命令用来打开 ARP 欺骗攻击防范功能，并使用非宽松检测模式；**firewall defend arp-spoofing loose** 命令用来打开 ARP 欺骗攻击防范功能，并使用宽松检测模式。

undo firewall defend arp-spoofing 命令用来关闭 ARP 欺骗攻击防范功能；**undo firewall defend arp-spoofing loose** 命令用来取消宽松检测，使用非宽松检测模式。

ARP 欺骗攻击防范有两种模式，一种为宽松检测模式，一种为非宽松检测模式。当使用非宽松检测（即不配置 **loose** 选项）时，防火墙会将目的 MAC 地址为单播地

址的 ARP 请求视为攻击报文，并将其丢弃。若使用宽松检测（即配置 **loose** 选项），目的 MAC 地址为单播地址的 ARP 请求不被视为攻击报文，且不进行丢弃。

缺省情况下，关闭 ARP 欺骗攻击防范功能。

【举例】

打开 ARP 欺骗攻击防范功能，并使用非宽松检测模式。

```
[SecBlade_FW] firewall defend arp-spoofing
```

7.1.7 firewall defend fraggle

【命令】

firewall defend fraggle

undo firewall defend fraggle

【视图】

系统视图

【参数】

无

【描述】

firewall defend fraggle 命令用来打开 Fraggle 攻击防范功能开关，**undo firewall defend fraggle** 命令用来关闭 Fraggle 攻击防范功能开关。

系统缺省为关闭 Fraggle 攻击防范功能开关。

【举例】

打开 Fraggle 攻击防范功能开关。

```
[SecBlade_FW] firewall defend fraggle
```

7.1.8 firewall defend frag-flood

【命令】

firewall defend frag-flood [**max-identical-rate** *max-identical-rate*] [**max-total-rate** *max-total-rate*]

undo firewall defend frag-flood [**max-identical-rate**] [**max-total-rate**]

【视图】

系统视图

【参数】

max-identical-rate：最大相同分片报文速率，范围为 1～10,000，缺省值为 50。

max-total-rate：最大分片报文速率，范围为 1～10,000，缺省值为 100。

【描述】

firewall defend frag-flood 命令用来打开 Frag Flood 攻击防范功能，**undo firewall defend frag-flood** 命令用来关闭 Frag Flood 攻击防范功能。

对于目的地为防火墙自身的分片报文攻击，防火墙只告警，但不丢弃报文。否则，防火墙将告警，并丢弃报文。

缺省情况下，关闭 Frag Flood 攻击防范功能。

【举例】

打开 Frag Flood 攻击防范功能。

```
[SecBlade_FW] firewall defend frag-flood
```

7.1.9 firewall defend icmp-flood

【命令】

firewall defend icmp-flood { **ip** *ip-address* | **zone** *zone-name* } [**max-rate** *rate-number*]

undo firewall defend icmp-flood [**ip** [*ip-address* [**max-rate**]] | **zone** [*zone-name* [**max-rate**]]]

【视图】

系统视图

【参数】

ip *ip-address*：设定受保护的主机 IP 地址。如果 undo 形式只列出 **ip** 而不指定具体 *ip-address*，则关闭对所有已配置了 IP 保护的主机进行 ICMP Flood 检测。

zone *zone-name*：设定受保护的安全区域名，此参数表示对安全区域内的所有 IP 地址使能 ICMP Flood 攻击检测功能。如果 undo 形式只列出 **zone** 而不指定具体安全区域名 *zone-name*，则关闭对所有已配置了保护的安全区域进行 ICMP Flood 检测。

max-rate *rate-number*：设定连接特定目的 IP 的 ICMP 包速率的阈值，即一秒钟出现 ICMP 包的总数，超过该阈值将视为攻击。*rate-number* 的默认值为 1000 包/秒，取值范围为 1～1,000,000 包/秒。

【描述】

firewall defend icmp-flood 命令用来使能 ICMP Flood 攻击检测功能，该命令可选择对指定 IP 或指定安全区域进行保护； **undo firewall defend icmp-flood** 命令用来关闭 ICMP Flood 攻击检测功能。

ICMP Flood 的 IP 配置的优先级比安全区域配置的优先级高。如果对特定 IP 配置开启 ICMP Flood 攻击防范功能，同时也对该 IP 所在的安全区域内的所有 IP 配置开启了防范功能，则该 IP 的各检测参数以 IP 配置为准；若此时取消 IP 配置，则该 IP 的各检测参数以安全区域配置为准。

系统缺省为关闭 ICMP Flood 攻击检测功能。

除使用命令 **firewall defend icmp-flood** 外，使能 ICMP Flood 攻击检测功能还需使用命令 **firewall defend icmp-flood enable** 打开全局开关，并开启受保护 IP 或安全区域入方向的 IP 统计功能。

【举例】

打开对 Trust 安全区域内的所有 IP 进行 ICMP Flood 攻击检测的开关，设定 ICMP 包连接速率的阈值为 500 包/秒。

```
[SecBlade_FW] firewall defend icmp-flood zone trust max-rate 500
```

7.1.10 firewall defend icmp-flood enable

【命令】

firewall defend icmp-flood enable

undo firewall defend icmp-flood enable

【视图】

系统视图

【参数】

无

【描述】

firewall defend icmp-flood enable 命令用来打开 ICMP Flood 攻击检测功能；**undo firewall defend icmp-flood enable** 命令用来关闭 ICMP Flood 攻击检测功能。

系统缺省为关闭 ICMP Flood 攻击检测功能。

【举例】

打开 ICMP Flood 攻击检测功能。

```
[SecBlade_FW] firewall defend icmp-flood enable
```

7.1.11 firewall defend icmp-redirect

【命令】

firewall defend icmp-redirect

undo firewall defend icmp-redirect

【视图】

系统视图

【参数】

无

【描述】

firewall defend icmp-redirect 命令用来打开 ICMP 重定向报文攻击防范功能，**undo firewall defend icmp-redirect** 命令用来关闭 ICMP 重定向报文攻击防范功能。

系统缺省为关闭 ICMP 重定向报文攻击防范功能。

【举例】

打开 ICMP 重定向报文攻击防范功能开关。

```
[SecBlade_FW] firewall defend icmp-redirect
```

7.1.12 firewall defend icmp-unreachable

【命令】

firewall defend icmp-unreachable

undo firewall defend icmp- unreachable

【视图】

系统视图

【参数】

无

【描述】

firewall defend icmp-unreachable 命令用来打开 ICMP 不可达报文攻击防范功能开关，**undo firewall defend icmp-unreachable** 命令用来关闭 ICMP 不可达报文攻击防范功能开关。

系统缺省为关闭 ICMP 不可达报文攻击防范功能开关。

【举例】

打开 ICMP 不可达报文攻击防范功能开关。

```
[SecBlade_FW] firewall defend icmp-unreachable
```

7.1.13 firewall defend ip-fragment

【命令】

firewall defend ip-fragment

undo firewall defend ip-fragment

【视图】

系统视图

【参数】

无

【描述】

firewall defend ip-fragment 命令用来打开 IP 分片报文检测功能开关，**undo firewall defend ip-fragment** 命令用来关闭 IP 分片报文检测功能开关。

系统缺省为关闭 IP 分片报文检测功能开关。

【举例】

打开 IP 分片报文检测功能开关。

```
[SecBlade_FW] firewall defend ip-fragment
```

7.1.14 firewall defend ip-spoofing

【命令】

firewall defend ip-spoofing

undo firewall defend ip-spoofing

【视图】

系统视图

【参数】

无

【描述】

firewall defend ip-spoofing 命令用来打开 IP 欺骗防范功能开关，**undo firewall defend ip-spoofing** 命令用来关闭 IP 欺骗防范功能开关。

系统缺省为关闭 IP 欺骗防范功能开关。

📖 **说明：**

IP 欺骗攻击防范功能不能在透明模式下应用。

【举例】

打开 IP 欺骗防范功能开关。

```
[SecBlade_FW] firewall defend ip-spoofing
```

7.1.15 firewall defend ip-sweep

【命令】

firewall defend ip-sweep [**max-rate** *rate-number*] [**blacklist-timeout** *minutes*]

undo firewall defend ip-sweep

【视图】

系统视图

【参数】

max-rate *rate-number*：设定从同一源地址向外发送报文的目的地址变化速率的阈值。*rate-number* 默认值为 4000 次/秒，取值范围为 1～10,000 次/秒。

blacklist-timeout *minutes*：将攻击源 IP 加入黑名单并设定其在黑名单内的保持时间，*minutes* 取值范围为 0～1000 分钟，默认值为 0，表示不加入黑名单。

【描述】

firewall defend ip-sweep 命令用来打开地址扫描攻击防范功能开关，**undo firewall defend ip-sweep** 命令用来关闭地址扫描攻击防范功能开关。

加入黑名单的老化时间应该大于防火墙会话的超时时间（使用命令 **firewall session aging-time** 设置），否则会导致攻击通过 SecBlade。必须使能防火墙的黑名单功能后，此命令设置的黑名单功能才能生效。

缺省情况下为关闭地址扫描攻击防范功能开关。

此命令只有在配置了相关源 IP 或安全区域出方向的 IP 统计功能才起作用。

相关配置命令请参考 **firewall blacklist**。

【举例】

打开地址扫描攻击防范功能开关，设定扫描速率的阈值为 1000，加入黑名单的时间为 5 分钟，并使能黑名单功能。

```
[SecBlade_FW] firewall defend ip-sweep max-rate 1000 blacklist-timeout 5
[SecBlade_FW] firewall blacklist enable
```

7.1.16 firewall defend land

【命令】

firewall defend land

undo firewall defend land

【视图】

系统视图

【参数】

无

【描述】

firewall defend land 命令用来打开 Land 攻击防范功能开关，**undo firewall defend land** 命令用来关闭 Land 攻击防范功能开关。

系统缺省为关闭 Land 攻击防范功能开关。

【举例】

打开 Land 攻击防范功能开关。

```
[SecBlade_FW] firewall defend land
```

7.1.17 firewall defend large-icmp

【命令】

firewall defend large-icmp [*length*]

undo firewall defend large-icmp

【视图】

系统视图

【参数】

length：允许通过的 ICMP 报文的最大长度，*length* 的默认值为 4000 字节，取值范围为 28～65535 字节。

【描述】

firewall defend large-icmp 命令用来打开超大 ICMP 报文攻击检测功能开关，**undo firewall defend large-icmp** 命令用来关闭超大 ICMP 报文攻击检测功能开关。

系统缺省为关闭超大 ICMP 报文攻击检测功能开关。

【举例】

打开超大 ICMP 报文攻击检测功能开关，设定允许报文长度小于 4000 字节的 ICMP 报文通过。

```
[SecBlade_FW] firewall defend large-icmp 4000
```

7.1.18 firewall defend ping-of-death

【命令】

firewall defend ping-of-death

undo firewall defend ping-of-death

【视图】

系统视图

【参数】

无

【描述】

firewall defend ping-of-death 命令用来打开 ping-of-death 攻击检测功能开关，**undo firewall defend ping-of-death** 命令用来关闭 ping-of-death 攻击检测功能开关。

系统缺省为关闭 ping-of-death 攻击检测功能开关。

【举例】

打开 ping-of-death 攻击检测功能开关。

```
[SecBlade_FW] firewall defend ping-of-death
```

7.1.19 firewall defend port-scan

【命令】

firewall defend port-scan [**max-rate** *rate-number*] [**blacklist-timeout** *minutes*]

undo firewall defend port-scan

【视图】

系统视图

【参数】

max-rate *rate-number*：设定从同一源地址向外发送报文的目的端口变化速率的阈值。*rate-number* 默认值为 4000 次/秒，取值范围为 1～10,000 次/秒。

blacklist-timeout *minutes*：将攻击源 IP 加入黑名单并设定其在黑名单内的保持时间，*minutes* 取值范围为 0～1000 分钟，默认值为 0，表示不加入黑名单。

【描述】

firewall defend port-scan 命令用来打开端口扫描攻击防范功能开关，**undo firewall defend port-scan** 命令用来关闭端口扫描攻击防范功能开关。

加入黑名单的老化时间应该大于防火墙会话的超时时间（使用命令 **firewall session aging-time** 设置），否则会导致攻击通过 SecBlade，必须使能防火墙的黑名单功能后，此命令设置的黑名单功能才能生效。

缺省情况下为关闭端口扫描攻击防范功能开关。

此命令只有在配置了相关源 IP 或安全区域出方向的 IP 统计功能后才起作用。

相关配置命令请参考 **firewall blacklist**。

【举例】

打开端口扫描攻击防范功能开关，设定扫描速率的阈值为 1000，加入黑名单的时间为 5 分钟，并使能黑名单功能。

```
[SecBlade_FW] firewall defend port-scan max-rate 1000 blacklist-timeout 5
[SecBlade_FW] firewall blacklist enable
```

7.1.20 firewall defend route-record

【命令】

firewall defend route-record

undo firewall defend route-record

【视图】

系统视图

【参数】

无

【描述】

firewall defend route-record 命令用来打开带路由记录选项报文攻击防范功能开关，**undo firewall defend route-record** 命令用来关闭带路由记录选项报文攻击防范功能开关。

系统缺省为关闭带路由记录选项报文攻击防范功能开关。

【举例】

打开带路由记录选项报文攻击防范功能开关。

```
[SecBlade_FW] firewall defend route-record
```

7.1.21 firewall defend smurf

【命令】

firewall defend smurf

undo firewall defend smurf

【视图】

系统视图

【参数】

无

【描述】

firewall defend smurf 命令用来打开 Smurf 攻击防范功能开关，**undo firewall defend smurf** 命令用来关闭 Smurf 攻击防范功能开关。

系统缺省为关闭 Smurf 攻击防范功能开关。

【举例】

打开 Smurf 攻击防范功能开关。

```
[SecBlade_FW] firewall defend smurf
```

7.1.22 firewall defend source-route

【命令】

firewall defend source-route

undo firewall defend source-route

【视图】

系统视图

【参数】

无

【描述】

firewall defend source-route 命令用来打开带源路由选项报文攻击防范功能开关，**undo firewall defend source-route** 命令用来关闭带源路由选项报文攻击防范功能开关。

系统缺省为关闭带源路由选项报文攻击防范功能开关。

【举例】

打开带源路由选项报文攻击防范功能开关。

```
[SecBlade_FW] firewall defend source-route
```

7.1.23 firewall defend syn-flood

【命令】

firewall defend syn-flood { **ip** *ip-address* | **zone** *zone-name* } [**max-rate** *rate-number*] [**tcp-proxy**]

undo firewall defend syn-flood [**ip** [*ip-address*] [**max-rate**] [**tcp-proxy**]] | **zone** [*zone-name* [**max-rate**] [**tcp-proxy**]]]

【视图】

系统视图

【参数】

ip *ip-address*：设定受保护的主机 IP 地址。如果 undo 形式只列出 **ip** 而不指定具体 *ip-address*，则关闭对所有已配置了 IP 保护的主机进行 SYN Flood 检测。

zone *zone-name*：设定受保护的安全区域名，此参数表示对安全区域内的所有 IP 地址使能 SYN Flood 攻击检测功能。如果 undo 形式只列出 **zone** 而不指定具体安全区域名 *zone-name*，则关闭对所有已配置了保护的安全区域进行 SYN Flood 检测。

max-rate *rate-number*：设定连接特定目的 IP 的 SYN 包速率的阈值，即一秒钟出现 SYN 包的总数，超过该阈值将视为攻击，*rate-number* 的默认值为 1000 包/秒，取值范围为 1～1,000,000 包/秒。

tcp-proxy：启动 TCP 代理。当检测到受保护主机受到 SYN Flood 攻击时，TCP 代理自动启动；当不再受到攻击时，TCP 代理自动关闭。

【描述】

firewall defend syn-flood 命令用来使能 SYN Flood 攻击检测功能，该命令可选择对指定 IP 或指定安全区域进行保护；**undo firewall defend syn-flood** 命令用来关闭 SYN Flood 攻击检测功能。

SYN Flood 的 IP 配置的优先级比安全区域配置的优先级高。如果对特定 IP 配置开启 SYN Flood 攻击防范功能，同时也对该 IP 所在的安全区域内的所有 IP 配置开启了防范功能，则该 IP 的各检测参数以 IP 配置为准；若此时取消 IP 配置，则该 IP 的各检测参数以安全区域配置为准。

若要对 SYN Flood 攻击进行防范，则必须配置 TCP 代理。

系统缺省为关闭 SYN Flood 攻击检测功能。

除使用命令 **firewall defend syn-flood** 外，使能 SYN Flood 攻击检测功能还需使用命令 **firewall defend syn-flood enable** 打开全局开关，并开启受保护 IP 或安全区域入方向的 IP 统计功能。

【举例】

打开对 Trust 安全区域内所有 IP 的进行 SYN Flood 攻击检测的开关，设定 SYN 包连接速率的阈值为 100 包/秒，并启动 TCP 代理功能。

```
[SecBlade_FW] firewall defend syn-flood zone trust max-rate 100 tcp-proxy
```

7.1.24 firewall defend syn-flood enable

【命令】

firewall defend syn-flood enable

undo firewall defend syn-flood enable

【视图】

系统视图

【参数】

无

【描述】

firewall defend syn-flood enable 命令用来打开 SYN Flood 攻击检测功能的全局开关，**undo firewall defend syn-flood enable** 命令用来关闭 SYN Flood 攻击检测功能的全局开关。

系统缺省为关闭 SYN Flood 攻击检测功能的全局开关。

【举例】

打开 SYN Flood 攻击检测功能的全局开关。

```
[SecBlade_FW] firewall defend syn-flood enable
```

7.1.25 firewall defend tcp-flag

【命令】

firewall defend tcp-flag

undo firewall defend tcp-flag

【视图】

系统视图

【参数】

无

【描述】

firewall defend tcp-flag 命令用来打开 TCP 报文标志合法性检测功能开关，**undo firewall defend tcp-flag** 命令用来关闭 TCP 报文标志合法性检测功能开关。

系统缺省为关闭 TCP 报文标志合法性检测功能开关。

【举例】

打开 TCP 报文标志合法性检测功能开关。

```
[SecBlade_FW] firewall defend tcp-flag
```

7.1.26 firewall defend teardrop

【命令】

firewall defend teardrop

undo firewall defend teardrop

【视图】

系统视图

【参数】

无

【描述】

firewall defend teardrop 命令用来打开 teardrop 攻击检测功能开关，**undo firewall defend teardrop** 命令用来关闭 teardrop 攻击检测功能开关。

系统缺省为关闭 teardrop 攻击检测功能开关。

【举例】

打开 teardrop 攻击检测功能开关。

```
[SecBlade_FW] firewall defend teardrop
```

7.1.27 firewall defend tracert

【命令】

firewall defend tracert

undo firewall defend tracert

【视图】

系统视图

【参数】

无

【描述】

firewall defend tracert 命令用来打开 tracert 报文攻击防范功能开关，**undo firewall defend tracert** 命令用来关闭 tracert 报文攻击防范功能开关。

系统缺省为关闭 tracert 报文攻击防范功能开关。

【举例】

打开 tracert 报文攻击防范功能开关。

```
[SecBlade_FW] firewall defend tracert
```

7.1.28 firewall defend udp-flood

【命令】

firewall defend udp-flood { **ip** *ip-address* | **zone** *zone-name* } [**max-rate** *rate-number*]

undo firewall defend udp-flood [**ip** [*ip-address* [**max-rate**]] | **zone** [*zone-name* [**max-rate**]]]

【视图】

系统视图

【参数】

ip *ip-address*：设定受保护的主机 IP 地址。如果 undo 形式只列出 **ip** 而不指定具体 *ip-address*，则关闭对所有已配置了 IP 保护的主机进行 UDP Flood 检测。

zone *zone-name*：设定受保护的安全区域名，此参数表示对安全区域内的所有 IP 地址使能 UDP Flood 攻击检测功能。如果 undo 形式只列出 **zone** 而不指定具体安全区域名 *zone-name*，则关闭对所有已配置了保护的安全区域进行 UDP Flood 检测。

max-rate *rate-number*：设定连接特定目的 IP 的 UDP 包速率的阈值，即一秒钟出现 UDP 包的总数，超过该阈值将视为攻击，*rate-number* 的默认值为 1000 包/秒，取值范围为 1～1,000,000 包/秒。

【描述】

firewall defend udp-flood 命令用来使能 UDP Flood 攻击检测功能，该命令可选择对指定 IP 或指定安全区域进行保护，**undo firewall defend udp-flood** 命令用来关闭 UDP Flood 攻击检测功能。

UDP Flood 的 IP 配置的优先级比安全区域配置的优先级高。如果对特定 IP 配置开启 UDP Flood 攻击防范功能，同时也对该 IP 所在的安全区域内的所有 IP 配置开启了防范功能，则该 IP 的各检测参数以 IP 配置为准；若此时取消 IP 配置，则该 IP 的各检测参数以安全区域配置为准。

系统缺省为关闭 UDP Flood 攻击检测功能。

除使用命令 **firewall defend udp-flood** 外，使能 UDP Flood 攻击检测功能还需使用命令 **firewall defend udp-flood enable** 打开全局开关，并开启受保护 IP 或安全区域入方向的 IP 统计功能。

【举例】

打开对 Trust 安全区域内的所有 IP 进行 UDP Flood 攻击检测的开关，设定 UDP 包连接速率的阈值为 500 包/秒。

```
[SecBlade_FW] firewall defend udp-flood zone trust max-rate 500
```

7.1.29 firewall defend udp-flood enable

【命令】

firewall defend udp-flood enable

undo firewall defend udp-flood enable

【视图】

系统视图

【参数】

无

【描述】

firewall defend udp-flood enable 命令用来打开 UDP Flood 攻击检测功能的全局开关；**undo firewall defend udp-flood enable** 命令用来关闭 UDP Flood 攻击检测功能的全局开关。

系统缺省为关闭 UDP Flood 攻击检测功能的全局开关。

【举例】

打开 UDP Flood 攻击检测功能的全局开关。

```
[SecBlade_FW] firewall defend udp-flood enable
```

7.1.30 firewall defend winnuke

【命令】

firewall defend winnuke

undo firewall defend winnuke

【视图】

系统视图

【参数】

无

【描述】

firewall defend winnuke 命令用来打开 WinNuke 攻击防范功能开关，**undo firewall defend winnuke** 命令用来关闭 WinNuke 攻击防范功能开关。

系统缺省为关闭 WinNuke 攻击防范功能开关。

【举例】

打开 WinNuke 攻击防范功能开关。

```
[SecBlade_FW] firewall defend winnuke
```

7.1.31 firewall tcp-proxy

【命令】

firewall tcp-proxy { **ip** *ip-address* | **zone** *zone-name* }

undo firewall tcp-proxy { **ip** *ip-address* | **zone** *zone-name* }

【视图】

系统视图

【参数】

ip *ip-address*：设定受保护的主机 IP 地址。

zone *zone-name*：设定受保护的安全区域名。

【描述】

firewall tcp-proxy 命令用来配置为特定主机或安全区域启用 TCP 代理，**undo firewall tcp-proxy** 命令用来配置为特定主机或安全区域关闭 TCP 代理。

缺省情况下，未对任何 IP 地址或安全区域启用 TCP 代理。

🕮 **说明：**

如果在配置 SYN Flood 攻击时也启用了 TCP 代理（参见命令 **firewall defend syn-flood**），则在此处的配置优先于 SYN Flood 攻击中的配置，即无论是否受到 SYN Flood 攻击，都启用 TCP 代理，对目的主机或目的安全区域进行保护。

【举例】

为 Trust 区域中的所有主机启用 TCP 代理。

```
[SecBlade_FW] firewall tcp-proxy zone trust
```

第8章 IDS 联动配置命令

8.1 IDS 联动配置命令

8.1.1 Ids-acl enable

【命令】

ids-acl enable

undo ids-acl enable

【视图】

接口视图

【参数】

无

【描述】

ids-acl enable 命令用来允许在接口下发 IDS 联动的 ACL 规则，**undo ids-acl enable** 命令用来取消在接口下发 IDSl 联动的 ACL 规则。

缺省情况下，不在任何接口下发 IDS 联动规则。

【举例】

在接口 GigabitEthernet 0/0 下发 IDS 联动的 ACL 规则。

```
[SecBlade_FW] interface GigabitEthernet 0/0
[SecBlade_FW-GigabitEthernet0/0] ids-acl enable
```

8.1.2 display ids

【命令】

display ids { **all** | **controlled-interface** | **name** *name* | **source** *ip-addr* | **destination** *ip-addr* }

【视图】

所有视图

【参数】

all：显示所有 IDS 联动信息内容。

controled-interface：显示当前使能 IDS 联动的 ACL 规则下发的接口列表。

name *name*：显示指定名称的 IDS 联动信息。

source *ip-addr*：显示指定源 IP 地址的 IDS 联动信息。

destination *ip-addr*：显示指定目的 IP 地址的 IDS 联动信息。

【描述】

display ids 命令用来显示 IDS 联动信息。

【举例】

显示所有 IDS 联动信息。

```
<SecBlade_FW> display ids all
Port list under IDS control is:
      GigabitEthernet0/0
Number of items 4, running items 4
ACL rules created by IDS is:
    1   Name 00000000000000000000000000001111
        Action deny,  time 12000,  curtime 11740
        Smac any,  sip 1.1.1.1,  swild 255.255.255.255,  sport 1234,  prot 6
        Dmac any,  dip 2.2.2.2,  dwild 255.255.255.255,  dport 444,  prot 6
        Interface(s) all, direction all
    2   Name 00000000000000000000000000001112
        Action deny,  time 12000,  curtime 11790
        Smac any,  sip any,  swild 0.0.0.0,  sport 0,  prot any
        Dmac any,  dip any,  dwild 0.0.0.0,  dport 0,  prot any
        Interface(s) all, direction inbound
    3   Name 00000000000000000000000000001113
        Action deny,  time 12000,  curtime 11820
        Smac any,  sip 5.5.5.5,  swild 255.255.255.255,  sport 0,  prot any
        Dmac any,  dip any,  dwild 0.0.0.0,  dport 0,  prot any
        Interface(s) all, direction all
    4   Name 00000000000000000000000000001114
        Action deny,  time 12000,  curtime 11860
        Smac any,  sip 3.3.3.3,  swild 255.255.255.255,  sport 0,  prot 1
        Dmac any,  dip 4.4.4.4,  dwild 255.255.255.255,  dport 0,  prot 1
        Interface(s) all, direction all
Number of items 4, running items 4
```

8.1.3 display ids-acl

【命令】

display ids-acl { **all** | **name** *name* }

【视图】

所有视图

【参数】

all：显示所有 IDS 联动信息生成的 ACL 规则。

name *name*：显示指定名称的 IDS 联动信息生成的 ACL 规则。

【描述】

display ids-acl 命令用来显示 IDS 联动信息生成的 ACL 规则。

【举例】

显示所有 IDS 联动信息生成 ACL 规则。

```
<SecBlade_FW> dis ids-acl all

(Total ACL number is 7)

Interface: GigabitEthernet0/0
IDS_ACL Direction: InBound
 rule 0 deny tcp source 1.1.1.1 0 source-port eq 1234 destination 2.2.2.2 0
destination-port eq 444 (0 times matched)
 rule 1 deny ip (0 times matched)
 rule 2 deny ip source 5.5.5.5 0 (0 times matched)
 rule 3 deny icmp source 3.3.3.3 0 destination 4.4.4.4 0 (0 times matched)
IDS_ACL Direction: OutBound
 rule 0 deny tcp source 1.1.1.1 0 source-port eq 1234 destination 2.2.2.2 0
destination-port eq 444 (0 times matched)
 rule 1 deny ip source 5.5.5.5 0 (0 times matched)
 rule 2 deny icmp source 3.3.3.3 0 destination 4.4.4.4 0 (0 times matched)
```

8.1.4 debugging ids

【命令】

debugging ids

undo debugging ids

【视图】

用户视图

【参数】

无

【描述】

debugging ids 命令用来打开 IDS 联动功能的调试开关，**undo debugging ids** 命令用来关闭 IDS 联动功能的调试开关。

【举例】

打开 IDS 联动功能的调试开关。

```
<SecBlade_FW> debugging ids
```

第9章 报文统计与日志配置命令

9.1 报文统计配置命令

9.1.1 display firewall statistic

【命令】

display firewall statistic { **system** | **zone** *zone-name* { **inzone** | **outzone** } | **ip** { *ip-address* { **source-ip** | **destination-ip** | **both** } | **which** } }

【视图】

所有视图

【参数】

system：显示防火墙系统的统计信息。

zone *zone-name*：显示安全区域的统计信息。*zone-name* 是安全区域名称，包括 **dmz**、**trust**、**untrust** 和 **local**。

ip *ip-address*：显示 IP 地址的统计信息。*ip-address* 为指定的 IP 地址。

inzone：指定安全区域的入方向的统计信息；

outzone：指定安全区域的出方向的统计信息；

source-ip：源地址表的统计信息；

destination-ip：目的地址表的统计信息。

which：显示 IP 地址。

【描述】

display firewall statistic 命令用来显示通过防火墙模块处理的系统统计信息，或者显示通过防火墙模块处理的基于指定安全区域的入/出方向统计信息，或者显示通过防火墙模块处理的某 IP 地址在源/目的地址表的统计信息。

【举例】

显示系统全局统计信息。

```
<SecBlade_FW> display firewall statistic system
Firewall system statistic information:
       TotalBootCon,             787,  Total connection(s) since last reboot
        CurTotalCon,                4,  Current total connection(s)
       MaxSessSpeed,                9,  Peak session speed(num/s)
```

```
          CurSessSpeed,                0,  Current session speed(num/s)
            CurTcpSess,                2,  Total current TCP session(s)
            CurUdpSess,                2,  Total current UDP session(s)
           CurIcmpSess,                0,  Total current ICMP session(s)
            CurFtpSess,                0,  Current FTP session(s)
           CurHttpSess,                0,  Current Http session(s)
           CurH323Sess,                0,  Current H.323 session(s)
           CurRtspSess,                0,  Current RTSP session(s)
           CurSmtpSess,                0,  Current SMTP session(s)
             CurFrgTbls                0,  Current frag table number
        CurTcpproxySess,               0,  Total current TCP-Proxy session(s)
            RcvSynPkts,              724,  TCP SYN packet(s) received
            RcvFinPkts,              929,  TCP FIN packet(s) received
         RcvSynAckPkts,              578,  TCP SYNACK packet(s) received
            RcvRstPkts,              358,  TCP RST packet(s) received
           RcvIcmpPkts,               10,  Received ICMP packet(s)
           RcvIcmpOcts,              840,  Received ICMP byte(s)
          PassIcmpPkts,               10,  Passed ICMP packet(s)
          PassIcmpOcts,              840,  Passed ICMP byte(s)
            RcvTcpPkts,            11732,  Received TCP packet(s)
            RcvTcpOcts,          3288722,  Received TCP byte(s)
           PassTcpPkts,            11729,  Passed TCP packet(s)
           PassTcpOcts,          3288578,  Passed TCP byte(s)
            RcvUdpPkts,             2675,  Received UDP packet(s)
            RcvUdpOcts,           225437,  Received UDP byte(s)
           PassUdpPkts,             2535,  Passed UDP packet(s)
           PassUdpOcts,           211363,  Passed UDP byte(s)
            RcvEtcPkts,                0,  Received Etc packet(s)
            RcvEtcOcts,                0,  Received Etc byte(s)
           PassEtcPkts,                0,  Passed Etc packet(s)
           PassEtcOcts,                0,  Passed Etc byte(s)
           RcvFragPkts,                0,  Received frag packet(s)
           RcvFragOcts,                0,  Received frag byte(s)
            RcvFtpPkts,                0,  Received FTP packet(s)
            RcvFtpOcts,                0,  Received FTP byte(s)
           RcvSmtpPkts,                0,  Received SMTP packet(s)
           RcvSmtpOcts,                0,  Received SMTP byte(s)
           RcvHttpPkts,             7934,  Received Http packet(s)
           RcvHttpOcts,          3096083,  Received Http byte(s)
           RcvH323Pkts,                0,  Received H.323 packet(s)
           RcvH323Octs,                0,  Received H.323 byte(s)
           RcvRtspPkts,                0,  Received RTSP packet(s)
```

```
          RcvRtspOcts,                0,  Received RTSP byte(s)
          BlsDscdPkts,                0,  Black list discard packet(s)
          BlsDscdOcts,                0,  Black list discard byte(s)
        SessDscdPkts,               0,  Failed session table discard packet(s)
        SessDscdOcts,               0,  Failed session table discard byte(s)
           TotalPkts,           14417,  Received Total packet(s)
           TotalOcts,         3514999,  Received Total byte(s)
```

📖 **说明：**

- 以上显示信息中的报文均是指通过防火墙检测的报文。
- **display firewall statistic** 命令显示的统计信息是指自统计功能使能后的统计信息，不包括统计功能使能前的信息。如 **display firewall statistic system** 命令中显示的 CurTotalCon 表示自系统统计功能使能后的系统连接数，与系统当前的 session 数可能不一致；**display firewall statistic zone trust inzone** 命令中显示的 CurTotalCon 表示自 trust 区域的入域统计功能使能后的该域的连接数。
- **display firewall statistic system** 命令中显示的收到的报文是指防火墙所有安全域出方向的报文总和，包括从本地域发出的报文；该命令中显示的通过的报文是指防火墙所有安全域入方向的报文总和，包括发往本地域的报文。

9.1.2 display firewall statistic system defend

【命令】

display firewall statistic system defend

【视图】

所有视图

【参数】

无

【描述】

display firewall statistic system defend 命令用来显示收到的各种类型攻击的报文数目或攻击次数。

【举例】

显示收到的各种类型攻击的报文数目或攻击次数。

```
<SecBlade_FW> display firewall statistic system defend
  Display firewall defend statistic:
                      IP-spoofing,           7 time(s)
                             Land,           0 time(s)
```

```
                    Smurf,          0 time(s)
                  Fraggle,          0 time(s)
                  Winnuke,          0 time(s)
                 SYN-flood,         0 time(s)
                ICMP-flood,         0 time(s)
                 UDP-flood,         0 time(s)
              ICMP-redirect,        0 time(s)
            ICMP-unreachable,       0 time(s)
                  Tracert,          0 time(s)
                 Tcp-flag,          0 time(s)
              Ping-of-death,        0 time(s)
                 Teardrop,          0 time(s)
               IP-fragment,         0 time(s)
                  IP-sweep,         2 time(s)
                Large-icmp,         0 time(s)
        Source-route attack,        0 time(s)
        Route-record attack,        0 time(s)
               ARP-spoofing,        0 time(s)
                  ARP-flood,        0 time(s)
                 Frag-flood,        0 time(s)
              TCP port-scan,        0 time(s)
              UDP port-scan,        0 time(s)
               Other attack,        0 time(s)
                      total,        9 time(s)
```

9.1.3 display firewall statistic system flow-percent

【命令】

display firewall statistic system flow-percent [**default**]

【视图】

所有视图

【参数】

default：报文流量百分比的缺省值。

【描述】

display firewall statistic system flow-percent 命令用来显示报文流量的百分比信息。

【举例】

显示报文流量百分比信息。

```
<SecBlade_FW> display firewall statistic system flow-percent

  Current tcp percent:   75
  Current udp percent:   15
  Current icmp percent:  5
  Current alternation:   25
  Current time interval: 60 minutes
```

9.1.4 firewall statistic system connect-number

【命令】

firewall statistic system connect-number { **tcp** | **udp** } { **high** *high-value* **low** *low-value* }

undo firewall statistic system connect-number { **tcp** | **udp** }

【视图】

系统视图

【参数】

tcp：TCP 连接。

udp：UDP 连接。

high *high-value*：上限阈值，基于系统的 TCP 和 UDP 连接的上限阈值范围为 1-500000，缺省值为 500000。

low *low-value*：下限阈值，基于系统的 TCP 和 UDP 连接的下限阈值范围为 1-500000，缺省值为 1。

【描述】

firewall statistic system connect-number 命令用来设置基于系统的 TCP 连接和 UDP 连接总数的上限阈值和下限阈值。**undo firewall statistic system connect-number** 命令用来恢复缺省值。

基于系统的连接数阈值没有方向，指的是系统的总的连接数；当连接数大于上限阈值时，表明发生异常情况，输出日志告警，而连接数小于下限阈值时，表明系统恢复正常，也输出日志告警。

注意：**firewall statistic system connect-number** 命令在系统视图下使用，用于配置系统相关的阈值；**statistic connect-number** 命令在安全区域视图下使用，用于配置安全区域或 IP 地址相关的阈值。

【举例】

设置基于系统的 TCP 连接总数的上限阀值是 120000，下限阀值是 60000。

```
[SecBlade_FW] firewall statistic system connect-number tcp high 120000 low
60000
```

9.1.5 firewall statistic system enable

【命令】

firewall statistic system enable

undo firewall statistic system enable

【视图】

系统视图

【参数】

无

【描述】

firewall statistic system enable 命令用来使能全局统计功能，**undo firewall statistic system enable** 命令用来禁止全局统计功能。

缺省情况下为使能。

【举例】

使能全局统计功能。

```
[SecBlade_FW] firewall statistic system enable
```

9.1.6 firewall statistic system flow-percent

【命令】

firewall statistic system flow-percent { **tcp** *tcp-percent* **udp** *udp-percent* **icmp** *icmp-percent* **alteration** *alteration-percent* [**time** *time-value*] }

undo firewall statistic system flow-percent

【视图】

系统视图

【参数】

tcp-percent：TCP 报文所占的百分比比率，取值范围是 0～100，缺省值是 75。

udp-percent：UDP 报文所占的百分比比率，取值范围是 0～100，缺省值是 15。

icmp-percent：ICMP 报文所占的百分比比率，取值范围是 0～100，缺省值是 5。

alteration-percent：各种报文所允许的百分比的变动范围，分别取为各类型报文正常百分比值的百分比，取值范围是 0～25，缺省值是 25。

time-value：进行检测计算的时间周期（单位：分钟），取值范围是 0～6000 分，缺省值是 60 分钟。

【描述】

firewall statistic system flow-percent 命令用来设置不同类型的报文在正常情况下一定时间内所占的百分比以及允许的变动范围，并且进行检测的时间周期可设置。**undo firewall statistic system flow-percent** 命令用来恢复缺省值。

如果某类型（TCP、UDP、ICMP 或其他）报文百分比超过配置的上限阈值（加波动范围）或低于配置的下限阈值（减波动范围），则系统输出日志告警。

此命令 TCP、UDP、ICMP 三种报文所占百分比需要同时被配置，并且三种报文所占百分比之和必须小于或等于 100；如果 TCP、UDP、ICMP 三种报文百分比之和超过 100％，则命令不会生效。

【举例】

配置 TCP、UDP、ICMP 和其它报文分别所占的百分比分别为 50、25、15，允许波动 10%。

```
[SecBlade_FW] firewall statistic system flow-percent tcp 50 udp 25 icmp 15
alteration 10
```

9.1.7 firewall statistic warning-level drop

【命令】

firewall statistic warning-level drop

undo firewall statistic warning-level drop

【视图】

系统视图

【参数】

无

【描述】

firewall statistic warning-level drop 命令用来设置防火墙连接数量和连接速率监控的告警级别为输出告警信息，并丢弃报文。

undo firewall statistic warning-level drop 命令用来设置防火墙连接数量和连接速率监控的告警级别为仅输出告警信息。

告警级别分为两种，一种为“告警”，是指当连接数量和连接速率超过设置的上限阈值时，仅输出告警信息；另一种为“丢弃”，是指当连接数量或连接速率超过设

置的上限阈值时，输出告警信息，并且丢弃后续报文。仅当连接数量或连接速率恢复到设置的下限阈值时，不再丢弃报文。

该命令仅对基于安全区域和 IP 的统计功能有效，对于系统统计功能无效。

缺省情况下，告警级别为仅输出告警信息。

相关配置命令可参考 **statistic connect-number ip**，**statistic connect-number zone**，**statistic connect-speed ip**，**statistic connect-speed zone**。

【举例】

设置告警级别为输出告警信息，并丢弃报文。

```
[SecBlade_FW] firewall statistic warning-level drop
```

9.1.8 reset firewall statistic ip

【命令】

reset firewall statistic ip *ip-address* { **source-ip** | **destination-ip | both** }

【视图】

用户视图

【参数】

ip *ip-address*：清除指定 IP 地址的统计信息。

source-ip：清除源地址表表项。

destination-ip：清除目的地址表表项。

both：清除源地址表和目的地址表表项。

【描述】

reset firewall statistic ip 用来清除源/目的地址表中的统计数据。

如果指定的 IP 地址不存在，则命令无效果。

【举例】

清除指定 IP 地址 1.1.1.1 在源地址表中的统计信息。

```
<SecBlade_FW> reset firewall statistic ip 1.1.1.1 source-ip
```

9.1.9 reset firewall statistic system

【命令】

reset firewall statistic system [**defend** | **current**]

【视图】

用户视图

【参数】

defend：清除攻击防范信息。

current：清除当前连接数。

【描述】

reset firewall statistic system 命令用来清除全局统计信息或全局攻击防范信息。

【举例】

清除全局统计信息。

```
<SecBlade_FW> reset firewall statistic system
```

9.1.10 reset firewall statistic zone

【命令】

reset firewall statistic zone *zone-name* { **inzone** | **outzone** }

【视图】

用户视图

【参数】

zone *zone-name*：清除基于安全区域统计信息，*zone-name* 是指定安全区域的名称。

inzone：安全区域入方向。

outzone：安全区域出方向。

【描述】

reset firewall statistic zone 用来清除当前安全区域的入/出方向的统计数据。

如果指定的安全区域不存在，则命令无效果。

【举例】

清除 Trust 安全区域在出方向的统计信息。

```
<SecBlade_FW> reset firewall statistic zone trust outzone
```

9.1.11 statistic connect-number ip

【命令】

statistic connect-number ip outzone { **tcp** | **udp** } **high** *high-limit* **low** *low-limit*

statistic connect-number id *id* **ip outzone** { **tcp** | **udp** } **high** *high-limit* **low** *low-limit* **acl-number** *acl-number*

undo statistic connect-number [**id** *id*] **ip outzone** { **tcp** | **udp** }

statistic connect-number ip inzone { **tcp** | **udp** } **high** *high-limit* **low** *low-limit*

undo statistic connect-number ip inzone { **tcp** | **udp** }

【视图】

安全区域视图

【参数】

id *id*：规则的编号，范围为 1～99。

ip：基于 IP 的阈值。

inzone：安全区域的入方向。

outzone：安全区域的出方向。

tcp：TCP 连接。

udp：UDP 连接。

high *high-value*：基于 IP 地址的 TCP 和 UDP 连接的上限阈值，范围为 1～500000，缺省值为 500000。

low *low-value*：基于 IP 地址的 TCP 和 UDP 连接的下限阈值，范围为 1～500000，缺省值为 450000。

acl-number *acl-number*：指定基本 ACL 的编号，范围为 2000～2999。通过指定 ACL 可以控制对哪些 IP 地址进行限制。

【描述】

statistic connect-number ip 命令用来设置基于 IP 地址的某一方向上发起的 TCP 连接和 UDP 连接总数的上限阈值和下限阈值。**undo statistic connect-number ip** 命令用来恢复缺省值。

基于 IP 地址的连接数阈值则要根据数据包流向相对安全区域的方向分别进行设置。当连接数量超过设定的阈值上限或恢复到阈值下限时，系统将根据 **firewall statistic warning-level** 命令的设置采取相应操作。

相关配置命令可参考 **firewall statistic warning-level**。

【举例】

设置向 Untrust 安全区域的入方向发起 TCP 连接总数的基于 IP 地址的上限阈值为 5000，下限阈值为 500。

```
[SecBlade_FW-zone-untrust] statistic connect-number ip inzone tcp high 5000 low 500
```

9.1.12 statistic connect-number zone

【命令】

statistic connect-number zone { **inzone** | **outzone** } { **tcp** | **udp** } **high** *high-limit* **low** *low-limit*

undo statistic connect-number zone { **inzone** | **outzone** } { **tcp** | **udp** }

【视图】

安全区域视图

【参数】

zone：基于安全区域的阈值。

inzone：安全区域的入方向。

outzone：安全区域的出方向。

tcp：TCP 连接。

udp：UDP 连接。

high *high-value*：基于安全区域的 TCP 和 UDP 连接的上限阈值，范围为 1～500000，缺省值为 500000。

low *low-value*：基于安全区域的 TCP 和 UDP 连接的下限阈值，范围为 1～500000，缺省值为 450000。

【描述】

statistic connect-number 命令用来设置基于安全区域或者 IP 地址的某一方向上发起的 TCP 连接和 UDP 连接总数的上限阈值和下限阈值。**undo statistic connect-number** 命令用来恢复缺省值。

基于安全区域或 IP 地址的连接数阈值则要根据数据包流向相对安全区域的方向分别进行设置。

当连接数量超过设定的阈值上限或恢复到阈值下限时，系统将根据 **firewall statistic warning-level** 命令的设置采取相应操作。

相关配置命令可参考 **firewall statistic warning-level**。

【举例】

设置 Untrust 安全区域的入方向发起 TCP 连接总数的上限阈值为 25000，下限阈值为 10000。

```
[SecBlade_FW-zone-untrust] statistic connect-number zone inzone tcp high 25000 low 10000
```

9.1.13 statistic connect-speed ip

【命令】

statistic connect-speed ip outzone { **tcp** | **udp** } **high** *high-limit* **low** *low-limit*

statistic connect-speed id *id* **ip outzone** { **tcp** | **udp** } **high** *high-limit* **low** *low-limit* **acl-number** *acl-number*

undo statistic connect-speed [**id** *id*] **ip outzone** { **tcp** | **udp** }

statistic connect-speed ip inzone { **tcp** | **udp** } **high** *high-limit* **low** *low-limit*

undo statistic connect-speed ip inzone { **tcp** | **udp** }

【视图】

安全区域视图

【参数】

id *id*：规则的编号，范围为 1～99。

ip：基于 IP 的阈值。

inzone：安全区域的入方向。

outzone：安全区域的出方向。

tcp：TCP 连接。

udp：UDP 连接。

high *high-value*：基于 IP 地址的 TCP 和 UDP 连接速率的上限阈值，范围为 1～10000，缺省值为 10000。

low *low-value*：基于 IP 地址的 TCP 和 UDP 连接速率的下限阈值，范围为 1～10000，缺省值为 9000。

acl-number *acl-number*：指定基本 ACL 的编号，范围为 2000～2999。通过指定 ACL 可以控制对哪些 IP 地址进行限制。

【描述】

statistic connect-speed ip 命令用来设置基于 IP 地址的某一方向上发起的 TCP 连接和 UDP 连接速率（每秒）的上限阈值和下限阈值。**undo statistic connect-speed ip** 命令用来恢复缺省值。

连接速率阈值是数据包相对安全区域的流向，基于 IP 地址来分别设定的。当连接速率超过设定的阈值上限或恢复到阈值下限时，系统将根据 **firewall statistic warning-level** 命令的设置采取相应操作。

相关配置命令可参考 **firewall statistic warning-level**。

【举例】

设置向 Untrust 安全区域的入方向发起 TCP 连接速率的基于 IP 地址的上限阈值为 5000，下限阈值为 500。

```
[SecBlade_FW-zone-untrust] statistic connect-speed ip inzone tcp high 5000 low 500
```

9.1.14 statistic connect-speed zone

【命令】

statistic connect-speed zone { **inzone** | **outzone** } { **tcp** | **udp** } **high** *high-value* **low** *low-value*

undo statistic connect-speed zone { **inzone** | **outzone** } { **tcp** | **udp** }

【视图】

安全区域视图

【参数】

zone：基于安全区域的阈值。

inzone：安全区域的入方向。

outzone：安全区域的出方向。

tcp：TCP 连接。

udp：UDP 连接。

high *high-value*：基于安全区域的 TCP 和 UDP 连接速率的上限阈值，范围为 1～10000，缺省值为 10000。

low *low-value*：基于安全区域的 TCP 和 UDP 连接速率的下限阈值，范围为 1～10000，缺省值为 9000。

【描述】

statistic connect-speed zone 命令用来设置基于安全区域的某一方向上发起的 TCP 连接和 UDP 连接速率（每秒）的上限阈值和下限阈值。**undo statistic connect-speed zone** 命令用来恢复缺省值。

连接速率阈值是数据包相对安全区域的流向，基于安全区域来分别设定的。当连接速率超过设定的阈值上限或恢复到阈值下限时，系统将根据 **firewall statistic warning-level** 命令的设置采取相应操作。

相关配置命令可参考 **firewall statistic warning-level**。

【举例】

设置向 Trust 安全区域的入方向发起 TCP 连接速率（每秒）的基于安全区域的上限阈值为 2500，下限阈值为 1000。

```
[SecBlade_FW-zone-trust] statistic connect-speed zone inzone tcp high 2500 low 1000
```

9.1.15 statistic enable

【命令】

statistic enable { **ip** | **zone** } { **inzone** | **outzone** }

undo statistic enable { **ip** | **zone** } { **inzone** | **outzone** }

【视图】

安全区域视图

【参数】

inzone：基于安全区域或基于 IP 统计入方向数据包，入方向数据包是指目的地址为本安全区域的数据包。如果基于 IP 进行统计，则数据包只根据目的地址进行统计。

outzone：基于安全区域或基于 IP 统计出方向数据包，出方向数据包是指源地址为本安全区域的数据包。如果基于 IP 进行统计，则数据包只根据源地址进行统计。

【描述】

statistic enable 命令用来使能基于安全区域和 IP 的统计功能，**undo statistic enable** 命令用来禁止基于安全区域和 IP 的统计功能。

缺省情况下为禁止。

【举例】

在 Trust 安全区域上配置基于 IP 地址的统计功能，对入安全区域方向数据包进行统计（只统计其目的地址）。

```
[SecBlade_FW-zone-trust] statistic enable ip inzone
```

在 Untrust 安全区域上配置基于安全区域的统计功能，对出安全区域方向数据包进行统计。

```
[SecBlade_FW-zone-trust] statistic enable zone outzone
```

9.2 SMTP 客户端配置命令

9.2.1 debugging smtpc

【命令】

debugging smtpc

undo debugging smtpc

【视图】

用户视图

【参数】

无

【描述】

debugging smtpc 命令用来打开 SMTP 客户端的调试开关，**undo debugging smtpc** 命令用来关闭 SMTP 客户端的调试开关。

缺省情况下，关闭 SMTP 客户端的调试开关。

【举例】

打开 SMTP 客户端的调试开关。

```
<SecBlade_FW> debugging smtpc
  The debug switch for smtp client opened.
```

9.2.2 display smtpc

【命令】

display smtpc [**administrator** | **trigger**]

【视图】

所有视图

【参数】

administrator：显示邮件收件人信息。

trigger：显示邮件触发时间信息。

【描述】

display smtpc 命令用来显示 SMTP 客户端的配置信息。

【举例】

显示邮件的收件人信息。

```
<SecBlade_FW> display smtpc administrator
  The following mail address configured:
         administrator@secpath.com
         admin@ms.com
```

显示邮件触发时间信息。

```
<SecBlade_FW> display smtpc trigger
  The following trigger time configured:

         10:30   12:00   15:15   17:30
```

9.2.3 smtpc administrator mail

【命令】

smtpc administrator mail *mail-address*

undo smtpc administrator { **all** | **mail** *mail-address* }

【视图】

系统视图

【参数】

mail-address：邮件的收件人地址。

all：所有收件人地址。

【描述】

smtpc administrator mail 命令用来配置邮件的收件人地址，**undo smtpc administrator** 命令用来删除邮件的收件人地址。

添加的收件人地址必须符合 SMTP 邮件地址的格式。通过多次执行此命令，可以添加多个收件人地址，最多可配置 5 个。

缺省情况下，未配置邮件的收件人地址。

【举例】

添加邮件的收件人地址 administrator@secpath.com

```
[SecBlade_FW] smtpc administrator mail administrator@secpath.com
  The mail address administrator@secpath.com has been added.
```

9.2.4 smtpc trigger time

【命令】

smtpc trigger time *hh:mm*

undo smtpc trigger { **all** | **time** *hh:mm* }

【视图】

系统视图

【参数】

hh:mm：定时邮件的触发时间，范围为 00:00～23:59。

all：所有已配置的触发时间。

【描述】

smtpc trigger time 命令用来配置定时邮件每日的触发时间点，**undo smtpc trigger** 命令用来取消配置的邮件触发时间点。

通过多次执行此命令，可以添加多个触发时间点，最多可配置 5 个。

缺省情况下，未配置邮件的触发时间点。

【举例】

配置在 17:30 发送定时邮件。

```
[SecBlade_FW] smtpc trigger time 17:30
  The trigger time 17:30 has been added.
```

9.3 DNS 客户端配置命令

9.3.1 debugging dnsc

【命令】

debugging dnsc

undo debugging dnsc

【视图】

用户视图

【参数】

无

【描述】

debugging dnsc 命令用来打开 DNS 客户端的调试开关，**undo debugging dnsc** 命令用来关闭 DNS 客户端的调试开关。

缺省情况下，关闭 DNS 客户端的调试开关。

【举例】

打开 DNS 客户端的调试开关。

```
<SecBlade_FW> debugging dnsc
```

9.3.2 display dnsc

【命令】

display dnsc { **server** | **cache** }

【视图】

所有视图

【参数】

server：显示配置的 DNS 服务器。

cache：显示 DNS 缓存条目。

【描述】

display dnsc 命令用来显示 DNS 客户端的配置信息。

【举例】

显示配置的 DNS 服务器。

```
<SecBlade_FW> display dnsc server
  10.1.1.1
  10.1.1.2
  10.1.1.3
  Total 3 dns server configed.
```

9.3.3 dnsc server

【命令】

dnsc server ip *ip-address*

undo dnsc server { **all** | **ip** *ip-address* }

【视图】

系统视图

【参数】

ip *ip-address*：DNS 服务器的 IP 地址。

all：所有 DNS 服务器。

【描述】

dnsc server 命令用来配置 DNS 服务器，**undo dnsc server** 命令用来删除配置的 DNS 服务器。

缺省情况下，未配置 DNS 服务器。

【举例】

配置 DNS 服务器的 IP 地址为 10.1.1.3。

```
[SecBlade_FW] dnsc server ip 10.1.1.3
```

9.3.4 dnsc cache

【命令】

dnsc cache add domain *domain-name* **type** { **a** | **mx** } **ip** *ip-address* **ttl** *ttl*

dnsc cache delete domain *domain-name* **type** { **a** | **mx** }

undo dnsc cache { **all** | **domain** *domain-name* **type** { **a** | **mx** } }

【视图】

系统视图

【参数】

add：添加 DNS 缓存条目。

delete：删除 DNS 缓存条目。

domain *domain-name*：域名，长度为 3～255 个字符。

type：缓存条目的类型。

a：主机（A）记录。

mx：邮件交换记录（Mail Exchange）。

ip *ip-address*：域名对应的 IP 地址。

ttl *ttl*：缓存条目的生存周期，范围为 0～4294967295，单位为毫秒（ms）。

all：所有缓存条目。

【描述】

dnsc cache add 命令用来添加 DNS 缓存条目，**dnsc cache delete** 命令和 **undo dnsc cache** 命令用来删除 DNS 缓存条目。

缺省情况下，未配置 DNS 缓存条目。

【举例】

添加类型为 MX 的缓存条目。

```
[SecBlade_FW] dnsc cache add domain h3c.com type mx ip 1.1.1.1 ttl 600000
```

9.4 日志配置命令

9.4.1 firewall session log-type

【命令】

firewall session log-type syslog

undo firewall session log-type

【视图】

系统视图

【参数】

syslog：设置流日志输出方式为文本格式。

【描述】

firewall session log-type 命令用来设置流日志的输出方式，**undo firewall session log-type** 命令用来设置流日志的输出方式为缺省方式。

【举例】

设置流日志输出为 syslog 方式。

```
[SecBlade_FW] firewall session log-type syslog
```

9.4.2 firewall log-time

【命令】

firewall { **defend** | **statistic** | **http** | **smtp** } **log-time** *time*

undo firewall { **defend** | **statistic** | **http** | **smtp** } **log-time**

【视图】

系统视图

【参数】

defend：攻击防范信息。

statistic：流量统计信息。

http：HTTP 过滤信息。

smtp：SMTP 过滤信息。

time：日志缓冲区的扫描时间，单位秒，范围 1～65535。

【描述】

firewall log-time 命令用来设置日志缓冲区的扫描时间。**undo firewall log-time** 命令恢复日志缓冲区扫描时间的缺省值。

缺省情况下，日志缓冲区的扫描时间为 30 秒。

【举例】

设置攻击防范日志缓冲区的扫描时间为 100 秒。

```
[SecBlade_FW] firewall defend log-time 100
```

9.4.3 reset firewall log-buf

【命令】

reset firewall log-buf { **session** | **defend** | **statistic** | **http** | **smtp** }

【视图】

用户视图

【参数】

session：清除 NAT/ASPF 流的日志缓冲区。

defend：清除攻击防范的日志缓冲区。

statistic：清除流量监控的日志缓冲区。

http：清除 HTTP 过滤信息。

smtp：清除 SMTP 过滤信息。

【描述】

reset firewall log-buf 用来清除日志缓冲区的内容。

【举例】

清除 NAT/ASPF 流的日志缓冲区内容。

```
<SecBlade_FW> reset firewall log-buf session
```

可靠性

目 录

第 1 章 VRRP配置命令 1-1
1.1 VRRP配置命令 1-1
1.1.1 debugging vrrp 1-1
1.1.2 display vrrp 1-1
1.1.3 vrrp authentication-mode 1-2
1.1.4 vrrp ping-enable 1-3
1.1.5 vrrp un-check ttl 1-4
1.1.6 vrrp vrid preempt-mode 1-4
1.1.7 vrrp vrid priority 1-5
1.1.8 vrrp vrid timer advertise 1-6
1.1.9 vrrp vrid track 1-7
1.1.10 vrrp vrid virtual-ip 1-8

第1章 VRRP 配置命令

1.1 VRRP 配置命令

> 说明：
> 下面的命令在 SecBlade_VPN 提示符下同样适用。

1.1.1 debugging vrrp

【命令】

debugging vrrp { **packet** | **state** }

undo debugging vrrp { **packet** | **state** }

【视图】

用户视图

【参数】

packet：VRRP 报文调试功能。

state：VRRP 状态调试功能。

【描述】

debugging vrrp 命令用来使能 VRRP 的调试功能，**undo debugging vrrp** 命令用来禁止 VRRP 的调试功能。

缺省情况下，VRRP 的调试功能被禁止。

【举例】

使能 VRRP 的报文调试功能。

```
<SecBlade_FW> debugging vrrp packet
```

1.1.2 display vrrp

【命令】

display vrrp [**interface** *type number* [*virtual-router-ID*]]

【视图】

所有视图

【参数】

interface *type number*：接口类型和接口号。

virtual-router-ID：备份组号。

【描述】

display vrrp 命令用来显示 VRRP 的状态信息。

可以查看当前 VRRP 的状态信息和配置参数。如果不指定接口和备份组号，则显示所有备份组的状态信息；如果只指定接口，则显示该接口上的所有备份组的状态信息；如果指定接口和备份组号，则显示指定备份组的状态信息。

【举例】

显示全部备份组信息。

```
<SecBlade_FW> display vrrp
Virtual Ip Ping : Disable
   GigabitEthernet0/0.1 | Virtual Router 1
          state : Initialize
     Virtual IP : 22.2.2.2
Config Priority : 100
   Run Priority : 100
        Preempt : YES   Delay Time : 0
          Timer : 1
      Auth Type : NONE

   GigabitEthernet0/0.2 | Virtual Router 1
          state : Initialize
     Virtual IP : 1.1.11.1
Config Priority : 100
   Run Priority : 100
        Preempt : YES   Delay Time : 0
          Timer : 1
      Auth Type : NONE
```

1.1.3 vrrp authentication-mode

【命令】

vrrp authentication-mode { **md5** *key* | **simple** *key* }

undo vrrp authentication-mode

【视图】

接口视图

【参数】

simple：表示进行明文字符认证。

md5：表示利用 MD5 算法进行密文认证。

key：认证字。当采用 **simple** 认证方式时，*key* 为明文验证字，长度为 1～8 个字符；当采用 **md5** 认证方式时，*key* 为 MD5 密文验证字，如果以明文形式输入，长度为 1～8 个字符，如：1234567；如果以密文形式输入，长度必须为 24，并且必须是密文形式，如：_(TT8F]Y\5SQ=^Q`MAF4<1!!。

【描述】

vrrp authentication-mode 命令用来设置 VRRP 备份组的认证方式和认证字。**undo vrrp authentication-mode** 命令用来取消 VRRP 备份组的认证。

缺省情况下，不进行认证。

这条命令是为一个接口上的所有 VRRP 备份组设置认证方式和认证字，这是由于协议规定一个接口上的备份组应当使用相同的认证方式和认证字。另外，加入同一备份组的成员也应该设置相同的认证方式和认证字。

认证方式和认证字的设置，认证字区分大小写。

【举例】

设置子接口 GigabitEthernet0/0.1 上所有 VRRP 备份组的认证方式和认证字。

```
[SecBlade_FW-GigabitEthernet0/0.1] vrrp authentication-mode simple aabbcc
```

1.1.4 vrrp ping-enable

【命令】

vrrp ping-enable

undo vrrp ping-enable

【视图】

系统视图

【参数】

无

【描述】

vrrp ping-enable 命令用来使备份组的虚拟 IP 地址可以被 ping 通，**undo vrrp ping-enable** 命令用来恢复为缺省情况，使备份组的虚拟 IP 地址不能被 ping 通。

缺省情况下，虚拟备份组的 IP 地址不能被 ping 通。

需要注意的是，本命令需要在配置备份组之前使用。在创建了备份组之后，系统将不允许再使用本命令和命令的 **undo** 形式。

【举例】

使备份组的虚拟 IP 地址可以被 ping 通。

```
[SecBlade_FW] vrrp ping-enable
```

1.1.5 vrrp un-check ttl

【命令】

vrrp un-check ttl

undo vrrp un-check ttl

【视图】

接口视图

【参数】

无

【描述】

vrrp un-check ttl 命令用来取消检查 VRRP 报文的 TTL 值。**undo vrrp un-check ttl** 命令用来恢复检查 VRRP 报文中的 TTL 值。

协议中规定 VRRP 报文的 TTL 值必须为 255，如果备份安全网关收到报文后，检查到 TTL 值不等于 255，就将其丢弃。

缺省情况下，需要检查 VRRP 报文的 TTL 值。

【举例】

取消检查 VRRP 报文的 TTL 值。

```
[SecBlade_FW- GigabitEthernet0/0.1] vrrp un-check ttl
```

1.1.6 vrrp vrid preempt-mode

【命令】

vrrp vrid *virtual-router-ID* **preempt-mode** [**timer delay** *delay-value*]

undo vrrp vrid *virtual-router-ID* **preempt-mode**

【视图】

接口视图

【参数】

virtual-router-ID：VRRP 备份组号，备份组号范围为从 1～255。

delay-value：延迟时间，单位为秒，取值范围为从 0～255。缺省情况下，为抢占，延迟时间为 0 秒。

【描述】

vrrp vrid preempt-mode 命令用来设置备份组中安全网关的抢占方式和延迟时间，**undo vrrp vrid preempt-mode** 命令用来取消备份组的抢占方式。

如果需要优先级高的安全网关能够主动的抢占成为 Master，就需要将这台安全网关设置为抢占方式。如果需要将抢占的时间延长，还可以设置延迟时间。当设置为不抢占时，延迟时间会自动被置为 0 秒。

缺省情况下，为抢占方式，延迟时间为 0 秒。

【举例】

设置抢占。

```
[SecBlade_FW-GigabitEthernet0/0.1] vrrp vrid 1 preempt-mode
```

设置抢占的延迟时间。

```
[SecBlade_FW-GigabitEthernet0/0.1] vrrp vrid 1 preempt-mode timer delay 5
```

设置不抢占。

```
[SecBlade_FW-GigabitEthernet0/0.1] undo vrrp vrid 1 preempt-mode
```

1.1.7 vrrp vrid priority

【命令】

vrrp vrid *virtual-router-ID* **priority** *priority-value*

undo vrrp vrid *virtual-router-ID* **priority**

【视图】

接口视图

【参数】

virtual-router-ID：VRRP 备份组号，范围为 1～255。

priority-value：优先级的值，可配置的范围最小值为 1，最大值为 254。缺省情况下，*priority-value* 值为 100。

【描述】

vrrp vrid priority 命令用来设置 SecBlade 在备份组中的优先级。**undo vrrp vrid priority** 命令用来将优先级恢复为缺省值。

优先级决定 SecBlade 在备份组中的地位，优先级越高，越有可能成为 Master。优先级 0 是系统保留为特殊用途来使用的，255 则是系统保留给 IP 地址拥有者的。

缺省情况下，优先级为 100。

【举例】

设置 SecBlade 在备份组 1 中的优先级为 150。

```
[SecBlade_FW-GigabitEthernet0/0.1] vrrp vrid 1 priority 150
```

1.1.8 vrrp vrid timer advertise

【命令】

vrrp vrid *virtual-router-ID* **timer advertise** *adver-interval*

undo vrrp vrid *virtual-router-ID* **timer advertise**

【视图】

接口视图

【参数】

virtual-router-ID：VRRP 备份组号，范围为从 1～255。

adver-interval：备份组中的 Master 发送 VRRP 报文的间隔时间，单位为秒，取值范围从 1 到 255。缺省情况下，为 1 秒。

【描述】

vrrp vrid timer advertise 命令用来设置备份组的定时器。**undo vrrp vrid timer advertise** 命令用来恢复为缺省值。

用户可以通过这条命令来设置 Master 发送 VRRP 报文的间隔时间。

缺省情况下，定时器的值为 1 秒。

【举例】

设置备份组 1 的 Master 发送 VRRP 报文的间隔时间为 5 秒。

```
[SecBlade_FW-GigabitEthernet0/0.1] vrrp vrid 1 timer advertise 5
```

1.1.9 vrrp vrid track

【命令】

vrrp vrid *virtual-router-ID* **track** *interface-type interface-number* [**reduced** *priority-reduced*]

undo vrrp vrid *virtual-router-ID* **track** [*interface-type interface-number*]

【视图】

接口视图

【参数】

virtual-router-ID：VRRP 备份组号，范围为从 1～255。

interface-type interface-number：被监视的接口类型及接口号。

priority-reduced：优先级降低的数额，取值范围从 1～255。缺省情况下，优先级降低的数额为 10。

【描述】

vrrp vrid track 命令用来设置监视接口。**undo vrrp vrid track** 命令用来取消监视指定接口。

VRRP 的监视接口功能，更好的扩充了备份功能，即不仅在 SecBlade 出现故障时提供备份功能，而且在某网络接口 DOWN 掉时，也可以实现备份功能。配置命令后，如果被监视接口 DOWN 掉，则 SecBlade 的优先级就会降低，备份组内的其它成员的优先级就会变成最高的优先级，从而成为新的 MASTER，实现备份功能。当 SecBlade 为 IP 地址拥有者时，不允许对其进行监视接口的配置。

缺省情况下，运行优先级降低的数额为 10。

【举例】

设置监视子接口 GigabitEthernet0/0.1。

```
[SecBlade_FW-GigabitEthernet0/0.1] vrrp vrid 1 track GigabitEthernet0/0.300 reduced 50
```

取消监视子接口 GigabitEthernet0/0.1。

```
[SecBlade_FW-GigabitEthernet0/0.1] undo vrrp vrid 1 track GigabitEthernet0/0.300
```

1.1.10 vrrp vrid virtual-ip

【命令】

vrrp vrid *virtual-router-ID* **virtual-ip** *virtual-address*

undo vrrp vrid *virtual-router-ID* **virtual-ip** [*virtual-address*]

【视图】

接口视图

【参数】

virtual-router-ID：VRRP 备份组号，范围从 1～255。

virtual-address：虚拟 IP 地址。

【描述】

vrrp vrid virtual-ip 命令用来创建一个备份组，并添加虚拟 IP 地址，**undo vrrp vrid** 命令用来删除备份组。

缺省情况下，系统无备份组。

用户可以通过这条命令来创建一个备份组，也可以向一个已经存在的备份组中添加虚拟 IP 地址，一个备份组最多可以添加 16 个虚拟 IP 地址。用户还可以通过 **undo vrrp vrid** *virtual-router-ID* 命令来删除一个已经存在的备份组，或者用 **undo vrrp vrid** *virtual-router-ID* **virtual-ip** *virtual-address* 命令删除备份组中的某个虚拟地址。如果备份组中的地址被删除完，则系统也会自动将这个备份组删除。

【举例】

创建一个备份组。

```
[SecBlade_FW-GigabitEthernet0/0.1] vrrp vrid 1 virtual-ip 10.10.10.10
```

向一个已经存在的备份组添加虚拟 IP 地址。

```
[SecBlade_FW-GigabitEthernet0/0.1] vrrp vrid 1 virtual-ip 10.10.10.11
```

删除一个虚拟 IP 地址。

```
[SecBlade_FW-GigabitEthernet0/0.1] undo vrrp vrid 1 virtual-ip 10.10.10.10
```

附录

目 录

附录 A 命令总索引 A-1

附录 A 命令总索引

本命令索引包括手册中所出现的全部命令，按字母序排列，左边为命令行，右边为该命令所在的功能模块和页码。

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

access-limit 安全 1-1
accounting 安全 1-2
accounting optional 安全 1-2
accounting optional 安全 1-20
acl 安全 2-1
acl number 安全 5-1
add interface 安全 4-34
aging-time 安全 4-8
ah authentication-algorithm VPN 3-1
algorithm-suite VPN 6-1
allow l2tp VPN 1-1
aspf session limit 安全 4-27
aspf-policy 安全 4-9
authentication 安全 1-3
authentication super hwtacacs-scheme 安全 1-4
authentication-algorithm VPN 4-1
authentication-client method VPN 6-2
authentication-method VPN 4-1
authentication-server method VPN 6-2
authorization 安全 1-5

B

bridge vlanid-transparent-transmit enable 安全 5-1

C

ca identifier VPN 5-1

certificate request entity VPN 5-1
certificate request from VPN 5-2
certificate request mode VPN 5-3
certificate request polling VPN 5-3
certificate request url VPN 5-4
common-name VPN 5-9
connection-limit default 安全 3-1
connection-limit default amount 安全 3-1
connection-limit enable 安全 3-2
connection-limit policy 安全 3-3
country VPN 5-10
crl check disable VPN 5-5
crl update-period VPN 5-5
crl url VPN 5-6

D

data algorithm-suite VPN 6-3
data ipsec-sa duration VPN 6-4
data-flow-format 安全 1-21
data-flow-format 安全 1-47
debugging aspf 安全 4-9
debugging aspf http 安全 4-10
debugging connection-limit 安全 3-3
debugging dnsc 安全 9-17
debugging dvpn VPN 6-4
debugging encrypt-card host VPN 3-39
debugging firewall blacklist 安全 4-28
debugging firewall defend 安全 7-1
debugging firewall eff 安全 5-2
debugging firewall mac-binding 安全 4-30
debugging firewall packet-filter 安全 4-1
debugging firewall packet-filter fragments-inspect events 安全 4-2
debugging firewall smtp-filter 安全 6-19
debugging firewall transparent-mode eth-forwarding 安全 5-4

debugging firewall transparent-mode ip-forwarding	安全	5-5
debugging firewall url-filter host	安全	6-1
debugging firewall url-filter parameter	安全	6-1
debugging firewall webdata-filter	安全	6-2
debugging hwtacacs	安全	1-48
debugging ids	安全	8-3
debugging ike	VPN	4-2
debugging ike dpd	VPN	3-2
debugging ipsec	VPN	3-2
debugging l2tp	VPN	1-2
debugging local-server	安全	1-22
debugging nat	安全	3-4
debugging pki	VPN	5-17
debugging radius	安全	1-22
debugging smtpc	安全	9-15
debugging tunnel	VPN	2-1
debugging vrrp	可靠性	1-1
default-login-user	简介	1-1
description	安全	2-2
destination	VPN	2-1
detect	安全	4-11
detect http	安全	4-12
dh	VPN	4-3
display acl	安全	2-2
display aspf all	安全	4-13
display aspf interface	安全	4-14
display aspf policy	安全	4-15
display aspf session	安全	4-16
display aspf statistics	安全	4-17
display connection	安全	1-6
display connection-limit policy	安全	3-4
display connection-limit statistics	安全	3-5
display dnsc	安全	9-18
display domain	安全	1-7

display dvpn info	VPN	6-7
display dvpn ipsec-sa	VPN	6-5
display dvpn map	VPN	6-6
display dvpn online-user	VPN	6-9
display dvpn session	VPN	6-7
display encrypt-card fast-switch	VPN	3-40
display firewall blacklist	安全	4-28
display firewall defend flag	安全	7-1
display firewall ethernet-frame-filter	安全	5-7
display firewall fragment	安全	4-2
display firewall fragment	安全	4-17
display firewall mac-binding	安全	4-31
display firewall mode	安全	5-8
display firewall packet-filter statistics	安全	4-3
display firewall session aging-time	安全	4-18
display firewall session table	安全	4-19
display firewall smtp-filter	安全	6-20
display firewall statistic	安全	9-1
display firewall statistic system defend	安全	9-3
display firewall statistic system flow-percent	安全	9-4
display firewall tcp-proxy session	安全	7-2
display firewall transparent-mode address-table	安全	5-8
display firewall transparent-mode config	安全	5-9
display firewall transparent-mode traffic	安全	5-10
display firewall url-filter host	安全	6-3
display firewall url-filter parameter	安全	6-4
display firewall url-filter parameter counter detail	安全	6-4
display firewall webdata-filter	安全	6-5
display hwtacacs scheme	安全	1-49
display ids	安全	8-1
display ids-acl	安全	8-2
display ike dpd	VPN	3-3
display ike peer	VPN	4-4
display ike proposal	VPN	4-4

display ike sa	VPN	4-5
display interface encrypt	VPN	3-40
display interface tunnel	VPN	2-2
display interzone	安全	4-34
display ipsec policy	VPN	3-4
display ipsec policy-template	VPN	3-7
display ipsec proposal	VPN	3-8
display ipsec sa	VPN	3-9
display ipsec statistics	VPN	3-12
display ipsec tunnel	VPN	3-13
display l2tp session	VPN	1-3
display l2tp tunnel	VPN	1-4
display l2tp user	VPN	1-5
display local-server statistics	安全	1-23
display local-user	安全	1-8
display nat	安全	3-6
display nat connection-limit	安全	3-8
display pki certificate	VPN	5-21
display pki crl	VPN	5-23
display port-mapping	安全	4-20
display radius scheme	安全	1-24
display radius statistics	安全	1-25
display secblade module	简介	1-1
display smtpc	安全	9-15
display stop-accounting-buffer	安全	1-29
display stop-accounting-buffer hwtacacs-scheme	安全	1-51
display time-range	安全	2-8
display vrrp	可靠性	1-1
display zone	安全	4-35
dnsc cache	安全	9-19
dnsc server	安全	9-18
domain	安全	1-10
dpd	VPN	3-14
dvpn class	VPN	6-9

dvpn client register-dumb	VPN	6-10
dvpn client register-interval	VPN	6-10
dvpn client register-retry	VPN	6-11
dvpn dvpn-id	VPN	6-12
dvpn interface-type	VPN	6-12
dvpn policy	VPN	6-13
dvpn register-type	VPN	6-14
dvpn security	VPN	6-15
dvpn server	VPN	6-15
dvpn server authentication-client method	VPN	6-16
dvpn server map age-time	VPN	6-17
dvpn server pre-shared-key	VPN	6-17
dvpn service enable	VPN	6-18

E

encapsulation-mode	VPN	3-15
encrypt-card backuped	VPN	3-41
encrypt-card fast-switch	VPN	3-42
encryption-algorithm	VPN	4-6
esp authentication-algorithm	VPN	3-16
esp encryption-algorithm	VPN	3-17
exchange-mode	VPN	4-7

F

firewall arp-learning enable	安全	5-12
firewall aspf	安全	4-21
firewall blacklist	安全	4-29
firewall defend all	安全	7-4
firewall defend arp-flood	安全	7-4
firewall defend arp-spoofing	安全	7-5
firewall defend frag-flood	安全	7-6
firewall defend fraggle	安全	7-6
firewall defend icmp-flood	安全	7-7
firewall defend icmp-flood enable	安全	7-8
firewall defend icmp-redirect	安全	7-9

firewall defend icmp-unreachable	安全	7-9
firewall defend ip-fragment	安全	7-10
firewall defend ip-spoofing	安全	7-10
firewall defend ip-sweep	安全	7-11
firewall defend land	安全	7-12
firewall defend large-icmp	安全	7-12
firewall defend ping-of-death	安全	7-13
firewall defend port-scan	安全	7-14
firewall defend route-record	安全	7-14
firewall defend smurf	安全	7-15
firewall defend source-route	安全	7-16
firewall defend syn-flood	安全	7-16
firewall defend syn-flood enable	安全	7-17
firewall defend tcp-flag	安全	7-18
firewall defend teardrop	安全	7-18
firewall defend tracert	安全	7-19
firewall defend udp-flood	安全	7-19
firewall defend udp-flood enable	安全	7-20
firewall defend winnuke	安全	7-21
firewall ethernet-frame-filter	安全	5-13
firewall fragment limit	安全	4-27
firewall interzone	安全	4-36
firewall log-time	安全	9-20
firewall mac-binding	安全	4-32
firewall mac-binding enable	安全	4-33
firewall mode	安全	5-13
firewall packet-filter	安全	4-6
firewall packet-filter default	安全	4-3
firewall packet-filter enable	安全	4-4
firewall packet-filter fragments-inspect	安全	4-4
firewall packet-filter fragments-inspect { high | low }	安全	4-5
firewall session aging-time	安全	4-22
firewall session aging-time default	安全	4-23

firewall session limit	安全	4-26
firewall session log-type	安全	9-20
firewall smtp-filter attach add	安全	6-21
firewall smtp-filter attach clear	安全	6-22
firewall smtp-filter attach delete	安全	6-22
firewall smtp-filter attach enable	安全	6-23
firewall smtp-filter attach load-file	安全	6-23
firewall smtp-filter attach save-file	安全	6-24
firewall smtp-filter content add	安全	6-24
firewall smtp-filter content clear	安全	6-25
firewall smtp-filter content delete	安全	6-25
firewall smtp-filter content enable	安全	6-26
firewall smtp-filter content load-file	安全	6-26
firewall smtp-filter content save-file	安全	6-27
firewall smtp-filter rcptto add	安全	6-27
firewall smtp-filter rcptto clear	安全	6-28
firewall smtp-filter rcptto default	安全	6-29
firewall smtp-filter rcptto delete	安全	6-29
firewall smtp-filter rcptto enable	安全	6-30
firewall smtp-filter rcptto load-file	安全	6-30
firewall smtp-filter rcptto save-file	安全	6-31
firewall smtp-filter subject add	安全	6-31
firewall smtp-filter subject clear	安全	6-32
firewall smtp-filter subject delete	安全	6-32
firewall smtp-filter subject enable	安全	6-33
firewall smtp-filter subject load-file	安全	6-33
firewall smtp-filter subject save-file	安全	6-34
firewall statistic system connect-number	安全	9-5
firewall statistic system enable	安全	9-6
firewall statistic system flow-percent	安全	9-6
firewall statistic warning-level drop	安全	9-7
firewall system-ip	安全	5-14
firewall tcp-proxy	安全	7-22

firewall transparent-mode aging-time	安全	5-15
firewall transparent-mode transmit	安全	5-16
firewall unknown-mac	安全	5-16
firewall unknown-mac broadcast	安全	5-17
firewall unknown-mac multicast	安全	5-18
firewall unknown-mac unicast	安全	5-18
firewall url-filter host acl-number	安全	6-6
firewall url-filter host add	安全	6-6
firewall url-filter host clear	安全	6-7
firewall url-filter host default	安全	6-7
firewall url-filter host delete	安全	6-8
firewall url-filter host enable	安全	6-8
firewall url-filter host ip-address	安全	6-9
firewall url-filter host load-file	安全	6-10
firewall url-filter host save-file	安全	6-9
firewall url-filter parameter add	安全	6-10
firewall url-filter parameter add-default	安全	6-11
firewall url-filter parameter clear	安全	6-12
firewall url-filter parameter delete	安全	6-12
firewall url-filter parameter enable	安全	6-13
firewall url-filter parameter load-file	安全	6-13
firewall url-filter parameter save-file	安全	6-14
firewall webdata-filter add	安全	6-14
firewall webdata-filter clear	安全	6-15
firewall webdata-filter delete	安全	6-16
firewall webdata-filter enable	安全	6-16
firewall webdata-filter load-file	安全	6-17
firewall webdata-filter save-file	安全	6-18
firewall zone	安全	4-37
firewall zone name	安全	4-37
fqdn	VPN	5-8

G

gre checksum	VPN	2-4

gre key	VPN	2-4

H

hwtacacs nas-ip	安全	1-52
hwtacacs scheme	安全	1-53

I

Ids-acl enable	安全	8-1
id-type	VPN	4-8
ike dpd	VPN	3-18
ike encrypt-card dh-computation disabled	VPN	4-8
ike local-name	VPN	4-9
ike next-payload check disabled	VPN	4-10
ike peer	VPN	4-10
ike proposal	VPN	4-11
ike sa keepalive-timer interval	VPN	4-13
ike sa keepalive-timer timeout	VPN	4-13
ike sa nat-keepalive-timer interval	VPN	4-14
ike-peer	VPN	4-11
interface encrypt	VPN	3-43
interface tunnel	VPN	2-5
interface virtual-template	VPN	1-6
interval-time	VPN	3-18
ip	VPN	5-10
ip pool	安全	1-11
ipsec card-proposal	VPN	3-43
ipsec policy	VPN	3-19
ipsec policy policy-name	VPN	3-20
ipsec policy-template	VPN	3-21
ipsec proposal	VPN	3-22
ipsec sa global-duration	VPN	3-23

J

K

keepalive	VPN	2-6

key 安全 1-30
key 安全 1-53

L

l2tp enable VPN 1-6
l2tp-auto-client enable VPN 1-7
l2tp-group VPN 1-7
l2tpmoreexam enable VPN 1-8
ldap-server VPN 5-6
level 安全 1-12
limit 安全 3-9
local VPN 4-15
local-address VPN 4-15
locality VPN 5-11
local-server 安全 1-31
local-user VPN 6-18
local-user 安全 1-13
local-user password-display-mode 安全 1-14
log enable 安全 4-23

M

mandatory-chap VPN 1-9
mandatory-lcp VPN 1-9
map to slot 简介 1-2

N

nas-ip 安全 1-32
nas-ip 安全 1-54
nat address-group 安全 3-10
nat aging-time 安全 3-11
nat alg 安全 3-12
nat connection-limit-policy 安全 3-13
nat dns-map 安全 3-13
nat outbound 安全 3-14
nat outbound interface 安全 3-15

nat outbound static	安全	3-16
nat overlapaddress	安全	3-17
nat server	安全	3-18
nat static	安全	3-20
nat static inside	安全	3-21
nat traversal	VPN	4-16

O

organization	VPN	5-11
organization-unit	VPN	5-12

P

password	安全	1-14
peer	VPN	4-17
pfs	VPN	3-24
pki delete-certificate	VPN	5-13
pki domain	VPN	5-7
pki entity	VPN	5-13
pki import-certificate	VPN	5-14
pki request-certificate	VPN	5-15
pki retrieval-certificate	VPN	5-15
pki retrieval-crl	VPN	5-16
pki validate-certificate	VPN	5-16
port-mapping	安全	4-24
pre-shared-key	VPN	4-17
pre-shared-key	VPN	6-20
primary accounting	安全	1-32
primary accounting	安全	1-55
primary authentication	安全	1-33
primary authentication	安全	1-56
primary authorization	安全	1-56
private-ip	VPN	6-20
proposal	VPN	3-25
public-ip	VPN	6-19

Q

R

radius nas-ip	安全	1-35
radius scheme	安全	1-34
radius trap	安全	1-36
remote-address	VPN	4-18
remote-name	VPN	4-18
reset acl counter	安全	2-3
reset aspf session	安全	4-25
reset aspf statistic http	安全	4-25
reset counters interface encrypt	VPN	3-44
reset dvpn all	VPN	6-21
reset dvpn map	VPN	6-21
reset dvpn session	VPN	6-22
reset dvpn statistics	VPN	6-22
reset encrypt-card fast-switch	VPN	3-45
reset encrypt-card sa	VPN	3-46
reset encrypt-card statistics	VPN	3-46
reset encrypt-card syslog	VPN	3-47
reset firewall ethernet-frame-filter	安全	5-19
reset firewall log-buf	安全	9-21
reset firewall mac-binding	安全	4-33
reset firewall packet-filter statistics	安全	4-7
reset firewall session table	安全	4-26
reset firewall smtp-filter counter	安全	6-34
reset firewall statistic ip	安全	9-8
reset firewall statistic system	安全	9-8
reset firewall statistic zone	安全	9-9
reset firewall transparent-mode address-table	安全	5-19
reset firewall transparent-mode traffic	安全	5-20
reset firewall url-filter host counter	安全	6-18
reset firewall url-filter parameter counter	安全	6-18

reset firewall webdata-filter counter	安全	6-19
reset hwtacacs statistics	安全	1-57
reset ike sa	VPN	4-19
reset ipsec sa	VPN	3-26
reset ipsec statistics	VPN	3-27
reset l2tp session	VPN	1-10
reset l2tp tunnel	VPN	1-11
reset l2tp user	VPN	1-11
reset nat	安全	3-22
reset radius statistics	安全	1-36
reset stop-accounting-buffer	安全	1-37
reset stop-accounting-buffer	安全	1-58
retry	安全	1-38
retry realtime-accounting	安全	1-39
retry stop-accounting	安全	1-39
retry stop-accounting	安全	1-58
root-certificate fingerprint	VPN	5-8
rule	安全	2-3
rule	安全	5-20
rule comment	安全	2-7

S

sa authentication-hex	VPN	3-28
sa duration	VPN	3-29
sa duration	VPN	4-20
sa encryption-hex	VPN	3-30
sa spi	VPN	3-32
sa string-key	VPN	3-33
scheme	安全	1-15
secblade aggregation slot	简介	1-3
secblade module	简介	1-3
secblade slot	简介	1-4
secblade-interface	简介	1-4
secondary accounting	安全	1-40

secondary accounting	安全	1-59
secondary authentication	安全	1-41
secondary authentication	安全	1-60
secondary authorization	安全	1-60
security acl	VPN	3-35
security-vlan	简介	1-5
server-type	安全	1-42
service-type	安全	1-16
service-type dvpn	安全	1-17
service-type ftp	安全	1-17
service-type ppp	安全	1-18
session algorithm-suite	VPN	6-23
session idle-time	VPN	1-12
session idle-time	VPN	6-24
session keepalive-interval	VPN	6-24
session setup-interval	VPN	6-25
set priority	安全	4-36
smtpc administrator mail	安全	9-16
smtpc trigger time	安全	9-17
snmp-agent trap enable encrypt-card	VPN	3-48
source	VPN	2-6
start l2tp	VPN	1-12
start l2tp tunnel	VPN	1-13
state	VPN	5-12
state	安全	1-19
state	安全	1-42
statistic connect-number ip	安全	9-10
statistic connect-number zone	安全	9-11
statistic connect-speed ip	安全	9-12
statistic connect-speed zone	安全	9-13
statistic enable	安全	9-14
stop-accounting-buffer enable	安全	1-43
stop-accounting-buffer enable	安全	1-61
super authentication-mode	安全	1-19

T

time-out	VPN	3-35
timer quiet	安全	1-44
timer quiet	安全	1-62
timer realtime-accounting	安全	1-45
timer realtime-accounting	安全	1-62
timer response-timeout	安全	1-46
timer response-timeout	安全	1-63
time-range	安全	2-9
transform	VPN	3-36
tunnel authentication	VPN	1-14
tunnel avp-hidden	VPN	1-15
tunnel flow-control	VPN	1-15
tunnel keepstanding	VPN	1-16
tunnel local	VPN	3-37
tunnel name	VPN	1-17
tunnel password	VPN	1-17
tunnel remote	VPN	3-38
tunnel timer hello	VPN	1-18
tunnel-protocol gre	VPN	2-7
tunnel-protocol udp dvpn	VPN	6-25

U

use encrypt-card	VPN	3-48
user-name-format	安全	1-46
user-name-format	安全	1-64

V

vrrp authentication-mode	可靠性	1-2
vrrp ping-enable	可靠性	1-3
vrrp un-check ttl	可靠性	1-4
vrrp vrid preempt-mode	可靠性	1-4
vrrp vrid priority	可靠性	1-5
vrrp vrid timer advertise	可靠性	1-6

vrrp vrid track 可靠性 1-7
vrrp vrid virtual-ip 可靠性 1-8

W

X

Y

Z