目 录

1 攻击检测及防范

1.1 攻击检测及防范配置命令

1.1.1 attack-defense apply policy

【命令】

attack-defense apply policy *policy-number*

undo attack-defense apply policy

【视图】

接口视图

【缺省级别】

2：系统级

【参数】

policy-number：攻击防范策略编号，取值范围为 1～128。

【描述】

attack-defense apply policy 命令用来在接口上应用攻击防范策略。**undo attack-defense apply policy** 命令用来恢复缺省情况。

缺省情况下，接口上未应用任何攻击防范策略。

需要注意的是：

- 在接口上应用的攻击防范策略必须提前通过 **attack-defense policy** 命令创建。
- 一个接口上只能应用一个攻击防范策略（可多次配置，最后一次配置的有效），但一个攻击防范策略可应用到多个接口上。

相关配置可参考命令 **attack-defense policy** 和 **display attack-defense policy**。

【举例】

将攻击防范策略 1 应用到接口 GigabitEthernet3/0/1 上。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] attack-defense apply policy 1
```

1.1.2 attack-defense logging enable

【命令】

attack-defense logging enable

undo attack-defense logging enable

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

无

【描述】

attack-defense logging enable 命令用来开启攻击防范日志的记录功能。**undo attack-defense logging enable** 命令用来关闭攻击防范日志的记录功能。

缺省情况下，未开启攻击防范日志记录功能。

【举例】

开启攻击防范日志记录功能。

```
<Sysname> system-view
[Sysname] attack-defense logging enable
```

1.1.3 attack-defense policy

【命令】

attack-defense policy *policy-number* [**interface** *interface-type interface-number*]

undo attack-defense policy *policy-number* [**interface** *interface-type interface-number*]

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

policy-number：攻击防范策略编号，取值范围为 1～128，即最多可以配置 128 个攻击防范策略。

interface *interface-type interface-number*：指定独享此策略的接口。其中，*interface-type interface-number* 表示接口类型和接口编号。若指定该参数，则表示该策略仅能应用于这一个指定的接口上，否则可应用于多个接口上。

【描述】

attack-defense policy 命令用来创建一个攻击防范策略，并进入攻击防范策略视图。**undo attack-defense policy** 命令用来删除指定的攻击防范策略。

缺省情况下，不存在任何攻击防范策略。

相关配置可参考命令 **display attack-defense policy**。

【举例】

创建攻击防范策略 1。

```
<Sysname> system-view
[Sysname] attack-defense policy 1
[Sysname-attack-defense-policy-1]
```

1.1.4 blacklist enable

【命令】

blacklist enable

undo blacklist enable

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

无

【描述】

blacklist enable 命令用来使能黑名单功能。**undo blacklist enable** 命令用来恢复缺省情况。

缺省情况下，黑名单功能处于未使能状态。

黑名单功能使能后，可以手工或自动添加黑名单表项。自动添加黑名单功能可与扫描攻击防范功能以及用户登录认证功能进行配合，关于扫描攻击防范功能的具体配置请参见命令 **defense scan add-to-blacklist**。

相关配置可参考命令 **display attack-defense policy** 和 **defense scan**。

【举例】

使能黑名单功能。

```
<Sysname> system-view
[Sysname] blacklist enable
```

1.1.5 blacklist ip

【命令】

blacklist ip *source-ip-address* [**timeout** *minutes*]

undo blacklist { **all** | **ip** *source-ip-address* [**timeout**] }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

source-ip-address：加入黑名单的 IP 地址，用于匹配报文的源 IP。

all：指定所有的黑名单表项。

timeout *minutes*：指定黑名单表项的老化时间。其中 *minutes* 表示老化时间，取值范围为 1～1000，单位为分钟。若不配置该参数，那么该黑名单表项永不老化，除非用户手动将其删除。

【描述】

blacklist ip 命令用来添加黑名单表项。将指定 IP 地址加入黑名单后，设备将会过滤来自这个 IP 地址的所有报文。**undo blacklist** 命令用来删除黑名单表项或取消指定黑名单表项的老化时间。

需要注意的是：

- **undo blacklist ip** *source-ip-address* **timeout** 命令用来取消为 *source-ip-address* 配置的老化时间，并将该黑名单表项恢复为永不老化。
- 所有的黑名单表项只有在黑名单功能处于使能状态的情况下才生效。
- 已经存在的黑名单表项的老化时间可以修改，修改后的值立即生效。

相关配置可参考命令 **blacklist enable** 和 **display blacklist**。

【举例】

将 IP 地址 192.168.1.2 加入黑名单，指定其老化时间为 20 分钟。

```
<Sysname> system-view
[Sysname] blacklist ip 192.168.1.2 timeout 20
```

1.1.6 defense icmp-flood action drop-packet

【命令】

defense icmp-flood action drop-packet

undo defense icmp-flood action

【视图】

攻击防范策略视图

【缺省级别】

2：系统级

【参数】

无

【描述】

defense icmp-flood action drop-packet 命令用来配置对 ICMP Flood 攻击报文的处理方式为丢弃。**undo defense icmp-flood action** 命令用来恢复缺省情况。

缺省情况下，检测到 ICMP Flood 攻击后，不进行处理。

相关配置可参考命令 **defense icmp-flood enable**、**defense icmp-flood rate-threshold**、**defense icmp-flood ip** 和 **display attack-defense policy**。

【举例】

在攻击防范策略 1 中配置丢弃 ICMP Flood 攻击报文。

```
<Sysname> system-view
[Sysname] attack-defense policy 1
[Sysname-attack-defense-policy-1] defense icmp-flood action drop-packet
```

1.1.7 defense icmp-flood enable

【命令】

defense icmp-flood enable

undo defense icmp-flood enable

【视图】

攻击防范策略视图

【缺省级别】

2：系统级

【参数】

无

【描述】

defense icmp-flood enable 命令用来使能 ICMP Flood 攻击防范。**undo defense icmp-flood enable** 命令用来恢复缺省情况。

缺省情况下，ICMP Flood 攻击防范处于未使能状态。

相关配置可参考命令 **defense icmp-flood rate-threshold**、**defense icmp-flood ip**、**defense icmp-flood action drop-packet** 和 **display attack-defense policy**。

【举例】

在攻击防范策略 1 中使能 ICMP Flood 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy 1
[Sysname-attack-defense-policy-1] defense icmp-flood enable
```

1.1.8 defense icmp-flood ip

【命令】

defense icmp-flood ip *ip-address* **rate-threshold high** *rate-number* [**low** *rate-number*]

undo defense icmp-flood ip *ip-address* [**rate-threshold**]

【视图】

攻击防范策略视图

【缺省级别】

2：系统级

【参数】

ip-address：指定要保护的 IP 地址。该 IP 地址不能为广播地址、127.0.0.0/8、D 类地址或 E 类地址。

high *rate-number*：指定攻击防范的触发阈值。其中，*rate-number* 为向指定 IP 地址每秒发送的 ICMP 报文数目，取值范围为 1～64000。使能 ICMP Flood 攻击防范后，设备处于攻击检测状态，当它监测到向指定 IP 地址发送 ICMP 报文的速率持续达到或超过了该触发阈值时，即认为该 IP 地址受到了 ICMP Flood 攻击，则进入攻击防范状态，并根据配置启动相应的防范措施。

low *rate-number*：指定攻击检测的恢复阈值。其中，*rate-number* 为向指定 IP 地址每秒发送的 ICMP 报文数目，取值范围为 1～64000，缺省值为触发阈值的 3/4。当处于攻击防范状态的设备监测到向指定 IP 地址发送 ICMP 报文的速率低于该恢复阈值时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

【描述】

defense icmp-flood ip 命令用来对指定 IP 地址配置 ICMP Flood 攻击防范参数，包括触发阈值和恢复阈值。**undo defense icmp-flood ip** 命令用来取消对指定 IP 地址的 ICMP Flood 攻击防范参数配置。

缺省情况下，未对任何指定 IP 地址配置 ICMP Flood 攻击防范参数。

每个攻击防范策略下最多可以同时对 32 个 IP 地址配置 ICMP Flood 攻击防范参数。

相关配置可参考命令 **defense icmp-flood enable**、**defense icmp-flood action drop-packet** 和 **display attack-defense policy**。

【举例】

指定针对 IP 地址 192.168.1.2 的 ICMP Flood 攻击防范参数，触发阈值为 2000，恢复阈值为 1000。当设备监测到向该 IP 地址每秒发送的 ICMP 报文数持续达到或超过 2000 时，启动攻击防范措施；当设备监测到该值低于 1000 时，认为攻击结束，并恢复为攻击检测状态。

```
<Sysname> system-view
[Sysname] attack-defense policy 1
[Sysname-attack-defense-policy-1] defense icmp-flood ip 192.168.1.2 rate-threshold high
2000 low 1000
```

1.1.9 defense icmp-flood rate-threshold

【命令】

defense icmp-flood rate-threshold high *rate-number* [**low** *rate-number*]

undo defense icmp-flood rate-threshold

【视图】

攻击防范策略视图

【缺省级别】

2：系统级

【参数】

high *rate-number*：指定攻击防范的触发阈值。其中，*rate-number* 为向某 IP 地址每秒发送的 ICMP 报文数目，取值范围为 1～64000。使能 ICMP Flood 攻击防范后，设备处于攻击检测状态，当它监测到向某 IP 地址发送 ICMP 报文的速率持续达到或超过了该触发阈值时，即认为该 IP 地址受到了 ICMP Flood 攻击，则进入攻击防范状态，并根据配置启动相应的防范措施。

low *rate-number*：指定攻击检测的恢复阈值。其中，*rate-number* 为向某 IP 地址每秒发送的 ICMP 报文数目，取值范围为 1～64000。当处于攻击防范状态的设备监测到向某 IP 地址发送 ICMP 报文的速率低于该恢复阈值时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

【描述】

defense icmp-flood rate-threshold 命令用来配置 ICMP Flood 攻击防范的全局参数，包括触发阈值和恢复阈值。对于没有专门配置 ICMP Flood 攻击防范参数的 IP 地址，设备采用该全局参数设置来进行保护。**undo defense icmp-flood rate-threshold** 命令用来恢复缺省配置。

缺省情况下，触发阈值为每秒 1000 个报文数，恢复阈值为每秒 750 个报文数。

阈值的取值需要根据实际网络应用场景进行调整，通常情况下网络中的 ICMP 报文流量相对 TCP 流量、UDP 流量而言较小，因此可以适当调小触发阈值；若到被保护网络的带宽较小，可承受的流量压力较小，则建议调小恢复阈值，反之，可以将恢复阈值调大一些。

相关配置可参考命令 **defense icmp-flood enable**、**defense icmp-flood action drop-packet** 和 **display attack-defense policy**。

【举例】

指定 ICMP Flood 攻击防范的全局参数，触发阈值为 3000，恢复阈值为 1000。当设备监测到向某 IP 地址每秒发送的 ICMP 报文数持续达到或超过 3000 时，启动攻击防范措施；当设备监测到该值低于 1000 时，认为攻击结束，并恢复为攻击检测状态。

```
<Sysname> system-view
[Sysname] attack-defense policy 1
[Sysname-attack-defense-policy-1] defense icmp-flood rate-threshold high 3000 low 1000
```

1.1.10 defense scan add-to-blacklist

【命令】

defense scan add-to-blacklist

undo defense scan add-to-blacklist

【视图】

攻击防范策略视图

【缺省级别】

2：系统级

【参数】

无

【描述】

defense scan add-to-blacklist 命令用来使能扫描攻击防范的黑名单添加功能。**undo defense scan add-to-blacklist** 命令用来恢复缺省情况。

缺省情况下，扫描攻击防范的黑名单添加功能处于未使能状态。

在扫描攻击防范使能的情况下，若设备监测到某 IP 地址发起的新建连接的速率达到或超过指定阈值（由 **defense scan max-rate** 命令配置），则认为该 IP 地址发起了扫描攻击，并丢弃该 IP 地址的后续报文，直到监测值低于阈值才认为攻击结束。若同时使能了扫描攻击防范的黑名单添加功能，则设备会将检测到的扫描攻击报文的源 IP 地址加入黑名单，由黑名单对攻击报文进行过滤，该黑名单表项在指定的老化时间（由 **defense scan blacklist-timeout** 命令配置）后被删除。

需要注意的是：

- 要使扫描攻击防范添加的黑名单生效，必须保证黑名单功能处于使能状态。

- 扫描攻击检测自动添加某黑名单表项后，如果在短时间内（目前为 1 秒）手动将其删除，则系统不会再次添加，因为系统会把再次检测到的攻击报文认为是同一次攻击尚未结束的报文。

相关配置可参考命令 **defense scan blacklist-timeout**、**defense scan enable**、**defense scan max-rate** 和 **blacklist enable**。

【举例】

使能扫描攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy 1
[Sysname-attack-defense-policy-1] defense scan enable
```

指定启动扫描攻击防范的连接速率阈值为每秒 2000 个连接。

```
[Sysname-attack-defense-policy-1] defense scan max-rate 2000
```

配置将检测到的扫描攻击报文的源 IP 地址加入黑名单，黑名单表项的老化时间为 20 分钟。

```
[Sysname-attack-defense-policy-1] defense scan add-to-blacklist
[Sysname-attack-defense-policy-1] defense scan blacklist-timeout 20
[Sysname-attack-defense-policy-1] quit
```

为使黑名单添加功能生效，使能黑名单功能。

```
[Sysname] blacklist enable
```

1.1.11 defense scan blacklist-timeout

【命令】

defense scan blacklist-timeout *minutes*

undo defense scan blacklist-timeout

【视图】

攻击防范策略视图

【缺省级别】

2：系统级

【参数】

minutes：黑名单表项的老化时间，取值范围为 1～1000，单位为分钟。

【描述】

defense scan blacklist-timeout 命令用来配置扫描攻击防范添加的黑名单的老化时间。**undo defense scan blacklist-timeout** 命令用来恢复缺省情况。

缺省情况下，黑名单表项的老化时间为 10 分钟。

相关配置可参考命令 **defense scan add-to-blacklist**、**defense scan enable**、**defense scan max-rate** 和 **blacklist enable**。

【举例】

配置扫描攻击防范添加的黑名单的老化时间为 20 分钟。

```
<Sysname> system-view
[Sysname] attack-defense policy 1
[Sysname-attack-defense-policy-1] defense scan blacklist-timeout 20
```

1.1.12 defense scan enable

【命令】

defense scan enable

undo defense scan enable

【视图】

攻击防范策略视图

【缺省级别】

2：系统级

【参数】

无

【描述】

defense scan enable 命令用来使能扫描攻击防范。**undo defense scan enable** 命令用来恢复缺省情况。

缺省情况下，扫描攻击防范处于未使能状态。

在扫描攻击防范使能的情况下，若设备监测到某 IP 地址发起的新建连接的速率达到或超过指定阈值（由 **defense scan max-rate** 命令配置），则认为该 IP 地址发起了扫描攻击，并丢弃该 IP 地址的后续报文，直到监测值低于阈值才认为攻击结束。

相关配置可参考命令 **defense scan add-to-blacklist**、**defense scan blacklist-timeout**、**defense scan max-rate** 和 **blacklist enable**。

【举例】

使能扫描攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy 1
[Sysname-attack-defense-policy-1] defense scan enable
```

1.1.13 defense scan max-rate

【命令】

defense scan max-rate *rate-number*

undo defense scan max-rate

【视图】

攻击防范策略视图

【缺省级别】

2：系统级

【参数】

rate-number：表示每秒新建连接的数目阈值，取值范围为 1～10000。

【描述】

defense scan max-rate 命令用来配置启动扫描攻击防范的连接速率阈值。**undo defense scan max-rate** 命令用来恢复缺省情况。

缺省情况下，连接速率阈值为每秒 4000 个连接。

在扫描攻击防范使能的情况下，若设备监测到某 IP 地址发起的新建连接的速率达到或超过指定阈值，则认为该 IP 地址发起了扫描攻击，并丢弃该 IP 地址的后续报文，直到监测值低于阈值才认为攻击结束。

相关配置可参考命令 **defense scan add-to-blacklist**、**defense scan blacklist-timeout**、**defense scan enable** 和 **blacklist enable**。

【举例】

使能扫描攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy 1
[Sysname-attack-defense-policy-1] defense scan enable
```

指定启动扫描攻击防范的连接速率阈值为每秒 2000 个连接。

```
[Sysname-attack-defense-policy-1] defense scan max-rate 2000
```

1.1.14 defense syn-flood action

【命令】

defense syn-flood action { **drop-packet** | **trigger-tcp-proxy** }

undo defense syn-flood action

【视图】

攻击防范策略视图

【缺省级别】

2：系统级

【参数】

drop-packet：表示丢弃 SYN Flood 攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有新建连接的报文都会被丢弃。

trigger-tcp-proxy：表示自动触发 TCP Proxy 功能，即设备检测到攻击发生后，会自动将受攻击的 IP 地址添加到受保护 IP 表项中，并对客户端与受保护 IP 地址之间的 TCP 连接进行代理。

【描述】

defense syn-flood action 命令用来配置对 SYN Flood 攻击报文的处理方式。**undo defense syn-flood action** 命令用来恢复缺省情况。

缺省情况下，对 SYN Flood 攻击报文不进行处理。

相关配置可参考命令 **tcp-proxy enable**、**defense syn-flood enable** 和 **display attack-defense policy**。

【举例】

配置对 SYN Flood 攻击报文的处理方式为丢弃后续报文。

```
<Sysname> system-view
[Sysname] attack-defense policy 1
[Sysname-attack-defense-policy-1] defense syn-flood action drop-packet
```

1.1.15 defense syn-flood enable

【命令】

defense syn-flood enable

undo defense syn-flood enable

【视图】

攻击防范策略视图

【缺省级别】

2：系统级

【参数】

无

【描述】

defense syn-flood enable 命令用来使能 SYN Flood 攻击防范。**undo defense syn-flood enable** 命令用来恢复缺省情况。

缺省情况下，SYN Flood 攻击防范处于未使能状态。

相关配置可参考命令 **display attack-defense policy** 和 **defense syn-flood**。

【举例】

在攻击防范策略 1 中使能 SYN Flood 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy 1
[Sysname-attack-defense-policy-1] defense syn-flood enable
```

1.1.16 defense syn-flood ip

【命令】

defense syn-flood ip *ip-address* **rate-threshold high** *rate-number* [**low** *rate-number*]

undo defense syn-flood ip *ip-address* [**rate-threshold**]

【视图】

攻击防范策略视图

【缺省级别】

2：系统级

【参数】

ip-address：指定要保护的 IP 地址。该 IP 地址不能为广播地址、127.0.0.0/8、D 类地址或 E 类地址。

high *rate-number*：指定攻击防范的触发阈值。其中，*rate-number* 为向指定 IP 地址每秒发送的 SYN 报文数目，取值范围为 1～64000。使能 SYN Flood 攻击防范后，设备处于攻击检测状态，当它监

测到向指定 IP 地址发送 SYN 报文的速率持续达到或超过了该触发阈值时，即认为该 IP 地址受到了 SYN Flood 攻击，则进入攻击防范状态，并根据配置启动相应的防范措施。

low *rate-number*：指定攻击检测的恢复阈值。其中，*rate-number* 为向指定 IP 地址每秒发送的 SYN 报文数目，取值范围为 1～64000，缺省值为触发阈值的 3/4。当处于攻击防范状态的设备监测到向指定 IP 地址发送 SYN 报文的速率低于该恢复阈值时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。若不指定该参数，则恢复阈值为触发阈值的 3/4。

【描述】

defense syn-flood ip 命令用来对指定 IP 地址配置 SYN Flood 攻击防范参数，包括触发阈值和恢复阈值。**undo defense syn-flood ip** 命令用来取消对指定 IP 地址的 SYN Flood 攻击防范参数配置。

缺省情况下，未对任何指定 IP 地址配置 SYN Flood 攻击防范参数。

每个攻击防范策略下可以指定多个要保护的 IP 地址，每个策略中最多可以保护的 IP 地址为 32 个。

相关配置可参考命令 **defense syn-flood enable**、**defense syn-flood action drop-packet** 和 **display attack-defense policy**。

【举例】

指定针对 IP 地址 192.168.1.2 的 SYN Flood 攻击防范参数，触发阈值为 2000，恢复阈值为 1000。当设备监测到向该 IP 地址每秒发送的 SYN 报文数持续达到或超过 2000 时，启动攻击防范措施；当设备监测到该值低于 1000 时，认为攻击结束，并恢复为攻击检测状态。

```
<Sysname> system-view
[Sysname] attack-defense policy 1
[Sysname-attack-defense-policy-1] defense syn-flood ip 192.168.1.2 rate-threshold high 2000 low 1000
```

1.1.17 defense syn-flood rate-threshold

【命令】

defense syn-flood rate-threshold high *rate-number* [**low** *rate-number*]

undo defense syn-flood rate-threshold

【视图】

攻击防范策略视图

【缺省级别】

2：系统级

【参数】

high *rate-number*：指定攻击防范的触发阈值。其中，*rate-number* 为向某 IP 地址每秒发送的 SYN 报文数目，取值范围为 1～64000。使能 SYN Flood 攻击防范后，设备处于攻击检测状态，当它监测到向某 IP 地址发送 SYN 报文的速率持续达到或超过了该触发阈值时，即认为该 IP 地址受到了 SYN Flood 攻击，则进入攻击防范状态，并根据配置启动相应的防范措施。

low *rate-number*：指定攻击检测的恢复阈值。其中，*rate-number* 为向某 IP 地址每秒发送的 SYN 报文数目，取值范围为 1～64000。当处于攻击防范状态的设备监测到向某 IP 地址发送 SYN 报文的速率低于该恢复阈值时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

【描述】

defense syn-flood rate-threshold 命令用来配置 SYN Flood 攻击防范的全局参数，包括触发阈值和恢复阈值。对于没有专门配置 SYN Flood 攻击参数的 IP 地址，设备采用全局的参数设置来进行保护。**undo defense syn-flood rate-threshold** 命令用来恢复缺省情况。

缺省情况下，触发阈值为每秒 1000 个报文数，恢复阈值为每秒 750 个报文数。

阈值的取值需要根据实际网络应用场景进行调整，对于正常情况下到被保护对象（HTTP 服务器或者 FTP 服务器）的 SYN 报文流量较大的应用场景，建议调大触发阈值，以免阈值太小对正常的业务流量造成影响；对于网络状况较差，且对攻击流量比较敏感的场景，可以适当调小触发阈值。若到被保护网络的带宽较小，可承受的流量压力较小，则建议调小恢复阈值，反之，可以将恢复阈值调大一些。

相关配置可参考命令 **defense syn-flood enable** 和 **display attack-defense policy**。

【举例】

指定 SYN Flood 攻击防范的全局参数，触发阈值为 3000，恢复阈值为 1000。当设备监测到向某 IP 地址每秒发送的 SYN 报文数持续达到或超过 3000 时，启动攻击防范措施；当设备监测到该值低于 1000 时，认为攻击结束，并恢复为攻击检测状态。

```
<Sysname> system-view
[Sysname] attack-defense policy 1
[Sysname-attack-defense-policy-1] defense syn-flood rate-threshold high 3000 low 1000
```

1.1.18 defense udp-flood action drop-packet

【命令】

defense udp-flood action drop-packet

undo defense udp-flood action

【视图】

攻击防范策略视图

【缺省级别】

2：系统级

【参数】

无

【描述】

defense udp-flood action drop-packet 命令用来配置对 UDP Flood 攻击报文的处理方式为丢弃。**undo defense udp-flood action** 命令用来恢复缺省情况。

缺省情况下，检测到 UDP Flood 攻击后，不进行处理。

相关配置可参考命令 **defense udp-flood enable**、**defense udp-flood rate-threshold**、**defense udp-flood ip** 和 **display attack-defense policy**。

【举例】

在攻击防范策略 1 中配置丢弃后续的 UDP Flood 攻击报文。

```
<Sysname> system-view
[Sysname] attack-defense policy 1
```

```
[Sysname-attack-defense-policy-1] defense udp-flood action drop-packet
```

1.1.19 defense udp-flood enable

【命令】

defense udp-flood enable

undo defense udp-flood enable

【视图】

攻击防范策略视图

【缺省级别】

2：系统级

【参数】

无

【描述】

defense udp-flood enable 命令用来使能 UDP Flood 攻击防范。**undo defense udp-flood enable** 命令用来恢复缺省情况。

缺省情况下，UDP Flood 攻击防范处于未使能状态。

相关配置可参考命令 **defense udp-flood rate-threshold**、**defense udp-flood ip**、**defense udp-flood action drop-packet** 和 **display attack-defense policy**。

【举例】

在攻击防范策略 1 中使能 UDP Flood 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy 1
[Sysname-attack-defense-policy-1] defense udp-flood enable
```

1.1.20 defense udp-flood ip

【命令】

defense udp-flood ip *ip-address* **rate-threshold high** *rate-number* [**low** *rate-number*]

undo defense udp-flood ip *ip-address* [**rate-threshold**]

【视图】

攻击防范策略视图

【缺省级别】

2：系统级

【参数】

ip-address：指定要保护的 IP 地址。该 IP 地址不能为广播地址、127.0.0.0/8、D 类地址或 E 类地址。

high *rate-number*：指定攻击防范的触发阈值。其中，*rate-number* 为向指定 IP 地址每秒发送的 UDP 报文数目，取值范围为 1～64000。使能 UDP Flood 攻击防范后，设备处于攻击检测状态，当它监

测到向指定 IP 地址发送 UDP 报文的速率持续达到或超过了该触发阈值时，即认为该 IP 地址受到了 UDP Flood 攻击，则进入攻击防范状态，并根据配置启动相应的防范措施。

low *rate-number*：指定攻击检测的恢复阈值。其中，*rate-number* 为向指定 IP 地址每秒发送的 UDP 报文数目，取值范围为 1～64000，缺省值为触发阈值的 3/4。当处于攻击防范状态的设备监测到向指定 IP 地址发送 UDP 报文的速率低于该恢复阈值时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。若不指定该参数，则恢复阈值为触发阈值的 3/4。

【描述】

defense udp-flood ip 命令用来对指定 IP 地址配置 UDP Flood 攻击防范参数，包括触发阈值和恢复阈值。**undo defense udp-flood ip** 命令用来取消对指定 IP 地址的 UDP Flood 攻击防范参数配置。

缺省情况下，未对任何指定 IP 地址配置 UDP Flood 攻击防范参数。

每个攻击防范策略下最多可以同时对 32 个 IP 地址配置 UDP Flood 攻击防范参数。

相关配置可参考命令 **defense udp-flood enable**、**defense udp-flood action drop-packet** 和 **display attack-defense policy**。

【举例】

指定针对 IP 地址 192.168.1.2 的 UDP Flood 攻击防范参数，触发阈值为 2000，恢复阈值为 1000。当设备监测到向该 IP 地址每秒发送的 UDP 报文数持续达到或超过 2000 时，启动攻击防范措施；当设备监测到该值低于 1000 时，认为攻击结束，并恢复为攻击检测状态。

```
<Sysname> system-view
[Sysname] attack-defense policy 1
[Sysname-attack-defense-policy-1] defense udp-flood ip 192.168.1.2 rate-threshold high 2000 low 1000
```

1.1.21 defense udp-flood rate-threshold

【命令】

defense udp-flood rate-threshold high *rate-number* [**low** *rate-number*]

undo defense udp-flood rate-threshold

【视图】

攻击防范策略视图

【缺省级别】

2：系统级

【参数】

high *rate-number*：指定攻击防范的触发阈值。其中，*rate-number* 为向某 IP 地址每秒发送的 UDP 报文数目，取值范围为 1～64000。使能 UDP Flood 攻击防范后，设备处于攻击检测状态，当它监测到向某 IP 地址发送 UDP 报文的速率持续达到或超过了该触发阈值时，即认为该 IP 地址受到了 UDP Flood 攻击，则进入攻击防范状态，并根据配置启动相应的防范措施。

low *rate-number*：指定攻击检测的恢复阈值。其中，*rate-number* 为向某 IP 地址每秒发送的 UDP 报文数目，取值范围为 1～64000。当处于攻击防范状态的设备监测到向某 IP 地址发送 UDP 报文

的速率低于该恢复阈值时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

【描述】

defense udp-flood rate-threshold 命令用来配置启动 UDP Flood 攻击防范的全局参数，包括触发阈值和恢复阈值。对于没有专门配置 UDP Flood 攻击防范参数的 IP 地址，设备采用该全局参数来进行保护。**undo defense udp-flood rate-threshold** 命令用来恢复缺省情况。

缺省情况下，触发阈值为每秒 1000 个报文数，恢复阈值为每秒 750 个报文数。

阈值的取值需要根据实际网络应用场景进行调整，对于正常情况下到被保护对象的 UDP 报文流量较大的应用场景，建议调大触发阈值，以免阈值太小对正常的业务流量造成影响；对于网络状况较差，且对攻击流量比较敏感的场景，可以适当调小触发阈值。若到被保护网络的带宽较小，可承受的流量压力较小，则建议调小恢复阈值，反之，可以将恢复阈值调大一些。

相关配置可参考命令 **defense udp-flood enable**、**defense udp-flood action drop-packet** 和 **display attack-defense policy**。

【举例】

指定 UDP Flood 攻击防范的全局参数，触发阈值为 3000，恢复阈值为 1000。当设备监测到向某 IP 地址每秒发送的 UDP 报文数持续达到或超过 3000 时，启动攻击防范措施；当设备监测到该值低于 1000 时，认为攻击结束，并恢复为攻击检测状态。

```
<Sysname> system-view
[Sysname] attack-defense policy 1
[Sysname-attack-defense-policy-1] defense udp-flood rate-threshold high 3000 low 1000
```

1.1.22 display attack-defense policy

【命令】

display attack-defense policy [*policy-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

policy-number：攻击防范策略编号，取值范围为 1～128。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display attack-defense policy 命令用来显示攻击防范策略的配置信息，主要包括各类型攻击防范的使能情况、对攻击报文的处理方式和相关的阈值参数。

如果不指定参数 *policy-number*，则显示所有攻击防范策略的摘要信息。

相关配置可参考命令 **attack-defense policy**。

【举例】

显示攻击防范策略 1 的配置信息。

```
<Sysname> display attack-defense policy 1
          Attack-defense Policy Information
-------------------------------------------------------------
Policy number                         : 1
Bound interfaces                      : GigabitEthernet3/0/1
-------------------------------------------------------------
Smurf attack-defense                  : Enabled
ICMP redirect attack-defense          : Disabled
ICMP unreachable attack-defense       : Disabled
Large ICMP attack-defense             : Enabled
    Max-length                        : 250 bytes
TCP flag attack-defense               : Enabled
Tracert attack-defense                : Enabled
Fraggle attack-defense                : Enabled
WinNuke attack-defense                : Enabled
LAND attack-defense                   : Enabled
Source route attack-defense           : Enabled
Route record attack-defense           : Enabled
Scan attack-defense                   : Enabled
    Add to blacklist                  : Enabled
    Blacklist timeout                 : 10 minutes
    Max-rate                          : 1000 connections/s
Signature-detect action               : Drop-packet
-----------------------------------------------------------------------------
ICMP flood attack-defense             : Enabled
ICMP flood action                     : Syslog
ICMP flood high-rate                  : 2000 packets/s
ICMP flood low-rate                   : 750 packets/s
ICMP flood attack-defense for specific IP addresses:
    IP              High-rate(packets/s)    Low-rate(packets/s)
    192.168.1.1     1000                    500
    192.168.2.1     2000                    1000
-----------------------------------------------------------------------------
UDP flood attack-defense              : Enabled
UDP flood action                      : Drop-packet
UDP flood high-rate                   : 2000 packets/s
UDP flood low-rate                    : 750 packets/s
UDP Flood attack-defense for specific IP addresses:
    IP              High-rate(packets/s)    Low-rate(packets/s)
```

```
    192.168.1.1     1000                    500
    192.168.2.1     2000                    500
------------------------------------------------------------------------------
SYN flood attack-defense              : Enabled
SYN flood action                      : Drop-packet
SYN flood high-rate                   : 2000 packets/s
SYN flood low-rate                    : 750 packets/s
SYN Flood attack-defense for specific IP addresses:
    IP              High-rate(packets/s)    Low-rate(packets/s)
    192.168.1.1     1000                    750
    192.168.2.1     2000                    1000
```

表1-1 display attack-defense policy 命令显示信息描述表

字段	描述
Policy number	攻击防范策略编号
Bound interfaces	攻击防范策略应用的接口名
Smurf attack-defense	Smurf攻击防范的状态
ICMP redirect attack-defense	ICMP Redirect攻击防范的状态
ICMP unreachable attack-defense	ICMP Unreachable攻击防范的状态
Large ICMP attack-defense	Large ICMP攻击防范的状态
Max-length	ICMP报文所允许的最大长度
TCP flag attack-defense	TCP Flag攻击防范的状态
Tracert attack-defense	Tracert攻击防范的状态
Fraggle attack-defense	Fraggle攻击防范的状态
WinNuke attack-defense	WinNuke攻击防范的状态
LAND attack-defense	LAND攻击防范的状态
Source route attack-defense	Source Route攻击防范的状态
Route record attack-defense	Route Record攻击防范的状态
Scan attack-defense	扫描攻击防范的状态
Add to blacklist	扫描攻击防范的黑名单添加功能状态
Blacklist timeout	黑名单的老化时间
Max-rate	每秒新建连接的数目阈值
Signature-detect action	对单包攻击报文的处理方式，包括丢弃（Drop-packet）和输出告警日志（Syslog）
ICMP flood attack-defense	ICMP Flood攻击防范的状态
ICMP flood action	对ICMP Flood攻击报文的处理方式，包括丢弃（Drop-packet）和输出告警日志（Syslog）
ICMP flood high-rate	ICMP Flood攻击防范的触发阈值

字段	描述
ICMP flood low-rate	ICMP Flood攻击检测的恢复阈值
ICMP flood attack-defense for specific IP addresses	对指定IP地址的ICMP Flood攻击防范配置
UDP flood attack-defense	UDP Flood攻击防范的状态
UDP flood action	对UDP Flood攻击报文的处理方式，包括丢弃（Drop-packet）和输出告警日志（Syslog）
UDP flood high-rate	UDP Flood攻击防范的触发阈值
UDP flood low-rate	UDP Flood攻击检测的恢复阈值
UDP flood attack on IP	对指定IP地址的UDP Flood攻击防范配置
SYN flood attack-defense	SYN Flood攻击防范的状态
SYN flood action	对SYN Flood攻击报文的处理方式，包括丢弃（Drop-packet）和输出告警日志（Syslog）
SYN flood high-rate	SYN Flood攻击防范的触发阈值
SYN flood low-rate	SYN Flood攻击检测的恢复阈值
SYN flood attack on IP	对指定IP地址的SYN Flood攻击防范配置

显示所有攻击防范策略的概要配置信息。

```
<Sysname> display attack-defense policy
          Attack-defense Policy Brief Information
------------------------------------------------------------
Policy Number       Bound Interface
1                   GigabitEthernet3/0/1
50                  None
128                 GigabitEthernet3/0/2
```

表1-2 display attack-defense policy 命令显示信息描述表

字段	描述
Policy number	攻击防范策略编号
Bound Interface	攻击防范策略应用的接口名

1.1.23 display attack-defense statistics interface

【命令】

display attack-defense statistics interface *interface-type interface-number* [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

interface-type interface-number：接口类型和接口编号。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display attack-defense statistics interface 命令用来显示接口上的攻击防范统计信息，主要包括检测到的攻击次数以及丢弃的攻击报文数。

相关配置可参考命令 **attack-defense policy** 和 **attack-defense apply policy**。

【举例】

显示接口 GigabitEthernet3/0/1 上的攻击防范统计信息。

```
<Sysname> display attack-defense statistics interface gigabitethernet 3/0/1
               Attack-defense Statistics Information
 ------------------------------------------------------------
 Interface                              : GigabitEthernet3/0/1
 ------------------------------------------------------------
 Attack policy number                   : 1
 Fraggle attacks                        : 1
 Fraggle packets dropped                : 100
 ICMP redirect attacks                  : 1
 ICMP redirect packets dropped          : 100
 ICMP unreachable attacks               : 1
 ICMP unreachable packets dropped       : 100
 LAND attacks                           : 1
 LAND attack packets dropped            : 100
 Large ICMP attacks                     : 1
 Large ICMP packets dropped             : 100
 Route record attacks                   : 1
 Route record packets dropped           : 100
 Source route attacks                   : 1
 Source route packets dropped           : 100
 Smurf attacks                          : 1
 Smurf packets dropped                  : 100
 TCP flag attacks                       : 1
 TCP flag packets dropped               : 100
 Tracert attacks                        : 1
 Tracert packets dropped                : 100
 WinNuke attacks                        : 1
```

```
WinNuke packets dropped                : 100
Scan attacks                           : 1
Scan attack packets dropped            : 100
SYN flood attacks                      : 1
SYN flood packets dropped              : 100
ICMP flood attacks                     : 1
ICMP flood packets dropped             : 100
UDP flood attacks                      : 1
UDP flood packets dropped              : 100
```

表1-3 display attack-defense statistics interface 命令显示信息描述表

字段	描述
Interface	攻击防范策略应用的接口名
Attack policy number	攻击防范策略编号
Fraggle attacks	Fraggle攻击次数
Fraggle packets dropped	丢弃的Fraggle报文数
ICMP redirect attacks	ICMP Redirect攻击次数
ICMP redirect packets dropped	丢弃的ICMP Redirect报文数
ICMP unreachable attacks	ICMP Unreachable攻击次数
ICMP unreachable packets dropped	丢弃的ICMP Unreachable报文数
LAND attacks	LAND攻击次数
LAND attack packets dropped	丢弃的LAND报文数
Large ICMP attacks	Large ICMP攻击次数
Large ICMP packets dropped	丢弃的Large ICMP报文数
Route record attacks	Route Record攻击次数
Route record packets dropped	丢弃的Route Record报文数
Source route attacks	Source Route攻击次数
Source route packets dropped	Source Route报文数
Smurf attacks	Smurf攻击次数
Smurf attack packets dropped	丢弃的Smurf报文数
TCP flag attacks	TCP Flag攻击次数
TCP flag packets dropped	丢弃的TCP Flag报文数
Tracert attacks	Tracert攻击次数
Tracert packets dropped	丢弃的Tracert报文数
WinNuke attacks	WinNuke攻击次数
WinNuke packets dropped	丢弃的WinNuke报文数
Scan attacks	扫描攻击次数

字段	描述
Scan attack packets dropped	丢弃的扫描攻击报文数
SYN flood attacks	SYN Flood攻击次数
SYN flood attack packets dropped	丢弃的SYN Flood攻击报文数
ICMP flood attacks	ICMP Flood攻击次数
ICMP flood attack packets dropped	丢弃的ICMP Flood攻击报文数
UDP flood attacks	UDP Flood攻击次数
UDP flood attack packets dropped	丢弃的UDP Flood攻击报文数

1.1.24 display blacklist

【命令】

display blacklist { **all** | **ip** *source-ip-address* [**slot** *slot-number*] | **slot** *slot-number* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

ip *source-ip-address*：显示指定 IP 地址的黑名单表项。其中，*source-ip-address* 表示黑名单表项的 IP 地址，该 IP 地址不能为广播地址、127.0.0.0/8、D 类地址或 E 类地址。

all：显示所有黑名单表项。

slot *slot-number*：显示指定单板上的黑名单表项，*slot-number* 表示单板所在槽位号。如果不指定该参数，则表示显示所有单板上的黑名单表项。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

SR6600/SR6600-X 路由器各款型对于本节所描述的参数的支持情况有所不同，详细差异信息如下：

型号	参数	描述
SR6602	**slot** *slot-number*	不支持
SR6602-X		支持
SR6604/SR6608/SR6616		支持
SR6604-X/SR6608-X/SR6616-X		支持

【描述】

display blacklist 命令用来显示黑名单信息，主要包括黑名单的使能情况、黑名单的配置以及相关统计信息。

相关配置可参考命令 **blacklist enable** 和 **blacklist ip**。

【举例】

显示所有黑名单表项的相关信息。

```
<Sysname> display blacklist all
                  Blacklist information
------------------------------------------------------------------------------
Blacklist                              : enabled
Blacklist items                        : 1
------------------------------------------------------------------------------
IP              Type   Aging started       Aging finished      Dropped packets
                       YYYY/MM/DD hh:mm:ss YYYY/MM/DD hh:mm:ss

Total blacklist items on slot 0        : 3
2.2.1.2         manual 2008/08/27 19:15:39 Never               0
1.1.1.2         auto   2008/09/01 18:26:31 2008/09/01 18:36:31 4294967295
1.1.1.3         manual 2008/09/02 06:13:20 2008/09/02 07:54:47 4294967295
------------------------------------------------------------------------------
```

表1-4 display blacklist all 命令显示信息描述表

字段	描述
Blacklist	黑名单功能的使能情况
Blacklist items	已有的黑名单表项数目
IP	黑名单表项的IP地址
Type	黑名单表项的类型 • manual：手工添加 • auto：扫描攻击防范时自动添加
Aging started	黑名单表项的添加时间
Aging finished	黑名单表项的老化时间；若永不老化，则显示Never
Dropped packets	丢弃来自该IP地址的报文数目
Total blacklist items on slot 0	0槽位上主控的黑名单表项数目，SR6602无此字段

1.1.25 display flow-statistics statistics

【命令】

display flow-statistics statistics [**slot** *slot-number*] { **destination-ip** *dest-ip-address* | **source-ip** *src-ip-address* } [**vpn-instance** *vpn-instance-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

destination-ip *dest-ip-address*：显示指定目的 IP 地址的流量统计信息。其中，*dest-ip-address* 表示目的 IP 地址，该 IP 地址不能为广播地址、127.0.0.0、D 类地址或 E 类地址。

source-ip *src-ip-address*：显示指定源 IP 地址的流量统计信息。其中，*src-ip-address* 表示源 IP 地址，该 IP 地址不能为广播地址、127.0.0.0、D 类地址或 E 类地址。

vpn-instance *vpn-instance-name*：显示指定 VPN 实例的流量统计信息。其中，*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示待查询的统计对象位于公网中。

slot *slot-number*：显示指定单板上的流量统计信息，*slot-number* 表示单板所在槽位号。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

SR6600/SR6600-X 路由器各款型对于本节所描述的参数的支持情况有所不同，详细差异信息如下：

型号	参数	描述
SR6602	**slot** *slot-number*	不支持
SR6602-X		支持
SR6604/SR6608/SR6616		支持
SR6604-X/SR6608-X/SR6616-X		支持

【描述】

display flow-statistics statistics 命令用来显示接口上基于 IP 地址的流量统计信息。

【举例】

显示源 IP 地址为 192.168.1.2 的流量统计信息。

```
<Sysname> display flow-statistics statistics source-ip 192.168.1.2
```

```
              Flow Statistics Information
-------------------------------------------------------------
IP Address                              :  192.168.1.2
-------------------------------------------------------------
Total number of existing sessions       :  70
Session establishment rate              :  10/s
TCP sessions                            :  10
Half-open TCP sessions                  :  10
Half-close TCP sessions                 :  10
TCP session establishment rate          :  10/s
UDP sessions                            :  10
UDP session establishment rate          :  10/s
ICMP sessions                           :  10
ICMP session establishment rate         :  10/s
RAWIP sessions                          :  10
RAWIP session establishment rate        :  10/s
```

表1-5 display flow-statistics statistics 命令显示信息描述表

字段	描述
IP Address	统计对象的源IP地址
Total number of existing sessions	所有连接数目
Session establishment rate	新建连接的速率
TCP sessions	TCP连接的数目
Half-open TCP sessions	半开连接的数目
Half-close TCP sessions	半闭连接的数目
TCP session establishment rate	新建TCP连接的速率
UDP sessions	UDP连接的数目
UDP session establishment rate	新建UDP连接的速率
ICMP sessions	ICMP连接的数目
ICMP session establishment rate	新建ICMP连接的速率
RAWIP sessions	RAWIP连接的数目
RAWIP session establishment rate	新建RAWIP连接的速率

1.1.26 display flow-statistics statistics interface

【命令】

display flow-statistics statistics interface *interface-type interface-number* { **inbound** | **outbound** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

interface-type interface-number：接口类型和接口编号。

inbound：显示接口入方向的流量统计信息。

outbound：显示接口出方向的流量统计信息。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display flow-statistics statistics interface 命令用来显示接口上的流量统计信息。

【举例】

显示接口 GigabitEthernet3/0/1 入方向上的流量统计信息。

```
<Sysname> display flow-statistics statistics interface gigabitethernet 3/0/1 inbound
              Flow Statistics Information
 ------------------------------------------------------------
 Interface                               : GigabitEthernet3/0/1
 ------------------------------------------------------------
 Total number of existing sessions      :  70
 Session establishment rate             :  10/s
 TCP sessions                           :  10
 Half-open TCP sessions                 :  10
 Half-close TCP sessions                :  10
 TCP session establishment rate         :  10/s
 UDP sessions                           :  10
 UDP session establishment rate         :  10/s
 ICMP sessions                          :  10
 ICMP session establishment rate        :  10/s
 RAWIP sessions                         :  10
 RAWIP session establishment rate       :  10/s
```

表1-6 display flow-statistics statistics interface 命令显示信息描述表

字段	描述
Interface	进行流量统计的接口名
Total number of existing sessions	所有连接数目
Session establishment rate	新建连接的速率
TCP sessions	TCP连接的数目
Half-open TCP sessions	半开连接的数目

字段	描述
Half-close TCP sessions	半闭连接的数目
TCP session establishment rate	新建TCP连接的速率
UDP sessions	UDP连接的数目
UDP session establishment rate	新建UDP连接的速率
ICMP sessions	ICMP连接的数目
ICMP session establishment rate	新建ICMP连接的速率
RAWIP sessions	RAWIP连接的数目
RAWIP session establishment rate	新建RAWIP连接的速率

1.1.27 display tcp-proxy protected-ip

【命令】

display tcp-proxy protected-ip [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

slot *slot-number*：显示指定单板上的受保护 IP 表项，*slot-number* 表示单板所在槽位号。

SR6600/SR6600-X 路由器各款型对于本节所描述的参数的支持情况有所不同，详细差异信息如下：

型号	参数	描述
SR6602	**slot** *slot-number*	不支持
SR6602-X		支持
SR6604/SR6608/SR6616		支持
SR6604-X/SR6608-X/SR6616-X		支持

【描述】

display tcp-proxy protected-ip 命令用来显示受 TCP Proxy 保护的 IP 表项信息。

需要注意的是：

对于 SR6602-X/SR6604/SR6608/SR6616/SR6604-X/SR6608-X/SR6616-X 路由器，如果不指定任何参数，则显示所有单板上的受保护 IP 表项信息。

【举例】

显示所有受 TCP Proxy 保护 IP 表项信息。

```
<Sysname> display tcp-proxy protected-ip
Protected IP    Port Number  Type        Lifetime(min) Rejected packets
1.1.1.1         any          Dynamic     1             2
```

表1-7 display tcp-proxy protected-ip 命令显示信息描述表

字段	描述
Protected IP	受保护IP地址
Port Number	TCP连接的目的端口 any表示对该IP地址的所有端口的TCP连接请求都做代理
Type	该受保护IP表项的类型，Dynamic表示该表项为设备动态添加
Lifetime(min)	动态添加的受保护IP表项的存活时间 当存活时间为0时，该动态受保护IP表项将被删除
Rejected packets	收到的匹配该受保护IP表项，但未通过验证的TCP连接请求报文数

1.1.28 flow-statistics enable

【命令】

flow-statistics enable { **destination-ip** | **inbound** | **outbound** | **source-ip** }

undo flow-statistics enable { **destination-ip** | **inbound** | **outbound** | **source-ip** }

【视图】

接口视图

【缺省级别】

2：系统级

【参数】

destination-ip：表示按照目的 IP 地址进行流量统计，即对该接口上发送的报文按照目的 IP 地址进行流量统计。

inbound：表示按照接口的入方向进行流量统计，即对该接口上收到的报文进行流量统计。

outbound：表示按照接口的出方向进行流量统计，即对该接口上发送的报文进行流量统计。

source-ip：表示按照源 IP 地址进行流量统计，即对该接口上收到的报文按照源 IP 地址进行流量统计。

【描述】

flow-statistics enable 命令用来使能接口上的流量统计功能。**undo flow-statistics enable** 命令用来恢复缺省情况。

缺省情况下，接口上未使能任何类型的流量统计功能。

接口上可使能多种类型的流量统计功能，不同类型的统计结果可通过相关的显示命令分别查看。

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

【举例】

在接口 GigabitEthernet3/0/1 上使能基于目的 IP 地址的流量统计功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] flow-statistics enable destination-ip
```

可通过如下命令来查看该接口上发送的目的 IP 地址为 2.2.2.2 的报文统计信息（此处目的 IP 地址请根据实际情况配置）。

```
[Sysname-GigabitEthernet3/0/1] display flow-statistics statistics destination-ip 2.2.2.2
```

1.1.29 reset attack-defense statistics interface

【命令】

reset attack-defense statistics interface *interface-type interface-number*

【视图】

用户视图

【缺省级别】

1：监控级

【参数】

interface-type interface-number：接口类型和接口编号。

【描述】

reset attack-defense statistics interface 命令用来清除接口上的攻击防范统计信息。

相关配置可参考命令 **display attack-defense statistics interface**。

【举例】

清除接口 GigabitEthernet3/0/1 上的攻击防范统计信息。

```
<Sysname> reset attack-defense statistics interface gigabitethernet 3/0/1
```

1.1.30 signature-detect

【命令】

signature-detect { **fraggle** | **icmp-redirect** | **icmp-unreachable** | **land** | **large-icmp** | **route-record** | **smurf** | **source-route** | **tcp-flag** | **tracert** | **winnuke** } **enable**

undo signature-detect { **fraggle** | **icmp-redirect** | **icmp-unreachable** | **land** | **large-icmp** | **route-record** | **smurf** | **source-route** | **tcp-flag** | **tracert** | **winnuke** } **enable**

【视图】

攻击防范策略视图

【缺省级别】

2：系统级

【参数】

fraggle：表示 Fraggle 类型的报文攻击。

icmp-redirect：表示 ICMP Redirect 类型的报文攻击。

icmp-unreachable：表示 ICMP Unreachable 类型的报文攻击。

land：表示 LAND 类型的报文攻击。

large-icmp：表示 Large ICMP 类型的报文攻击。

route-record：表示 Route Record 类型的报文攻击。

smurf：表示 Smurf 类型的报文攻击。

source-route：表示 Source Route 类型的报文攻击。

tcp-flag：表示 TCP Flag 类型的报文攻击。

tracert：表示 Tracert 类型的报文攻击。

winnuke：表示 WinNuke 类型的报文攻击。

【描述】

signature-detect 命令用来使能对单包攻击报文的特征检测。**undo signature-detect** 命令用来去使能指定类型的单包攻击报文的特征检测。

缺省情况下，所有类型的单包攻击报文的特征检测均处于未使能状态。

相关配置可参考命令 **display attack-defense policy**。

【举例】

在攻击防范策略 1 中使能对 Fraggle 攻击的特征检测。

```
<Sysname> system-view
[Sysname] attack-defense policy 1
[Sysname-attack-defense-policy-1] signature-detect fraggle enable
```

1.1.31 signature-detect action drop-packet

【命令】

signature-detect action drop-packet

undo signature-detect action

【视图】

攻击防范策略视图

【缺省级别】

2：系统级

【参数】

无

【描述】

signature-detect action drop-packet 命令用来配置对单包攻击报文的处理方式为丢弃。**undo signature-detect action** 命令用来恢复缺省情况。

缺省情况下，检测到单包攻击后，不对报文进行处理。

相关配置可参考命令 **display attack-defense policy**。

【举例】

在攻击防范策略 1 中配置丢弃单包攻击报文。

```
<Sysname> system-view
[Sysname] attack-defense policy 1
[Sysname-attack-defense-policy-1] signature-detect action drop-packet
```

1.1.32 signature-detect large-icmp max-length

【命令】

signature-detect large-icmp max-length *length*

undo signature-detect large-icmp max-length

【视图】

攻击防范策略视图

【缺省级别】

2：系统级

【参数】

length：表示 ICMP 报文的最大长度，取值范围为 28～65534，单位为字节。

【描述】

signature-detect large-icmp max-length 命令用来配置启动 Large ICMP 攻击防范的 ICMP 报文的长度阈值。**undo signature-detect large-icmp max-length** 命令用来恢复缺省情况。

缺省情况下，启动 Large ICMP 攻击防范的 ICMP 报文的长度阈值为 4000 个字节。

在 Large ICMP 攻击报文的特征检测已使能的情况下，若设备监测到某 ICMP 报文的长度超过了指定的阈值，则认为该报文为 Large ICMP 攻击报文。

需要注意的是，该命令仅在 Large ICMP 攻击报文的特征检测已使能的情况下有效。

相关配置可参考命令 **display attack-defense policy** 和 **signature-detect large-icmp enable**。

【举例】

使能 Large ICMP 攻击防范，配置启动 Large ICMP 攻击防范的 ICMP 报文的长度阈值为 5000 个字节，并对超过指定报文长度的 ICMP 报文进行丢弃处理。

```
<Sysname> system-view
[Sysname] attack-defense policy 1
[Sysname-attack-defense-policy-1] signature-detect large-icmp enable
[Sysname-attack-defense-policy-1] signature-detect large-icmp max-length 5000
[Sysname-attack-defense-policy-1] signature-detect action drop-packet
```

1.1.33 tcp-proxy enable

【命令】

tcp-proxy enable

undo tcp-proxy enable

【视图】

接口视图

【缺省级别】

2：系统级

【参数】

无

【描述】

tcp-proxy enable 命令用来在接口上使能 TCP Proxy 功能。**undo tcp-proxy enable** 命令用来关闭 TCP Proxy 功能。

缺省情况下，接口上的 TCP Proxy 功能处于关闭状态。

该功能一般应用在设备连接外部网络的接口上，用来保护内部网络的服务器免受外部网络中非法客户端发起的 SYN Flood 攻击。当设备监测到某服务器受到了 SYN Flood 攻击时，会根据 **defense syn-flood action** 的配置启动相应的防范措施。若防范措施配置为对攻击报文进行 TCP Proxy，则设备会将该服务器 IP 地址添加到受保护 IP 表项中（可通过 **display tcp-proxy protected-ip** 命令查看），并按照指定的 TCP Proxy 工作模式，对后续新建 TCP 连接的协商报文进行合法性检查，过滤非法客户端发起的 TCP 连接报文。

只有 TCP Proxy 功能处于使能状态时，设备在检测到 SYN Flood 攻击后，对后续报文进行的 TCP Proxy 才能生效。

相关配置可参考命令 **defense syn-flood action**、**tcp-proxy mode** 和 **display tcp-proxy protected-ip**。

【举例】

在接口 GigabitEthernet3/0/1 上使能 TCP Proxy 功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] tcp-proxy enable
```

1.1.34 tcp-proxy mode

【命令】

tcp-proxy mode unidirection

undo tcp-proxy mode

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

unidirection：指定 TCP Proxy 的工作模式为单向代理模式。

【描述】

tcp-proxy mode 命令用来配置 TCP Proxy 的工作模式。**undo tcp-proxy mode** 命令用来恢复缺省情况。

缺省情况下，TCP Proxy 工作模式为双向代理模式。

相关配置可参考命令 **tcp-proxy enable** 和 **display tcp-proxy protected-ip**。

【举例】

配置 TCP Proxy 的工作模式为单向代理模式。

```
<Sysname>system-view
[Sysname] tcp-proxy mode unidirection
```