

目 录

1 攻击检测与防范.....	1-1
1.1 攻击检测与防范配置命令.....	1-1
1.1.1 ack-flood action.....	1-1
1.1.2 ack-flood detect.....	1-1
1.1.3 ack-flood detect non-specific.....	1-3
1.1.4 ack-flood threshold.....	1-3
1.1.5 attack-defense apply policy.....	1-4
1.1.6 attack-defense local apply policy.....	1-5
1.1.7 attack-defense login reauthentication-delay.....	1-6
1.1.8 attack-defense policy.....	1-7
1.1.9 attack-defense signature log non-aggregate.....	1-8
1.1.10 attack-defense tcp fragment enable.....	1-8
1.1.11 display attack-defense flood statistics ip.....	1-9
1.1.12 display attack-defense flood statistics ipv6.....	1-11
1.1.13 display attack-defense policy.....	1-13
1.1.14 display attack-defense policy ip.....	1-19
1.1.15 display attack-defense policy ipv6.....	1-20
1.1.16 display attack-defense scan attacker ip.....	1-22
1.1.17 display attack-defense scan attacker ipv6.....	1-23
1.1.18 display attack-defense scan victim ip.....	1-25
1.1.19 display attack-defense scan victim ipv6.....	1-26
1.1.20 display attack-defense statistics interface.....	1-27
1.1.21 display attack-defense statistics local.....	1-33
1.1.22 dns-flood action.....	1-39
1.1.23 dns-flood detect.....	1-40
1.1.24 dns-flood detect non-specific.....	1-41
1.1.25 dns-flood port.....	1-42
1.1.26 dns-flood threshold.....	1-43
1.1.27 exempt acl.....	1-44
1.1.28 fin-flood action.....	1-45
1.1.29 fin-flood detect.....	1-46
1.1.30 fin-flood detect non-specific.....	1-47
1.1.31 fin-flood threshold.....	1-48

1.1.32 http-flood action	1-49
1.1.33 http-flood detect	1-49
1.1.34 http-flood detect non-specific	1-51
1.1.35 http-flood port	1-52
1.1.36 http-flood threshold	1-53
1.1.37 icmp-flood action	1-53
1.1.38 icmp-flood detect ip	1-54
1.1.39 icmp-flood detect non-specific	1-55
1.1.40 icmp-flood threshold	1-56
1.1.41 icmpv6-flood action	1-57
1.1.42 icmpv6-flood detect ipv6	1-58
1.1.43 icmpv6-flood detect non-specific	1-59
1.1.44 icmpv6-flood threshold	1-60
1.1.45 reset attack-defense policy flood	1-61
1.1.46 reset attack-defense statistics interface	1-62
1.1.47 reset attack-defense statistics local	1-62
1.1.48 rst-flood action	1-63
1.1.49 rst-flood detect	1-63
1.1.50 rst-flood detect non-specific	1-65
1.1.51 rst-flood threshold	1-65
1.1.52 scan detect	1-66
1.1.53 signature { large-icmp large-icmpv6 } max-length	1-67
1.1.54 signature detect	1-68
1.1.55 signature level action	1-71
1.1.56 signature level detect	1-72
1.1.57 syn-ack-flood action	1-73
1.1.58 syn-ack-flood detect	1-74
1.1.59 syn-ack-flood detect non-specific	1-75
1.1.60 syn-ack-flood threshold	1-76
1.1.61 syn-flood action	1-77
1.1.62 syn-flood detect	1-78
1.1.63 syn-flood detect non-specific	1-79
1.1.64 syn-flood threshold	1-80
1.1.65 udp-flood action	1-81
1.1.66 udp-flood detect	1-81
1.1.67 udp-flood detect non-specific	1-83

1.1.68 udp-flood threshold.....	1-83
---------------------------------	------

1 攻击检测与防范

1.1 攻击检测与防范配置命令

1.1.1 ack-flood action

ack-flood action 命令用来配置 ACK flood 攻击防范的全局处理行为。

undo ack-flood action 命令用来恢复缺省情况。

【命令】

```
ack-flood action { drop | logging } *  
undo ack-flood action
```

【缺省情况】

不对检测到的 ACK flood 攻击采取任何措施。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 ACK 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息。

【举例】

在攻击防范策略 atk-policy-1 中配置 ACK flood 攻击防范的全局处理行为是丢弃后续报文。

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

【相关命令】

- **ack-flood threshold**
- **ack-flood detect**
- **ack-flood detect non-specific**

1.1.2 ack-flood detect

ack-flood detect 命令用来开启对指定 IP 地址的 ACK flood 攻击防范检测，并配置 ACK flood 攻击防范的触发阈值和对 ACK flood 攻击的处理行为。

undo ack-flood detect 命令用来关闭对指定 IP 地址的 ACK flood 攻击防范检测。

【命令】

```
ack-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance  
vpn-instance-name ] [ threshold threshold-value ] [ action { { drop | logging }  
* | none } ]  
  
undo ack-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance  
vpn-instance-name ]
```

【缺省情况】

未对任何指定 IP 地址开启 ACK flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

ip *ipv4-address*: 指定要保护的 IPv4 地址。该 IPv4 地址不能为全 1 地址或全 0 地址。

ipv6 *ipv6-address*: 指定要保护的 IPv6 地址。

vpn-instance *vpn-instance-name*: 受保护 IP 地址所属的 VPN 实例。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。若未指定本参数，则表示该保护 IP 地址属于公网。

threshold *threshold-value*: 指定 ACK flood 攻击防范的触发阈值。其中，*threshold-value* 为向指定 IP 地址每秒发送的 ACK 报文数目，取值范围为 1~1000000。

action: 设置对 ACK flood 攻击的处理行为。若未指定本参数，则表示采用 ACK flood 攻击防范的全局处理行为。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 ACK 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息。

none: 表示不采取任何动作。

【使用指导】

使能 ACK 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 ACK 报文的速率持续达到或超过了触发阈值时，即认为该 IP 地址受到了 ACK 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。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）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。

每个攻击防范策略下可以同时为多个 IP 地址配置 ACK flood 攻击防范检测。

【举例】

在攻击防范策略 **atk-policy-1** 中开启对 IP 地址 192.168.1.2 的 ACK flood 攻击防范检测，并指定触发阈值为 2000。当设备监测到向该 IP 地址每秒发送的 ACK 报文数持续达到或超过 2000 时，启动 ACK flood 攻击防范。

```
<Sysname> system-view
```

```
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] ack-flood detect ip 192.168.1.2 threshold 2000
```

【相关命令】

- **ack-flood action**
- **ack-flood detect non-specific**
- **ack-flood threshold**

1.1.3 ack-flood detect non-specific

ack-flood detect non-specific 命令用来对所有非受保护 IP 地址开启 ACK flood 攻击防范检测。

undo ack-flood detect non-specific 命令用来关闭对所有非受保护 IP 地址的 ACK flood 攻击防范检测。

【命令】

```
ack-flood detect non-specific
undo ack-flood detect non-specific
```

【缺省情况】

未对任何非受保护 IP 地址开启 ACK flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【使用指导】

对所有未配置具体攻击防范策略的 IP 地址开启 ACK flood 攻击防范检测后，设备将采用全局的阈值设置（由 **ack-flood threshold** 命令设置）和处理行为（由 **ack-flood action** 命令配置）对这些 IP 地址进行保护。

【举例】

在攻击防范策略 atk-policy-1 中，对所有非受保护 IP 地址开启 ACK flood 攻击防范检测。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] ack-flood detect non-specific
```

【相关命令】

- **ack-flood action**
- **ack-flood detect**
- **ack-flood threshold**

1.1.4 ack-flood threshold

ack-flood threshold 命令用来配置 ACK flood 攻击防范的全局触发阈值。

undo ack-flood threshold 命令用来恢复缺省情况。

【命令】

```
ack-flood threshold threshold-value
undo ack-flood threshold
```

【缺省情况】

ACK flood 攻击防范的全局触发阈值为 1000。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

threshold-value: 指定向某 IP 地址每秒发送的 ACK 报文数目，取值范围为 1~1000000。

【使用指导】

使能 ACK 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 ACK 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 ACK 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。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）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。

对于未专门配置 ACK flood 攻击防范检测的 IP 地址，设备采用全局的阈值设置来进行保护。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 ACK 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。

【举例】

在攻击防范策略 atk-policy-1 中配置 ACK flood 攻击防范的全局触发阈值为 100，即当设备监测到向某 IP 地址每秒发送的 ACK 报文数持续达到或超过 100 时，启动 ACK flood 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] ack-flood threshold 100
```

【相关命令】

- **ack-flood action**
- **ack-flood detect**
- **ack-flood detect non-specific**

1.1.5 attack-defense apply policy

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。

【命令】

```
attack-defense apply policy policy-name  
undo attack-defense apply policy
```

【缺省情况】

接口上未应用任何攻击防范策略。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

policy-name: 攻击防范策略名称，为 1~31 个字符的字符串，不区分大小写。合法取值包括大写字母、小写字母、数字、特殊字符“_”和“-”。

【使用指导】

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。

【举例】

```
# 将攻击防范策略 atk-policy-1 应用到接口 Ten-GigabitEthernet1/0/25 上。  
<Sysname> system-view  
[Sysname] interface ten-gigabitethernet 1/0/25  
[Sysname-Ten-GigabitEthernet1/0/25] attack-defense apply policy atk-policy-1
```

【相关命令】

- **attack-defense policy**
- **display attack-defense policy**

1.1.6 attack-defense local apply policy

attack-defense local apply policy 命令用来在本机应用安全攻击防范策略。

undo attack-defense local apply policy 命令用来恢复缺省情况。

【命令】

```
attack-defense local apply policy policy-name  
undo attack-defense local apply policy
```

【缺省情况】

本机未应用任何攻击防范策略。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

policy-name: 攻击防范策略名称，为 1~31 个字符的字符串，不区分大小写。合法取值包括大写字母、小写字母、数字、特殊字符“_”和“-”。

【使用指导】

通过在本机应用攻击防范策略，使已配置的攻击防范策略对目的地址为本机的报文生效。

缺省情况下设备将需要转发的报文下发给硬件转发，只有目的地址是本机的报文才会由软件处理，但软件没有攻击防范功能。因此在设备上，为处理针对本机的攻击，需要通过在本机上应用攻击防范策略来实现。

本机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除了可以应用到本机外，还可应用到多个接口上。

当同时在接口和本机应用攻击防范策略时，目的地址是本机的报文到达设备后，将会被根据应用在接口上的策略和应用在本机的策略先后检测两次。

【举例】

在本机应用攻击防范策略 *atk-policy-1*。

```
<Sysname> system-view
```

```
[Sysname] attack-defense local apply policy atk-policy-1
```

【相关命令】

- **attack-defense policy**
- **display attack-defense policy**

1.1.7 attack-defense login reauthentication-delay

attack-defense login reauthentication-delay 命令用来配置 Login 用户登录失败后重新进行认证的等待时长。

undo attack-defense login reauthentication-delay 命令用来恢复缺省情况。

【命令】

```
attack-defense login reauthentication-delay seconds
```

```
undo attack-defense login reauthentication-delay
```

【缺省情况】

Login 用户登录失败后重新进行认证不需要等待。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

seconds: 设备管理用户登录失败后重新进行认证的等待时长，取值范围为 4~60，单位为秒。

【使用指导】

Login 用户登录失败后，若设备上配置了重新进行认证的等待时长，则系统将会延迟一定的时长之后再允许用户进行认证，可以避免设备受到字典式攻击。

Login 用户延迟认证功能与 **Login** 用户攻击防范功能无关，只要配置了延迟认证等待时间，即可生效。

【举例】

配置 **Login** 用户登录失败后重新进行认证的等待时长为 5 秒钟。

```
<Sysname> system-view
[Sysname] attack-defense login reauthentication-delay 5
```

1.1.8 attack-defense policy

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。如果指定的攻击防范策略已经存在，则直接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。

【命令】

```
attack-defense policy policy-name
undo attack-defense policy policy-name
```

【缺省情况】

不存在任何攻击防范策略。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

policy-name: 攻击防范策略名称，为 1~31 个字符的字符串，不区分大小写。合法取值包括大写字母、小写字母、数字、特殊字符“_”和“-”。

【举例】

创建攻击防范策略 **atk-policy-1**，并进入攻击防范策略视图。

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

【相关命令】

- **attack-defense apply policy**
- **display attack-defense policy**

1.1.9 attack-defense signature log non-aggregate

attack-defense signature log non-aggregate 命令用来指定对单包攻击防范日志非聚合输出。

undo attack-defense signature log non-aggregate 命令用来恢复缺省情况。

【命令】

```
attack-defense signature log non-aggregate
undo attack-defense signature log non-aggregate
```

【缺省情况】

单包攻击防范的日志信息经系统聚合后再输出。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

对日志进行聚合输出是指，在一定时间内，对在本机、同一个接口上检测到的相同攻击类型、相同攻击防范动作、相同的源/目的地址以及属于相同 VPN 的单包攻击的所有日志聚合成一条日志输出。通常不建议开启单包攻击防范的日志非聚合输出功能，因为在单包攻击较为频繁的情况下，它会导致大量日志信息输出，占用控制台的显示资源。

【举例】

```
# 开启对单包攻击防范日志的非聚合输出功能。
<Sysname> system-view
[Sysname] attack-defense signature log non-aggregate
```

【相关命令】

- **signature detect**

1.1.10 attack-defense tcp fragment enable

attack-defense tcp fragment enable 命令用来开启 TCP 分片攻击防范功能。

undo attack-defense tcp fragment enable 命令用来关闭 TCP 分片攻击防范功能。

【命令】

```
attack-defense tcp fragment enable
undo attack-defense tcp fragment enable
```

【缺省情况】

TCP 分片攻击防范功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

设备的包过滤功能一般是通过判断 TCP 首个分片中的五元组（源 IP 地址、源端口号、目的 IP 地址、目的端口号、传输层协议号）信息来决定后续 TCP 分片是否允许通过。RFC 1858 对 TCP 分片报文进行了规定，认为 TCP 分片报文中，首片报文中 TCP 报文长度小于 20 字节，或后续分片报文中分片偏移量等于 8 字节的报文为 TCP 分片攻击报文。这类报文可以成功绕过上述包过滤功能，对设备造成攻击。为防止这类攻击，可以在设备上开启 TCP 分片攻击防范功能，对 TCP 分片攻击报文进行丢弃。

如果设备上开启了 TCP 分片攻击防范功能，并应用了单包攻击防范策略，则 TCP 分片攻击防范功能会先于单包攻击防范策略检测并处理入方向的 TCP 报文。

【举例】

开启 TCP 分片攻击防范功能。

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

1.1.11 display attack-defense flood statistics ip

display attack-defense flood statistics ip 命令用来显示 IPv4 flood 攻击防范统计信息。

【命令】

```
display attack-defense { ack-flood | dns-flood | fin-flood | flood |
http-flood | icmp-flood | rst-flood | syn-ack-flood | syn-flood | udp-flood }
statistics ip [ ip-address [ vpn vpn-instance-name ] ] [ [ interface
interface-type interface-number | local ] [ slot slot-number ] ] [ count ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

ack-flood: 显示 ACK flood 攻击防范统计信息。

dns-flood: 显示 DNS flood 攻击防范统计信息。

fin-flood: 显示 FIN flood 攻击防范统计信息。

flood: 显示所有类型的 IPv4 flood 攻击防范统计信息。

http-flood: 显示 HTTP flood 攻击防范统计信息。

icmp-flood: 显示 ICMP flood 攻击防范统计信息。

rst-flood: 显示 RST flood 攻击防范统计信息。

syn-ack-flood: 显示 SYN-ACK flood 攻击防范统计信息。

syn-flood: 显示 SYN flood 攻击防范统计信息。

udp-flood: 显示 UDP flood 攻击防范统计信息。

ip-address: 显示指定目的 IPv4 地址的 flood 攻击防范统计信息。若未指定本参数，则显示所有目的 IPv4 地址的 flood 攻击防范统计信息。

vpn-instance vpn-instance-name: 指定 IPv4 地址所属的 VPN 实例。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。若未指定本参数，则表示该 IPv4 地址属于公网。

interface interface-type interface-number: 显示指定接口的 flood 攻击防范统计信息，interface-type interface-number 表示接口类型和接口编号。

local: 显示本机上进行检测的 flood 攻击防范统计信息。

slot slot-number: 显示指定成员设备上的 flood 攻击防范统计信息，slot-number 表示设备在 IRF 中的成员编号。该参数仅在指定本机或指定全局接口（例如 VLAN 接口）时可见。若未指定本参数，则表示显示所有成员设备上的 flood 攻击防范统计信息。

count: 显示符合指定条件的被进行 flood 攻击检测的 IPv4 地址数目。

【使用指导】

由于 flood 攻击不关心源地址，因此本命令显示的是对指定目的 IPv4 地址的攻击防范统计信息。若未指定 **interface** 和 **local** 参数，则显示所有接口以及本机上的 flood 攻击防范统计信息。

【举例】

```
# 显示所有类型的 IPv4 flood 攻击防范统计信息。
<Sysname> display attack-defense flood statistics ip
slot 1:
IP address      VPN      Detected on  Detect type  State  PPS    Dropped
192.168.100.221 --      XGE1/0/26   SYN-ACK-FLOOD Normal  1000   4294967295
192.168.11.5    --      XGE1/0/27   ACK-FLOOD    Normal  1000   222222222
201.55.7.44     --      Local       DNS-FLOOD    Normal  1000   111111111
192.168.11.4    --      Local       ACK-FLOOD    Normal  1000   22222222
slot 2:
IP address      VPN      Detected on  Detect type  State  PPS    Dropped
201.55.1.10     --      XGE1/0/27   ACK-FLOOD    Normal  1000   222222222
192.168.100.30  --      XGE1/0/28   DNS-FLOOD    Normal  1000   333333333
192.168.100.66  --      Local       SYN-ACK-FLOOD Normal  1000   165467998

# 显示所有类型的 flood 攻击检测的 IPv4 地址数目。
<Sysname> display attack-defense flood statistics ip count
Slot 1:
Totally 2 flood entries.
Slot 2:
Totally 1 flood entries.
```

表1-1 display attack-defense flood statistics ip 命令显示信息描述表

字段	描述
IP address	被检测的目的IPv4地址
VPN	目的IPv4地址所属的MPLS L3VPN实例名称，属于公网时显示为 “--”

字段	描述
Detected on	进行攻击检测的位置，包括接口和本机（Local）
Detect type	检测的flood攻击类型
State	接口或本机是否处于攻击状态，可包括以下取值： <ul style="list-style-type: none"> Attacked: 受攻击状态 Normal: 正常状态（当前并未受到攻击）
PPS	指定的目的IPv4地址收到flood攻击报文的速率（单位为报文每秒）
Dropped	接口或本机丢弃的flood攻击报文数目
Totally 2 flood entries	被检测的IPv4地址数目

1.1.12 display attack-defense flood statistics ipv6

display attack-defense flood statistics ipv6 命令用来显示 IPv6 flood 攻击防范统计信息。

【命令】

```
display attack-defense { ack-flood | dns-flood | fin-flood | flood |
http-flood | icmpv6-flood | rst-flood | syn-flood | syn-ack-flood | udp-flood }
statistics ipv6 [ ipv6-address [ vpn vpn-instance-name ] ] [ [ interface
interface-type interface-number | local ] [ slot slot-number ] ] [ count ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

ack-flood: 显示指定 ACK flood 类型统计信息。
dns-flood: 显示指定 DNS flood 类型统计信息。
fin-flood: 显示指定 FIN flood 类型统计信息。
flood: 显示所有类型的 IPv6 flood 攻击防范统计信息。
http-flood: 显示 HTTP flood 攻击防范统计信息。
icmpv6-flood: 显示指定 ICMPv6 flood 类型统计信息。
rst-flood: 显示指定 RST flood 类型统计信息。
syn-flood: 显示指定 SYN flood 类型统计信息。
syn-ack-flood: 显示 SYN-ACK flood 攻击防范统计信息。
udp-flood: 显示指定 UDP flood 类型统计信息。

ipv6-address: 显示指定目的 IPv6 地址的 flood 攻击防范统计信息。若未指定本参数，则显示所有目的 IPv6 地址的 flood 攻击防范统计信息。

vpn vpn-instance-name: 指定 IPv6 地址所属的 VPN 实例。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。若未指定本参数，则表示该 IPv6 地址属于公网。

interface interface-type interface-number: 显示指定接口的 flood 攻击防范统计信息，*interface-type interface-number* 表示接口类型和接口编号。

local: 显示本机上进行检测的 flood 攻击防范统计信息。

slot slot-number: 显示指定成员设备上的 flood 攻击防范统计信息，*slot-number* 表示设备在 IRF 中的成员编号。该参数仅在指定本机或指定全局接口（例如 VLAN 接口）时可见。若未指定本参数，则表示显示所有成员设备上的 flood 攻击防范统计信息。

count: 仅显示符合指定条件的被进行 flood 攻击检测的 IPv6 地址数目。

【使用指导】

由于 flood 攻击不关心源地址，因此本命令显示的是对指定目的 IPv6 地址的攻击防范统计信息。若未指定 **interface** 和 **local** 参数，则显示所有接口以及本机上的 flood 攻击防范统计信息。

【举例】

显示所有类型的 IPv6 flood 攻击防范统计信息。

```
<Sysname> display attack-defense flood statistics ipv6
Slot 1:
IPv6 address      VPN      Detected on Detect type  State   PPS    Dropped
1::2              --      XGE1/0/26   DNS-FLOOD   Normal  1000   111111111
1::3              --      XGE1/0/27   SYN-ACK-FLOOD Normal  1000   222222222
1::4              --      Local       ACK-FLOOD   Normal  1000   111111111
1::5              --      Local       SYN-FLOOD   Normal  1000   222222222
Slot 2:
IPv6 address      VPN      Detected on Detect type  State   PPS    Dropped
1::2              --      XGE1/0/27   SYN-FLOOD   Normal  1000   468792363
1::5              --      XGE1/0/27   ACK-FLOOD   Normal  1000   452213396
1::6              --      Local       DNS-FLOOD   Normal  1000   12569985
```

显示所有类型的 flood 攻击检测的 IPv6 地址数目。

```
<Sysname> display attack-defense flood statistics ipv6 count
Slot 1:
Totally 4 flood entries.
Slot 2:
Totally 3 flood entries.
```

表1-2 display attack-defense flood statistics ipv6 命令显示信息描述表

字段	描述
IPv6 address	被检测的目的IPv6地址
VPN	目的IPv6地址所属的MPLS L3VPN实例名称，属于公网时显示为“--”
Detected on	进行攻击检测的位置，包括接口和本机（Local）

字段	描述
Detect type	检测的flood攻击类型
State	接口或本机是否处于攻击状态，可包括以下取值： <ul style="list-style-type: none"> Attacked: 受攻击状态 Normal: 正常状态（当前并未受到攻击）
PPS	指定的目的IPv6地址收到报文的速率（单位为报文每秒）
Dropped	接口或本机丢弃的flood攻击报文数目
Totally 4 flood entries	被检测的IPv6地址数目

1.1.13 display attack-defense policy

display attack-defense policy 用来显示攻击防范策略的配置信息。

【命令】

display attack-defense policy [*policy-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

policy-name: 攻击防范策略名称，为 1~31 个字符的字符串，包括英文大/小写字母、数字、下划线和连字符，不区分大小写。若未指定本参数，则表示显示所有攻击防范策略的摘要信息。

【使用指导】

本命令显示的内容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。

【举例】

显示指定攻击防范策略 **abc** 的配置信息。

```
<Sysname> display attack-defense policy abc
      Attack-defense Policy Information
-----
Policy name           : abc
Applied list          : Local
                      XGE1/0/25
                      Vlan1
-----
Exempt IPv4 ACL:      : Not configured
Exempt IPv6 ACL:      : vip
-----
Actions: CV-Client verify  BS-Block source  L-Logging  D-Drop  N-None
```


Signature attack defense configuration:

Signature name	Defense	Level	Actions
Fragment	Enabled	Info	L
Impossible	Enabled	Info	L
Teardrop	Disabled	Info	L
Tiny fragment	Disabled	Info	L
IP option abnormal	Disabled	Info	L
Smurf	Disabled	Info	N
Traceroute	Disabled	Medium	L,D
Ping of death	Disabled	Low	L
Large ICMP	Disabled	Medium	L,D
Max length	4000 bytes		
Large ICMPv6	Disabled	Low	L
Max length	4000 bytes		
TCP invalid flags	Disabled	medium	L,D
TCP null flag	Disabled	Low	L
TCP all flags	Enabled	Info	L
TCP SYN-FIN flags	Disabled	Info	L
TCP FIN only flag	Enabled	Info	L
TCP Land	Disabled	Info	L
Winnuke	Disabled	Info	L
UDP Bomb	Disabled	Info	L
UDP Snork	Disabled	Info	L
UDP Fraggle	Enabled	Info	L
IP option record route	Disabled	Info	L
IP option internet timestamp	Enabled	Info	L
IP option security	Disabled	Info	L
IP option loose source routing	Enabled	Info	L
IP option stream ID	Disabled	Info	L
IP option strict source routing	Disabled	Info	L
IP option route alert	Disabled	Info	L
ICMP echo request	Disabled	Info	L
ICMP echo reply	Disabled	Info	L
ICMP source quench	Disabled	Info	L
ICMP destination unreachable	Enabled	Info	L
ICMP redirect	Enabled	Info	L
ICMP time exceeded	Enabled	Info	L
ICMP parameter problem	Disabled	Info	L
ICMP timestamp request	Disabled	Info	L
ICMP timestamp reply	Disabled	Info	L
ICMP information request	Disabled	Info	L
ICMP information reply	Disabled	Medium	L,D
ICMP address mask request	Disabled	Medium	L,D
ICMP address mask reply	Disabled	Medium	L,D
ICMPv6 echo request	Enabled	Medium	L,D
ICMPv6 echo reply	Disabled	Medium	L,D
ICMPv6 group membership query	Disabled	Medium	L,D

ICMPv6 group membership report	Disabled	Medium	L,D
ICMPv6 group membership reduction	Disabled	Medium	L,D
ICMPv6 destination unreachable	Enabled	Medium	L,D
ICMPv6 time exceeded	Enabled	Medium	L,D
ICMPv6 parameter problem	Disabled	Medium	L,D
ICMPv6 packet too big	Disabled	Medium	L,D

Scan attack defense configuration:

Defense: Disabled

Level: Medium

Actions: L

Flood attack defense configuration:

Flood type	Global thres(pps)	Global actions	Service ports	Non-specific
SYN flood	1000(default)	-	-	Disabled
ACK flood	1000(default)	-	-	Enabled
SYN-ACK flood	1000(default)	-	-	Disabled
RST flood	200	-	-	Enabled
FIN flood	1000(default)	L,D	-	Disabled
UDP flood	1000(default)	-	-	Disabled
ICMP flood	1000(default)	-	-	Disabled
ICMPv6 flood	1000(default)	CV	-	Disabled
DNS flood	10000	-	30,61 to 62	Enabled
HTTP flood	10000	-	80,8080	Enabled

Flood attack defense for protected IP addresses:

Address	VPN instance	Flood type	Thres(pps)	Actions	Ports
1::1	--	FIN-FLOOD	10	L,D	-
192.168.1.1	--	SYN-ACK-FLOOD	10	-	-
1::1	--	FIN-FLOOD	-	L	-
2013:2013:2013:2013: 2013:2013:2013:2013	--	DNS-FLOOD	100	L,CV	53

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

字段	描述
Policy name	攻击防范策略名称
Applied list	攻击防范策略应用的对象列表，包括接口名称和本机（Local）
Exempt IPv4 ACL	IPv4例外列表
Exempt IPv6 ACL	IPv6例外列表
Actions	攻击防范的处理行为，包括以下取值： <ul style="list-style-type: none"> • CV: 启用客户端验证 • L: 输出告警日志 • D: 丢弃报文 • N: 不采用任何处理行为

字段	描述
Signature attack defense configuration	单包攻击防范配置信息
Signature name	单包的类型
Defense	攻击防范的开启状态，包括以下取值： Enabled: 开启 Disabled: 关闭
Level	单包攻击的级别，包括以下取值： <ul style="list-style-type: none"> Info: 提示级别 low: 低级别 medium: 中级别 high: 高级别（目前暂无实例）
IP option record route	IP 选项record route攻击
IP option security	IP 选项security攻击
IP option stream ID	IP 选项stream identifier攻击
IP option internet timestamp	IP 选项 internet timestamp攻击
IP option loose source routing	IP 选项loose source routing攻击
IP option strict source routing	IP 选项strict source routing攻击
IP option abnormal	IP 选项异常攻击
IP option route alert	IP 选项route alert攻击
Fragment	IP分片异常攻击
IP impossible	IP impossible攻击
Tiny fragment	IP tiny fragment攻击
Teardrop	IP teardrop攻击，又称IP overlapping fragments
Large ICMP	Large ICMP攻击
Max length	ICMP报文所允许的最大长度
Smurf	Smurf攻击
Traceroute	Traceroute攻击
Ping of death	Ping of death攻击
ICMP echo request	ICMP echo request攻击
ICMP echo reply	ICMP echo reply攻击
ICMP source quench	ICMP source quench攻击
ICMP redirect	ICMP redirect攻击
ICMP parameter problem	ICMP parameter problem攻击
ICMP timestamp request	ICMP timestamp request攻击

字段	描述
ICMP timestamp reply	ICMP timestamp reply攻击
ICMP information request	ICMP information request攻击
ICMP information reply	ICMP information reply攻击
ICMP address mask request	ICMP address mask request攻击
ICMP address mask reply	ICMP address mask reply攻击
ICMP destination unreachable	ICMP destination unreachable攻击
ICMP time exceeded	ICMP time exceeded攻击
Large ICMPv6	Large ICMPv6攻击
ICMPv6 echo request	ICMPv6 echo request攻击
ICMPv6 echo reply	ICMPv6 echo reply攻击
ICMPv6 group membership query	ICMPv6 group membership query攻击
ICMPv6 group membership report	ICMPv6 group membership report攻击
ICMPv6 group membership reduction	ICMPv6 group membership reduction攻击
ICMPv6 destination unreachable	ICMPv6 destination unreachable攻击
ICMPv6 time exceeded	ICMPv6 time exceeded攻击
ICMPv6 parameter problem	ICMPv6 parameter problem攻击
ICMPv6 packet too big	ICMPv6 packet too big攻击
Winnuke	Winnuke攻击
TCP Land	Land攻击
TCP NULL flag	TCP NULL flag攻击
TCP invalid flags	TCP invalid flags攻击
TCP all flags	TCP所有标志位均被置位攻击，又称圣诞树攻击
TCP SYN-FIN flags	TCP SYN和FIN被同时置位攻击
TCP FIN only flag	TCP 只有FIN被置位的攻击
Fraggle	Fraggle攻击，又称UDP chargen DoS attack
UDP Bomb	UDP Bomb攻击
Snork	Snork攻击
Scan attack defense configuration	扫描攻击防范配置信息
Level	扫描攻击的级别，包括以下取值： <ul style="list-style-type: none"> low: 低级别 medium: 中级别 high: 高级别
Flood attack defense configuration	flood攻击防范配置信息

字段	描述
Flood type	<p>flood攻击类型，包括以下取值：</p> <ul style="list-style-type: none"> • ACK flood • DNS flood • FIN flood • ICMP flood • ICMPv6 flood • SYN flood • SYN-ACK flood • UDP flood • RST flood • HTTP flood
Global thres(pps)	flood攻击防范的全局触发阈值，单位为每秒报文数，默认为1000pps
Global actions	<p>flood攻击防范的全局处理行为，包括以下取值：</p> <ul style="list-style-type: none"> • D：丢弃报文 • L：输出告警日志， • CV：启用客户端验证 • -：未配置
Service ports	flood攻击防范的全局检测端口号。该字段只对DNS flood攻击防范和HTTP flood攻击防范生效，对于其它flood攻击防范，显示为“-”
Non-specific	对非受保护IP地址开启SYN flood攻击防范检测的状态
Flood attack defense for protected IP addresses	对受保护IP地址的flood攻击防范配置
Address	指定的IP地址
VPN instance	所属的VPN实例名称，未配置时显示为“-”
Thres(pps)	攻击防范检测的触发阈值，单位为报文每秒，未配置时显示为“-”
Ports	Flood攻击防范的检测端口号。该字段只对DNS flood攻击防范和HTTP flood攻击防范生效，对于其他攻击防范，显示为“-”

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 Name          Applied list
Atk-policy-1         Ten-GigabitEthernet1/0/25
                     Ten-GigabitEthernet1/0/26
P2                   None
P123                 Ten-GigabitEthernet1/0/26
```

```
p1 Local
p12 Local
```

表1-4 display attack-defense policy 命令显示信息描述表

字段	描述
Policy Name	攻击防范策略名称
Applied list	攻击防范策略应用的对象列表，包括接口名称和本机（Local）

【相关命令】

- **attack-defense policy**

1.1.14 display attack-defense policy ip

display attack-defense policy ip 命令用来显示 flood 攻击防范的 IPv4 类型的受保护 IP 表项。

【命令】

```
display attack-defense policy policy-name { ack-flood | dns-flood |
fin-flood | flood | http-flood | icmp-flood | rst-flood | syn-ack-flood |
syn-flood | udp-flood } ip [ ip-address [ vpn vpn-instance-name ] ] [ slot
slot-number ] [ count ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
```

【参数】

policy-name: 攻击防范策略名称，为 1~31 个字符的字符串，不区分大小写。合法取值包括大写字母、小写字母、数字、特殊字符“_”和“-”。

ack-flood: 显示 ACK flood 攻击防范受保护 IP 表项。

dns-flood: 显示 DNS flood 攻击防范受保护 IP 表项。

fin-flood: 显示 FIN flood 攻击防范受保护 IP 表项。

flood: 显示所有类型的 flood 攻击防范受保护 IP 表项。

http-flood: 显示 HTTP flood 攻击防范受保护 IP 表项。

icmp-flood: 显示 ICMP flood 攻击防范受保护 IP 表项。

rst-flood: 显示 RST flood 攻击防范受保护 IP 表项。

syn-ack-flood: 显示 SYN-ACK flood 攻击防范受保护 IP 表项。

syn-flood: 显示 SYN flood 攻击防范受保护 IP 表项。

udp-flood: 显示 UDP flood 攻击防范受保护 IP 表项。

ip ip-address: 显示指定 IPv4 地址的受保护 IP 表项。若未指定 *ip-address* 参数，则表示显示所有 IPv4 类型的受保护 IP 表项。

vpn-instance vpn-instance-name: 显示指定 VPN 实例的受保护 IP 表项。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。若未指定本参数，则表示显示指公网的受保护 IP 表项。

slot slot-number: 显示指定成员设备上的受保护 IP 表项，*slot-number* 表示设备在 IRF 中的成员编号。如果不指定该参数，则表示显示所有成员设备上的受保护 IP 表项。

count: 显示符合指定条件的 flood 受保护 IP 表项的数目。

【举例】

显示指定攻击防范策略 abc 中所有 flood 攻击防范的 IPv4 类型受保护 IP 表项的信息。

```
<Sysname> display attack-defense policy abc flood ip
Slot 1:
IP address      VPN instance    Type              Rate threshold(PPS) Dropped
123.123.123.123 --              SYN-ACK-FLOOD    100                4294967295
201.55.7.45     --              ICMP-FLOOD       100                10
192.168.11.5    --              DNS-FLOOD        23                 100
Slot 2:
IP address      VPN instance    Type              Rate threshold(PPS) Dropped
```

显示指定攻击防范策略 abc 中所有 IPv4 类型 flood 受保护 IP 表项的个数。

```
<Sysname> display attack-defense policy abc flood ip count
Slot 1:
Totally 3 flood protected IP addresses.
Slot 2:
Totally 0 flood protected IP addresses.
```

表1-5 display attack-defense flood ip 命令显示信息描述表

字段	描述
Totally 3 flood protected IP addresses	IPv4类型受保护IP表项数目
IP address	受保护的IPv4地址
VPN instance	受保护的IPv4地址所属的MPLS L3VPN实例名称，未指定时显示为“--”
Type	flood攻击类型
Rate threshold(PPS)	配置的flood攻击防范触发阈值（单位为报文每秒），未配置时显示“-”
Dropped	检测到flood攻击后的丢包数，若只输出日志该项显示为0

1.1.15 display attack-defense policy ipv6

display attack-defense policy ipv6 命令用来显示 flood 攻击防范的 IPv6 类型的受保护 IP 表项。

【命令】

```
display attack-defense policy policy-name { ack-flood | dns-flood |  
fin-flood | flood | http-flood | icmpv6-flood | rst-flood | syn-ack-flood  
| syn-flood | udp-flood } ipv6 [ ipv6-address [ vpn vpn-instance-name ] ]  
[ slot slot-number ] [ count ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

policy-name: 攻击防范策略名称，为 1~31 个字符的字符串，不区分大小写。合法取值包括大写字母、小写字母、数字、特殊字符“_”和“-”。

ack-flood: 显示 ACK flood 攻击防范受保护 IP 表项。

dns-flood: 显示 DNS flood 攻击防范受保护 IP 表项。

fin-flood: 显示 FIN flood 攻击防范受保护 IP 表项。

flood: 显示所有类型的 flood 攻击防范受保护 IP 表项。

http-flood: 显示 HTTP flood 攻击防范受保护 IP 表项。

icmpv6-flood: 显示 ICMPv6 flood 攻击防范受保护 IP 表项。

rst-flood: 显示 RST flood 攻击防范受保护 IP 表项。

syn-ack-flood: 显示 SYN-ACK flood 攻击防范受保护 IP 表项。

syn-flood: 显示 SYN flood 攻击防范受保护 IP 表项。

udp-flood: 显示 UDP flood 攻击防范受保护 IP 表项。

ipv6 ipv6-address: 显示指定 IPv6 地址的受保护 IP 表项。若未指定 *ipv6-address* 参数，则表示所有 IPv6 类型的受保护 IP 表项。

vpn-instance vpn-instance-name: 显示指定 VPN 实例的受保护 IP 表项。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。

slot slot-number: 显示指定成员设备上的受保护 IP 表项，*slot-number* 表示设备在 IRF 中的成员编号。如果不指定该参数，则表示显示所有成员设备上的受保护 IP 表项。

count: 显示符合指定条件的 flood 受保护 IP 表项的数目。

【举例】

显示指定攻击防范策略 abc 中所有 flood 攻击防范的 IPv6 类型受保护 IP 表项。

```
<Sysname> display attack-defense policy abc flood ipv6
```

```
Slot 1:
```

IPv6 address	VPN instance	Type	Rate threshold(PPS)	Dropped
2013::127f	--	SYN-ACK-FLOOD	100	4294967295
2::5	--	ACK-FLOOD	100	10
1::5	--	ACK-FLOOD	100	23


```

Slot 2:
IPv6 address      VPN instance      Type              Rate threshold(PPS) Dropped
# 显示指定攻击防范策略 abc 中所有 flood 攻击防范的 IPv6 类型受保护 IP 表项的个数。
<Sysname> display attack-defense policy abc flood ipv6 count
Slot 1:
Totally 3 flood protected IP addresses.
Slot 2:
Totally 0 flood protected IP addresses.

```

表1-6 display flood ipv6 命令显示信息描述表

字段	描述
Totally 3 flood protected IP addresses	IPv6类型受保护IP表项数目
IPv6 address	受保护的IPv6地址
VPN instance	受保护的IPv6地址所属的MPLS L3VPN实例名称，未指定时显示为“--”
Type	flood攻击类型
Rate threshold(PPS)	配置的flood攻击防范触发阈值（单位为报文每秒），未配置时显示“-”
Dropped	检测到flood攻击后的丢包数，若只输出日志该项显示为0

1.1.16 display attack-defense scan attacker ip

display attack-defense scan attacker ip 命令用来显示扫描攻击者的 IPv4 地址表项。

【命令】

```

display attack-defense scan attacker ip [ [ interface interface-type
interface-number | local ] [ slot slot-number ] ] [ count ]

```

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator

```

【参数】

interface interface-type interface-number: 显示指定接口上检测到的扫描攻击者的 IPv4 地址表项，*interface-type interface-number* 表示接口类型和接口编号。

local: 显示本机检测到的扫描攻击者 IPv4 地址表项。

slot slot-number: 显示指定成员设备上的扫描攻击者的 IPv4 地址表项，*slot-number* 表示设备在 IRF 中的成员编号。该参数仅在指定本机或指定全局接口（例如 VLAN 接口）时可见。如果不指定该参数，则表示显示所有成员设备上的扫描攻击者的 IPv4 地址表项。

count: 显示符合指定条件的当前扫描攻击者的 IPv4 地址表项数目。

【使用指导】

若未指定任何参数，则表示显示所有扫描攻击者的 IPv4 地址表项。

【举例】

显示所有扫描攻击者的 IPv4 地址表项。

```
<Sysname> display attack-defense scan attacker ip
Slot 1:
IP address      VPN instance    Detected on      Duration(min)
192.168.31.2    --              XGE1/0/26       1284
2.2.2.3         --              XGE1/0/26       23
192.68.11.2     --              Local           782
Slot 2:
IP address      VPN instance    Detected on      Duration(min)
192.168.1.100   --              XGE1/0/26       1586
202.2.1.172     --              XGE1/0/26       258
```

显示所有扫描攻击者的 IPv4 地址表项的个数。

```
<Sysname> display attack-defense scan attacker ip count
Slot 1:
Totally 3 attackers.
Slot 2:
Totally 2 attackers.
```

表1-7 display attack-defense scan attacker ip 命令显示信息描述表

字段	描述
Totally 3 attackers	扫描攻击者的数目
IP address	发起攻击的IPv4地址
VPN instance	所属的MPLS L3VPN实例名称，属于公网时显示为“--”
Detected on	进行攻击检测的位置，包括接口或本机（Local）
Duration(min)	检测到攻击持续的时间，单位为分钟

【相关命令】

- **display attack-defense scan victim ip**
- **scan detect**

1.1.17 display attack-defense scan attacker ipv6

display attack-defense scan attacker ipv6 命令用来显示扫描攻击者的 IPv6 地址表项。

【命令】

```
display attack-defense scan attacker ipv6 [ [ interface interface-type interface-number | local ] [ slot slot-number ] ] [ count ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface *interface-type interface-number*: 显示指定接口的扫描攻击者的 IPv6 地址表项, *interface-type interface-number* 表示接口类型和接口编号。

local: 显示本机检测到的扫描攻击者 IPv6 地址表项。

slot *slot-number*: 显示指定成员设备上的扫描攻击者的 IPv6 地址表项, *slot-number* 表示设备在 IRF 中的成员编号。该参数仅在指定本机或指定全局接口（例如 VLAN 接口）时可见。如果不指定该参数, 则表示显示所有成员设备上的扫描攻击者的 IPv6 地址表项。

count: 显示符合指定条件的当前扫描攻击者的 IPv6 地址表项数目。

【使用指导】

若未指定任何参数, 则表示显示所有扫描攻击者的 IPv6 地址表项。

【举例】

显示扫描攻击者的 IPv6 地址表项。

```
<Sysname> display attack-defense scan attacker ipv6
Slot 1:
IPv6 address      VPN instance      Detected on        Duration(min)
2013::2           --                XGE1/0/28         1234
1230::22          --                XGE1/0/28         10
1002: : 20        --                Local              782
Slot 2:
IPv6 address      VPN instance      Detected on        Duration(min)
```

显示扫描攻击者的 IPv6 地址表项的个数。

```
<Sysname> display attack-defense scan attacker ipv6 count
Slot 1:
Totally 3 attackers.
Slot 2:
Totally 0 attackers.
```

表1-8 display attack-defense scan attacker ipv6 命令显示信息描述表

字段	描述
Totally 3 attackers	攻击者的数目
IPv6 address	发起攻击的IPv6地址
VPN instance	所属的MPLS L3VPN实例名称, 属于公网时显示为 “--”
Detected on	进行攻击检测的位置, 包括接口或本机 (Local)
Duration(min)	检测到攻击持续的时间, 单位为分钟

【相关命令】

- **display attack-defense scan victim ipv6**

- `scan detect`

1.1.18 display attack-defense scan victim ip

`display attack-defense scan victim ip` 命令用来显示扫描攻击被攻击者的 IPv4 地址表项。

【命令】

```
display attack-defense scan victim ip [ [ interface interface-type
interface-number | local ] [ slot slot-number ] ] [ count ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface interface-type interface-number: 显示指定接口的被攻击者的 IPv4 地址表项, *interface-type interface-number* 表示接口类型和接口编号。

local: 显示本机检测到的被攻击者的 IPv4 地址表项。

slot slot-number: 显示指定成员设备上的被攻击者的 IPv4 地址表项, *slot-number* 表示设备在 IRF 中的成员编号。该参数仅在指定本机或指定全局接口（例如 VLAN 接口）时可见。如果不指定该参数, 则表示显示所有成员设备上的被攻击者的 IPv4 地址表项。

count: 显示符合指定条件的被攻击者的 IPv4 地址表项数目。

【使用指导】

若未指定任何参数, 则表示显示所有扫描攻击的被攻击者的 IPv4 地址表项。

【举例】

显示扫描攻击的被攻击者的 IPv4 地址表项。

```
<Sysname> display attack-defense scan victim ip
Slot 1:
IP address      VPN instance    Detected on      Duration(min)
192.168.31.2    --              XGE1/0/28       21
2.2.2.3         --              XGE1/0/28       1234
192.168.24.82   --              Local            782
Slot 2:
IP address      VPN instance    Detected on      Duration(min)
```

显示扫描攻击的被攻击者的 IPv4 地址表项的个数。

```
<Sysname> display attack-defense scan victim ip count
Slot 1:
Totally 3 victim IP addresses.
Slot 2:
Totally 0 victim IP addresses.
```

表1-9 display attack-defense scan victim ip 命令显示信息描述表

字段	描述
Totally 3 victim IP addresses	被攻击者的数目
IP address	被攻击的IPv4地址
VPN instance	所属的MPLS L3VPN实例名称，属于公网时显示为“--”
Detected on	进行攻击检测的位置，包括接口或本机（Local）
Duration(min)	检测到被攻击的持续时间，单位为分钟

【相关命令】

- `display attack-defense scan attacker ip`
- `scan detect`

1.1.19 display attack-defense scan victim ipv6

`display attack-defense scan victim ipv6` 命令用来显示扫描攻击被攻击者 IPv6 表项。

【命令】

```
display attack-defense scan victim ipv6 [ [ interface interface-type
interface-number | local ] [ slot slot-number ] ] [ count ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface interface-type interface-number: 显示指定接口的被攻击者的 IPv6 地址表项，*interface-type interface-number* 表示接口类型和接口编号。

slot slot-number: 显示指定成员设备上的被攻击者的 IPv6 地址表项，*slot-number* 表示设备在 IRF 中的成员编号。该参数仅在指定本机或指定全局接口（例如 VLAN 接口）时可见。如果不指定该参数，则表示显示所有成员设备上的被攻击者的 IPv6 地址表项。

local: 显示本机检测到的被攻击者的 IPv6 地址表项。

count: 仅显示符合指定条件的当前被攻击者的数目。

【使用指导】

若未指定任何参数，则表示显示所有扫描攻击的被攻击者的 IPv6 地址表项。

【举例】

显示扫描攻击的被攻击者的 IPv6 地址表项。

```
<Sysname> display attack-defense scan victim ipv6
Slot 1:
```

IPv6 address	VPN instance	Detected on	Duration(min)
2013::2	--	XGE1/0/28	210
1230::22	--	XGE1/0/28	13
1002::20	--	Local	28

Slot 2:

IPv6 address	VPN instance	Detected on	Duration(min)
--------------	--------------	-------------	---------------

显示扫描攻击的被攻击者的 IPv6 地址表项的个数。

<Sysname> display attack-defense scan victim ipv6 count

Slot 1:

Totally 3 victim IP addresses.

Slot 2:

Totally 0 victim IP addresses.

表1-10 display attack-defense scan victim ipv6 命令显示信息描述表

字段	描述
Totally 3 victim IP addresses	被攻击者的数目
IPv6 address	被攻击的IPv6地址
VPN instance	所属的MPLS L3VPN实例名称，属于公网时显示为“--”
Detected on	进行攻击检测的位置，包括接口或本机（Local）
Duration(min)	检测到被攻击的持续时间，单位为分钟

【相关命令】

- **display attack-defense scan attacker ipv6**
- **scan detect**

1.1.20 display attack-defense statistics interface

display attack-defense statistics interface 命令用来显示接口上的攻击防范统计信息。

【命令】

display attack-defense statistics interface *interface-type*
interface-number [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface-type interface-number: 表示指定接口的接口类型和接口编号。

slot slot-number: 显示接口在指定成员设备上的攻击防范统计信息，*slot-number* 表示设备在 IRF 中的成员编号。如果不指定该参数，则表示显示所有成员设备上的攻击防范统计信息。该参数仅在指定全局接口（例如 VLAN 接口）时可见。

【举例】

显示接口 Ten-GigabitEthernet1/0/25 上的攻击防范统计信息。

```
<Sysname> display attack-defense statistics interface ten-gigabitethernet 1/0/25
```

```
Attack policy name: abc
```

```
Slot 1:
```

```
Scan attack defense statistics:
```

AttackType	AttackTimes	Dropped
Port scan	2	23
IP sweep	3	33
Distribute port scan	1	10

```
Flood attack defense statistics:
```

AttackType	AttackTimes	Dropped
SYN flood	1	0
ACK flood	1	0
SYN-ACK flood	3	5000
RST flood	2	0
FIN flood	2	0
UDP flood	1	0
ICMP flood	1	0
ICMPv6 flood	1	0
DNS flood	1	0
HTTP flood	1	0

```
Signature attack defense statistics:
```

AttackType	AttackTimes	Dropped
IP option record route	1	100
IP option security	2	0
IP option stream ID	3	0
IP option internet timestamp	4	1
IP option loose source routing	5	0
IP option strict source routing	6	0
IP option route alert	3	0
Fragment	1	0
Impossible	1	1
Teardrop	1	1
Tiny fragment	1	0
IP options abnormal	3	0
Smurf	1	0
Ping of death	1	0
Traceroute	1	0
Large ICMP	1	0
TCP NULL flag	1	0
TCP all flags	1	0
TCP SYN-FIN flags	1	0
TCP FIN only flag	1	0

TCP invalid flag	1	0
TCP Land	1	0
Winnuke	1	0
UDP Bomb	1	0
Snork	1	0
Fraggle	1	0
Large ICMPv6	1	0
ICMP echo request	1	0
ICMP echo reply	1	0
ICMP source quench	1	0
ICMP destination unreachable	1	0
ICMP redirect	2	0
ICMP time exceeded	3	0
ICMP parameter problem	4	0
ICMP timestamp request	5	0
ICMP timestamp reply	6	0
ICMP information request	7	0
ICMP information reply	4	0
ICMP address mask request	2	0
ICMP address mask reply	1	0
ICMPv6 echo request	1	1
ICMPv6 echo reply	1	1
ICMPv6 group membership query	1	0
ICMPv6 group membership report	1	0
ICMPv6 group membership reduction	1	0
ICMPv6 destination unreachable	1	0
ICMPv6 time exceeded	1	0
ICMPv6 parameter problem	1	0
ICMPv6 packet too big	1	0

Slot 2:

Scan attack defense statistics:

AttackType	AttackTimes	Dropped
Port scan	1	12
IP sweep	2	35
Distribute port scan	5	48

Flood attack defense statistics:

AttackType	AttackTimes	Dropped
SYN flood	1	0
ACK flood	1	0
SYN-ACK flood	3	4200
RST flood	2	0
FIN flood	2	0
UDP flood	1	0
ICMP flood	1	0
ICMPv6 flood	1	0
DNS flood	1	0
HTTP flood	1	0

Signature attack defense statistics:

AttackType	AttackTimes	Dropped
IP option record route	1	100
IP option security	2	0
IP option stream ID	3	0
IP option internet timestamp	4	1
IP option loose source routing	5	0
IP option strict source routing	6	0
IP option route alert	3	0
Fragment	1	0
Impossible	1	1
Teardrop	1	1
Tiny fragment	1	0
IP options abnormal	3	0
Smurf	3	0
Ping of death	1	0
Traceroute	1	2
Large ICMP	2	0
TCP NULL flag	1	0
TCP all flags	1	0
TCP SYN-FIN flags	1	0
TCP FIN only flag	1	0
TCP invalid flag	1	0
TCP Land	1	0
Winnuke	1	0
UDP Bomb	1	0
Snork	1	0
Fraggle	1	0
Large ICMPv6	1	0
ICMP echo request	1	0
ICMP echo reply	1	0
ICMP source quench	1	0
ICMP destination unreachable	1	0
ICMP redirect	2	0
ICMP time exceeded	3	0
ICMP parameter problem	4	0
ICMP timestamp request	5	0
ICMP timestamp reply	6	0
ICMP information request	7	0
ICMP information reply	4	0
ICMP address mask request	2	0
ICMP address mask reply	1	0
ICMPv6 echo request	1	1
ICMPv6 echo reply	1	1
ICMPv6 group membership query	1	0
ICMPv6 group membership report	1	0
ICMPv6 group membership reduction	1	0
ICMPv6 destination unreachable	1	0
ICMPv6 time exceeded	1	0

ICMPv6 parameter problem	1	0
ICMPv6 packet too big	1	0

表1-11 display attack-defense statistics interface 命令显示信息描述表

字段	描述
AttackType	攻击类型
AttackTimes	受到攻击的次数
Dropped	丢弃报文的数目
SYN flood	SYN flood攻击，当AttackTimes为0时，该列不显示
ACK flood	ACK flood攻击，当AttackTimes为0时，该列不显示
SYN-ACK flood	SYN-ACK flood攻击，当AttackTimes为0时，该列不显示
RST flood	RST flood攻击，当AttackTimes为0时，该列不显示
FIN flood	FIN flood攻击，当AttackTimes为0时，该列不显示
UDP flood	UDP flood 攻击，当AttackTimes为0时，该列不显示
ICMP flood	ICMP flood攻击，当AttackTimes为0时，该列不显示
ICMPv6 flood	ICMPv6 flood攻击，当AttackTimes为0时，该列不显示
DNS flood	DNS flood攻击，当AttackTimes为0时，该列不显示
HTTP flood	HTTP flood攻击，当AttackTimes为0时，该列不显示
Port scan	端口扫描攻击，当AttackTimes 为0时，该列不显示
IP Sweep	IP扫描攻击，当AttackTimes 为0时，该列不显示
Distribute port scan	分布式端口扫描攻击，当AttackTimes为0时，该列不显示
IP option record route	IP选项record route攻击，当AttackTimes为0时，该列不显示
IP option security	IP选项security攻击，当AttackTimes 为0时，该列不显示
IP option stream ID	IP选项stream identifier攻击，当AttackTimes 为0时，该列不显示
IP option internet timestamp	IP选项 internet timestamp攻击，当AttackTimes为0时，该列不显示
IP option loose source routing	IP选项loose source routing攻击，当AttackTimes为0时，该列不显示
IP option strict source routing	IP选项strict source routing攻击，当AttackTimes为0时，该列不显示
IP option route alert	IP 选项strict source routing攻击，当AttackTimes为0时，该列不显示
Fragment	IP分片异常攻击，当AttackTimes为0时，该列不显示
Impossible	IP impossible攻击，当AttackTimes为0时，该列不显示
Teardrop	IP teardrop攻击，又称IP overlapping fragments，当AttackTimes为0时，该列不显示

字段	描述
Tiny fragment	IP tiny fragment攻击
IP option abnormal	IP选项异常攻击，当AttackTimes为0时，该列不显示
Smurf	Smurf攻击，当AttackTimes为0时，该列不显示
Ping of death	Ping of death攻击，当AttackTimes为0时，该列不显示
Traceroute	Traceroute攻击，当AttackTimes为0时，该列不显示
Large ICMP	Large ICMP攻击，当AttackTimes为0时，该列不显示
TCP NULL flag	TCP NULL flag攻击，当AttackTimes为0时，该列不显示
TCP all flags	TCP所有标志位均被置位攻击，又称圣诞树攻击，当AttackTimes为0时，该列不显示
TCP SYN-FIN flags	TCP SYN和FIN被同时置位攻击，当AttackTimes为0时，该列不显示
TCP FIN only flag	TCP 只有FIN被置位的攻击，当AttackTimes为0时，该列不显示
TCP invalid flag	TCP 非法标志位攻击，当AttackTimes 为0时，该列不显示
TCP Land	TCP Land攻击，当AttackTimes为0时，该列不显示
Winnuke	Winnuke攻击，当AttackTimes为0时，该列不显示
UDP Bomb	UDP Bomb攻击，当AttackTimes为0时，该列不显示
Snork	UDP snork攻击，当AttackTimes为0时，该列不显示
Fraggle	Fraggle攻击，又称UDP chargen DoS attack，当AttackTimes为0时，该列不显示
Large ICMPv6	Large ICMPv6攻击，当AttackTimes为0时，该列不显示
ICMP echo request	ICMP echo request攻击，当AttackTimes为0时，该列不显示
ICMP echo reply	ICMP echo reply攻击，当AttackTimes为0时，该列不显示
ICMP source quench	ICMP source quench攻击，当AttackTimes为0时，该列不显示
ICMP destination unreachable	ICMP destination unreachable攻击，当AttackTimes为0时，该列不显示
ICMP redirect	ICMP redirect攻击，当AttackTimes为0时，该列不显示
ICMP time exceeded	ICMP time exceeded攻击，当AttackTimes为0时，该列不显示
ICMP parameter problem	ICMP parameter problem攻击，当AttackTimes 为0时，该列不显示
ICMP timestamp request	ICMP timestamp request攻击，当AttackTimes为0时，该列不显示
ICMP timestamp reply	ICMP timestamp reply攻击，当AttackTimes为0时，该列不显示

字段	描述
ICMP information request	ICMP information request攻击，当AttackTimes为0时，该列不显示
ICMP information reply	ICMP information reply攻击，当AttackTimes为0时，该列不显示
ICMP address mask request	ICMP address mask request攻击，当AttackTimes为0时，该列不显示
ICMP address mask reply	ICMP address mask reply攻击，当AttackTimes为0时，该列不显示
ICMPv6 echo request	ICMPv6 echo request攻击，当AttackTimes 为0时，该列不显示
ICMPv6 echo reply	ICMPv6 echo reply攻击，当AttackTimes为0时，该列不显示
ICMPv6 group membership query	ICMPv6 group membership query攻击，当AttackTimes为0时，该列不显示
ICMPv6 group membership report	ICMPv6 group membership report攻击，当AttackTimes为0时，该列不显示
ICMPv6 group membership reduction	ICMPv6 group membership reduction攻击，当AttackTimes为0时，该列不显示
ICMPv6 destination unreachable	ICMPv6 destination unreachable攻击，当AttackTimes为0时，该列不显示
ICMPv6 time exceeded	ICMPv6 time exceeded攻击，当AttackTimes为0时，该列不显示
ICMPv6 parameter problem	ICMPv6 parameter problem攻击，当AttackTimes为0时，该列不显示
ICMPv6 packet too big	ICMPv6 packet too big攻击，当AttackTimes为0时，该列不显示

1.1.21 display attack-defense statistics local

display attack-defense statistics local 命令用来显示本机攻击防范的统计信息。

【命令】

display attack-defense statistics local [*slot slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot slot-number: 显示本机攻击防范在指定成员设备上的统计信息，*slot-number* 表示设备在 IRF 中的成员编号。如果不指定该参数，则表示显示所有成员设备上检测到的本机攻击防范统计信息。

【举例】

显示本机攻击防范统计信息。

```
<Sysname> display attack-defense statistics local
Attack policy name: abc
Slot 1:
Scan attack defense statistics:
  AttackType                AttackTimes Dropped
  Port scan                  2             23
  IP sweep                    3             33
  Distribute port scan       1             10
Flood attack defense statistics:
  AttackType                AttackTimes Dropped
  SYN flood                  1             0
  ACK flood                  1             0
  SYN-ACK flood              3            5000
  RST flood                  2             0
  FIN flood                  2             0
  UDP flood                  1             0
  ICMP flood                 1             0
  ICMPv6 flood               1             0
  DNS flood                  1             0
  HTTP flood                 1             0
Signature attack defense statistics:
  AttackType                AttackTimes Dropped
  IP option record route     1            100
  IP option security         2             0
  IP option stream ID        3             0
  IP option internet timestamp 4             1
  IP option loose source routing 5             0
  IP option strict source routing 6             0
  IP option route alert      3             0
  Fragment                   1             0
  Impossible                  1             1
  Teardrop                    1             1
  Tiny fragment               1             0
  IP options abnormal         3             0
  Smurf                       1             0
  Ping of death               1             0
  Traceroute                  1             0
  Large ICMP                  1             0
  TCP NULL flag               1             0
  TCP all flags               1             0
```

TCP SYN-FIN flags	1	0
TCP FIN only flag	1	0
TCP invalid flag	1	0
TCP Land	1	0
Winnuke	1	0
UDP Bomb	1	0
Snork	1	0
Fraggle	1	0
Large ICMPv6	1	0
ICMP echo request	1	0
ICMP echo reply	1	0
ICMP source quench	1	0
ICMP destination unreachable	1	0
ICMP redirect	2	0
ICMP time exceeded	3	0
ICMP parameter problem	4	0
ICMP timestamp request	5	0
ICMP timestamp reply	6	0
ICMP information request	7	0
ICMP information reply	4	0
ICMP address mask request	2	0
ICMP address mask reply	1	0
ICMPv6 echo request	1	1
ICMPv6 echo reply	1	1
ICMPv6 group membership query	1	0
ICMPv6 group membership report	1	0
ICMPv6 group membership reduction	1	0
ICMPv6 destination unreachable	1	0
ICMPv6 time exceeded	1	0
ICMPv6 parameter problem	1	0
ICMPv6 packet too big	1	0

Slot 2:

Scan attack defense statistics:

AttackType	AttackTimes	Dropped
Port scan	4	46
IP sweep	2	28
Distribute port scan	1	10

Flood attack defense statistics:

AttackType	AttackTimes	Dropped
SYN flood	1	0
ACK flood	1	0
SYN-ACK flood	2	4200
RST flood	2	0
FIN flood	2	20
UDP flood	1	0
ICMP flood	1	0
ICMPv6 flood	1	0
DNS flood	1	0

HTTP flood	1	0
Signature attack defense statistics:		
AttackType	AttackTimes	Dropped
IP option record route	2	230
IP option security	2	0
IP option stream ID	3	0
IP option internet timestamp	4	1
IP option loose source routing	5	0
IP option strict source routing	2	0
IP option route alert	3	12
Fragment	1	0
Impossible	1	1
Teardrop	1	1
Tiny fragment	1	0
IP options abnormal	3	0
Smurf	1	0
Ping of death	1	0
Traceroute	1	0
Large ICMP	1	0
TCP NULL flag	1	0
TCP all flags	1	0
TCP SYN-FIN flags	1	0
TCP FIN only flag	1	0
TCP invalid flag	1	0
TCP Land	1	0
Winnuke	1	0
UDP Bomb	1	0
Snork	1	0
Fraggle	1	0
Large ICMPv6	1	0
ICMP echo request	1	0
ICMP echo reply	1	0
ICMP source quench	1	0
ICMP destination unreachable	1	0
ICMP redirect	2	3
ICMP time exceeded	3	0
ICMP parameter problem	4	0
ICMP timestamp request	5	0
ICMP timestamp reply	6	0
ICMP information request	7	0
ICMP information reply	4	0
ICMP address mask request	2	0
ICMP address mask reply	1	0
ICMPv6 echo request	1	1
ICMPv6 echo reply	1	1
ICMPv6 group membership query	1	0
ICMPv6 group membership report	1	0
ICMPv6 group membership reduction	1	0

ICMPv6 destination unreachable	1	0
ICMPv6 time exceeded	1	0
ICMPv6 parameter problem	1	0
ICMPv6 packet too big	1	0

表1-12 display attack-defense statistics local 命令显示信息描述表

字段	描述
AttackType	攻击类型
AttackTimes	受到攻击的次数
Dropped	丢弃报文的数目
Port scan	端口扫描攻击，当AttackTimes为0时，该列不显示
IP Sweep	IP扫描攻击，当AttackTimes为0时，该列不显示
Distribute port scan	分布式端口扫描攻击，当AttackTimes为0时，该列不显示
SYN flood	SYN flood攻击，当AttackTimes 为0时，该列不显示
ACK flood	ACK flood攻击，当AttackTimes 为0时，该列不显示
SYN-ACK flood	SYN-ACK flood攻击，当AttackTimes为0时，该列不显示
RST flood	RST flood攻击，当AttackTimes为0时，该列不显示
FIN flood	FIN flood攻击，当AttackTimes为0时，该列不显示
UDP flood	UDP flood 攻击，当AttackTimes为0时，该列不显示
ICMP flood	ICMP flood攻击，当AttackTimes为0时，该列不显示
ICMPv6 flood	ICMPv6 flood攻击，当AttackTimes为0时，该列不显示
DNS flood	DNS flood攻击，当AttackTimes为0时，该列不显示
HTTP flood	HTTP flood攻击，当AttackTimes为0时，该列不显示
IP option record route	IP 选项record route攻击，当AttackTimes为0时，该列不显示
IP option security	IP 选项security攻击，当AttackTimes为0时，该列不显示
IP option stream ID	IP 选项stream identifier攻击，当AttackTimes为0时，该列不显示
IP option internet timestamp	IP 选项 internet timestamp攻击，当AttackTimes为0时，该列不显示
IP option loose source routing	IP 选项loose source routing攻击，当AttackTimes为0时，该列不显示
IP option strict source routing	IP 选项strict source routing攻击，当AttackTimes为0时，该列不显示
IP option route alert	IP 选项strict source routing攻击，当AttackTimes为0时，该列不显示
Fragment	IP分片异常攻击，当AttackTimes为0时，该列不显示
Impossible	IP impossible攻击，当AttackTimes为0时，该列不显示
Teardrop	IP teardrop攻击，又称IP overlapping fragments，当AttackTimes为0时，该列不显示
Tiny fragment	IP tiny fragment攻击
IP option abnormal	IP 选项异常攻击，当AttackTimes为0时，该列不显示

字段	描述
Smurf	Smurf攻击，当AttackTimes为0时，该列不显示
Ping of death	Ping of death攻击，当AttackTimes为0时，该列不显示
Traceroute	Traceroute攻击，当AttackTimes为0时，该列不显示
Large ICMP	Large ICMP攻击，当AttackTimes为0时，该列不显示
TCP NULL flag	TCP NULL flag攻击，当AttackTimes为0时，该列不显示
TCP all flags	TCP所有标志位均被置位攻击，又称圣诞树攻击，当AttackTimes为0时，该列不显示
TCP SYN-FIN flags	TCP SYN和FIN被同时置位攻击，当AttackTimes为0时，该列不显示
TCP FIN only flag	TCP只有FIN被置位的攻击，当AttackTimes为0时，该列不显示
TCP invalid flag	TCP非法标志位攻击，当AttackTimes为0时，该列不显示
TCP Land	TCP Land攻击，当AttackTimes为0时，该列不显示
Winnuke	Winnuke攻击，当AttackTimes为0时，该列不显示
UDP Bomb	UDP Bomb攻击，当AttackTimes为0时，该列不显示
Snork	Snork攻击，当AttackTimes为0时，该列不显示
Fraggle	Fraggle攻击，又称UDP chargen DoS attack，当AttackTimes为0时，该列不显示
Large ICMPv6	Large ICMPv6攻击，当AttackTimes为0时，该列不显示
ICMP echo request	ICMP echo request攻击，当AttackTimes 为0时，该列不显示
ICMP echo reply	ICMP echo reply攻击，当AttackTimes为0时，该列不显示
ICMP source quench	ICMP source quench攻击，当AttackTimes为0时，该列不显示
ICMP destination unreachable	ICMP destination unreachable攻击，当AttackTimes为0时，该列不显示
ICMP redirect	ICMP redirect攻击，当AttackTimes为0时，该列不显示
ICMP time exceeded	ICMP time exceeded攻击，当AttackTimes为0时，该列不显示
ICMP parameter problem	ICMP parameter problem攻击，当AttackTimes为0时，该列不显示
ICMP timestamp request	ICMP timestamp request攻击，当AttackTimes为0时，该列不显示
ICMP timestamp reply	ICMP timestamp reply攻击，当AttackTimes为0时，该列不显示
ICMP information request	ICMP information request攻击，当AttackTimes为0时，该列不显示
ICMP information reply	ICMP information reply攻击，当AttackTimes为0时，该列不显示
ICMP address mask request	ICMP address mask request攻击，当AttackTimes为0时，该列不显示
ICMP address mask reply	ICMP address mask reply攻击，当AttackTimes为0时，该列不显示
ICMPv6 echo request	ICMPv6 echo request攻击，当AttackTimes 为0时，该列不显示
ICMPv6 echo reply	ICMPv6 echo reply攻击，当AttackTimes为0时，该列不显示
ICMPv6 group membership query	ICMPv6 group membership query攻击，当AttackTimes 为0时，该列不

字段	描述
	显示
ICMPv6 group membership report	ICMPv6 group membership report攻击，当AttackTimes为0时，该列不显示
ICMPv6 group membership reduction	ICMPv6 group membership reduction攻击，当AttackTimes为0时，该列不显示
ICMPv6 destination unreachable	ICMPv6 destination unreachable攻击，当AttackTimes为0时，该列不显示
ICMPv6 time exceeded	ICMPv6 time exceeded攻击，当AttackTimes为0时，该列不显示
ICMPv6 parameter problem	ICMPv6 parameter problem攻击，当AttackTimes为0时，该列不显示
ICMPv6 packet too big	ICMPv6 packet too big攻击，当AttackTimes为0时，该列不显示

【相关命令】

- `reset attack-defense statistics local`

1.1.22 dns-flood action

`dns-flood action` 命令用来配置对 DNS flood 攻击防范的全局处理行为。

`undo dns-flood action` 命令用来恢复缺省情况。

【命令】

```
dns-flood action { drop | logging } *
undo dns-flood action
```

【缺省情况】

不对检测到的 DNS flood 攻击采取任何措施。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 DNS 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息。

【举例】

在攻击防范策略 `atk-policy-1` 中配置对 DNS flood 攻击防范的全局处理行为是丢弃后续报文。

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

【相关命令】

- `dns-flood detect`
- `dns-flood detect non-specific`
- `dns-flood threshold`

1.1.23 dns-flood detect

`dns-flood detect` 命令用来开启对指定 IP 地址的攻击防范检测，并配置 DNS flood 攻击防范检测的触发阈值和对 DNS flood 攻击的处理行为。

`undo dns-flood detect` 命令用来关闭对指定 IP 地址的 DNS flood 攻击防范检测。

【命令】

```
dns-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance  
vpn-instance-name ] [ port port-list ] [ threshold threshold-value ] [ action  
{ { drop | logging } * | none } ]  
undo dns-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance  
vpn-instance-name ]
```

【缺省情况】

未对任何指定 IP 地址配置 DNS flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

ip *ipv4-address*: 指定要保护的 IPv4 地址。该 IPv4 地址不能为全 1 地址或全 0 地址。

ipv6 *ipv6-address*: 指定要保护的 IPv6 地址。

vpn-instance *vpn-instance-name*: 受保护 IP 地址所属的 VPN 实例。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。若未指定本参数，则表示该保护 IP 地址属于公网。

port *port-list*: 指定开启 DNS flood 攻击防范检测的端口列表，表示方式为 { *start-port-number* [**to** *end-port-number*] } &<1-65535>。&<1-65535>表示前面的参数最多可以输入 65535 次。*end-port-number* 必须大于或等于 *start-port-number*。若未指定本参数，则表示使用全局配置的检测端口列表。

threshold *threshold-value*: 指定 DNS flood 攻击防范的触发阈值。其中，*threshold-value* 为向指定 IP 地址每秒发送的 DNS 报文数目，取值范围为 1~1000000。

action: 设置对 DNS flood 攻击的处理行为。若未指定本参数，则表示采用 DNS flood 攻击防范的全局处理行为。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 DNS 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息。

none: 表示不采取任何动作。

【使用指导】

使能 DNS 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 DNS 报文的速率持续达到或超过了触发阈值时，即认为该 IP 地址受到了 DNS 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。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）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。

每个攻击防范策略下可以同时多个 IP 地址配置 DNS flood 攻击防范检测。

【举例】

在攻击防范策略 **atk-policy-1** 中开启对 IP 地址 **192.168.1.2** 的 DNS flood 攻击防范检测，并指定检测端口为 **53**、触发阈值为 **2000**。当设备监测到向该 IP 地址的 **53** 端口每秒发送的 DNS 报文数持续达到或超过 **2000** 时，启动 DNS flood 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-flood detect ip 192.168.1.2 port 53
threshold 2000
```

【相关命令】

- **dns-flood action**
- **dns-flood detect non-specific**
- **dns-flood threshold**
- **dns-flood port**

1.1.24 dns-flood detect non-specific

dns-flood detect non-specific 命令用来对所有非受保护 IP 地址开启 DNS flood 攻击防范检测。

undo dns-flood detect non-specific 命令用来关闭对所有非受保护 IP 地址的 DNS flood 攻击防范检测。

【命令】

```
dns-flood detect non-specific
undo dns-flood detect non-specific
```

【缺省情况】

未对任何非受保护 IP 地址开启 DNS flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【使用指导】

对所有非受保护 IP 地址开启 DNS flood 攻击防范检测后，设备将采用全局的阈值设置（由 **dns-flood threshold** 命令设置）和处理行为（由 **dns-flood action** 命令配置）对这些 IP 地址进行保护。

【举例】

在攻击防范策略 **atk-policy-1** 中，对所有非受保护 IP 地址开启 DNS flood 攻击防范检测。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-flood detect non-specific
```

【相关命令】

- **dns-flood action**
- **dns-flood detect**
- **dns-flood threshold**

1.1.25 dns-flood port

dns-flood port 命令用来配置 DNS flood 攻击防范的全局检测端口号。

undo dns-flood port 命令用来恢复缺省情况。

【命令】

```
dns-flood port port-list
undo dns-flood port
```

【缺省情况】

DNS flood 攻击防范的全局检测端口号为 53。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

port-list: 指定开启 DNS flood 攻击防范检测的端口列表，表示方式为 { *start-port-number* [**to** *end-port-number*] } <1-65535>。<1-65535>表示前面的参数最多可以输入 65535 次。*end-port-number* 必须大于或等于 *start-port-number*。

【使用指导】

设备只对指定检测端口上收到的报文进行 DNS flood 攻击检测。

对于所有非受保护 IP 地址，或未指定检测端口的受保护 IP 地址，设备采用全局的检测端口进行 DNS flood 攻击检测。对于所有指定检测端口的受保护 IP 地址，设备针对为每个受保护 IP 地址指定的端口进行 DNS flood 攻击检测。

【举例】

在攻击防范策略 `atk-policy-1` 中配置 DNS flood 攻击防范的全局检测端口为 53 与 61000，当设备检测到访问 53 端口或 61000 端口的 DNS flood 攻击时，启动攻击防范措施。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-flood port 53 61000
```

【相关命令】

- `dns-flood action`
- `dns-flood detect`
- `dns-flood detect non-specific`

1.1.26 dns-flood threshold

`dns-flood threshold` 命令用来配置 DNS flood 攻击防范的全局触发阈值。

`undo dns-flood threshold` 命令用来恢复缺省情况。

【命令】

```
dns-flood threshold threshold-value
undo dns-flood threshold
```

【缺省情况】

DNS flood 攻击防范的全局触发阈值为 1000。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

`threshold-value`: 指定向某 IP 地址每秒发送的 DNS 报文数目，取值范围为 1~1000000。

【使用指导】

使能 DNS 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 DNS 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 DNS 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。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）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。

对于未专门配置 DNS flood 攻击防范检测的 IP 地址，设备采用全局的阈值设置来进行保护。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（DNS 服务器）的 DNS 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。

【举例】

在攻击防范策略 **atk-policy-1** 中配置 **DNS flood** 攻击防范的全局触发阈值为 **100**，即当设备监测到向某 IP 地址每秒发送的 DNS 报文数持续达到或超过 **100** 时，启动攻击防范措施。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-flood threshold 100
```

【相关命令】

- **dns-flood action**
- **dns-flood detect ip**
- **dns-flood detect non-specific**

1.1.27 exempt acl

exempt acl 命令用来配置攻击防范例外列表。

undo exempt acl 命令用来恢复缺省情况。

【命令】

```
exempt acl [ ipv6 ] { acl-number | name acl-name }
undo exempt acl [ ipv6 ]
```

【缺省情况】

未配置攻击防范例外列表。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

ipv6：指定 IPv6 ACL。如果未指定本参数，则表示 IPv4 ACL。

acl-number：表示 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000～2999：表示基本 ACL。
- 3000～3999：表示高级 ACL。

name acl-name：指定 ACL 的名称。**acl-name** 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 **a～z** 或 **A～Z** 开头。为避免混淆，ACL 的名称不允许使用英文单词 **all**。

【使用指导】

通过配置例外列表，使用 ACL 过滤不需要进行攻击防范检测的主机报文。当本机、接口上收到的报文与攻击防范例外列表引用的 ACL 中的 **permit** 规则匹配时，设备不对其进行攻击防范检测。该配置用于过滤某些被信任的安全主机发送的报文，可以有效的减小误报率，并提高服务器处理效率。例外列表引用的 ACL 的 **permit** 规则中仅源地址、目的地址、源端口、目的端口、协议号、L3VPN 和非首片分片标记参数用于匹配报文。

如果配置的攻击防范例外列表中引用的 ACL 不存在，或引用的 ACL 中未定义任何规则，例外列表不会生效。

【举例】

在攻击防范策略 **atk-policy-1** 中配置例外列表 **ACL 2001**，过滤来自主机 **1.1.1.1** 的报文，不对其进行攻击防范检测。

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] attack-defense policy atk-policy-1
[attack-defense-policy-atk-policy-1] exempt acl 2001
```

【相关命令】

- **attack-defense policy**

1.1.28 fin-flood action

fin-flood action 命令用来配置对 **FIN flood** 攻击防范的全局处理行为。

undo fin-flood action 命令用来恢复缺省情况。

【命令】

```
fin-flood action { drop | logging } *
undo fin-flood action
```

【缺省情况】

不对检测到的 **FIN flood** 攻击采取任何处理行为。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 **FIN** 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息

【举例】

#在攻击防范策略 **atk-policy-1** 配置对 **FIN flood** 攻击防范的全局处理行为是丢弃后续报文。

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

【相关命令】

- **fin-flood detect**
- **fin-flood detect non-specific**

- **fin-flood threshold**

1.1.29 fin-flood detect

fin-flood detect 命令用来开启对指定 IP 地址的 FIN flood 攻击防范检测，并配置 FIN flood 攻击防范检测的触发阈值和对 FIN flood 攻击的处理行为。

undo fin-flood detect 命令用来关闭对指定 IP 地址的 FIN flood 攻击防范检测。

【命令】

```
fin-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance  
vpn-instance-name ] [ threshold threshold-value ] [ action { { drop | logging }  
* | none } ]  
undo fin-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance  
vpn-instance-name ]
```

【缺省情况】

未对任何指定 IP 地址配置 FIN flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

ip ipv4-address: 指定要保护的 IPv4 地址。该 IPv4 地址不能为全 1 地址或全 0 地址。

ipv6 ipv6-address: 指定要保护的 IPv6 地址。

vpn-instance vpn-instance-name: 受保护 IP 地址所属的 VPN 实例。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。若未指定本参数，则表示该保护 IP 地址属于公网。

threshold threshold-value: 指定攻击防范的触发阈值。其中，*threshold-value* 为向指定 IP 地址每秒发送的 FIN 报文数目，取值范围为 1~1000000。

action: 设置对 FIN flood 攻击的处理行为。若未指定本参数，则表示采用 FIN flood 攻击防范的全局处理行为。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 FIN 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息。

none: 表示不采取任何动作。

【使用指导】

使能 FIN 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 FIN 报文的速率持续达到或超过了触发阈值时，即认为该 IP 地址受到了 FIN 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。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）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。

每个攻击防范策略下可以同时为多个 IP 地址配置 FIN flood 攻击防范检测。

【举例】

在攻击防范策略 **atk-policy-1** 中开启对 IP 地址 **192.168.1.2** 的 **FIN flood** 攻击防范检测，并指定触发阈值为 **2000**。当设备监测到向该 IP 地址每秒发送的 **FIN** 报文数持续达到或超过 **2000** 时，启动 **FIN flood** 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] fin-flood detect ip 192.168.1.2 threshold 2000
```

【相关命令】

- **fin-flood action**
- **fin-flood detect non-specific**
- **fin-flood threshold**

1.1.30 fin-flood detect non-specific

fin-flood detect non-specific 命令用来对所有非受保护 IP 地址开启 **FIN flood** 攻击防范检测。

undo fin-flood detect non-specific 命令用来关闭对所有非受保护 IP 地址的 **FIN flood** 攻击防范检测。

【命令】

```
fin-flood detect non-specific
undo fin-flood detect non-specific
```

【缺省情况】

未对任何非受保护 IP 地址开启 **FIN flood** 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

无

【使用指导】

对所有非受保护 IP 地址开启 **FIN flood** 攻击防范检测后，设备将采用全局的阈值设置（由 **fin-flood threshold** 命令设置）和处理行为（由 **fin-flood action** 命令配置）对这些 IP 地址进行保护。

【举例】

在攻击防范策略 **atk-policy-1** 中，对所有非受保护 IP 地址开启 **FIN flood** 攻击防范检测。

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

```
[Sysname-attack-defense-policy-atk-policy-1] fin-flood detect non-specific
```

【相关命令】

- **fin-flood action**
- **fin-flood detect**
- **fin-flood threshold**

1.1.31 fin-flood threshold

fin-flood threshold 命令用来配置 FIN flood 攻击防范的全局触发阈值。

undo fin-flood threshold 命令用来恢复缺省情况。

【命令】

```
fin-flood threshold threshold-value  
undo fin-flood threshold
```

【缺省情况】

FIN flood 攻击防范的全局触发阈值为 1000。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

threshold-value: 指定向某 IP 地址每秒发送的 FIN 报文数目，取值范围为 1~1000000。

【使用指导】

使能 FIN 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 FIN 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 FIN 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。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）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。

对于未专门配置 FIN flood 攻击防范检测的 IP 地址，设备采用全局的阈值设置来进行保护。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 FIN 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。

【举例】

在攻击防范策略 **atk-policy-1** 中配置 FIN flood 攻击防范检测的全局触发阈值为 100，即当设备监测到向某 IP 地址每秒发送的 FIN 报文数持续达到或超过 100 时，启动 FIN flood 攻击防范。

```
<Sysname> system-view  
[Sysname] attack-defense policy atk-policy-1  
[Sysname-attack-defense-policy-atk-policy-1] fin-flood threshold 100
```

【相关命令】

- `fin-flood action`
- `fin-flood detect`
- `fin-flood detect non-specific`

1.1.32 http-flood action

`http-flood action` 命令用来配置对 HTTP flood 攻击防范的全局处理行为。

`undo http-flood action` 命令用来恢复缺省情况。

【命令】

```
http-flood action { drop | logging } *  
undo http-flood action
```

【缺省情况】

不对检测到的 HTTP flood 攻击采取任何处理行为。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 HTTP 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息。

【举例】

在攻击防范策略 `atk-policy-1` 中配置对 HTTP flood 攻击防范的全局处理行为是丢弃后续报文。

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

【相关命令】

- `http-flood detect non-specific`
- `http-flood detect`
- `http-flood threshold`

1.1.33 http-flood detect

`http-flood detect` 命令用来开启对指定 IP 地址的 HTTP flood 攻击防范检测，并配置 HTTP flood 攻击防范的触发阈值和对 HTTP flood 攻击的处理行为。

`undo http-flood detect` 命令用来关闭对指定 IP 地址的 HTTP flood 攻击防范检测。

【命令】

```
http-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance  
vpn-instance-name ] [ port port-list ] [ threshold threshold-value ] [ action  
{ { drop | logging } * | none } ]  
undo http-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance  
vpn-instance-name ]
```

【缺省情况】

未对任何指定 IP 地址配置 HTTP flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

ip *ipv4-address*: 指定要保护的 IPv4 地址。该 IPv4 地址不能为全 1 地址或全 0 地址。

ipv6 *ipv6-address*: 指定要保护的 IPv6 地址。

vpn-instance *vpn-instance-name*: 受保护 IP 地址所属的 VPN 实例。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。若未指定本参数，则表示该保护 IP 地址属于公网。

port *port-list*: 指定开启 HTTP flood 攻击防范检测的端口列表，表示方式为 { *start-port-number* [**to** *end-port-number*] } <1-65535>。<1-65535>表示前面的参数最多可以输入 65535 次。*end-port-number* 必须大于或等于 *start-port-number*。若未指定本参数，则表示使用全局配置的检测端口列表。

threshold *threshold-value*: 指定攻击防范的触发阈值。其中，*threshold-value* 为向指定 IP 地址每秒发送的 HTTP 报文数目，取值范围为 1~1000000。

action: 设置对 HTTP flood 攻击的处理行为。若未指定本参数，则表示采用 HTTP flood 攻击防范的全局处理行为。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 HTTP 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息。

none: 表示不采取任何动作。

【使用指导】

使能 HTTP 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 HTTP 报文的速率持续达到或超过了触发阈值时，即认为该 IP 地址受到了 HTTP 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。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）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。

每个攻击防范策略下可以同时为多个 IP 地址配置 HTTP flood 攻击防范检测。

【举例】

在攻击防范策略 **atk-policy-1** 中开启对 IP 地址 **192.168.1.2** 的 **HTTP flood** 攻击防范检测，并指定检测端口为 **80** 与 **8080**、触发阈值为 **2000**。当设备监测到向该 IP 地址的 **80** 或 **8080** 端口每秒发送的 **HTTP** 报文数持续达到或超过 **2000** 时，启动 **HTTP flood** 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] http-flood detect ip 192.168.1.2 port 80 8080
threshold 2000
```

【相关命令】

- **http-flood action**
- **http-flood detect non-specific**
- **http-flood threshold**
- **http-flood port**

1.1.34 http-flood detect non-specific

http-flood detect non-specific 命令用来对所有非受保护 IPv4 地址开启 **HTTP flood** 攻击防范检测。

undo http-flood detect non-specific 命令用来关闭对所有非受保护 IPv4 地址的 **HTTP flood** 攻击防范检测。

【命令】

```
http-flood detect non-specific
undo http-flood detect non-specific
```

【缺省情况】

未对任何非受保护 IP 地址开启 **HTTP flood** 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【使用指导】

对所有非受保护 IP 地址开启 **HTTP flood** 攻击防范检测后，设备将采用全局的阈值设置（由 **http-flood threshold** 命令设置）和处理行为（由 **http-flood action** 命令配置）对这些 IP 地址进行保护。

【举例】

在攻击防范策略 **atk-policy-1** 中，对所有非受保护 IP 地址开启 **HTTP flood** 攻击防范检测。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] http-flood detect non-specific
```

【相关命令】

- `http-flood action`
- `http-flood detect`
- `http-flood threshold`

1.1.35 http-flood port

`http-flood port` 命令用来配置 HTTP flood 攻击防范的全局检测端口号。

`undo http-flood port` 命令用来恢复缺省情况。

【命令】

```
http-flood port port-list
undo http-flood port
```

【缺省情况】

HTTP flood 攻击防范的全局检测端口号为 80。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

port-list: 指定开启 HTTP flood 攻击防范检测的端口列表, 表示方式为 { *start-port-number* [*to end-port-number*] } &<1-65535>。&<1-65535> 表示前面的参数最多可以输入 65535 次。*end-port-number* 必须大于或等于 *start-port-number*。

【使用指导】

设备只对指定检测端口上收到的报文进行 HTTP flood 攻击检测。

对于所有非受保护 IP 地址, 或未指定检测端口的受保护 IP 地址, 设备采用全局的检测端口进行 HTTP flood 攻击检测。对于所有指定检测端口的受保护 IP 地址, 设备针对为每个受保护 IP 地址指定的端口进行 HTTP flood 攻击检测。

【举例】

在攻击防范策略 `atk-policy-1` 中配置 DNS flood 攻击防范的全局检测端口为 80 与 8080, 当设备检测到访问 80 端口或 8080 端口的 HTTP flood 攻击时, 启动攻击防范措施。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] http-flood port 80 8080
```

【相关命令】

- `http-flood action`
- `http-flood detect`
- `http-flood detect non-specific`

1.1.36 http-flood threshold

http-flood threshold 命令用来配置 HTTP flood 攻击防范的全局触发阈值。

undo http-flood threshold 命令用来恢复缺省情况。

【命令】

```
http-flood threshold threshold-value
undo http-flood threshold
```

【缺省情况】

缺省情况下，HTTP flood 攻击防范的全局触发阈值为 1000。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

threshold-value: 指定向某 IP 地址每秒发送的 HTTP 报文数目，取值范围为 1~1000000。

【使用指导】

使能 HTTP 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 HTTP 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 HTTP 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。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）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。

对于未专门配置 HTTP flood 攻击防范检测的 IP 地址，设备采用全局的阈值设置来进行保护。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）的 HTTP 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。

【举例】

在攻击防范策略 **atk-policy-1** 中配置 HTTP flood 攻击防范的全局触发阈值为 100，即当设备监测到向某 IP 地址每秒发送的 HTTP 报文数持续达到或超过 100 时，启动 HTTP flood 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] http-flood threshold 100
```

【相关命令】

- **http-flood action**
- **http-flood detect**
- **http-flood detect non-specific**

1.1.37 icmp-flood action

icmp-flood action 命令用来配置对 ICMP flood 攻击防范的全局处理行为。

undo icmp-flood action 命令用来恢复缺省情况。

【命令】

```
icmp-flood action { drop | logging } *  
undo icmp-flood action
```

【缺省情况】

不对检测到的 ICMP flood 攻击采取任何措施。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 ICMP 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息。

【举例】

在攻击防范策略 **atk-policy-1** 中配置对 ICMP flood 攻击防范的全局处理行为是丢弃后续报文。

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

【相关命令】

- **icmp-flood detect non-specific**
- **icmp-flood detect ip**
- **icmp-flood threshold**

1.1.38 icmp-flood detect ip

icmp-flood detect ip 命令用来开启对指定 IP 地址的 ICMP flood 攻击防范检测，并配置 ICMP flood 攻击防范检测的触发阈值和对 ICMP flood 攻击的处理行为。

undo icmp-flood detect ip 命令用来关闭对指定 IP 地址的 ICMP flood 攻击防范检测。

【命令】

```
icmp-flood detect ip ip-address [ vpn-instance vpn-instance-name ]  
[ threshold threshold-value ] [ action { { drop | logging } * | none } ]  
undo icmp-flood detect ip ip-address [ vpn-instance vpn-instance-name ]
```

【缺省情况】

未对任何指定 IP 地址配置 ICMP flood 攻击防范触发阈值。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

ip ip-address: 指定要保护的 IP 地址。该 IP 地址不能为全 1 地址或全 0 地址。

vpn-instance vpn-instance-name: 受保护 IP 地址所属的 VPN 实例。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。若未指定本参数，则表示该保护 IP 地址属于公网。

threshold threshold-value: 指定攻击防范的触发阈值。其中，*threshold-value* 为向指定 IP 地址每秒发送的 ICMP 报文数目，取值范围为 1~1000000。

action: 设置对 ICMP flood 攻击的处理行为。若未指定本参数，则表示采用 ICMP flood 攻击防范的全局处理行为。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 ICMP 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息。

none: 表示不采取任何动作。

【使用指导】

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。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）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。

每个攻击防范策略下可以同时多个 IP 地址配置 ICMP flood 攻击防范检测。

【举例】

在攻击防范策略 *atk-policy-1* 中开启对 IP 地址 192.168.1.2 的 ICMP flood 攻击防范检测，并指定触发阈值为 2000。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 ICMP flood 攻击防范。

```
<Sysname> system-view
```

```
[Sysname] attack-defense policy atk-policy-1
```

```
[Sysname-attack-defense-policy-atk-policy-1] icmp-flood detect ip 192.168.1.2 threshold 2000
```

【相关命令】

- **icmp-flood action**
- **icmp-flood threshold**
- **icmp-flood detect non-specific**

1.1.39 icmp-flood detect non-specific

icmp-flood detect non-specific 命令用来对所有非受保护 IPv4 地址开启 ICMP flood 攻击防范检测。

undo icmp-flood detect non-specific 命令用来关闭对所有非受保护 IPv4 地址的 ICMP flood 攻击防范检测。

【命令】

```
icmp-flood detect non-specific
undo icmp-flood detect non-specific
```

【缺省情况】

未对任何非受保护 IPv4 地址开启 ICMP flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【使用指导】

对任何非受保护 IPv4 地址开启 ICMP flood 攻击防范检测后，设备将采用全局的阈值设置（由 **icmp-flood threshold** 命令设置）和处理行为（由 **icmp-flood action** 命令配置）对这些 IP 地址进行保护。

【举例】

在攻击防范策略 **atk-policy-1** 中，对所有非受保护 IPv4 地址开启 ICMP flood 攻击防范检测。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmp-flood detect non-specific
```

【相关命令】

- **icmp-flood action**
- **icmp-flood detect ip**
- **icmp-flood threshold**

1.1.40 icmp-flood threshold

icmp-flood threshold 命令用来配置 ICMP flood 攻击防范的全局触发阈值。

undo icmp-flood threshold 命令用来恢复缺省情况。

【命令】

```
icmp-flood threshold threshold-value
undo icmp-flood threshold
```

【缺省情况】

ICMP flood 攻击防范的全局触发阈值为 1000。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

threshold-value: 指定向某 IP 地址每秒发送的 ICMP 报文数目，取值范围为 1~1000000。

【使用指导】

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。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）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。

对于未专门配置 ICMP flood 攻击防范检测的 IP 地址，设备采用全局的阈值设置来进行保护。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 ICMP 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。

【举例】

在攻击防范策略 **atk-policy-1** 中配置 ICMP flood 攻击防范检测的全局触发阈值为 100，即当设备监测到向某 IP 地址每秒发送的 ICMP 报文数持续达到或超过 100 时，启动 ICMP flood 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmp-flood threshold 100
```

【相关命令】

- **icmp-flood action**
- **icmp-flood detect**
- **icmp-flood detect non-specific**

1.1.41 icmpv6-flood action

icmpv6-flood action 命令用来配置对 ICMPv6 flood 攻击防范的全局处理行为。

undo icmpv6-flood action 命令用来恢复缺省情况。

【命令】

```
icmpv6-flood action { drop | logging } *
undo icmpv6-flood action
```

【缺省情况】

不对检测到的 ICMPv6 flood 攻击采取任何防范措施。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 ICMPv6 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息。

【举例】

在攻击防范策略 **atk-policy-1** 中配置对 ICMPv6 flood 攻击防范的全局处理行为是丢弃后续报文。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmpv6-flood action drop
```

【相关命令】

- **icmpv6-flood detect ipv6**
- **icmpv6-flood detect non-specific**
- **icmpv6-flood threshold**

1.1.42 icmpv6-flood detect ipv6

icmpv6-flood detect ipv6 命令用来开启对指定 IPv6 地址的 ICMPv6 flood 攻击防范检测，并配置 ICMPv6 flood 攻击防范检测的触发阈值和对 ICMPv6 flood 攻击的处理行为。

undo icmpv6-flood detect ipv6 命令用来关闭对指定 IPv6 地址的 ICMPv6 flood 攻击防范检测。

【命令】

```
icmpv6-flood detect ipv6 ipv6-address [ vpn-instance vpn-instance-name ]
[ threshold threshold-value ] [ action { { drop | logging } * | none } ]
undo icmpv6-flood detect ipv6 ipv6-address [ vpn-instance
vpn-instance-name ]
```

【缺省情况】

未对任何指定 IPv6 地址配置 ICMPv6 flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

ipv6-address: 指定要保护的 IPv6 地址。

vpn-instance vpn-instance-name: 受保护 IP 地址所属的 VPN 实例。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。若未指定本参数，则表示该保护 IP 地址属于公网。

threshold threshold-value: 指定攻击防范的触发阈值。其中，**threshold-value** 为向指定 IP 地址每秒发送的 ICMPv6 报文数目，取值范围为 1~1000000。

action: 设置对 ICMPv6 flood 攻击的处理行为。若未指定本参数，则表示采用 ICMPv6 flood 攻击防范的全局处理行为。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 ICMPv6 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息。

none: 表示不采取任何动作。

【使用指导】

使能 ICMPv6 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 ICMPv6 报文的速率持续达到或超过了触发阈值时，即认为该 IP 地址受到了 ICMPv6 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。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）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。

每个攻击防范策略下可以同时为多个 IPv6 地址配置 ICMPv6 flood 攻击防范检测。

【举例】

在攻击防范策略 `atk-policy-1` 中开启对 IP 地址 `2012::12` 的 ICMPv6 flood 攻击防范检测，并指定触发阈值为 `2000`。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 ICMPv6 flood 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmpv6-flood detect ipv6 2012::12 threshold 2000
```

【相关命令】

- `icmpv6-flood action`
- `icmpv6-flood detect non-specific`
- `icmpv6-flood threshold`

1.1.43 icmpv6-flood detect non-specific

`icmpv6-flood detect non-specific` 命令用来对所有非受保护 IPv6 地址开启 ICMPv6 flood 攻击防范检测。

`undo icmpv6-flood detect non-specific` 命令用来关闭对所有非受保护 IPv6 地址的 ICMPv6 flood 攻击防范检测。

【命令】

```
icmpv6-flood detect non-specific
undo icmpv6-flood detect non-specific
```

【缺省情况】

未对任何非受保护 IPv6 地址开启 ICMPv6 flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【使用指导】

对所有非受保护 IPv6 地址开启 ICMPv6 flood 攻击防范检测后，设备将采用全局的阈值设置（由 **icmpv6-flood threshold** 命令设置）和处理行为（由 **icmpv6-flood action** 命令配置）对这些 IP 地址进行保护。

【举例】

在攻击防范策略 **atk-policy-1** 中，对所有非受保护 IPv6 地址开启 ICMPv6 flood 攻击防范检测。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmpv6-flood detect non-specific
```

【相关命令】

- **icmpv6-flood action**
- **icmpv6-flood detect ipv6**
- **icmpv6-flood threshold**

1.1.44 icmpv6-flood threshold

icmpv6-flood threshold 命令用来配置 ICMPv6 flood 攻击防范的全局触发阈值。

undo icmpv6-flood threshold 命令用来恢复缺省情况。

【命令】

```
icmpv6-flood threshold threshold-value
undo icmpv6-flood threshold
```

【缺省情况】

ICMPv6 flood 攻击防范的全局触发阈值为 1000。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

threshold-value：指定向某 IP 地址每秒发送的 ICMPv6 报文数目，取值范围为 1~1000000。

【使用指导】

使能 ICMPv6 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 ICMPv6 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 ICMPv6 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。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）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。

对于未专门配置 ICMPv6 flood 攻击防范检测的 IP 地址，设备采用全局的阈值设置来进行保护。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 ICMPv6 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。

【举例】

在攻击防范策略 **atk-policy-1** 中配置 ICMPv6 flood 攻击防范检测的全局触发阈值为 100，即当设备监测到向某 IP 地址每秒发送的 ICMPv6 报文数持续达到或超过 100 时，启动 ICMPv6 flood 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmpv6-flood threshold 100
```

【相关命令】

- **icmpv6-flood action**
- **icmpv6-flood detect**
- **icmpv6-flood detect non-specific**

1.1.45 reset attack-defense policy flood

reset attack-defense policy flood 命令用来清除 flood 攻击防范受保护 IP 表项的统计信息。

【命令】

```
reset attack-defense policy policy-name flood protected { ip | ipv6 }
statistics
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

policy-name: 攻击防范策略名称，为 1~31 个字符的字符串，不区分大小写。合法取值包括大写字母、小写字母、数字、特殊字符“_”和“-”。

ip: 指定 IPv4 类型的 flood 受保护 IP 表项。

ipv6: 指定 IPv6 类型的 flood 受保护 IP 表项。

statistics: 清除指定类型的 flood 受保护 IP 表项的统计信息。

【举例】

清除攻击防范策略 **abc** 中所有 IPv4 类型的 flood 保护 IP 表项的统计信息

```
<Sysname> reset attack-defense policy abc flood protected ip statistics
```

清除攻击防范策略 **abc** 中所有 IPv6 类型的 Flood 保护 IP 表项的统计信息

```
<Sysname> reset attack-defense policy abc flood protected ipv6 statistics
```


【相关命令】

- `display attack-defense policy ip`
- `display attack-defense policy ipv6`

1.1.46 reset attack-defense statistics interface

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

【命令】

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

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface-type interface-number: 表示指定接口的接口类型和接口编号。

【举例】

清除接口 Ten-GigabitEthernet1/0/25 上的攻击防范的统计信息。

```
<Sysname> reset attack-defense statistics interface ten-gigabitethernet 1/0/25
```

【相关命令】

- `display attack-defense policy`

1.1.47 reset attack-defense statistics local

`reset attack-defense statistics local` 命令用来清除本机攻击防范的统计信息。

【命令】

`reset attack-defense statistics local`

【视图】

用户视图

【缺省用户角色】

network-admin

【举例】

清除本机上所有攻击防范的统计信息。

```
<Sysname> reset attack-defense statistics local
```

【相关命令】

- `display attack-defense statistics local`

1.1.48 rst-flood action

rst-flood action 命令用来配置对 RST flood 攻击防范的全局处理行为。

undo rst-flood action 命令用来恢复缺省情况。

【命令】

```
rst-flood action { drop | logging } *  
undo rst-flood action
```

【缺省情况】

不对检测到的 RST flood 攻击采取任何措施。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 RST 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息。

【举例】

在攻击防范策略 **atk-policy-1** 中配置对 RST flood 攻击防范的全局处理行为是丢弃后续报文。

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

【相关命令】

- **rst-flood detect**
- **rst-flood detect non-specific**
- **rst-flood threshold**

1.1.49 rst-flood detect

rst-flood detect 命令用来开启对指定 IP 地址的 RST flood 攻击防范检测，并配置 RST flood 攻击防范的触发阈值和对 RST flood 攻击的处理行为。

undo rst-flood 命令用来关闭对指定 IP 地址的 RST flood 攻击防范检测。

【命令】

```
rst-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance  
vpn-instance-name ] [ threshold threshold-value ] [ action { { drop | logging }  
* | none } ]  
undo rst-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance  
vpn-instance-name ]
```

【缺省情况】

未对任何指定 IP 地址配置 RST flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

ip *ipv4-address*: 指定要保护的 IPv4 地址。该 IPv4 地址不能为全 1 地址或全 0 地址。

ipv6 *ipv6-address*: 指定要保护的 IPv6 地址。

vpn-instance *vpn-instance-name*: 受保护 IP 地址所属的 VPN 实例。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。若未指定本参数，则表示该保护 IP 地址属于公网。

threshold *threshold-value*: 指定攻击防范的触发阈值。其中，*threshold-value* 为向指定 IP 地址每秒发送的 RST 报文数目，取值范围为 1~1000000。

action: 设置对 RST flood 攻击的处理行为。若未指定本参数，则表示采用 RST flood 攻击防范的全局处理行为。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 RST 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息。

none: 表示不采取任何动作。

【使用指导】

使能 RST 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 RST 报文的速率持续达到或超过了触发阈值时，即认为该 IP 地址受到了 RST 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。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）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。

每个攻击防范策略下可以同时为多个 IP 地址配置 RST flood 攻击防范检测。

【举例】

在攻击防范策略 **atk-policy-1** 中开启对 IP 地址 192.168.1.2 的 RST flood 攻击防范检测，并指定触发阈值为 2000。当设备监测到向该 IP 地址每秒发送的 RST 报文数持续达到或超过 2000 时，启动 RST flood 攻击防范。

```
<Sysname> system-view
```

```
[Sysname] attack-defense policy atk-policy-1
```

```
[Sysname-attack-defense-policy-atk-policy-1] rst-flood detect ip 192.168.1.2 threshold 2000
```

【相关命令】

- **rst-flood action**
- **rst-flood detect non-specific**
- **rst-flood threshold**

1.1.50 rst-flood detect non-specific

rst-flood detect non-specific 命令用来对所有非受保护 IP 地址开启 RST flood 攻击防范检测。

undo rst-flood detect non-specific 命令用来关闭对所有非受保护 IP 地址的 RST flood 攻击防范检测。

【命令】

```
rst-flood detect non-specific
undo rst-flood detect non-specific
```

【缺省情况】

未对任何非受保护 IP 地址开启 RST flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【使用指导】

对所有非受保护 IP 地址开启 RST flood 攻击防范检测后，设备将采用全局的阈值设置（由 **rst-flood threshold** 命令设置）和处理行为（由 **rst-flood action** 命令配置）对这些 IP 地址进行保护。

【举例】

在攻击防范策略 **atk-policy-1** 中，对所有非受保护 IP 地址开启 RST flood 攻击防范检测。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] rst-flood detect non-specific
```

【相关命令】

- **rst-flood action**
- **rst-flood detect**
- **rst-flood threshold**

1.1.51 rst-flood threshold

rst-flood threshold 命令用来配置 RST flood 攻击防范的全局触发阈值。

undo rst-flood threshold 命令用来恢复缺省情况。

【命令】

```
rst-flood threshold threshold-value
undo rst-flood threshold
```

【缺省情况】

RST flood 攻击防范的全局触发阈值为 1000。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

threshold-value: 指定向某 IP 地址每秒发送的 RST 报文数目，取值范围为 1~1000000。

【使用指导】

使能 RST 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 RST 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 RST 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。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）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。

对于未专门配置 RST flood 攻击防范检测的 IP 地址，设备采用全局的阈值设置来进行保护。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 RST 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。

【举例】

在攻击防范策略 `atk-policy-1` 中配置 RST flood 攻击防范检测的全局触发阈值为 100，即当设备监测到向某 IP 地址每秒发送的 RST 报文数持续达到或超过 100 时，启动 RST flood 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] rst-flood threshold 100
```

【相关命令】

- `rst-flood action`
- `rst-flood detect`
- `rst-flood detect non-specific`

1.1.52 scan detect

`scan detect` 命令用来配置开启指定级别的扫描攻击防范。

`undo scan detect` 命令用来关闭指定级别的扫描攻击防范。

【命令】

```
scan detect level { high | low | medium } action { drop | logging } *
undo scan detect level { high | low | medium }
```

【缺省情况】

扫描攻击防范处于关闭状态。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

level: 指定攻击防范的检测级别。

low: 表示低防范级别，该级别提供基本的扫描攻击检测，有很低的误报率，但对于一些扫描攻击类型不能检出。该级别的扫描攻击统计周期为 60 秒。

high: 表示高防范级别，该级别能检测出大部分的扫描攻击，但对活跃主机误报率较高，即将可提供服务的主机的报文错误判断为攻击报文的概率比较高。该级别的扫描攻击统计周期为 600 秒。

medium: 表示中防范级别，该级别有适中的攻击检出率与误报率，通常能够检测出 Filtered Scan 等攻击。该级别的扫描攻击统计周期为 90 秒。

action: 设置对扫描攻击的处理行为。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，由该攻击者发送的报文都将被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成记录告警信息。

【举例】

在攻击防范策略 **atk-policy-1** 中配置扫描攻击的检测级别为低级别，处理行为是丢弃后续报文。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] scan detect level low action drop
```

在攻击防范策略 **atk-policy-1** 中配置扫描攻击的检测级别为低级别，处理行为是发日志，阻断并丢弃来自该 IP 地址的后续报文。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] scan detect level low action logging
```

1.1.53 signature { large-icmp | large-icmpv6 } max-length

signature { large-icmp | large-icmpv6 } max-length 命令用来配置启动 Large ICMP 攻击防范的 ICMP 报文长度的最大值。

undo signature { large-icmp | large-icmpv6 } max-length 命令用来恢复缺省情况。

【命令】

```
signature { large-icmp | large-icmpv6 } max-length length
undo signature { large-icmp | large-icmpv6 } max-length
```

【缺省情况】

启动 Large ICMP 攻击防范的 ICMP 报文和 ICMPv6 报文长度的最大值均为 4000 字节。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

large-icmp: 表示超大 ICMP 报文攻击防范。

large-icmpv6: 表示超大 ICMPv6 报文攻击防范。

length: 表示 ICMP 报文长度的最大值, ICMP 报文取值范围为 28~65534, ICMPv6 报文取值范围为 48~65534, 单位为字节。

【举例】

在攻击防范策略 **atk-policy-1** 中配置启动 Large ICMP 攻击防范的 ICMP 报文长度的最大值为 50000 字节。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] signature large-icmp max-length 50000
```

【相关命令】

- **signature detect**

1.1.54 signature detect

signature detect 命令用来开启指定类型单包攻击报文的特征检测, 并设置攻击防范的处理行为。

undo signature detect 命令用来关闭对指定类型的单包攻击报文的特征检测。

【命令】

```
signature detect { fraggle | fragment | impossible | land | large-icmp |
large-icmpv6 | smurf | snork | tcp-all-flags | tcp-fin-only |
tcp-invalid-flags | tcp-null-flag | tcp-syn-fin | tiny-fragment | traceroute
| udp-bomb | winnuke } [ action { { drop | logging } * | none } ]
undo signature detect { fraggle | fragment | impossible | land | large-icmp |
large-icmpv6 | smurf | snork | tcp-all-flags | tcp-fin-only |
tcp-invalid-flags | tcp-null-flag | tcp-syn-fin | tiny-fragment | traceroute
| udp-bomb | winnuke }
signature detect { ip-option-abnormal | ping-of-death | teardrop } action
{ drop | logging } *
undo signature detect { ip-option-abnormal | ping-of-death | teardrop }
signature detect icmp-type { icmp-type-value | address-mask-reply |
address-mask-request | destination-unreachable | echo-reply | echo-request
| information-reply | information-request | parameter-problem | redirect
| source-quench | time-exceeded | timestamp-reply | timestamp-request }
[ action { { drop | logging } * | none } ]
undo signature detect icmp-type { icmp-type-value | address-mask-reply |
address-mask-request | destination-unreachable | echo-reply | echo-request
| information-reply | information-request | parameter-problem | redirect
| source-quench | time-exceeded | timestamp-reply | timestamp-request }
```

```
signature detect icmpv6-type { icmpv6-type-value | destination-unreachable
| echo-reply | echo-request | group-query | group-reduction | group-report
| packet-too-big | parameter-problem | time-exceeded } [ action { { drop |
logging } * | none } ]

undo signature detect icmpv6-type { icmpv6-type-value |
destination-unreachable | echo-reply | echo-request | group-query |
group-reduction | group-report | packet-too-big | parameter-problem |
time-exceeded }

signature detect ip-option { option-code | internet-timestamp |
loose-source-routing | record-route | route-alert | security | stream-id |
strict-source-routing } [ action { { drop | logging } * | none } ]

undo signature detect ip-option { option-code | internet-timestamp |
loose-source-routing | record-route | route-alert | security | stream-id |
strict-source-routing }

signature detect ipv6-ext-header ext-header-value [ action { { drop | logging }
* | none } ]

undo signature detect ipv6-ext-header next-header-value
```

【缺省情况】

所有类型的单包攻击报文的特征检测均处于关闭状态。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

fraggle: 表示 Fraggle 类型的报文攻击。

fragment: 表示 IP 分片报文攻击。

icmp-type: 表示 ICMP 类型的报文攻击。可以指定报文的类型值，或者指定报文的类型关键字。

- **icmp-type-value**: 表示 ICMP 报文类型的数值，取值范围为 0~255。
- **address-mask-reply**: 表示 ICMP address mask reply 类型的报文攻击。
- **address-mask-request**: 表示 ICMP address mask request 类型的报文攻击。
- **destination-unreachable**: 表示 ICMP destination unreachable 类型的报文攻击。
- **echo-reply**: 表示 ICMP echo reply 类型的报文攻击。
- **echo-request**: 表示 ICMP echo request 类型的报文攻击。
- **information-reply**: 表示 ICMP information reply 类型的报文攻击。
- **information-request**: 表示 ICMP information request 类型的报文攻击。
- **parameter-problem**: 表示 ICMP para problem 类型的报文攻击。
- **redirect**: 表示 ICMP redirect 类型的报文攻击。
- **source-quench**: 表示 ICMP source quench 类型的报文攻击。

- **time-exceeded**: 表示 ICMP time exceeded 类型的报文攻击。
- **timestamp-reply**: 表示 ICMP timestamp reply 类型的报文攻击。
- **timestamp-request**: 表示 ICMP timestamp request 类型的报文攻击。

icmpv6-type: 表示 ICMPv6 类型的报文攻击。可以指定报文的类型值，或者指定报文的类型关键字。

- **icmpv6-type-value**: 表示 ICMPv6 报文类型的数值，取值范围为 0~255。
- **destination-unreachable**: 表示 ICMPv6 destination unreachable 类型的报文攻击。
- **echo-reply**: 表示 ICMPv6 echo reply 类型的报文攻击。
- **echo-request**: 表示 ICMPv6 echo request 类型的报文攻击。
- **group-query**: 表示 ICMPv6 group query 类型的报文攻击。
- **group-reduction**: 表示 ICMPv6 group reduction 类型的报文攻击。
- **group-report**: 表示 ICMPv6 group report 类型的报文攻击。
- **packet-too-big**: 表示 ICMPv6 packet too big 类型的报文攻击。
- **parameter-problem**: 表示 ICMPv6 para problem 类型的报文攻击。
- **time-exceeded**: 表示 ICMPv6 time exceeded 类型的报文攻击。

impossible: 表示 IP 不可信报文的攻击。

ip-option: 表示 IP 选项类型的报文攻击。可以指定 IP 选项代码值，或者指定 IP 选项关键字。

- **option-code**: 表示 IP 选项代码值，取值范围为 0~255。
- **internet-timestamp**: 表示 IP 选项 timestamp 类型的报文攻击。
- **loose-source-routing**: 表示 IP 选项 loose source route 类型的报文攻击。
- **record-route**: 表示 IP 选项 record packet route 类型的报文攻击。
- **route-alert**: 表示 IP 选项 route alert 类型的报文攻击。
- **security**: 表示 IP 选项 security 类型的报文攻击。
- **stream-id**: 表示 IP 选项 stream identifier 类型的报文攻击。
- **strict-source-routing**: 表示 IP 选项 strict source route 类型的报文攻击。

ip-option-abnormal: 表示 IP 选项异常类型的报文攻击。

ipv6-ext-header ext-header-value: 表示 IPv6 扩展头参数值，取值范围在 0~255。

land: 表示 Land 类型的报文攻击。

large-icmp: 表示超大 ICMP 报文的攻击。

large-icmpv6: 表示超大 ICMPv6 报文的攻击。

ping-of-death: 表示 Ping-of-death 类型的报文攻击。

smurf: 表示 Smurf 类型的报文攻击。

snork: 表示 UDP Snork attack 类型的报文攻击。

tcp-all-flags: 表示 TCP 所有标志位均置位的报文攻击。

tcp-fin-only: 表示 TCP 仅 FIN 标志被置位的报文攻击。

tcp-invalid-flags: 表示 TCP 标志位非法的报文攻击。

tcp-null-flag: 表示 TCP 标志位为零的报文攻击。

tcp-syn-fin: 表示 TCP SYN 和 FIN 标志位被同时置位的报文攻击。

teardrop: 表示 teardrop 类型的报文攻击。

tiny-fragment: 表示 IP 分片报文的攻击。

traceroute: 表示 Trace route 类型的报文攻击。

udp-bomb: 表示 UDP Bomb attack 类型的报文攻击。

winnuke: 表示 WinNuke 类型的报文攻击。

action: 对指定报文攻击所采取的攻击防范处理行为。若未指定本参数，则采用该攻击报文所属的攻击防范级别所对应的默认处理行为。

- **drop:** 设置单包攻击的处理行为为丢弃报文。
- **logging:** 设置单包攻击的处理行为为发送日志。
- **none:** 不采取任何动作。

【使用指导】

可以通过多次执行本命令开启多种类型的单包攻击报文的特征检测。

若通过数值指定了报文类型，则当指定的数值为标准的报文类型值时，在显示信息中将会显示该数值对应的报文类型字符串，否则显示为数值。

【举例】

在攻击防范策略 **atk-policy-1** 中开启对 IP 分片攻击报文的特征检测，并指定攻击防范处理行为为丢弃报文。

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

【相关命令】

- **signature level action**

1.1.55 signature level action

signature level action 命令用来配置指定级别单包攻击的处理行为。

undo signature level action 命令用来恢复缺省情况。

【命令】

```
signature level { high | info | low | medium } action { { drop | logging } * | none }
undo signature level { high | info | low | medium } action
```

【缺省情况】

对提示级别和低级别的单包攻击的处理行为是发送日志；对中级别的单包攻击的处理行为是发送日志并丢包；对高级别的单包攻击的处理行为是发送日志并丢包。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

high: 表示高级别的单包攻击，暂无实例。

info: 表示提示级别的单包攻击，例如 Large ICMP。

low: 表示低级别的单包攻击，例如 Traceroute。

medium: 表示中级别的单包攻击，例如 Winnuke。

drop: 设置单包攻击的处理行为为丢弃报文。

logging: 设置单包攻击的处理行为为发送日志。

none: 不采取任何动作。

【使用指导】

系统根据单包攻击结果的严重程度由低到高将其划分为四个攻击级别：提示、低级、中级、高级。开启某一个级别的单包攻击报文的特征检测，相当于批量开启了属于该级别的所有类型的单包攻击报文的特征检测。

若同时通过 **signature detect** 命令开启了具体类型的单包攻击报文的特征检测，则以 **signature detect** 命令配置的参数为准。

【举例】

在攻击防范策略 **atk-policy-1** 中配置对提示级别的单包攻击的处理行为是丢弃后续报文。

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

【相关命令】

- **signature detect**
- **signature level detect**

1.1.56 signature level detect

signature level detect 命令用来开启指定级别单包攻击报文的特征检测。

undo signature level detect 命令用来关闭对指定级别的单包攻击报文的特征检测。

【命令】

```
signature level { high | info | low | medium } detect
undo signature level { high | info | low | medium } detect
```

【缺省情况】

未开启任何级别的单包攻击报文的特征检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

high: 表示高级别的单包攻击，暂无实例。

info: 表示提示级别的单包攻击，例如 Large ICMP 报文攻击。

low: 表示低级别的单包攻击，例如 Traceroute 报文攻击。

medium: 表示中级别的单包攻击，例如 Winnuke 报文攻击。

【使用指导】

系统根据单包攻击结果的严重程度将其划分为四个级别：提示、低级、中级、高级。开启某一个级别的单包攻击报文的特征检测，相当于批量开启了属于该级别的所有单包攻击报文的特征检测。针对某一级别的单包攻击的处理行为由 **signature level action** 命令指定。若通过 **signature detect** 命令开启了具体的单包攻击报文的特征检测，则对该类攻击报文的处理行为以 **signature detect** 命令配置的参数为准。

可通过 **display attack-defense policy** 命令查看各类型单包攻击所属的级别。

【举例】

在攻击防范策略 **atk-policy-1** 中开启提示级别的单包攻击报文的特征检测。

```
<Sysname> system-view
[Sysname] attack-defense policy 1
[Sysname-attack-defense-policy-1] signature level info detect
```

【相关命令】

- **display attack-defense policy**
- **signature detect**
- **signature level action**

1.1.57 syn-ack-flood action

syn-ack-flood action 命令用来配置对 SYN-ACK flood 攻击防范的全局处理行为。

undo syn-ack-flood action 命令用来恢复缺省情况。

【命令】

```
syn-ack-flood action { drop | logging } *
undo syn-ack-flood action
```

【缺省情况】

不对检测到的 SYN-ACK flood 攻击采取任何措施。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 SYN-ACK 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成记录告警信息。

【举例】

```
# 在攻击防范策略 atk-policy-1 中配置对 SYN-ACK flood 攻击防范的全局处理行为是丢弃后续报文。  
<Sysname> system-view  
[Sysname] attack-defense policy atk-policy-1  
[Sysname-attack-defense-policy-atk-policy-1] syn-ack-flood action drop
```

【相关命令】

- **syn-ack-flood detect**
- **syn-ack-flood detect non-specific**
- **syn-ack-flood threshold**

1.1.58 syn-ack-flood detect

syn-ack-flood detect 命令用来对指定 IP 地址的 SYN-ACK flood 攻击防范检测，并配置 SYN-ACK flood 攻击防范检测触发阈值和防范行为。

undo syn-ack-flood detect 命令用来关闭对指定 IP 地址的 SYN-ACK flood 攻击防范检测。

【命令】

```
syn-ack-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ] [ threshold threshold-value ] [ action { { drop | logging } * | none } ]  
undo syn-ack-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ]
```

【缺省情况】

未对任何指定 IP 地址配置 SYN-ACK flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

ip *ipv4-address*: 指定要保护的 IPv4 地址。该 IPv4 地址不能为全 1 地址或全 0 地址。

ipv6 *ipv6-address*: 指定要保护的 IPv6 地址。

vpn-instance *vpn-instance-name*: 受保护 IP 地址所属的 VPN 实例。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。若未指定本参数，则表示该保护 IP 地址属于公网。

threshold *threshold-value*: 指定 SYN-ACK flood 攻击防范的触发阈值。其中，*threshold-value* 为向指定 IP 地址每秒发送的 SYN-ACK 报文数目，取值范围为 1~1000000。

action: 设置对 SYN-ACK flood 攻击的处理行为。若未指定本参数，则表示采用 SYN-ACK flood 攻击防范的全局处理行为。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 SYN-ACK 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息。

none: 表示不采取任何动作。

【使用指导】

使能 SYN-ACK 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-ACK 报文的速率持续达到或超过了触发阈值时，即认为该 IP 地址受到了 SYN-ACK 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。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）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。

每个攻击防范策略下可以同时多个 IP 地址配置 SYN-ACK flood 攻击防范检测。

【举例】

开启对 IP 地址 192.168.1.2 的 SYN-ACK flood 攻击防范检测，并指定触发阈值为 2000。当设备监测到向该 IP 地址每秒发送的 SYN-ACK 报文数持续达到或超过 2000 时，启动 SYN-ACK 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-ack-flood detect ip 192.168.1.2 threshold 2000
```

【相关命令】

- **syn-ack-flood action**
- **syn-ack-flood detect non-specific**
- **syn-ack-flood threshold**

1.1.59 syn-ack-flood detect non-specific

syn-ack-flood detect non-specific 命令用来对所有非受保护 IP 地址开启 SYN-ACK flood 攻击防范检测。

undo syn-ack-flood detect non-specific 命令用来关闭对所有非受保护 IP 地址的 SYN-ACK flood 攻击防范检测。

【命令】

```
syn-ack-flood detect non-specific
undo syn-ack-flood detect non-specific
```

【缺省情况】

未对任何非受保护 IP 地址开启 SYN-ACK flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【使用指导】

对所有非受保护 IP 地址开启 SYN-ACK flood 攻击防范检测后，设备将采用全局的阈值设置（由 **syn-ack-flood threshold** 命令设置）和处理行为（由 **syn-ack-flood action** 命令配置）对这些 IP 地址进行保护。

【举例】

在攻击防范策略 **atk-policy-1** 中，对所有非受保护 IP 地址开启 UDP flood 攻击防范检测。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-ack-flood detect non-specific
```

【相关命令】

- **syn-ack flood action**
- **syn-ack-flood detect**
- **syn-ack-flood threshold**

1.1.60 syn-ack-flood threshold

syn-ack-flood threshold 命令用来配置 SYN-ACK flood 攻击防范的全局触发阈值。

undo syn-ack-flood threshold 命令用来恢复缺省情况。

【命令】

```
syn-ack-flood threshold threshold-value
undo syn-ack-flood threshold
```

【缺省情况】

SYN-ACK flood 攻击防范的全局触发阈值为 1000。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

threshold-value: 指定向某 IP 地址每秒发送的 SYN-ACK 报文数目，取值范围为 1~1000000。

【使用指导】

使能 SYN-ACK 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-ACK 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-ACK 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。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）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。

对于未专门配置 SYN-ACK flood 攻击防范检测的 IP 地址，设备采用全局的阈值设置来进行保护。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-ACK 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。

【举例】

在攻击防范策略 **atk-policy-1** 中配置 **SYN-ACK flood** 攻击防范的全局触发阈值为 100, 即当设备监测到向某 IP 地址每秒发送的 SYN-ACK 报文数持续达到或超过 100 时, 启动 **SYN-ACK flood** 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-ack-flood threshold 100
```

【相关命令】

- **syn-ack-flood action**
- **syn-ack-flood detect**
- **syn-ack-flood detect non-specific**

1.1.61 syn-flood action

syn-flood action 命令用来配置对 SYN flood 攻击防范的全局处理行为。

undo syn-flood action 命令用来恢复缺省情况。

【命令】

```
syn-flood action { drop | logging } *
undo syn-flood action
```

【缺省情况】

不对检测到的 SYN flood 攻击采取任何措施。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

drop: 表示丢弃攻击报文, 即设备检测到攻击发生后, 向被攻击者发送的后续所有 SYN 报文都会被丢弃。

logging: 表示输出告警日志, 即设备检测到攻击发生时, 生成告警信息。

【举例】

在攻击防范策略 **atk-policy-1** 中配置对 **SYN flood** 攻击防范的全局处理行为是丢弃后续报文。

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

【相关命令】

- **syn-flood detect non-specific**

- **syn-flood detect**
- **syn-flood threshold**

1.1.62 syn-flood detect

syn-flood detect 命令用来开启对指定 IP 地址的 SYN flood 攻击防范检测，并配置 SYN flood 攻击防范检测的触发阈值和对 SYN flood 攻击的处理行为。

undo syn-flood detect 命令用来关闭对指定 IP 地址的 SYN flood 攻击防范检测。

【命令】

```
syn-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance
vpn-instance-name ] [ threshold threshold-value ] [ action { { drop | logging }
* | none } ]
undo syn-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance
vpn-instance-name ]
```

【缺省情况】

未对任何指定 IP 地址配置 SYN flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

ip ipv4-address: 指定要保护的 IPv4 地址。该 IPv4 地址不能为全 1 地址或全 0 地址。

ipv6 ipv6-address: 指定要保护的 IPv6 地址。

vpn-instance vpn-instance-name: 受保护 IP 地址所属的 VPN 实例。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。若未指定本参数，则表示该保护 IP 地址属于公网。

threshold threshold-value: 指定 SYN flood 攻击防范的触发阈值。其中，*threshold-value* 为向指定 IP 地址每秒发送的 SYN 报文数目，取值范围为 1~1000000。

action: 设置对 SYN flood 攻击的处理行为。若未指定本参数，则表示采用 SYN flood 攻击防范的全局处理行为。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 SYN 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息。

none: 表示不采取任何动作。

【使用指导】

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。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触

发阈值的 3/4) 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。

每个攻击防范策略下可以同时多个 IP 地址配置 SYN flood 攻击防范检测。

【举例】

在攻击防范策略 **atk-policy-1** 中开启对 IP 地址 **192.168.1.2** 的 SYN flood 攻击防范检测, 并指定触发阈值为 **2000**。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 SYN flood 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-flood detect ip 192.168.1.2 threshold 2000
```

【相关命令】

- **syn-flood action**
- **syn-flood detect non-specific**
- **syn-flood threshold**

1.1.63 syn-flood detect non-specific

syn-flood detect non-specific 命令用来对所有非受保护 IP 地址开启 SYN flood 攻击防范检测。

undo syn-flood detect non-specific 命令用来关闭对所有非受保护 IP 地址的 SYN flood 攻击防范检测。

【命令】

```
syn-flood detect non-specific
undo syn-flood detect non-specific
```

【缺省情况】

未对任何非受保护 IP 地址开启 SYN flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【使用指导】

对所有非受保护 IP 地址开启 SYN flood 攻击防范检测后, 设备将采用全局的阈值设置 (由 **syn-flood threshold** 命令设置) 和处理行为 (由 **syn-flood action** 命令配置) 对这些 IP 地址进行保护。

【举例】

在攻击防范策略 **atk-policy-1** 中, 对所有非受保护 IP 地址开启 SYN flood 攻击防范检测。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-flood detect non-specific
```

【相关命令】

- `syn-flood action`
- `syn-flood detect`
- `syn-flood threshold`

1.1.64 syn-flood threshold

`syn-flood threshold` 命令用来配置 SYN flood 攻击防范的全局触发阈值。

`undo syn-flood threshold` 命令用来恢复缺省情况。

【命令】

```
syn-flood threshold threshold-value
undo syn-flood threshold
```

【缺省情况】

SYN flood 攻击防范的全局触发阈值为 1000。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

`threshold-value`: 指定向某 IP 地址每秒发送的 SYN 报文数目，取值范围为 1~1000000。

【使用指导】

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。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）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。

对于未专门配置 SYN flood 攻击防范检测的 IP 地址，设备采用全局的阈值设置来进行保护。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。

【举例】

在攻击防范策略 `atk-policy-1` 中配置 SYN flood 攻击防范的全局触发阈值为 100，即当设备监测到向某 IP 地址每秒发送的 SYN 报文数持续达到或超过 100 时，启动 SYN flood 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-flood threshold 100
```

【相关命令】

- `syn-flood action`

- **syn-flood detect**
- **syn-flood detect non-specific**

1.1.65 udp-flood action

udp-flood action 命令用来配置对 UDP flood 攻击防范的全局处理行为。

undo udp-flood action 命令用来恢复缺省情况。

【命令】

```
udp-flood action { drop | logging } *
undo udp-flood action
```

【缺省情况】

不对检测到的 UDP flood 攻击进行任何处理。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 UDP 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息。

【举例】

在攻击防范策略 **atk-policy-1** 中配置对 UDP flood 攻击防范的全局处理行为是丢弃后续报文。

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

【相关命令】

- **udp-flood detect**
- **udp-flood detect non-specific**
- **udp-flood threshold**

1.1.66 udp-flood detect

udp-flood detect 命令用来开启对指定 IP 地址的 UDP flood 攻击防范检测，并配置 UDP flood 攻击防范检测的触发阈值和对 UDP flood 攻击的处理行为。

undo udp-flood detect 命令用来关闭对指定 IP 地址的 UDP flood 攻击防范检测。

【命令】

```
udp-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance
vpn-instance-name ] [ threshold threshold-value ] [ action { { drop | logging }
* | none } ]
```

```
undo udp-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance  
vpn-instance-name ]
```

【缺省情况】

未对任何指定 IP 地址配置 UDP flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

ip *ipv4-address*: 指定要保护的 IPv4 地址。该 IPv4 地址不能为全 1 地址或全 0 地址。

ipv6 *ipv6-address*: 指定要保护的 IPv6 地址。

vpn-instance *vpn-instance-name*: 受保护 IP 地址所属的 VPN 实例。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。若未指定本参数，则表示该保护 IP 地址属于公网。

threshold *threshold-value*: 指定 UDP flood 攻击防范的触发阈值。其中，*threshold-value* 为向指定 IP 地址每秒发送的 UDP 报文数目，取值范围为 1~1000000。

action: 设置对 UDP flood 攻击的处理行为。若未指定本参数，则表示采用 UDP flood 攻击防范的全局处理行为。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 UDP 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息。

none: 表示不采取任何动作。

【使用指导】

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。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）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。

每个攻击防范策略下可以同时为多个 IP 地址配置 UDP flood 攻击防范参数。

【举例】

在攻击防范策略 **atk-policy-1** 中开启对 IP 地址 192.168.1.2 的 UDP flood 攻击防范检测，并指定触发阈值为 2000。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 UDP flood 攻击防范。

```
<Sysname> system-view
```

```
[Sysname] attack-defense policy atk-policy-1
```

```
[Sysname-attack-defense-policy-atk-policy-1] udp-flood detect ip 192.168.1.2 threshold 2000
```

【相关命令】

- **udp-flood action**

- `udp-flood detect non-specific`
- `udp-flood threshold`

1.1.67 udp-flood detect non-specific

`udp-flood detect non-specific` 命令用来对所有非受保护 IP 地址开启 UDP flood 攻击防范检测。

`undo udp-flood detect non-specific` 命令用来关闭对所有非受保护 IP 地址的 UDP flood 攻击防范检测。

【命令】

```
udp-flood detect non-specific
undo udp-flood detect non-specific
```

【缺省情况】

未对任何非受保护 IP 地址开启 UDP flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【使用指导】

对所有非受保护 IP 地址开启 UDP flood 攻击防范检测后，设备将采用全局的阈值设置（由 `udp-flood threshold` 命令设置）和处理行为（由 `udp-flood action` 命令配置）对这些 IP 地址进行保护。

【举例】

在攻击防范策略 `atk-policy-1` 中，对所有非受保护 IP 地址开启 UDP flood 攻击防范检测。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] udp-flood detect non-specific
```

【相关命令】

- `udp-flood action`
- `udp-flood detect`
- `udp-flood threshold`

1.1.68 udp-flood threshold

`udp-flood threshold` 命令用来配置 UDP flood 攻击防范的全局触发阈值。

`undo udp-flood threshold` 命令用来恢复缺省情况。

【命令】

```
udp-flood threshold threshold-value
undo udp-flood threshold
```

【缺省情况】

UDP flood 攻击防范的全局触发阈值为 1000。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

【参数】

threshold-value: 指定向某 IP 地址每秒发送的 UDP 报文数目，取值范围为 1~1000000。

【使用指导】

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。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）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。

对于未专门配置 UDP flood 攻击防范检测的 IP 地址，设备采用全局的阈值设置来进行保护。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 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。

【举例】

在攻击防范策略 *atk-policy-1* 中配置 UDP flood 攻击防范的全局触发阈值为 100，即当设备监测到向某 IP 地址每秒发送的 UDP 报文数持续达到或超过 100 时，启动 UDP flood 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] udp-flood threshold 100
```

【相关命令】

- **udp-flood action**
- **udp-flood detect**
- **udp-flood detect non-specific**