目 录

1 ASPF

1.1 ASPF配置命令

1.1.1 aspf apply policy

aspf apply policy 命令用来在安全域间实例上应用 ASPF 策略。

undo aspf apply policy 命令用来取消应用在安全域间实例上的指定 ASPF 策略。

【命令】

aspf apply policy *aspf-policy-number*

undo aspf apply policy *aspf-policy-number*

【缺省情况】

安全域间实例上应用了一个缺省的 ASPF 策略。

【视图】

安全域间实例视图

【缺省用户角色】

network-admin

context-admin

【参数】

aspf-policy-number：ASPF 策略号，取值范围为 1～256。

【使用指导】

创建安全域间实例时，系统默认为该实例应用一个缺省的 ASPF 策略。该策略支持对所有传输层协议和 FTP 协议报文进行 ASPF 检测，但是 ICMP 差错报文检查功能和非 SYN 的 TCP 首报文丢弃功能处于关闭状态，并且默认的策略不可改变，如果需要调整 ASPF 策略，需要自定义一个 ASPF 策略，并在安全域间实例上引用。

多次执行本命令，最后一次执行的命令生效。

【举例】

在安全域间实例上应用 ASPF 策略。

```
<Sysname> system-view
[Sysname] security-zone name trust
[Sysname-security-zone-Trust] import interface gigabitethernet 1/0/1
[Sysname-security-zone-Trust] quit
[Sysname] security-zone name untrust
[Sysname-security-zone-Untrust] import interface gigabitethernet 1/0/2
[Sysname-security-zone-Untrust] quit
[Sysname] zone-pair security source trust destination untrust
[Sysname-zone-pair-security-Trust-Untrust] aspf apply policy 1
```

【相关命令】

- **aspf policy**
- **display aspf all**
- **zone-pair security**（安全命令参考/安全域）

1.1.2 aspf icmp-error reply

aspf icmp-error reply 命令用来开启设备在域间策略丢包时，发送 ICMP 差错报文功能。

undo aspf icmp-error reply 命令用来恢复缺省情况。

【命令】

aspf icmp-error reply

undo aspf icmp-error reply

【缺省情况】

在域间策略丢包时，设备不发送 ICMP 差错报文。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

缺省情况下，设备在安全域间实例下配置安全域间策略，丢弃不符合策略的报文，但不发送 ICMP 差错报文，这样可以减少网络上的无用报文，节约带宽。

使用 traceroute 功能时，需要用到 ICMP 差错报文，需要开启发送 ICMP 差错报文的功能。

【举例】

开启设备在域间策略丢包时，发送 ICMP 差错报文功能。

```
<Sysname> system-view
[Sysname] aspf icmp-error reply
```

1.1.3 aspf log sending-realtime enable

aspf log sending-realtime enable 命令用来开启日志的实时发送功能。

undo aspf log sending-realtime enable 命令用来关闭日志的实时发送功能。

【命令】

aspf log sending-realtime enable

undo aspf log sending-realtime enable

【缺省情况】

日志的实时发送功能处于关闭状态，使用缓存方式发送。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

日志实时发送功能仅对安全策略、对象策略和包过滤模块的日志发送有效。

日志的发送方式支持如下两种：

- 缓存发送方式：同一数据流的首报文匹配相关策略生成并发送日志后，设备缓存此日志，同时启动发送日志的时间间隔定时器，只有时间间隔到达后，才会判断是否继续发送此日志。在此时间间隔内若有流量匹配此日志，则发送日志，若没有则删除缓存的此日志。日志缓存达到上限后，当后续新增数据流匹配相关策略时将不能生成日志。日志发送时间间隔缺省为 5 分钟，且不能修改。
- 实时发送方式：同一数据流的首报文匹配相关策略生成并发送日志后，设备不缓存此日志，因此此方式没有日志上限限制。对于一条不间断的流量，若匹配的策略允许报文通过，则设备仅发送一次日志，若匹配的策略拒绝报文通过，则设备将对此条数据流的每个报文均发送一次日志。

有关安全策略、对象策略和包过滤开启记录日志功能的详细介绍，请参见各自模块的相关配置介绍。

【举例】

开启日志的实时发送功能。

```
<Sysname> system-view
[Sysname] aspf log sending-realtime enable
```

【相关命令】

- **logging enable**（安全命令参考/安全策略）
- **rule** *rule-id* **logging**（安全命令参考/对象策略）
- **rule** *rule-id* **logging**（ACL 和 QoS 命令参考/ACL）

1.1.4 aspf policy

aspf policy 命令用来创建 ASPF 策略，并进入 ASPF 策略视图。如果指定的 ASPF 策略已经存在，则直接进入 ASPF 策略视图。

undo aspf policy 命令用来删除指定的 ASPF 策略。

【命令】

aspf policy *aspf-policy-number*

undo aspf policy *aspf-policy-number*

【缺省情况】

不存在 ASPF 策略。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

aspf-policy-number：ASPF 策略号，取值范围为 1～256。

【举例】

创建 ASPF 策略 1，并进入该 ASPF 策略视图。

```
<Sysname> system-view
[Sysname] aspf policy 1
[Sysname-aspf-policy-1]
```

【相关命令】

- **display aspf all**
- **display aspf policy**

1.1.5 detect

detect 命令用来为应用层协议配置 ASPF 检测。

undo detect 命令用来恢复缺省情况。

【命令】

detect { **dns** [**action** { **drop** | **logging** } *] | { **ftp** | **h323** | **http** | **sccp** | **sip** | **smtp** } [**action drop**] | **gtp** | **ils** | **mgcp** | **nbt** | **pptp** | **rsh** | **rtsp** | **sqlnet** | **tftp** | **xdmcp** }

undo detect { **dns** | **ftp** | **gtp** | **h323** | **http** | **ils** | **mgcp** | **nbt** | **pptp** | **rsh** | **rtsp** | **sccp** | **sip** | **smtp** | **sqlnet** | **tftp** | **xdmcp** }

【缺省情况】

对传输层协议和应用层协议 FTP 进行 ASPF 检测。

【视图】

ASPF 策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

dns：表示 DNS 协议，属于应用层协议；

ftp：表示 FTP 协议，属于应用层协议；

gtp：表示 GTP（GPRS Tunneling Protocol，GPRS 隧道协议）协议，属于应用层协议；

h323：表示 H.323 协议族，属于应用层协议；

http：表示 HTTP 协议，属于应用层协议；

ils：表示 ILS（Internet Locator Service，互联网定位服务）协议，属于应用层协议；

mgcp：表示 MGCP（Media Gateway Control Protocol，媒体网关控制协议）协议，属于应用层协议；

nbt：表示 NBT（NetBIOS over TCP/IP，基于 TCP/IP 的网络基本输入输出系统）协议，属于应用层协议；

pptp：表示 PPTP（Point-to-Point Tunneling Protocol，点到点隧道协议）协议，属于应用层协议；

rsh：表示 RSH（Remote Shell，远程外壳）协议，属于应用层协议；

rtsp：表示 RTSP（Real Time Streaming Protocol，实时流协议）协议，属于应用层协议；

sccp：表示 SCCP（Skinny Client Control Protocol，瘦小客户端控制协议）协议，属于应用层协议；

sip：表示 SIP（Session Iniation Protocol，会话初始化协议）协议，属于应用层协议；

smtp：表示 SMTP 协议，属于应用层协议；

sqlnet：表示 SQLNET 协议，属于应用层协议；

tftp：表示 TFTP 协议，属于应用层协议；

xdmcp：表示 XDMCP（X Display Manager Control Protocol，X 显示监控）协议，属于应用层协议；

action：设置对检测到的非法报文的处理行为。若不指定该参数，则表示放行报文。

drop：表示丢弃报文。

logging：表示生成日志信息。

【使用指导】

若配置了此命令，则对报文的应用层协议进行 ASPF 检查；若没有配置此命令，则仅对报文的传输层协议进行 ASPF 检查。

如果设备上其他业务模块开启 ALG 功能时，即便未配置多通道应用层协议的 ASPF 检测，多通道协议的数据连接也可以建立成功。例如：开启 DPI 相关业务功能时会打开 ALG 功能，此时 DPI 处理的多通道协议（如 SIP 等）报文进行 ASPF 处理时，即便未配置 SIP 协议的 ASPF 检测，SIP 协议的数据连接也可以建立成功；开启 NAT ALG 功能时，即便未配置多通道协议的 ASPF 检测，多通道协议的数据连接也可以建立成功。但是在设备上未配置 DPI（Deep Packet Inspection，深度报文检测）相关业务功能只配置了 ASPF 功能的情况下，必须配置此命令，否则会导致数据连接无法建立。此命令支持的应用层协议中除 HTTP、SMTP 和 TFTP 之外的所有应用层协议均为多通道应用层协议。

可通过多次执行本命令配置多种协议类型的 ASPF 检测。

ASPF 策略默认已经开启对传输层协议的检测，无需进行配置，也不能修改。检测的传输层协议包括：TCP 协议、UDP 协议、UDP-Lite 协议、SCTP 协议、Raw IP 协议、ICMP 协议、ICMPv6 协议和 DCCP 协议。

ASPF 策略可以根据需要配置应用层协议的检测。目前，设备对支持 **action** 参数的应用层协议（DNS、FTP、H323、HTTP、SCCP、SIP、SMTP）进行协议状态合法性检查，对不符合协议状态的报文根据 action 参数的配置进行丢弃处理。对于其它应用层协议，仅进行连接状态信息的维护，不做协议状态合法性检查。

【举例】

配置对 FTP 协议报文进行 ASPF 检测。

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

```
[Sysname] aspf policy 1
[Sysname-aspf-policy-1] detect ftp
```

配置对 DNS 协议进行应用层协议检测，丢弃不符合协议状态的报文，并生成日志信息。

```
<Sysname> system-view
[Sysname] aspf policy 1
[Sysname-aspf-policy-1] detect dns action drop logging
```

【相关命令】

- **display aspf policy**

1.1.6 display aspf all

display aspf all 命令用来查看 ASPF 策略配置信息及应用 ASPF 策略的信息。

【命令】

display aspf all

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【举例】

查看所有的 ASPF 策略配置信息。

```
<Sysname> display aspf all
ASPF policy configuration:
  Policy default:
    ICMP error message check: Disabled
    TCP SYN packet check: Disabled
    Inspected protocol    Action
      FTP                  None
  Policy number: 1
    ICMP error message check: Disabled
    TCP SYN packet check: Disabled
    Inspected protocol    Action
      FTP                  None

Zone-pair security application:
  Source Trust destination Untrust
    Apply ASPF policy: default
```

表1-1 display aspf all 命令显示信息描述表

字段	描述
ASPF policy configuration	ASPF策略的配置信息

字段	描述
Policy default	缺省ASPF策略
Policy number	ASPF策略号
ICMP error message check	ICMP差错报文检测功能的开启状态
TCP SYN packet check	非SYN的TCP首报文丢弃功能的开启状态
Inspected protocol	需要检测的应用层协议
Action	对检测到的非法协议报文的处理行为 • Drop：丢弃 • Log：生成日志信息 • None：不做处理，放行 “-”表示该协议不支持此配置项
Zone-pair security application	安全域间实例
Source *XXX* destination *XXX*	安全域间实例中的源安全域和目的安全域
Apply ASPF policy	在安全域间实例上应用的ASPF策略编号

【相关命令】

- **aspf apply policy**
- **aspf policy**
- **display aspf policy**

1.1.7 display aspf policy

display aspf policy 命令用来查看 ASPF 策略的配置信息。

【命令】

display aspf policy { *aspf-policy-number* | **default** }

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

aspf-policy-number：ASPF 策略号，取值范围为 1～256。

default：缺省 ASPF 策略。

【举例】

查看策略号为 1 的 ASPF 策略的配置信息。

```
<Sysname> display aspf policy 1
ASPF policy configuration:
  Policy number: 1
    ICMP error message check: Disabled
    TCP SYN packet check: Enabled
    Inspected protocol   Action
     FTP                  Drop
     HTTP                 None
     RSH                  -
```

表1-2 display aspf policy 命令显示信息描述表

字段	描述
ASPF policy configuration	ASPF策略的配置信息
Policy number	ASPF策略号
ICMP error message check	ICMP差错报文检测功能的开启状态
TCP SYN packet check	非SYN的TCP首报文丢弃功能的开启状态
Inspected protocol	需要检测的应用层协议
Action	对检测到的非法报文的处理行为 • Drop：丢弃 • Log：生成日志信息 • None：不做处理，放行 “-”表示该协议不支持此配置项

【相关命令】

- **aspf policy**

1.1.8 display aspf session

display aspf session 命令用来查看 ASPF 的会话表信息。

【命令】

（独立运行模式）

display aspf session [**ipv4** | **ipv6**] [**slot** *slot-number* [**cpu** *cpu-number*]] [**verbose**]

（IRF 模式）

display aspf session [**ipv4** | **ipv6**] [**chassis** *chassis-number* **slot** *slot-number* [**cpu** *cpu-number*]] [**verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

ipv4：查看 ASPF 创建的 IPv4 会话表。

ipv6：查看 ASPF 创建的 IPv6 会话表。

slot *slot-number*：显示指定单板上的 ASPF 会话表，*slot-number* 表示单板所在槽位号。不指定该参数时，显示所有单板上的 ASPF 会话表。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备的指定单板上的 ASPF 会话表，*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。不指定该参数时，显示所有成员设备的所有单板上的 ASPF 会话表。（IRF 模式）

cpu *cpu-number*：显示指定 CPU 上的 ASPF 会话表，*cpu-number* 表示 CPU 的编号。只有指定的 **slot** 支持多 CPU 时，才能配置该参数。

verbose：查看 ASPF 会话表的详细信息。若不指定该参数，则表示查看 ASPF 会话表的概要信息。

【使用指导】

不指定 **ipv4** 和 **ipv6** 参数时，表示查看所有的 ASPF 会话表信息。

【举例】

显示 ASPF 创建的 IPv4 会话表的概要信息。（独立运行模式）

```
<Sysname> display aspf session ipv4
Slot 1:
Initiator:
  Source      IP/port: 192.168.1.18/1877
  Destination IP/port: 192.168.1.55/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: SrcZone
Initiator:
  Source      IP/port: 192.168.1.18/1792
  Destination IP/port: 192.168.1.55/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: SrcZone

Total sessions found: 2
```

显示 IPv4 ASPF 会话的详细信息。（独立运行模式）

```
<Sysname> display aspf session ipv4 verbose
```

```
Slot 1:
Initiator:
  Source      IP/port: 192.168.1.18/1877
  Destination IP/port: 192.168.1.55/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: SrcZone
Responder:
  Source      IP/port: 192.168.1.55/22
  Destination IP/port: 192.168.1.18/1877
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: DestZone
State: TCP_SYN_SENT
Application: SSH
Start time: 2011-07-29 19:12:36  TTL: 28s
Initiator->Responder:         1 packets         48 bytes
Responder->Initiator:         0 packets          0 bytes

Initiator:
  Source      IP/port: 192.168.1.18/1792
  Destination IP/port: 192.168.1.55/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: SrcZone
Responder:
  Source      IP/port: 192.168.1.55/1792
  Destination IP/port: 192.168.1.18/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: DestZone
State: ICMP_REQUEST
Application: OTHER
Start time: 2011-07-29 19:12:33  TTL: 55s
Initiator->Responder:         1 packets         6048 bytes
Responder->Initiator:         0 packets          0 bytes

Total sessions found: 2
```

显示 ASPF 创建的 IPv4 会话表的概要信息。（独立运行模式）

```
<Sysname> display aspf session ipv4
```

```
CPU 0 on slot 1:
Initiator:
  Source      IP/port: 192.168.1.18/1877
  Destination IP/port: 192.168.1.55/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: SrcZone
Initiator:
  Source      IP/port: 192.168.1.18/1792
  Destination IP/port: 192.168.1.55/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: SrcZone

Total sessions found: 2
```

显示 IPv4 ASPF 会话的详细信息。（独立运行模式）

```
<Sysname> display aspf session ipv4 verbose
CPU 0 on slot 1:
Initiator:
  Source      IP/port: 192.168.1.18/1877
  Destination IP/port: 192.168.1.55/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: SrcZone
Responder:
  Source      IP/port: 192.168.1.55/22
  Destination IP/port: 192.168.1.18/1877
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: DestZone

State: TCP_SYN_SENT
Application: SSH
Start time: 2011-07-29 19:12:36  TTL: 28s
Initiator->Responder:         1 packets         48 bytes
Responder->Initiator:         0 packets          0 bytes

Initiator:
  Source      IP/port: 192.168.1.18/1792
  Destination IP/port: 192.168.1.55/2048
```

```
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: SrcZone
Responder:
  Source      IP/port: 192.168.1.55/1792
  Destination IP/port: 192.168.1.18/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: DestZone
State: ICMP_REQUEST
Application: OTHER
Start time: 2011-07-29 19:12:33  TTL: 55s
Initiator->Responder:         1 packets         6048 bytes
Responder->Initiator:         0 packets          0 bytes

Total sessions found: 2
```

表1-3 display aspf session 命令显示信息描述表

字段	描述
Initiator	发起方到响应方的连接对应的会话信息
Responder	响应方到发起方的连接对应的会话信息
Source IP/port	源IP地址/端口号
Destination IP/port	目的IP地址/端口号
DS-Lite tunnel peer	DS-Lite隧道对端地址。会话不属于任何DS-Lite隧道时，本字段显示为“-”
VPN-instance/VLAN ID/Inline ID	会话所属的MPLS L3VPN/二层转发时会话所属的VLAN ID/二层转发时会话所属的INLINE。未指定的参数则显示为“-”
Protocol	传输层协议类型，取值包括：DCCP、ICMP、ICMPv6、Raw IP 、SCTP、TCP、UDP、UDP-Lite 括号中的数字表示协议号
Inbound interface	报文的入接口
Source security zone	源安全域，即入接口所属的安全域。若接口不属于任何安全域，则显示为“-”
State	会话的协议状态
Application	应用层协议类型，取值包括：FTP、DNS等，OTHER表示未知协议类型，其对应的端口为非知名端口
Start time	会话的创建时间
TTL	会话剩余存活时间，单位为秒

字段	描述
Initiator->Responder	发起方到响应方的报文数、报文字节数
Responder->Initiator	响应方到发起方的报文数、报文字节数
Total sessions found	当前查找到的会话总数

【相关命令】

- **reset aspf session**

1.1.9 icmp-error drop

icmp-error drop 命令用来开启 ICMP 差错报文丢弃功能。

undo icmp-error drop 命令用来关闭 ICMP 差错报文丢弃功能。

【命令】

icmp-error drop

undo icmp-error drop

【缺省情况】

ICMP 差错报文丢弃功能处于关闭状态。

【视图】

ASPF 策略视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

正常 ICMP 差错报文中均携带有本报文对应连接的相关信息，根据这些信息可以匹配到相应的连接。如果匹配失败，则根据当前配置决定是否丢弃该 ICMP 报文。

【举例】

设置 ASPF 策略 1 丢弃非法的 ICMP 差错报文。

```
<Sysname> system-view
[Sysname] aspf policy 1
[Sysname-aspf-policy-1] icmp-error drop
```

【相关命令】

- **aspf policy**
- **display aspf policy**

1.1.10 reset aspf session

reset aspf session 命令用来删除 ASPF 的会话表项。

【命令】

（独立运行模式）

reset aspf session [**ipv4** | **ipv6**] [**slot** *slot-number* [**cpu** *cpu-number*]]

（IRF 模式）

reset aspf session [**ipv4** | **ipv6**] [**chassis** *chassis-number* **slot** *slot-number* [**cpu** *cpu-number*]]

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv4：删除 ASPF 创建的 IPv4 会话表项。

ipv6：删除 ASPF 创建的 IPv6 会话表项。

slot *slot-number*：删除指定单板上的所有 ASPF 创建的会话表项，*slot-number* 表示单板所在槽位号。不指定该参数时，删除所有单板上的所有 ASPF 创建的会话表项。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：删除指定成员设备的指定单板上的所有 ASPF 创建的会话表项，*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。不指定该参数时，删除所有成员设备的所有单板上的所有 ASPF 创建的会话表项。（IRF 模式）

cpu *cpu-number*：删除指定 CPU 上的所有 ASPF 创建的会话表项，*cpu-number* 表示 CPU 的编号。只有指定的 **slot** 支持多 CPU 时，才能配置该参数。

【使用指导】

如果不指定 **ipv4** 和 **ipv6** 参数，则表示删除 ASPF 创建的所有会话表项。

【举例】

清除 ASPF 创建的所有会话表项。

```
<Sysname> reset aspf session
```

【相关命令】

- **display aspf session**

1.1.11 tcp syn-check

tcp syn-check 命令用来开启非 SYN 的 TCP 首报文丢弃功能。

undo tcp syn-check 命令用来关闭非 SYN 的 TCP 首报文丢弃功能。

【命令】

tcp syn-check

undo tcp syn-check

【缺省情况】

非 SYN 的 TCP 首报文丢弃功能处于关闭状态。

【视图】

ASPF 策略视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

ASPF 对 TCP 连接的首报文进行检测，查看是否为 SYN 报文，如果不是 SYN 报文则根据当前配置决定是否丢弃该报文。

当设备首次加入网络时，网络中原有 TCP 连接的非首包在经过新加入的设备时如果被丢弃，会中断已有的连接，造成不好的用户体验，因此建议暂且不丢弃非 SYN 首包，等待网络拓扑稳定后，再开启非 SYN 首包丢弃功能。

【举例】

设置 ASPF 策略 1 丢弃非 SYN 的 TCP 首报文。

```
<Sysname> system-view
[Sysname] aspf policy 1
[Sysname-aspf-policy-1] tcp syn-check
```

【相关命令】

- **aspf policy**