目 录

1 防火墙

1.1 包过滤防火墙配置命令

1.1.1 display firewall ipv6 statistics

【命令】

display firewall ipv6 statistics { **all** | **interface** *interface-type interface-number* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

all：查看 IPv6 防火墙的所有接口的过滤报文统计信息。

interface *interface-type interface-number*：查看 IPv6 防火墙的指定接口的过滤报文统计信息。其中，*interface-type interface-number* 表示接口类型和接口编号。

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

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

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

【描述】

display firewall ipv6 statistics 命令用来查看 IPv6 防火墙的过滤报文统计信息。

【举例】

查看 IPv6 防火墙的过滤报文统计信息。

```
<Sysname> display firewall ipv6 statistics interface gigabitethernet 3/0/1
  Interface: GigabitEthernet3/0/1
  In-bound Policy: acl6 2000
  From 2008-06-04 10:25:21  to 2008-06-04 10:35:57
     0 packets, 0 bytes, 0% permitted
     0 packets, 0 bytes, 0% denied
     0 packets, 0 bytes, 0% permitted default
     0 packets, 0 bytes, 0% denied default
  Totally 0 packets, 0 bytes, 0% permitted
  Totally 0 packets, 0 bytes, 0% denied
```

表1-1 display firewall ipv6 statistics 命令显示信息描述表

字段	描述
Interface	配置了IPv6包过滤功能的接口
In-bound Policy	表示该接口上配置了入方向的ACL规则
Out-bound Policy	表示该接口上配置了出方向的ACL规则
acl6	IPv6 ACL编号
0 packets, 0 bytes, 0% permitted	表示匹配到IPv6 ACL规则，且被允许通行的报文个数、字节数和比例
0 packets, 0 bytes, 0% denied	表示匹配到IPv6 ACL规则，且被拒绝通行的报文个数、字节数和比例
0 packets, 0 bytes, 0% permitted default	表示未匹配到任何IPv6 ACL规则，且根据缺省过滤规则被允许通行的报文个数、字节数和比例
0 packets, 0 bytes, 0% denied default	表示未匹配到任何IPv6 ACL规则，且根据缺省过滤规则被拒绝通行的报文个数、字节数和比例
Totally 0 packets, 0 bytes, 0% permitted	总计被允许通行的报文个数、字节数和比例
Totally 0 packets, 0 bytes, 0% denied	总计被拒绝通行的报文个数、字节数和比例

1.1.2 display firewall-statistics

【命令】

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

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

all：查看 IPv4 防火墙的所有接口的过滤报文统计信息。

interface *interface-type interface-number*：查看 IPv4 防火墙的指定接口的过滤报文统计信息。其中，*interface-type interface-number* 表示接口类型和接口编号。

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

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

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

【描述】

display firewall-statistics 命令用来查看 IPv4 防火墙的过滤报文统计信息。

【举例】

查看 IPv4 防火墙的所有接口的过滤报文统计信息。

```
<Sysname> display firewall-statistics all
```

1.1.3 firewall default

【命令】

非 IRF 模式：

firewall default { **deny** | **permit** } { **all** | **slot** *slot-number* }

IRF 模式：

firewall default { **deny** | **permit** } { **all** | **chassis** *chassis-number* **slot** *slot-number* }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

deny：过滤方式为禁止报文通过。

permit：过滤方式为允许报文通过。

all：指定所有接口板。

slot *slot-number*：指定接口板。其中，*slot-number* 表示接口板所在槽位号。（非 IRF 模式）

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

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

chassis *chassis-number* **slot** *slot-number*：指定成员设备上的接口板。*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。（IRF 模式）

【描述】

firewall default 命令用来配置 IPv4 防火墙的缺省过滤方式。

缺省情况下，IPv4 防火墙的缺省过滤方式为允许报文通过（**permit**）。

【举例】

配置 IPv4 防火墙的缺省过滤方式为禁止报文通过。

```
<Sysname> system-view
[Sysname] firewall default deny
```

1.1.4 firewall enable

【命令】

非 IRF 模式：

firewall enable { **all** | **slot** *slot-number* }

undo firewall enable

IRF 模式：

firewall enable { **all** | **chassis** *chassis-number* **slot** *slot-number* }

undo firewall enable

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

all：指定所有接口板。

slot *slot-number*：指定接口板。其中，*slot-number* 表示接口板所在槽位号。（非 IRF 模式）

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

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

chassis *chassis-number* **slot** *slot-number*：指定成员设备上的接口板。*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。（IRF 模式）

【描述】

firewall enable 命令用来启用 IPv4 防火墙功能。**undo firewall enable** 命令用来关闭 IPv4 防火墙功能。

缺省情况下，IPv4 防火墙功能处于关闭状态。

【举例】

启用 IPv4 防火墙功能。

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

1.1.5 firewall ipv6 default

【命令】

firewall ipv6 default { **deny** | **permit** }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

deny：过滤方式为禁止报文通过。

permit：过滤方式为允许报文通过。

【描述】

firewall ipv6 default 命令用来配置 IPv6 防火墙的缺省过滤方式。对于未匹配到任何 IPv6 包过滤策略中引用的 ACL 规则的 IPv6 报文，防火墙使用默认的过滤方式对其进行过滤。

缺省情况下，IPv6 防火墙的缺省过滤方式为允许报文通过（**permit**）。

【举例】

配置 IPv6 防火墙的缺省过滤方式为禁止报文通过。

```
<Sysname> system-view
[Sysname] firewall ipv6 default deny
```

1.1.6 firewall ipv6 enable

【命令】

firewall ipv6 enable

undo firewall ipv6 enable

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

无

【描述】

firewall ipv6 enable 命令用来启用 IPv6 防火墙功能。**undo firewall enable** 命令用来关闭 IPv6 防火墙功能。

缺省情况下，IPv6 防火墙功能处于关闭状态。

【举例】

启用 IPv6 防火墙功能。

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

```
[Sysname] firewall ipv6 enable
```

1.1.7 firewall packet-filter

【命令】

firewall packet-filter { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

undo firewall packet-filter { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

【视图】

接口视图

【缺省级别】

2：系统级

【参数】

acl-number：基本或高级访问控制列表号，取值范围为 2000～3999。

name *acl-name*：指定基本或高级访问控制列表的名称。其中，*acl-name* 表示 IPv4 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，IPv4 ACL 的名称不可以使用英文单词 all。

inbound：过滤接口接收的数据包。

outbound：过滤接口转发的数据包。

【描述】

firewall packet-filter 命令用来配置接口的 IPv4 报文过滤功能。**undo firewall packet-filter** 命令用来取消接口的报文过滤功能。

缺省情况下，不对通过接口的报文进行过滤。

在接口的一个方向上，只能应用一个 IPv4 ACL 来进行报文过滤。

【举例】

使用 ACL 2001 在接口 GigabitEthernet3/0/1 上对出方向的报文进行过滤。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] firewall packet-filter 2001 outbound
```

1.1.8 firewall packet-filter ipv6

【命令】

firewall packet-filter ipv6 { *acl6-number* | **name** *acl6-name* } { **inbound** | **outbound** }

undo firewall packet-filter ipv6 [{ *acl6-number* | **name** *acl6-name* }] { **inbound** | **outbound** }

【视图】

接口视图

【缺省级别】

2：系统级

【参数】

acl6-number：基本或高级 IPv6 访问控制列表号，取值范围为 2000～3999。

name *acl6-name*：指定基本或高级访问控制列表的名称。其中，*acl6-name* 表示 IPv6 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，IPv6 ACL 的名称不可以使用英文单词 all。

inbound：过滤接口接收的数据包。

outbound：过滤接口转发的数据包。

【描述】

firewall packet-filter ipv6 命令用来配置接口的 IPv6 报文过滤功能。**undo firewall packet-filter ipv6** 命令用来取消接口的 IPv6 报文过滤功能。

缺省情况下，不对通过接口的 IPv6 报文进行过滤。

在接口的一个方向上，只能应用一个 IPv6 ACL 来进行报文过滤。

【举例】

使用 IPv6 ACL 2500 在接口 GigabitEthernet3/0/1 上进行 IPv6 报文过滤。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] firewall packet-filter ipv6 2500 outbound
```

1.1.9 reset firewall ipv6 statistics

【命令】

reset firewall ipv6 statistics { **all** | **interface** *interface-type interface-number* }

【视图】

用户视图

【缺省级别】

1：监控级

【参数】

all：清除 IPv6 防火墙的所有接口的过滤报文统计信息。

interface *interface-type interface-number*：表示清除 IPv6 防火墙的指定接口的过滤报文统计信息。其中，*interface-type interface-number* 表示接口类型和接口编号。

【描述】

reset firewall ipv6 statistics 命令用来清除 IPv6 防火墙的过滤报文统计信息。

相关配置可参考命令 **display firewall ipv6 statistics**。

【举例】

清除接口 GigabitEthernet3/0/1 上 IPv6 防火墙的过滤报文统计信息。

```
<Sysname> reset firewall ipv6 statistics interface gigabitethernet 3/0/1
```

1.1.10 reset firewall-statistics

【命令】

reset firewall-statistics { **all** | **interface** *interface-type interface-number* }

【视图】

用户视图

【缺省级别】

1：监控级

【参数】

all：清除 IPv4 防火墙的所有接口的过滤报文统计信息。

interface *interface-type interface-number*：表示清除 IPv4 防火墙的指定接口的过滤报文统计信息。其中，*interface-type interface-number* 表示接口类型和接口编号。

【描述】

reset firewall-statistics 命令用来清除 IPv4 防火墙的过滤报文统计信息。

【举例】

清除接口 GigabitEthernet3/0/1 上 IPv4 防火墙的过滤报文统计信息。

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

1.2 ASPF配置命令

1.2.1 aspf-policy

【命令】

aspf-policy *aspf-policy-number*

undo aspf-policy *aspf-policy-number*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

aspf-policy-number：ASPF 策略号，取值范围为 1～99。

【描述】

aspf-policy 命令用来创建 ASPF 策略，并进入 ASPF 策略视图。**undo aspf-policy** 命令用来删除 ASPF 策略。

对于一个已定义的 ASPF 策略，可通过策略号对该策略进行应用。

【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]
```

1.2.2 display aspf all

【命令】

display aspf all [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

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

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

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

【描述】

display aspf all 命令用来查看所有的 ASPF 策略信息。

【举例】

查看所有的 ASPF 策略信息。

```
<Sysname> display aspf all
[ASPF Policy Configuration]
  Policy Number 1:
    icmp-error drop
    tcp syn-check
  Policy Number 2:
    undo icmp-error drop
    undo tcp syn-check

[Interface Configuration]
   Interface                     InboundPolicy   OutboundPolicy
 ----------------------------------------------------------------
   GigabitEthernet3/0/1          1               2
```

表1-2 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
Policy Number	ASPF策略号
icmp-error drop	丢弃ICMP差错报文

字段	描述
tcp syn-check	丢弃非SYN的TCP首报文
undo icmp-error drop	不丢弃ICMP差错报文
undo tcp syn-check	不丢弃非SYN的TCP首报文
[Interface Configuration]	接口下应用ASPF策略的配置信息
Interface	应用ASPF策略的接口
InboundPolicy	入方向的ASPF策略
OutboundPolicy	出方向的ASPF策略

1.2.3 display aspf interface

【命令】

display aspf interface [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

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

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

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

【描述】

display aspf interface 命令用来查看接口上的 ASPF 策略信息。

【举例】

查看接口上的 ASPF 策略信息。

```
<Sysname> display aspf interface
[Interface Configuration]
   Interface                      InboundPolicy   OutboundPolicy
 ----------------------------------------------------------------
   GigabitEthernet3/0/1                    1               0
```

表1-3 display aspf interface 命令显示信息描述表

字段	描述
InboundPolicy	入方向的ASPF策略

字段	描述
OutboundPolicy	出方向的ASPF策略

1.2.4 display aspf policy

【命令】

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

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

aspf-policy-number：ASPF 策略号，取值范围为 1～99。

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

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

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

【描述】

display aspf policy 命令用来查看指定 ASPF 策略的信息。

【举例】

查看策略号为 1 的 ASPF 策略的信息。

```
<Sysname> display aspf policy 1
[ASPF Policy Configuration]
  Policy Number 1:
    icmp-error drop
    tcp syn-check
```

表1-4 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 drop	丢弃ICMP差错报文
tcp syn-check	丢弃非SYN的TCP首报文

1.2.5 display port-mapping

【命令】

display port-mapping [*application-name* | **port** *port-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

application-name：指定用于端口映射的应用的名称，其取值及含义如下：

- **ftp**：表示 FTP 协议；
- **h323**：表示 H323 协议；
- **http**：表示 HTTP 协议；
- **https**：表示 HTTPS 协议；
- **ike**：表示 IKE 协议；
- **rtsp**：表示 RTSP 协议；
- **smtp**：表示 SMTP 协议；
- **ssh:** 表示 SSH 协议；
- **vam:** 表示 VAM 协议；

port *port-number*：指定应用协议映射的端口。其中，*port-number* 表示映射端口号，取值范围为 0～65535。

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

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

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

【描述】

display port-mapping 命令用来查看端口映射信息。

相关配置可参考命令 **port-mapping**。

【举例】

查看端口映射的所有信息。

```
<Sysname> display port-mapping
  SERVICE    PORT       ACL        TYPE
 -------------------------------------------------
  ftp          21                   system defined
  h323       1720                   system defined
  http         80                   system defined
```

```
rtsp         554                 system defined
smtp          25                 system defined
ike           500                system defined
https         443                system defined
vam         18000                system defined
ssh           22                 system defined
```

表1-5 display port-mapping 命令显示信息描述表

字段	描述
SERVICE	进行端口映射的应用层协议
PORT	应用层协议映射的端口号
ACL	指定主机范围的ACL号
TYPE	端口映射类型，包括系统预定义和用户自定义两种类型

1.2.6 firewall aspf

【命令】

firewall aspf *aspf-policy-number* { **inbound** | **outbound** }

undo firewall aspf *aspf-policy-number* { **inbound** | **outbound** }

【视图】

接口视图

【缺省级别】

2：系统级

【参数】

aspf-policy-number：ASPF 策略号，取值范围为 1～99。

inbound：对接口入方向的报文应用 ASPF 策略。

outbound：对接口出方向的报文应用 ASPF 策略。

【描述】

firewall aspf 命令用来在接口上应用 ASPF 策略。**undo firewall aspf** 命令用来删除接口上的 ASPF 策略。

缺省情况下，接口上没有应用 ASPF 策略。

【举例】

在接口 GigabitEthernet3/0/1 的出方向上配置 ASPF 策略。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] firewall aspf 1 outbound
```

1.2.7 icmp-error drop

【命令】

icmp-error drop

undo icmp-error drop

【视图】

ASPF 策略视图

【缺省级别】

2：系统级

【参数】

无

【描述】

icmp-error drop 命令用来配置 ICMP 差错报文丢弃功能。**undo icmp-error drop** 命令用来恢复缺省情况。

缺省情况下，不丢弃 ICMP 差错报文。

相关配置可参考命令 **aspf-policy**。

【举例】

设置 ASPF 策略 1 丢弃 ICMP 差错报文。

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

1.2.8 port-mapping

【命令】

port-mapping *application-name* **port** *port-number* [**acl** *acl-number*]

undo port-mapping [*application-name* **port** *port-number* [**acl** *acl-number*]]

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

application-name：端口映射的应用名称，其取值及含义如下：

- **ftp**：表示 FTP 协议；
- **h323**：表示 H323 协议；
- **http**：表示 HTTP 协议；
- **https**：表示 HTTPS 协议；
- **ike**：表示 IKE 协议；

- **rtsp**：表示 RTSP 协议；
- **smtp**：表示 SMTP 协议；
- **ssh:** 表示 SSH 协议；
- **vam:** 表示 VAM 协议；

port *port-number*：应用层协议的端口。其中 *port-number* 表示端口号，取值范围为 0～65535。

acl *acl-number*：用来指定主机范围的 IPv4 访问控制列表。其中，*acl-number* 表示基本访问控制列表号，取值范围为 2000～2999。

【描述】

port-mapping 命令用来配置端口到应用层协议的映射。**undo port-mapping** 命令用来删除端口映射项。

缺省情况下，没有端口到应用层协议的映射关系。

相关配置可参考命令 **display port-mapping**。

【举例】

建立端口 3456 到 FTP 协议的映射。

```
<Sysname> system-view
[Sysname] port-mapping ftp port 3456
```

1.2.9 tcp syn-check

【命令】

tcp syn-check

undo tcp syn-check

【视图】

ASPF 策略视图

【缺省级别】

2：系统级

【参数】

无

【描述】

tcp syn-check 命令用来配置非 SYN 的 TCP 首报文丢弃功能。**undo tcp syn-check** 命令用来恢复缺省情况。

缺省情况下，不丢弃非 SYN 的 TCP 首报文。

相关配置可参考命令 **aspf-policy**。

【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
```