H3C SecPath 入侵防御系统

ACL 配置指导(V7)

新华三技术有限公司
http://www.h3c.com

资料版本：6W302-20201121
产品版本：

T5010/T5020	R8524
T5030/T5060/T5080/T5000-S/T5000-C	R8504
T1020/T1030/T1050/T1060/T1080	R8524
T1000-AK340/AK350	R8524
LSWM1IPSD0/LSQM1IPSDSC0/IM-IPSX-IV	R8522

前 言

本配置指导主要介绍 ACL 和时间段相关的特性。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

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

2. 图形界面格式约定

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

3. 各类标志

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

警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
说明	对操作内容的描述进行必要的补充和说明。
窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 ACL

1.1 ACL简介

ACL（Access Control List，访问控制列表）是一系列用于识别报文流的规则的集合。这里的规则是指描述报文匹配条件的判断语句，匹配条件可以是报文的源地址、目的地址、端口号等。设备依据 ACL 规则识别出特定的报文，并根据预先设定的策略对其进行处理，最常见的应用就是使用 ACL 进行报文过滤。此外，ACL 还可应用于诸如路由、安全等业务中识别报文，对这些报文的具体处理方式由应用 ACL 的业务模块来决定。

1.1.1 ACL 的编号和名称

用户在创建 ACL 时必须为其指定编号或名称，不同的编号对应不同类型的 ACL，如表 1-1 所示；当 ACL 创建完成后，用户就可以通过指定编号或名称的方式来应用和编辑该 ACL。

对于编号相同的基本 ACL 或高级 ACL，必须通过 **ipv6** 关键字进行区分。对于名称相同的 ACL，必须通过 **ipv6** 和 **mac** 关键字进行区分。

1.1.2 ACL 的分类

根据规则制订依据的不同，可以将 ACL 分为如表 1-1 所示的几种类型。

表1-1 ACL 的分类

ACL 类型	编号范围	适用的 IP 版本	规则制订依据
基本ACL	2000～2999	IPv4	报文的源IPv4地址
		IPv6	报文的源IPv6地址
高级ACL	3000～3999	IPv4	报文的源IPv4地址、目的IPv4地址、报文优先级、IPv4承载的协议类型及特性等三、四层信息
		IPv6	报文的源IPv6地址、目的IPv6地址、报文优先级、IPv6承载的协议类型及特性等三、四层信息
二层ACL	4000～4999	IPv4和IPv6	报文的源MAC地址、目的MAC地址、802.1p优先级、链路层协议类型等二层信息

1.1.3 ACL 的规则匹配顺序

当一个 ACL 中包含多条规则时，报文会按照一定的顺序与这些规则进行匹配，一旦匹配上某条规则便结束匹配过程。ACL 的规则匹配顺序有以下两种：

- 配置顺序：按照规则编号由小到大进行匹配。
- 自动排序：按照“深度优先”原则由深到浅进行匹配，各类型 ACL 的“深度优先”排序法则如表 1-2 所示。

表1-2 各类型 ACL 的“深度优先”排序法则

ACL 类型	“深度优先”排序法则
IPv4基本ACL	**1.** 先判断规则的匹配条件中是否包含 VPN 实例，包含者优先 **2.** 如果 VPN 实例的包含情况相同，再比较源 IPv4 地址范围，较小者优先 **3.** 如果源 IPv4 地址范围也相同，再比较配置的先后次序，先配置者优先
IPv4高级ACL	**4.** 先判断规则的匹配条件中是否包含 VPN 实例，包含者优先 **5.** 如果 VPN 实例的包含情况相同，再比较协议范围，指定有 IPv4 承载的协议类型者优先 **6.** 如果协议范围也相同，再比较源 IPv4 地址范围，较小者优先 **7.** 如果源 IPv4 地址范围也相同，再比较目的 IPv4 地址范围，较小者优先 **8.** 如果目的 IPv4 地址范围也相同，再比较四层端口（即 TCP/UDP 端口）号的覆盖范围，较小者优先 **9.** 如果四层端口号的覆盖范围无法比较，再比较配置的先后次序，先配置者优先
IPv6基本ACL	**10.** 先判断规则的匹配条件中是否包含 VPN 实例，包含者优先 **11.** 如果 VPN 实例的包含情况相同，再比较源 IPv6 地址范围，较小者优先 **12.** 如果源 IPv6 地址范围也相同，再比较配置的先后次序，先配置者优先
IPv6高级ACL	**13.** 先判断规则的匹配条件中是否包含 VPN 实例，包含者优先 **14.** 如果 VPN 实例的包含情况相同，再比较协议范围，指定有 IPv6 承载的协议类型者优先 **15.** 如果协议范围相同，再比较源 IPv6 地址范围，较小者优先 **16.** 如果源 IPv6 地址范围也相同，再比较目的 IPv6 地址范围，较小者优先 **17.** 如果目的 IPv6 地址范围也相同，再比较四层端口（即 TCP/UDP 端口）号的覆盖范围，较小者优先 **18.** 如果四层端口号的覆盖范围无法比较，再比较配置的先后次序，先配置者优先
二层ACL	**19.** 先比较源 MAC 地址范围，较小者优先 **20.** 如果源 MAC 地址范围相同，再比较目的 MAC 地址范围，较小者优先 **21.** 如果目的 MAC 地址范围也相同，再比较配置的先后次序，先配置者优先

说明

- 比较 IPv4 地址范围的大小，就是比较 IPv4 地址通配符掩码中“0”位的多少：“0”位越多，范围越小。通配符掩码（又称反向掩码）以点分十进制表示，并以二进制的“0”表示“匹配”，“1”表示“不关心”，这与子网掩码恰好相反，譬如子网掩码 255.255.255.0 对应的通配符掩码就是 0.0.0.255。此外，通配符掩码中的“0”或“1”可以是不连续的，这样可以更加灵活地进行匹配，譬如 0.255.0.255 就是一个合法的通配符掩码。
- 比较 IPv6 地址范围的大小，就是比较 IPv6 地址前缀的长短：前缀越长，范围越小。
- 比较 MAC 地址范围的大小，就是比较 MAC 地址掩码中“1”位的多少：“1”位越多，范围越小。

1.1.4 ACL 的步长

ACL 中的每条规则都有自己的编号，这个编号在该 ACL 中是唯一的。在创建规则时，可以手工为其指定一个编号，如未手工指定编号，则由系统为其自动分配一个编号。由于规则的编号可能影响规则匹配的顺序，因此当由系统自动分配编号时，为了方便后续在已有规则之前插入新的规则，系统通常会在相邻编号之间留下一定的空间，这个空间的大小（即相邻编号之间的差值）就称为 ACL 的步长。譬如，当步长为 5 时，系统会将编号 0、5、10、15……依次分配给新创建的规则。

系统为规则自动分配编号的方式如下：系统从规则编号的起始值开始，自动分配一个大于现有最大编号的步长最小倍数。譬如原有编号为 0、5、9、10 和 12 的五条规则，步长为 5，此时如果创建一条规则且不指定编号，那么系统将自动为其分配编号 15。

如果步长发生了改变，ACL 内原有全部规则的编号都将自动从规则编号的起始值开始按步长重新排列。譬如，某 ACL 内原有编号为 0、5、9、10 和 15 的五条规则，当修改步长为 2 之后，这些规则的编号将依次变为 0、2、4、6 和 8。

1.1.5 ACL 对分片报文的处理

传统报文过滤只对分片报文的首个分片进行匹配过滤，对后续分片一律放行，因此网络攻击者通常会构造后续分片进行流量攻击。为提高网络安全性，ACL 规则缺省会匹配所有非分片报文和分片报文的全部分片，但这样又带来效率低下的问题。为了兼顾网络安全和匹配效率，可将过滤规则配置为仅对后续分片有效。

1.2 ACL配置限制和指导

通过编号创建的 ACL，只能通过 **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } *acl-number* 命令进入其视图。

通过名称创建的 ACL，只能通过 **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } **name** *acl-name* 命令进入其视图。

如果 ACL 规则的匹配项中包含了除 IP 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）、ICMP 报文的消息类型和消息码信息、VPN 实例、日志操作和时间段之外的其它匹配项，则设备转发 ACL 匹配的这类报文时会启用慢转发流程。慢转发时设备会将报文上送控制平面，计算报文相应的表项信息。执行慢转发流程时，设备的转发能力将会有所降低。

1.3 ACL配置任务简介

ACL 配置任务如下

- 配置不同类型的 ACL
  - 配置基本 ACL
  - 配置高级 ACL
  - 配置二层 ACL
- （可选）复制 ACL
- （可选）配置 ACL 规则的加速匹配功能
- （可选）应用 ACL 进行报文过滤

1.4 配置基本ACL

1.4.1 功能简介

基本 ACL 根据报文的源 IP 地址来制订规则，对报文进行匹配。

1.4.2 配置限制和指导

当 ACL 规则中配置了 **logging** 参数，且引用该 ACL 的模块支持并开启了日志记录功能时，logging 功能生成的日志信息不会输出到控制台和监视终端。此时如需获取该日志，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

1.4.3 配置 IPv4 基本 ACL

(1) 进入系统视图。

system-view

(2) 创建 IPv4 基本 ACL。

acl basic { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

(3) （可选）配置 ACL 的描述信息。

description *text*

缺省情况下，未配置 ACL 的描述信息。

(4) （可选）配置规则编号的步长。

step *step-value*

缺省情况下，规则编号的步长为 5，起始值为 0。

(5) 创建规则。

rule [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **source** { **object-group** *address-group-name* | *source-address source-wildcard* | **any** } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

logging 参数是否生效取决于引用该 ACL 的模块是否支持日志记录功能，例如报文过滤支持日志记录功能，如果其引用的 ACL 规则中配置了 **logging** 参数，该参数可以生效。

(6) （可选）为规则配置描述信息。

rule *rule-id* **comment** *text*

缺省情况下，未配置规则的描述信息。

1.4.4 配置 IPv6 基本 ACL

(1) 进入系统视图。

system-view

(2) 创建 IPv6 基本 ACL。

acl ipv6 basic { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

(3) （可选）配置 ACL 的描述信息。

description *text*

缺省情况下，未配置 ACL 的描述信息。

(4) （可选）配置规则编号的步长。

step *step-value*

缺省情况下，规则编号的步长为 5，起始值为 0。

(5) 创建规则。

rule [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **routing** [**type** *routing-type*] | **source** { **object-group** *address-group-name* | *source-address source-prefix* | *source-address*/*source-prefix* | **any** } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

logging 参数是否生效取决于引用该 ACL 的模块是否支持日志记录功能，例如报文过滤支持日志记录功能，如果其引用的 ACL 规则中配置了 **logging** 参数，该参数可以生效。

(6) （可选）为规则配置描述信息。

rule *rule-id* **comment** *text*

缺省情况下，未配置规则的描述信息。

1.5 配置高级ACL

1.5.1 功能简介

高级 ACL 可根据报文的源地址、目的地址、报文优先级、承载的协议类型及特性（如 TCP/UDP 的源端口和目的端口、TCP 报文标识、ICMP 或 ICMPv6 协议的消息类型和消息码等），对报文进行匹配。用户可利用高级 ACL 制订比基本 ACL 更准确、丰富、灵活的规则。

1.5.2 配置限制和指导

当 ACL 规则中配置了 **logging** 参数，且引用该 ACL 的模块支持并开启了日志记录功能时，logging 功能生成的日志信息不会输出到控制台和监视终端。此时如需获取该日志，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

1.5.3 配置 IPv4 高级 ACL

(1) 进入系统视图。

system-view

(2) 创建 IPv4 高级 ACL。

acl advanced { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

(3) （可选）配置 ACL 的描述信息。

description *text*

缺省情况下，未配置 ACL 的描述信息。

(4) （可选）配置规则编号的步长。

step *step-value*

缺省情况下，规则编号的步长为 5，起始值为 0。

(5) 创建规则。

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { **object-group** *address-group-name* | *dest-address dest-wildcard* | **any** } | **destination-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **logging** | **source** { **object-group** *address-group-name* | *source-address source-wildcard* | **any** } | **source-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

logging 参数是否生效取决于引用该 ACL 的模块是否支持日志记录功能，例如报文过滤支持日志记录功能，如果其引用的 ACL 规则中配置了 **logging** 参数，该参数可以生效。

(6) （可选）为规则配置描述信息。

rule *rule-id* **comment** *text*

缺省情况下，未配置规则的描述信息。

1.5.4 配置 IPv6 高级 ACL

(1) 进入系统视图。

system-view

(2) 创建 IPv6 高级 ACL。

acl ipv6 advanced { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

(3) （可选）配置 ACL 的描述信息。

description *text*

缺省情况下，未配置 ACL 的描述信息。

(4) （可选）配置规则编号的步长。

step *step-value*

缺省情况下，规则编号的步长为 5，起始值为 0。

(5) 创建规则。

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { **object-group** *address-group-name* | *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** } | **destination-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | **dscp** *dscp* | **flow-label**

flow-label-value | **fragment** | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **logging** | **routing** [**type** *routing-type*] | **hop-by-hop** [**type** *hop-type*] | **source** { **object-group** *address-group-name* | *source-address source-prefix* | *source-address/source-prefix* | **any** } | **source-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

logging 参数是否生效取决于引用该 ACL 的模块是否支持日志记录功能，例如报文过滤支持日志记录功能，如果其引用的 ACL 规则中配置了 **logging** 参数，该参数可以生效。

(6) （可选）为规则配置描述信息。

rule *rule-id* **comment** *text*

缺省情况下，未配置规则的描述信息。

1.6 配置二层ACL

1. 功能简介

二层 ACL 可根据报文的源 MAC 地址、目的 MAC 地址、802.1p 优先级、链路层协议类型、报文的封装类型等二层信息来制订规则，对报文进行匹配。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建二层 ACL。

acl mac { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

(3) （可选）配置 ACL 的描述信息。

description *text*

缺省情况下，未配置 ACL 的描述信息。

(4) （可选）配置规则编号的步长。

step *step-value*

缺省情况下，规则编号的步长为 5，起始值为 0。

(5) 创建规则。

rule [*rule-id*] { **deny** | **permit** } [**cos** *dot1p* | **counting** | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *

(6) （可选）为规则配置描述信息。

rule *rule-id* **comment** *text*

缺省情况下，未配置规则的描述信息。

1.7 复制ACL

1. 功能简介

用户可通过复制一个已存在的 ACL（即源 ACL），来生成一个新的同类型 ACL（即目的 ACL）。除了 ACL 的编号和名称不同外，目的 ACL 与源 ACL 完全相同。

2. 配置限制和指导

目的 ACL 要与源 ACL 的类型相同，且目的 ACL 必须不存在，否则将导致复制 ACL 失败。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 复制并生成一个新的 ACL。

acl [**ipv6** | **mac**] **copy** { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }

1.8 配置ACL规则的加速匹配功能

1. 功能简介

在对基于会话的业务报文（如 NAT、ASPF 等）进行规则匹配时，通常只对首个报文进行匹配以加快报文的处理速度，但这有时并不足以解决报文匹配的效率问题。譬如，当有大量用户同时与设备新建连接时，需要对每个新建连接都进行规则匹配，如果 ACL 内包含有大量规则，那么这个匹配过程将很长，这会导致用户建立连接时间超长，从而影响设备新建连接的性能。

ACL 规则的加速匹配功能则可以解决上述问题，当对包含大量规则的 ACL 开启了加速匹配功能之后，其规则匹配速度将大大提高，从而提升设备的转发性能以及新建连接的性能。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 ACL，并进入 ACL 视图。

acl { [**ipv6**] { **advanced** | **basic** } { *acl-number* | **name** *acl-name* } | **mac** { *acl-number* | **name** *acl-name* } } [**match-order** { **auto** | **config** }]

(3) 配置 ACL 规则的加速匹配功能。

accelerate

缺省情况下，ACL 规则的加速匹配功能处于关闭状态。

1.9 应用ACL进行报文过滤

1.9.1 功能简介

ACL 最基本的应用就是进行报文过滤。

1.9.2 在安全域间实例上应用 ACL 进行报文过滤

1. 配置限制和指导

一个安全域间实例上最多可应用 32 个 ACL 进行报文过滤。有关安全域间实例的详细介绍和配置，请参见“基础配置指导”中的“安全域”。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入安全域间实例视图。

zone-pair security source *source-zone-name* **destination** *destination-zone-name*

(3) 在安全域间实例上应用 ACL 进行报文过滤。

packet-filter [**ipv6**] { *acl-number* | **name** *acl-name* }

缺省情况下，安全域间实例不对报文进行过滤。

1.9.3 配置报文过滤日志信息或告警信息的生成与发送周期

1. 功能简介

报文过滤日志或告警信息的生成与发送周期起始于报文过滤中 ACL 匹配数据流的第一个数据包，报文过滤日志或告警信息包括周期内被匹配的报文数量以及所使用的 ACL 规则。在一个周期内：

- 对于规则匹配数据流的第一个数据包，设备会立即生成报文过滤日志或告警信息；
- 对于规则匹配数据流的其他数据包，设备将在周期结束后生成报文过滤日志或告警信息。

设备生成的报文过滤日志将发送给信息中心，有关信息中心的详细介绍，请参见“网络管理和监控配置指导”中的“信息中心”。

设备生成的告警信息将发送给 SNMP，有关 SNMP 的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置报文过滤日志信息或告警信息的生成与发送周期。

acl { **logging** | **trap** } **interval** *interval*

缺省情况下，报文过滤日志信息或告警信息的生成与发送周期为 0 分钟，即不记录报文过滤的日志和告警信息。

1.10 ACL显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示 ACL 配置后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 ACL 的统计信息。

表1-3 ACL 显示和维护

配置	命令
显示ACL的配置和运行情况	**display acl** [**ipv6** | **mac**] { *acl-number* | **all** | **name** *acl-name* }
显示ACL的加速状态	**display acl accelerate** { **summary** [**ipv6** | **mac**] | **verbose** [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } **slot** *slot-number* }
显示ACL在报文过滤中的应用情况	**display packet-filter zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*] [**slot** *slot-number*]
显示ACL在报文过滤中应用的统计信息	**display packet-filter statistics zone-pair security source** *source-zone-name* **destination** *destination-zone-name* [[**ipv6**] { *acl-number* | **name** *acl-name* }] [**brief**]
显示ACL在报文过滤中的详细应用情况	**display packet-filter verbose zone-pair security source** *source-zone-name* **destination** *destination-zone-name* [[**ipv6**] { *acl-number* | **name** *acl-name* }] [**slot** *slot-number*]
清除ACL的统计信息	**reset acl** [**ipv6** | **mac**] **counter** { *acl-number* | **all** | **name** *acl-name* }
清除ACL在报文过滤中应用的统计信息	**reset packet-filter statistics zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*] [**ipv6**] { *acl-number* | **name** *acl-name* }

1.11 ACL典型配置举例

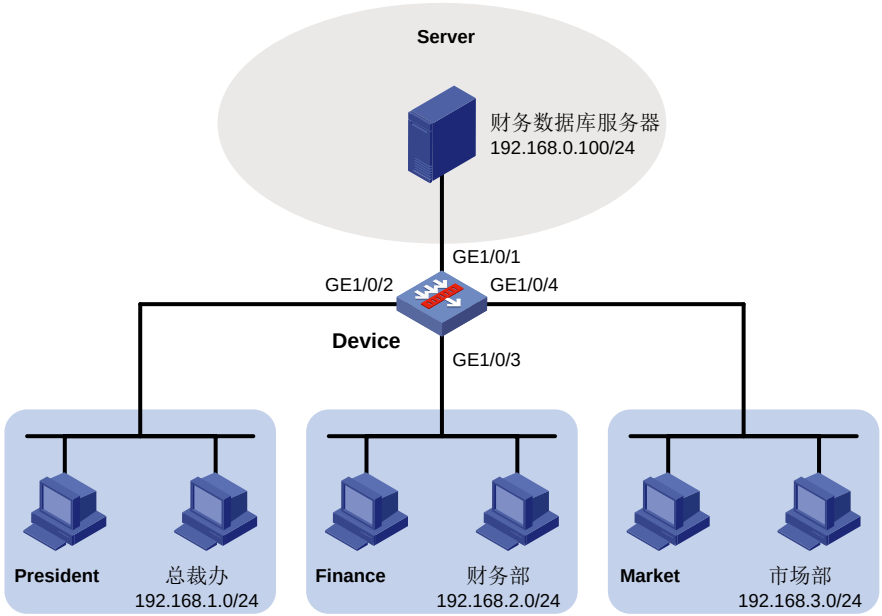
1.11.1 在安全域间实例上应用包过滤的 ACL 配置举例

1. 组网需求

- 某公司内的各部门之间通过 Device 实现互连，总裁办、财务部和市场部分别属于 President 域、Finance 域和 Market 域。该公司的工作时间为每周工作日的 8 点到 18 点。
- 通过在安全域间实例上配置包过滤，允许总裁办在任意时间、财务部在工作时间访问财务数据库服务器，禁止其它部门在任何时间、财务部在非工作时间访问该服务器。

2. 组网图

图1-1 在安全域间实例上应用包过滤的 ACL 配置组网图



3. 配置步骤

(1) 配置接口 IP 地址、路由保证路由可达，具体配置步骤略

(2) 创建安全域并将接口加入安全域

将接口 GigabitEthernet1/0/1 加入 Server 域。

```
<Device> system-view
[Device] security-zone name Server
[Device-security-zone-Server] import interface gigabitethernet 1/0/1
[Device-security-zone-Server] quit
```

将接口 GigabitEthernet1/0/2 加入 President 域。

```
[Device] security-zone name President
[Device-security-zone-President] import interface gigabitethernet 1/0/2
[Device-security-zone-President] quit
```

将接口 GigabitEthernet1/0/3 加入 Finance 域。

```
[Device] security-zone name Finance
[Device-security-zone-Finance] import interface gigabitethernet 1/0/3
[Device-security-zone-Finance] quit
```

将接口 GigabitEthernet1/0/4 加入 Market 域。

```
[Device] security-zone name Market
[Device-security-zone-Market] import interface gigabitethernet 1/0/4
[Device-security-zone-Market] quit
```

(3) 配置时间段

创建名为 work 的时间段，其时间范围为每周工作日的 8 点到 18 点。

```
[Device] time-range work 08:00 to 18:00 working-day
```

(4) 创建 ACL

创建 IPv4 高级 ACL 3000，允许总裁办在任意时间访问财务数据库服务器。

```
[Device] acl advanced 3000
[Device-acl-ipv4-adv-3000] rule permit ip source 192.168.1.0 0.0.0.255 destination
192.168.0.100 0
[Device-acl-ipv4-adv-3000] quit
```

创建 IPv4 高级 ACL 3001，允许财务部在工作时间访问财务数据库服务器。

```
[Device] acl advanced 3001
[Device-acl-ipv4-adv-3001] rule permit ip source 192.168.2.0 0.0.0.255 destination
192.168.0.100 0 time-range work
[Device-acl-ipv4-adv-3001] quit
```

创建 IPv4 高级 ACL 3002，禁止其它部门在任何时间访问财务数据库服务器。

```
[Device] acl advanced 3002
[Device-acl-ipv4-adv-3002] rule deny ip source any destination 192.168.0.100 0
[Device-acl-ipv4-adv-3002] quit
```

(5) 在安全域间实例应用包过滤策略

创建安全域间实例（源安全域为 President、目的安全域为 Server），并在该安全域间实例上引用 ACL 3000 进行包过滤。

```
[Device] zone-pair security source president destination server
[Device-zone-pair-security-President-Server] packet-filter 3000
[Device-zone-pair-security-President-Server] quit
```

创建安全域间实例（源安全域为 Finance、目的安全域为 Server），并在该安全域间实例上引用 ACL 3001 进行包过滤。

```
[Device] zone-pair security source finance destination server
[Device-zone-pair-security-Finance-Server] packet-filter 3001
[Device-zone-pair-security-President-Server] quit
```

创建安全域间实例（源安全域为 Market、目的安全域为 Server），并在该安全域间实例上引用 ACL 3002 进行包过滤。

```
[Device] zone-pair security source market destination server
[Device-zone-pair-security-Market-Server] packet-filter 3002
[Device-zone-pair-security-Market-Server] quit
```

4. 验证配置

配置完成后，在各部门的 PC（假设均为 Windows XP 操作系统）上可以使用 **ping** 命令检验配置效果，在 Device 上可以使用 **display acl** 命令查看 ACL 的配置和运行情况。例如在工作时间：

在财务部的 PC 上检查到财务数据库服务器是否可达。

```
C:\> ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Reply from 192.168.0.100: bytes=32 time=1ms TTL=255
Reply from 192.168.0.100: bytes=32 time<1ms TTL=255
Reply from 192.168.0.100: bytes=32 time<1ms TTL=255
Reply from 192.168.0.100: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

由此可见，财务部的 PC 能够在工作时间访问财务数据库服务器。

在市场部的 PC 上检查财务数据库服务器是否可达。

```
C:\> ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

由此可见，市场部的 PC 不能在工作时间访问财务数据库服务器。

查看 IPv4 高级 ACL 3001 和 ACL 3002 的配置和运行情况。

```
[Device] display acl 3001
Advanced IPv4 ACL 3001, 1 rule,
ACL's step is 5
 rule 0 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.0.100 0 time-range work
(4 times matched) (Active)
[Device] display acl 3002
Advanced IPv4 ACL 3002, 1 rule,
ACL's step is 5
 rule 0 deny ip destination 192.168.0.100 0 (4 times matched)
```

由此可见，由于目前是工作时间，因此 ACL 3001 的规则 0 是生效的；且由于之前使用了 **ping** 命令的缘故，ACL 3001 和 ACL 3002 的规则 0 分别被匹配了 4 次。

目 录

1 时间段

1.1 时间段简介

时间段（Time Range）定义了一个时间范围。用户通过创建一个时间段并在某业务中将其引用，就可使该业务在此时间段定义的时间范围内生效。

譬如，当一个 ACL 规则只需在某个特定时间范围内生效时，就可以先配置好这个时间段，然后在配置该 ACL 规则时引用此时间段，这样该 ACL 规则就只能在该时间段定义的时间范围内生效。

在一个时间段中，可以使用以下两种方式定义时间范围：

- 周期时间段：表示以一周为周期（如每周一的 8 至 12 点）循环生效的时间段。
- 绝对时间段：表示在指定时间范围内（如 2015 年 1 月 1 日 8 点至 2015 年 1 月 3 日 18 点）生效的时间段。

当一个时间段内包含有多个周期时间段和绝对时间段时，系统将先分别取各周期时间段的并集和各绝对时间段的并集，再取这两个并集的交集作为该时间段最终生效的时间范围。

1.2 时间段配置限制和指导

如果一个业务所引用的时间段尚未配置或已被删除，该业务将不会生效。

用户最多可创建 1024 个不同名称的时间段。一个时间段内最多可以包含 32 个周期时间段和 12 个绝对时间段。

1.3 配置时间段

(1) 进入系统视图。

system-view

(2) 创建时间段。

time-range *time-range-name* { *start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* }

如果指定的时间段已经创建，则本命令可以修改时间段的时间范围。

1.4 时间段显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示时间段配置后的运行情况，通过查看显示信息验证配置的效果。

表1-1 时间段显示和维护

配置	命令
显示时间段的配置和状态信息	**display time-range** { *time-range-name* | **all** }