10
OPTION

安全技术— ACL 配置

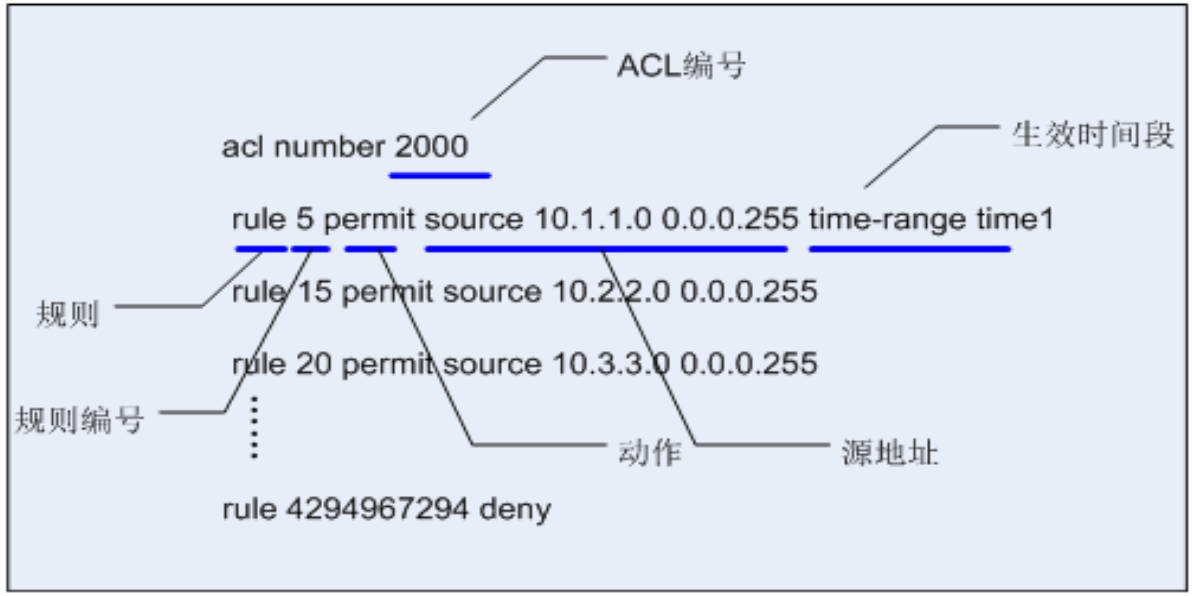
讲师：顾荣
Tel：13826101853(微信同号)
Mail： mygurong@126.com

2020.05

ACL 的基本原理

- ACL 由一系列规则组成，通过将报文与 ACL 规则进行匹配，设备可以过滤出特定的报文。设备支持的 ACL，有软件和硬件两种实现方式，两者在过滤的报文类型、报文过滤方式和对不匹配 ACL 的报文的处理动作这三个方面有所差异。

• ACL 的组成



- **ACL 编号**：用于标识 ACL ，表明该 ACL 是数字型 ACL 。
- **规则**：即描述报文匹配条件的判断语句。
  - **规则编号**：用于标识 ACL 规则。可以自行配置规则编号，也可以由系统自动分配。
  - ACL 规则的编号范围是 0 ～ 4294967294 ，所有规则均按照规则编号从小到大进行排序。所以，图中的 rule 5 排在首位，而规则编号最大的 rule 4294967294 排在末位。系统按照规则编号从小到大的顺序，将规则依次与报文匹配，一旦匹配上一条规则即停止匹配。
  - **动作**：包括 permit/deny 两种动作，表示允许 / 拒绝。
  - **匹配项**： ACL 定义了极其丰富的匹配项。

命名型 ACL 实际上是“名字 + 数字”的形式，可以在定义命名型 ACL 时同时指定 ACL 编号。如果不指定编号，则由系统自动分配。

acl name DENY-TELNET-LOGIN 3001

ACL 的步长设定

- 步长的含义
- 步长，是指系统自动为 ACL 规则分配编号时，每个相邻规则编号之间的差值。
- 系统为 ACL 中首条未手工指定编号的规则分配编号时，使用步长值作为该规则的起始编号；为后续规则分配编号时，则使用大于当前 ACL 内最大规则编号且是步长整数倍的最小整数作为规则编号。例如 ACL 中包含规则 rule 5 和 rule 12， ACL （特指基本 ACL 、高级 ACL 、二层 ACL 、用户自定义 ACL 、用户 ACL ）的缺省步长为 5，大于 12 且是 5 的倍数的最小整数是 15，所以系统分配给新配置的规则的编号为 15

- Step x

分类	适用的IP版本	规则定义描述	编号范围
基本ACL	IPv4	仅使用报文的源**IP**地址、分片信息和生效时间段信息来定义规则。	2000～2999
高级ACL	IPv4	既可使用IPv4报文的源**IP**地址，也可使用目的**IP**地址、IP协议类型、ICMP类型、TCP源/目的端口、UDP源/目的端口号、生效时间段等来定义规则。	3000～3999
二层ACL	IPv4&IPv6	使用报文的以太网帧头信息来定义规则，如根据源MAC（Media Access Control）地址、目的MAC地址、二层协议类型等。	4000～4999
用户ACL	IPv4	既可使用IPv4报文的源**IP**地址，也可使用目的**IP**地址、IP协议类型、ICMP类型、TCP源端口/目的端口、UDP源端口/目的端口号等来定义规则。	6000～6031
基本ACL6	IPv6	可使用IPv6报文的源**IPv6**地址、分片信息和生效时间段来定义规则。	2000～2999
高级ACL6	IPv6	可以使用IPv6报文的源**IPv6**地址、目的**IPv6**地址、IPv6协议类型、ICMPv6类型、TCP源/目的端口、UDP源/目的端口号、生效时间段等来定义规则。	3000～3999

ACL 的匹配顺序

- 设备支持两种 ACL 匹配顺序：配置顺序（ config 模式）和自动排序（ auto 模式）。**缺省的 ACL 匹配顺序是 config 模式**
- 自动排序，是指系统使用“深度优先”的原则，将规则按照精确度从高到低进行排序，并按照精确度从高到低的顺序进行报文匹配。规则中定义的匹配项限制越严格，规则的精确度就越高，即优先级越高，系统越先匹配

在 **auto** 模式的高级 ACL 3001 中，先后配置以下两条规则：

rule deny ip destination 10.1.0.0 0.0.255.255
// 表示拒绝目的 IP 地址为 10.1.0.0/16 网段地址的报文通过
rule permit ip destination 10.1.1.0 0.0.0.255
// 表示允许目的 IP 地址为 10.1.1.0/24 网段地址的报文通过，该网段地址范围小于 10.1.0.0/16 网段范围

根据”深度优先”匹配原则，接下来需要进一步比较规则的目的 IP 地址范围。由于 permit 规则指定的目的地址范围小于 deny 规则，所以 permit 规则的精确度更高，系统为其分配的规则编号更小。

配置完上述两条规则后， ACL 3001 的规则排序如下：

acl number 3001 **match-order auto**

rule 5 permit ip destination 10.1.1.0 0.0.0.255

rule 10 deny ip destination 10.1.0.0 0.0.255.255

ACL类型	匹配原则
基本ACL&ACL6	1. 先看规则中是否带VPN实例，带VPN实例的规则优先。 2. 再比较源IP地址范围，源IP地址范围小（IP地址通配符掩码中“0”位的数量多）的规则优先。 3. 如果源IP地址范围相同，则规则编号小的优先。
高级ACL&ACL6	1. 先看规则中是否带VPN实例，带VPN实例的规则优先。 2. 再比较协议范围，指定了IP协议承载的协议类型的规则优先。 3. 如果协议范围相同，则比较源IP地址范围，源IP地址范围小（IP地址通配符掩码中“0”位的数量多）的规则优先。 4. 如果协议范围、源IP地址范围相同，则比较目的IP地址范围，目的IP地址范围小（IP地址通配符掩码中“0”位的数量多）的规则优先。 5. 如果协议范围、源IP地址范围、目的IP地址范围相同，则比较四层端口号（TCP/UDP端口号）范围，四层端口号范围小的规则优先。 6. 如果上述范围都相同，则规则编号小的优先。

ACL 的常用匹配项

- **生效时间段**
- 格式： **time-range** *time-name*

- **IP 承载的协议类型**
- 格式： *protocol-number* | **icmp** | **tcp** | **udp** | **gre** | **igmp** | **ip** | **ipinip** | **ospf**

- **源 / 目的 IP 地址及其通配符掩码**
- 源 IP 地址及其通配符掩码格式： **source** { *source-address source-wildcard* | **any** }
- 目的 IP 地址及其通配符掩码格式： **destination** { *destination-address destination-wildcard* | **any** }
- IP 地址通配符掩码与 IP 地址的反向子网掩码类似，也是一个 32 比特位的数字字符串，用于指示 IP 地址中的哪些位将被检查。各比特位中，“0”表示“检查相应的位”，“1”表示“不检查相应的位”，概括为一句话就是“检查 0，忽略 1”。但与 IP 地址子网掩码不同的是，**子网掩码中的“0”和“1”要求必须连续，而通配符掩码中的“0”和“1”可以不连续。**
- 通配符掩码可以为 0，相当于 0.0.0.0，表示源 / 目的地址为主机地址；也可以为 255.255.255.255，表示任意 IP 地址，相当于指定 **any** 参数。
- 10.1.2.0　　0.0.254.255 （通配符掩码中的 1 和 0 不连续）
- 10.1.0.0/24 ～ 10.1.254.0/24 网段之间且第三个字节为偶数的 IP 地址，如 10.1.0.0/24 、 10.1.2.0/24 、 10.1.4.0/24 、 10.1.6.0/24 等。

- **TCP/UDP 端口号**
- 源端口号格式： **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }
- 目的端口号格式： **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }
- 在高级 ACL 中，当协议类型指定为 TCP 或 UDP 时，设备支持基于 TCP/UDP 的源 / 目的端口号过滤报文。
- 其中， TCP/UDP 端口号的比较符含义如下：
- **eq** *port* ：指定等于源 / 目的端口。
- **gt** *port* ：指定大于源 / 目的端口。
- **lt** *port* ：指定小于源 / 目的端口。
- **range** *port-start port-end* ：指定源 / 目的端口的范围。 *port-start* 是端口范围的起始， *port-end* 是端口范围的结束。

- **TCP 标志信息**
- 格式： **tcp-flag { ack | established | fin | psh | rst | syn | urg }***
- 在高级 ACL 中，当协议类型指定为 TCP 时，设备支持基于 TCP 标志信息过滤报文。

端口号	字符串	协议	说明
7	echo	Echo	Echo服务
9	discard		
13	daytime		
19	CHARgen		
20	ftp-data		
21	ftp		
23	telnet		
25	smtp		

端口号	字符串	协议	说明
7	echo	Echo	Echo服务
9	discard	Discard	用于连接测试的空服务
37	time	Time	时间协议
42	nameserver	Host Name Server	主机名服务
53	dns	Domain Name Service (DNS)	域名服务
65	tacacs-ds	TACACS-Database Service	TACACS数据库服务
67	bootps	Bootstrap Protocol Server	引导程序协议（BOOTP）服务端，DHCP服务使用
68	bootpc	Bootstrap Protocol Client	引导程序协议（BOOTP）客户端，DHCP客户使用
69	tftp	Trivial File Transfer Protocol (TFTP)	小文件传输协议

ACL 的生效时间段

- 第一种模式——周期时间段：以星期为参数来定义时间范围，表示规则以一周为周期（如每周一的 8 至 12 点）循环生效。
- 格式： **time-range** *time-name start-time* **to** *end-time* { *days* } &<1-7>*time-name* ： 时间段名称，以英文字母开头的字符串。
- *start-time* **to** *end-time* ： 开始时间和结束时间。格式为 [小时 : 分钟] to [小时 : 分钟] 。
- *days* ： 有多种表达方式。 **Mon** 、 **Tue** 、 **Wed** 、 **Thu** 、 **Fri** 、 **Sat** 、 **Sun** 中的一个或者几个的组合，也可以用数字表达， 0 表示星期日， 1 表示星期一，…… 6 表示星期六。
- **working-day** ： 从星期一到星期五，五天。
- **daily** ： 包括一周七天。
- **off-day** ： 包括星期六和星期日，两天。
- 第二种模式——绝对时间段：从某年某月某日的某一时间开始，到某年某月某日的某一时间结束，表示规则在这段时间范围内生效。
- 格式： **time-range** *time-name* **from** *time1 date1* [**to** *time2 date2*]*time-name* ： 时间段名称，以英文字母开头的字符串。
- *time1*/*time2* ： 格式为 [小时 : 分钟] 。
- *date1*/*date2* ： 格式为 [YYYY/MM/DD] ，表示年 / 月 / 日。

例如，在 ACL 2001 中引用了时间段“ test”， “ test” 包含了三个生效时间段：

```
time-range test 8:00 to 18:00 working-day
 time-range test 14:00 to 18:00 off-day
time-range test from 00:00 2014/01/01 to 23:59 2014/12/31
 acl number 2001
rule 5 permit time-range test
```

•第一个时间段，表示在周一到周五每天 8:00 到 18:00 生效，这是一个周期时间段。
•第二个时间段，表示在周六、周日下午 14:00 到 18:00 生效，这是一个周期时间段。
•第三个时间段，表示从 2014 年 1 月 1 日 00:00 起到 2014 年 12 月 31 日 23:59 生效，这是一个绝对时间段。
时间段“ test” 最终描述的时间范围为： 2014 年的周一到周五每天 8:00 到 18:00 以及周六和周日下午 14:00 到 18:00 。

使用基本 ACL 限制 Telnet 登录权限示例

配置思路

采用如下的思路配置通过 Telnet 登录设备：

1. 配置 Telnet 方式登录设备，以实现远程维护网络设备。
2. 配置管理员的用户名和密码，并配置 AAA 认证策略，保证只有认证通过的用户才能登录设备。
3. 配置安全策略，保证只有符合安全策略的用户才能登录设备。

操作步骤

1. 使能服务器功能

```
telnet server enable
```

2. 配置 VTY 用户界面的相关参数

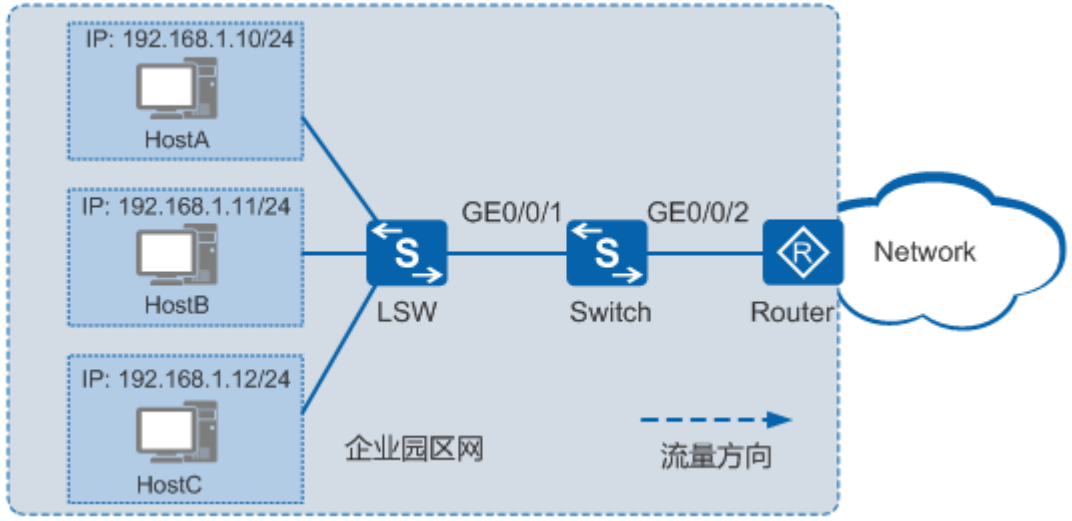
```
user-interface maximum-vty 15
# 配置允许用户登录设备的主机地址。
acl 2001
rule permit source 10.1.1.1 0
quit
user-interface vty 0 14
protocol inbound telnet
acl 2001 inbound
# 配置 VTY 用户界面的终端属性。
shell
idle-timeout 20
screen-length 0
history-command max-size 20
# 配置 VTY 用户界面的用户验证方式。
authentication-mode aaa
quit
```

3. 配置登录用户的相关信息

```
# 配置登录验证方式。
aaa
local-user admin1234 password irreversible-cipher Helloworld@6789
local-user admin1234 service-type telnet
local-user admin1234 privilege level 3
quit
```

4. 客户端登录

配置禁止指定主机访问网络示例



- 组网需求：
- 如图所示，企业用户通过 Switch 的接口 GE0/0/2 连接到外部网络设备。
- 每天 8:30 ～ 18:00 的时间段为工作时间，通过 GE0/0/1 接口对报文进行过滤，禁止访问外网。
- 配置思路

- 采用包含禁止动作的流策略方式实现报文过滤，具体配置思路如下： 1. 配置各接口，实现企业用户能通过 Switch 访问外部网络。
- 2. 配置时间范围，用于在 ACL 中引用。
- 3. 配置 ACL ，在工作时间段禁止报文通过。
- 4. 在接口的入方向配置报文过滤。

配置禁止指定主机访问网络示例

操作步骤
1. 创建 VLAN 并配置各接口

```
#  在 Switch 上创建 VLAN10 。
vlan 10
#  配置 Switch 上接口 GE0/0/1 和 GE0/0/2 为 Trunk 类型接口，并加入 VLAN10 。
interface gigabitethernet 0/0/1
port link-type trunk
port trunk allow-pass vlan 10
interface gigabitethernet 0/0/2
port link-type trunk
port trunk allow-pass vlan 10
#  创建 VLANIF10 ，并为 VLANIF10 配置 IP 地址 192.168.1.1/24 。
interface vlanif 10
ip address 192.168.1.1 24
```

请配置 Router 与 Switch 对接的接口 IP 地址为 192.168.1.2/24
2. 创建周期时间段 working_time ，时间范围为每天的 8:30 ～ 18:00 。

```
time-range working_time 08:30 to 18:00 working-day
```

3. 配置 ACL 3001 ，配置三条规则，分别为禁止源 IP 地址为 192.168.1.10 、 192.168.1.11 、 192.168.1.12 的报文在工作时间通过。

```
acl number 3001
rule deny ip source 192.168.1.10 0 time-range working_time
rule deny ip source 192.168.1.11 0 time-range working_time
rule deny ip source 192.168.1.12 0 time-range working_time
```

4. 在接口 GE0/0/1 的入方向配置报文过滤。

```
interface gigabitethernet 0/0/1
traffic-filter inbound acl 3001
```

5. 验证配置结果

```
#  看设备接口入方向上应用的 ACL 规则和流动作信息。
display traffic-applied interface gigabitethernet 0/0/1 inbound
```

单向访问控制

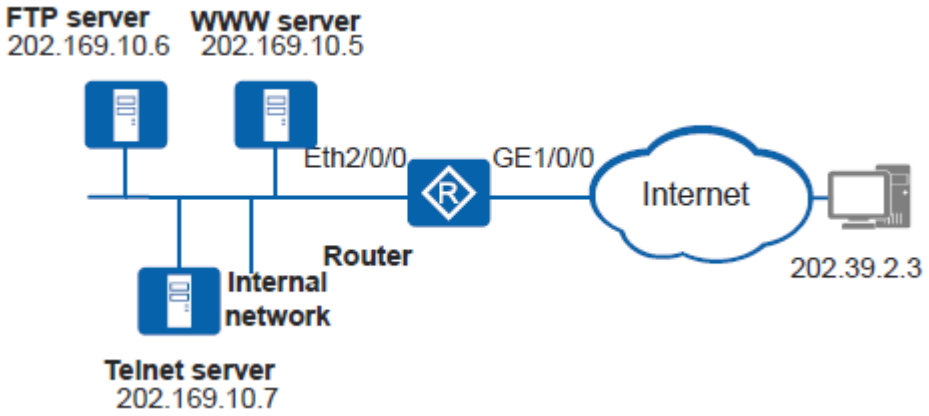
- 方式一：流策略
- a. 创建高级 ACL
- 在系统视图下，执行命令 **acl** [**number**] *acl-number* [**match-order** { **auto** |**config** }]，使用编号（3000 ～ 3999）创建高级 ACL 并进入高级 ACL 视图，或
- 者执行命令 **acl name** *acl-name* { **advance** | *acl-number* } [**match-order** { **auto** |**config** }]，使用名称创建高级 ACL 并进入高级 ACL 视图。
- b. 配置高级 ACL 规则
- 执行命令 **rule**，配置指定 **tcp-flag** 参数的高级 ACL 规则。假设，要求 192.168.1.0/24 网段用户可以主动访问 192.168.2.0/24 网段用户，但反过来 192.168.2.0/24 网段用户不能主动访问 192.168.1.0/24 。由 TCP 建立连接和关闭连接的过程可知，只有在 TCP 中间连接过程的报文才会 ACK=1 或者 RST=1 。根据这个特点，配置如下两种 ACL 规则，允许 TCP 中间连接过程的报文通过，拒绝该网段的其他 TCP 报文通过，就可以限制 192.168.2.0/24 网段主动发起的 TCP 连接。
  - 类型一：配置指定 **ack** 和 **rst** 参数的 ACL 规则
  - rule 5 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag ack // 允许 ACK=1 的 TCP 报文通过
  - rule 10 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag rst // 允许 RST=1 的 TCP 报文通过
  - rule 15 deny tcp source 192.168.2.0 0.0.0.255 // 拒绝该网段的其他 TCP 报文通过
  - 类型二：配置指定 **established** 参数的 ACL 规则
  - rule permit tcp source 192.168.2.0 0.0.0.255 tcp-flag established // established 表示 ACK=1 或者 RST=1，表示允许 TCP 中间连接过程的报文通过
  - rule deny tcp source 192.168.2.0 0.0.0.255 // 拒绝该网段的其他 TCP 报文通过
- c. 配置流分类
- i. 在系统视图下，执行命令 **traffic classifier** *classifier-name* [**operator** { **and** |**or** }]，进入流分类视图。
- ii. 执行命令 **if-match acl** { *acl-number* | *acl-name* }，配置基于 ACL 进行分类的匹配规则。
- d. 配置流行为
- 在系统视图下，执行命令 **traffic behavior** *behavior-name*，定义流行为并进入流行为视图。
- e. 配置流动作。
- 报文过滤有两种流动作： **deny** 或 **permit**
- f. 配置流策略
- i. 在系统视图下，执行命令 **traffic policy** *policy-name*，定义流策略并进入流策略视图。
- ii. 执行命令 **classifier** *classifier-name* **behavior** *behavior-name*，在流策略中为指定的流分类配置所需流行为，即绑定流分类和流行为。
- g. 应用流策略
- 在接口视图下，执行命令 **traffic-policy** *policy-name* { **inbound** | **outbound** }，应用流策略。

单向访问控制

- 方式二：简化流策略
- a. 配置高级 ACL 和 ACL 规则（同流策略方式）
- b. 应用简化流策略
- 在接口视图下，执行命令 **traffic-filter** { **inbound** | **outbound** } **acl xxx**，应用简化流策略（基于 ACL 的报文过滤）。

应用高级 ACL 配置防火墙示例

- 组网需求
- 如图 **5-19** 所示，某个对外提供 Web 、 FTP 和 Telnet 服务的企业通过 Router 的接口 GE1/0/0 访问外部网络，通过 Router 的接口 Eth2/0/0 加入 VLAN 。
- 已知企业的网段为 202.169.10.0/24 ，企业内部的 WWW 服务器、 FTP 服务器和 Telnet 服务器 IP 地址分别为 202.169.10.5/24 、 202.169.10.6/24 和 202.169.10.7/24 。
- 为了实现内部网络具备较高的安全性，企业希望在 Router 上配置防火墙功能，使外部网络只有特定用户可以访问内部服务器，企业内只有内部服务器可以访问外部网络。



应用高级 ACL 配置防火墙示例

- 配置思路
- 1. 为企业内部网络和外部网络配置不同的安全区域。
- 2. 配置安全域间，在安全域间使能防火墙功能。
- 3. 配置不同的高级 ACL ，对可以访问内部服务器的外部网络用户以及可以访问外部网络的内部服务器进行分类。
- 4. 在安全域间配置基于高级 ACL 的包过滤。

- 操作步骤
- 步骤 **1** 配置安全区域
- # 为企业内部网络配置安全区域。
- <Huawei> system-view
- [Huawei] sysname Router
- [Router] firewall zone company
- [Router-zone-company] priority 12
- [Router-zone-company] quit
- # 配置接口加入 VLAN ，并配置 VLANIF 接口的 IP 地址，将接口 VLANIF 100 加入安全区
- 域 company 。
- [Router] vlan batch 100
- [Router] interface ethernet 2/0/0
- [Router-Ethernet2/0/0] port link-type access
- [Router-Ethernet2/0/0] port default vlan 100
- [Router-Ethernet2/0/0] quit
- [Router] interface vlanif 100
- [Router-Vlanif100] ip address 202.169.10.1 255.255.255.0
- [Router-Vlanif100] zone company
- [Router-Vlanif100] quit

应用高级 ACL 配置防火墙示例

- # 为外部网络配置安全区域。
- [Router] firewall zone external
- [Router-zone-external] priority 5
- [Router-zone-external] quit
- # 将接口 GigabitEthernet1/0/0 加入安全区域 external 。
- [Router] interface gigabitethernet 1/0/0
- [Router-gigabitethernet1/0/0] ip address 129.39.10.8 255.255.255.0
- [Router-gigabitethernet1/0/0] zone external
- [Router-gigabitethernet1/0/0] quit
- 步骤 **2** 配置安全域间
- [Router] firewall interzone company external
- [Router-interzone-company-external] firewall enable
- [Router-interzone-company-external] quit
- 步骤 **3** 配置 ACL 3001
- # 创建 ACL 3001 。
- [Router] acl 3001
- # 配置允许特定用户从外部网络可以访问内部服务器。
- [Router-acl-adv-3001] rule permit tcp source 202.39.2.3 0.0.0.0 destination 202.169.10.5 0.0.0.0
- [Router-acl-adv-3001] rule permit tcp source 202.39.2.3 0.0.0.0 destination 202.169.10.6 0.0.0.0
- [Router-acl-adv-3001] rule permit tcp source 202.39.2.3 0.0.0.0 destination 202.169.10.7 0.0.0.0
- # 配置其他用户不能从外部网络访问企业内部的任何主机。
- [Router-acl-adv-3001] rule deny ip
- [Router-acl-adv-3001] quit

应用高级 ACL 配置防火墙示例

- 步骤 **4** 配置 ACL 3002
- # 创建 ACL 3002 。
- [Router] acl 3002
- # 配置允许内部服务器访问外部网络。
- [Router-acl-adv-3002] rule permit ip source 202.169.10.5 0.0.0.0
- [Router-acl-adv-3002] rule permit ip source 202.169.10.6 0.0.0.0
- [Router-acl-adv-3002] rule permit ip source 202.169.10.7 0.0.0.0
- # 配置网络内部的其他用户不能访问外部网络。
- [Router-acl-adv-3002] rule deny ip
- [Router-acl-adv-3002] quit
- 步骤 **5** 在安全域间配置基于高级 ACL 的包过滤
- [Router] firewall interzone company external
- [Router-interzone-company-external] packet-filter 3001 inbound
- [Router-interzone-company-external] packet-filter 3002 outbound
- [Router-interzone-company-external] quit
- 步骤 **6** 验证配置结果
- # 配置成功后，仅特定主机（ 202.39.2.3 ）可以访问内部服务器，仅内部服务器可以访
- 问外部网络。
- # 在 Router 上执行 **display firewall interzone** [*zone-name1 zone-name2*] 操作，结果如下。
- [Router] display firewall interzone company external
- interzone company external
- firewall enable
- packet-filter default deny inbound
- packet-filter default permit outbound
- packet-filter 3001 inbound
- packet-filter 3002 outbound

THANK YOU

吃透原理 - 认真实践

http://exp.lnc.edu.cn