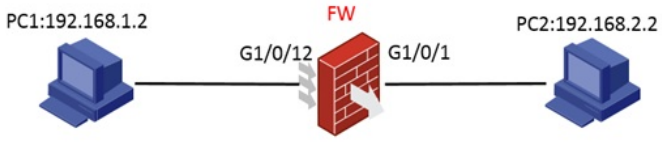
安全域中import ip和import interface匹配优先级

域间策略/安全域 **斑大人** 2018-11-04 发表

组网及说明

组网图如下：



问题描述

在安全域的配置当中，常用的是import interface，但是也可以import ip，若两者同时存在的情况下，优先应该根据哪种安全域来进行匹配，如果配置在同一安全域的情况下，与对象策略当中security-zone intra-zone default permit这条命令的匹配优先级又是怎样的?

过程分析

1. 首先将192.168.1.0/24与192.168.2.0/24网段放入同一个域ds，并放通策略；然后将报文出入接口加入到同一个安全域Untrust，放通域间策略。开通同域互通的命令（security-zone intra-zone default permit ）。配置如下：

```
#
 security-zone intra-zone default permit
#
object-group ip address PC1
 0 network subnet 192.168.1.0 255.255.255.0
#
object-group ip address PC2
 0 network subnet 192.168.2.0 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet1/0/12
 port link-mode route
 ip address 192.168.1.1 255.255.255.0
#
object-policy ip PC2-PC1
 rule 0 pass source-ip PC2 destination-ip PC1
 rule 100 pass logging counting
#
security-zone name ds
 import ip 192.168.1.0 24
 import ip 192.168.2.0 24
#
security-zone name untrust
 import interface GigabitEthernet1/0/1
#
security-zone name untrust
 import interface GigabitEthernet1/0/12
#
acl advanced 3010
 rule 0 permit icmp source 192.168.2.2 0 destination 192.168.1.2 0
 rule 5 permit icmp source 192.168.1.2 0 destination 192.168.2.2 0
#
zone-pair security source ds destination ds
 object-policy apply ip PC2-PC1
#
zone-pair security source Untrust destination Untrust
 object-policy apply ip PC2-PC1
```

#

实验结果如下： （debug object-policy）

[H3C]*Nov 2 07:59:21:960 2018 H3C FILTER/7/PACKET: -COntext=1; The packet is permitted. Src-ZOne=ds, Dst-ZOne=ds;If-In=GigabitEthernet1/0/1(2), If-Out=GigabitEthernet1/0/12(13); Packet Info: Src-IP=192.168.2.2, Dst-IP=192.168.1.2, VPN-Instance=,Src-Port=8, Dst-Port=0, Protocol=ICMP(1), Application=ICMP(22742), ObjectPolicy=PC2-PC1, Rule-ID=0.

可知优先匹配的是安全域中import ip的域间策略。

2. 删除安全域中import ip的相关配置之后，实验结论如下： （debug object-policy）

[H3C-security-zone-ds]undo import ip 192.168.1.0 24

[H3C-security-zone-ds]undo import ip 192.168.2.0 24

<H3C>*Nov 2 08:16:37:869 2018 H3C FILTER/7/PACKET: -COntext=1; The packet is permitted. Src-ZOne=untrust, Dst-ZOne=untrust;If-In=GigabitEthernet1/0/1(2), If-Out=GigabitEthernet1/0/12(13); Packet Info:Src-IP=192.168.2.2, Dst-IP=192.168.1.2, VPN-Instance=,Src-Port=8, Dst-Port=0, Protocol=ICMP(1), Application=ICMP(22742), ObjectPolicy=PC2-PC1, Rule-ID=0.

安全域中import ip的配置删除之后才会匹配安全域中import interface的域间策略。

3. 删除掉安全域中import interface的域间策略，实验结果如下：

实验结论是：删除掉该域间策略，可以ping通，但是debug域间策略无打印，说明匹配上的是 security-zone intra-zone default permit

[H3C]undo zone-pair security source untrust destination untrust

<H3C>debugging object-policy packet ip

This command is CPU intensive and might affect ongoing services. Are you sure you want to continue? [Y/N]:y

<H3C>terminal monitor

The current terminal is enabled to display logs.

<H3C>terminal debugging

The current terminal is enabled to display debugging logs.

C:\Users\ds>ping 192.168.1.2

正在 Ping 192.168.1.2 具有 32 字节的数据:

来自 192.168.1.2 的回复: 字节=32 时间<1ms TTL=128

来自 192.168.1.2 的回复: 字节=32 时间<1ms TTL=128

来自 192.168.1.2 的回复: 字节=32 时间<1ms TTL=128

来自 192.168.1.2 的回复: 字节=32 时间<1ms TTL=128

192.168.1.2 的 Ping 统计信息:

数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，

往返行程的估计时间(以毫秒为单位):

最短 = 0ms，最长 = 0ms，平均 = 0ms

解决方法

该案例说明：**安全域import ip策略（同域）高于安全域import interface（同域）高于security-zone intra-zone default permit**