NGFW安全策略与域间策略不生效排查方法

域间策略/安全域 张新姿 2020-12-14 发表

组网及说明

适用的产品系列

本案例适用于软件平台为Comware V7系列防火墙：如F1000-AK180、F1000-AK170等F1000-AK系列的防火墙。

注：本案例是在F100-C-G2的ersion 7.1.064, Release 9333P30版本上进行配置和验证的。

配置步骤

1.1 检查防火墙使用安全策略还是域间策略

Comware V7平台防火墙D022之前版本（不包括D022版本）只能支持域间策略，最新版本防火墙即D022版本之后支持安全策略与域间策略共存。

判断防火墙版本方法：

1、查询到此台防火墙软件版本为D032版本，为安全策略与域间策略共存：

<H3C>system-view

[H3C]probe

[H3C-probe]display system internal version

H3C SecPath F1070 V900R003B01D632SP20

Comware V700R001B64**D032**SP20

2、查询此防火墙软件版本为D012版本，只能使用域间策略：

[H3C-probe]display system internal version

H3C SecPath F1060 V900R003B01D612SP20

Comware V700R001B64**D012**SP20

同一台防火墙上安全策略与域间策略只能一种生效，缺省情况下防火墙域间策略生效，所以会出现在新版本防火墙中配置安全策略后发现策略不生效，并且在策略中也没有任何数据匹配的异常现象，原因就是设备默认是域间策略生效，所以如果防火墙配置安全策略则需要让防火墙安全策略生效，如果防火墙配置域间策略则需要关闭防火墙的安全策略。

如果能查到命令“security-policy disable”则域间策略生效：

[H3C]display current-configuration | include security-policy

 security-policy disable

没有查到任何命令则安全策略生效：

[H3C]display current-configuration | include security-policy

注：因为security-policy enable在命令行是不显示的，因此在输入上述命令无法查询到信息的就是安全策略生效。

另外在防火墙WEB网管界面配置时，旧版本（D022之前版本）防火墙在WEB界面配置完成后在命令行生成域间策略的配置、新版本（D022之后版本）防火墙在WEB界面配置完成后在命令行生成安全策略的配置，如果使用WEB界面配置安全策略后出现不生效情况很大可能是因为防火墙默认为域间策略生效。

举例：将防火墙从域间策略修改为安全策略：

<H3C>system-view

[H3C]undo security-policy disable

举例：将防火墙从安全策略修改为域间策略：

<H3C>system-view

[H3C]security-policy disable

1.2 检查防火墙策略是否开启

检查防火墙策略是否为开启状态，WEB界面策略开启方法：

如果在某条安全策略策略下出现“disable”字样则表示该策略已经被关闭需要打开策略后才能生效。

#

security-policy ip

 rule 0 name ipv4

disable

  action pass

  source-zone local

  source-zone trust

  source-zone untrust

  source-zone management

  destination-zone local

destination-zone trust
destination-zone untrust
destination-zone management

开启安全策略的命令：

<H3C>system-view
[H3C]security-policy ip
[H3C-security-policy-ip]rule 0
[H3C-security-policy-ip-0-ipv4]undo disable

域间策略开启策略方法：

在某条域间策略下出现“rule 1 pass disable”则表示这条规则已经被关闭，需要开启后才能生效；

#
object-policy ip ipv4
rule 1 pass disable
#

开启域间策略命令：

<H3C>system-view
[H3C]object-policy ip ipv4
[H3C-object-policy-ip-ipv4]rule 1 pass

注：因为域间策略开启或者关闭需要重写策略内容因此开关策略不建议在命令行执行。

1.3 检查策略匹配顺序

防火墙安全策略的匹配顺序是从上到下依次匹配，因此如果策略匹配条件相同时优先匹配最前的规则，因此会导致后续策略无法匹配。

举例：如图所示如果A策略匹配所有地址并放通，那么B策略就失去额意义。

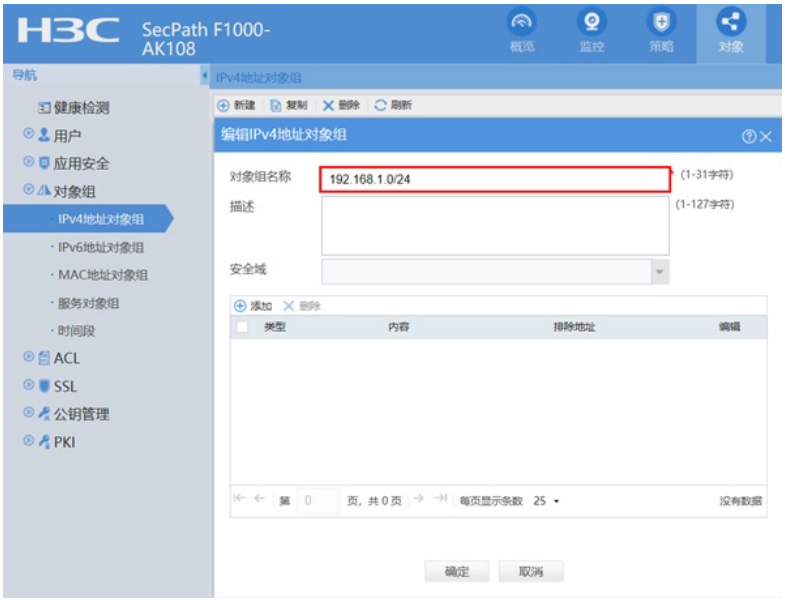
如意需要将策略顺序移动，要让B策略在A策略之前，那么就会先匹配B策略，匹配不到B策略后再匹配A策略。

正确的策略举例：

1.4 检查数据的源目地址是否与安全策略的匹配条件一致

如果上述内容排查均无问题则需要检查安全策略的匹配条件是否正确？比如匹配条件的掩码、IP、安全域是否选择正常。

错误案例举例：某局点防火墙配置安全策略后不生效，下图为当时IPV4对象的配置：



在配置过程中经常IPV4对象的名称错误的当做了匹配条件，上图中写的192.168.1.0/24只是一个名称没有任何内容导致了策略不生效，需要在下面空白栏中添加规则才能生效。

正确匹配规则举例：

1.5 检查接口是否绑定了接口对并开启了Bypass功能

在接口加入接口对并开启Bypass功能后通过接口的所有数据不再匹配安全策略，直接通过防火墙转发。

1.6 检查在接口绑定VPN实例情况下安全策略是否也绑定了VPN实例

特殊场景下需要防火墙作为MCE设备时，如果接口绑定了VPN实例，那么安全策略中也需要增加VPN实例后才能实现对实例内部数据进行控制。

1.7 检查需要控制的策略是否为IPV6报文

防火墙安全策略分为IPV4与IPV6安全策略，默认创建IPV4安全策略，如果需要匹配IPV6的报文则需要重新建立IPV6的安全策略，在创建策略时需要将策略类型选择为IPV6。

1.8 检查域间策略或者安全策略是否匹配

域间策略或者安全策略是否匹配可以在WEB界面查看对应策略的匹配次数，或者在“策略命中分析”中查证数据是否已经匹配了安全策略；

也可以在设备命令行下对于安全策略日志实时打印，观察数据是否有匹配到，相关排查方法如下：

1、包过滤策略排查方法（适用于域间策略调用了ACL情况）

<H3C>debugging packet-filter packet ip

<H3C>terminal debugging

<H3C>terminal monitor

举例：从设备本地Ping外部地址

<H3C>ping 1.1.1.2

Ping 1.1.1.2 (1.1.1.2): 56 data bytes, press CTRL_C to break

56 bytes from 1.1.1.2: icmp_seq=0 ttl=255 time=3.224 ms

56 bytes from 1.1.1.2: icmp_seq=1 ttl=255 time=3.056 ms

56 bytes from 1.1.1.2: icmp_seq=2 ttl=255 time=3.145 ms

56 bytes from 1.1.1.2: icmp_seq=3 ttl=255 time=3.068 ms

56 bytes from 1.1.1.2: icmp_seq=4 ttl=255 time=3.049 ms

原始Debugging信息：

*Aug 28 20:14:34:590 2019 H3C FILTER/7/PACKET: -COntext=1; The packet is permitted. Src-ZOne=Local, Dst-ZOne=Trust;If-In=InLoopBack0(132), If-Out=Reth1(134); Packet Info:Src-IP=1.1.1.1, Dst-IP=1.1.1.2, VPN-Instance=,Src-Port=8, Dst-Port=0, Protocol=ICMP(1), Application=ICMP(22742), ACL=3001, Rule-ID=5.

Debugging信息解释：

*Aug 28 20:14:34:590 2019 H3C FILTER/7/PACKET: -COntext=1; The packet is permitted.（这个包被放行）Src-ZOne=Local（源安全域为local）, Dst-ZOne=Trust（目的安全域为trust）;If-In=InLoopBack0(132), If-Out=Reth1(134)（从Reth1接口发出）; Packet Info:Src-IP=1.1.1.1, Dst-IP=1.1.1.2,（报文的源地址与目的地址） VPN-Instance=,Src-Port=8, Dst-Port=0（报文源端口和目的端口）, Protocol=ICMP(1), Application=ICMP(22742)（协议类型）, ACL=3001, Rule-ID=5.（调用的ACL编号与规则ID）

2、对象策略排查方法（适用于域间策略调用了对象策略情况）

<H3C>debugging aspf all

<H3C>terminal debugging

<H3C>terminal monitor
举例：从设备本地Ping外部地址
<H3C>ping 1.1.1.2
Ping 1.1.1.2 (1.1.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.1.2: icmp_seq=0 ttl=255 time=3.224 ms
56 bytes from 1.1.1.2: icmp_seq=1 ttl=255 time=3.056 ms
56 bytes from 1.1.1.2: icmp_seq=2 ttl=255 time=3.145 ms
56 bytes from 1.1.1.2: icmp_seq=3 ttl=255 time=3.068 ms
56 bytes from 1.1.1.2: icmp_seq=4 ttl=255 time=3.049 ms
Debugging信息：
*Aug 28 20:24:39:791 2019 H3C FILTER/7/PACKET: -COntext=1; The packet is permitted. Src-ZOne=Local, Dst-ZOne=Trust;If-In=InLoopBack0(132), If-Out=Reth1(134); Packet Info:Src-IP=1.1.1.1, Dst-IP=1.1.1.2, VPN-Instance=,Src-Port=8, Dst-Port=0, Protocol=ICMP(1), Application=ICMP(22742), ObjectPolicy=1, Rule-ID=1.
3、安全策略排查方法（适用于安全策略情况）
<H3C>debugging security-policy all
<H3C>terminal debugging
<H3C>terminal monitor
举例：从设备本地Ping外部地址
<H3C>ping 1.1.1.2
Ping 1.1.1.2 (1.1.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.1.2: icmp_seq=0 ttl=255 time=3.224 ms
56 bytes from 1.1.1.2: icmp_seq=1 ttl=255 time=3.056 ms
56 bytes from 1.1.1.2: icmp_seq=2 ttl=255 time=3.145 ms
56 bytes from 1.1.1.2: icmp_seq=3 ttl=255 time=3.068 ms
56 bytes from 1.1.1.2: icmp_seq=4 ttl=255 time=3.049 ms
Debugging信息：
*Aug 28 20:20:46:121 2019 H3C FILTER/7/PACKET: -COntext=1; The packet is permitted. Src-ZOne=Local, Dst-ZOne=Trust;If-In=InLoopBack0(132), If-Out=Reth1(134); Packet Info:Src-IP=1.1.1.1, Dst-IP=1.1.1.2, VPN-Instance=, Src-MacAddr=0000-0000-0000,Src-Port=8, Dst-Port=0, Protocol=ICMP(1), Application=ICMP(22742), SecurityPolicy=1, Rule-ID=1.

1.9 检查当前本是否为最新版本

防火墙早期版本出现过调整安全策略顺序后安全策略不生效问题，升级最新版本可以解决。

配置关键点

无