403 Forbidden
本电子书由CyberArticle制作。点击这里下载CyberArticle。注册版本不会显示该信息。 删除广告
本电子书由CyberArticle制作。点击这里下载CyberArticle。注册版本不会显示该信息。 删除广告
本电子书由CyberArticle制作。点击这里下载CyberArticle。注册版本不会显示该信息。 删除广告

NGFW防火墙安全策略解读

目录

1 防火墙的安全策略介绍

1.1 防火墙安全策略概念

防火墙的基本作用是保护特定网络免受“不信任”的网络的攻击，但是同时还必须允许两个网络之间可以进行合法的通信。安全策略的作用就是对通过防火墙的数据流进行检验，符合安全策略的合法数据流才能通过防火墙。

通过防火墙安全策略可以控制内网访问外网的权限、控制内网不同安全级别的子网间的访问权限等。同时也能够对设备本身的访问进行控制，例如限制哪些IP地址可以通过Telnet和Web等方式登录设备，控制网管服务器、NTP服务器等与设备的互访等。

1.2 防火墙安全策略的演进

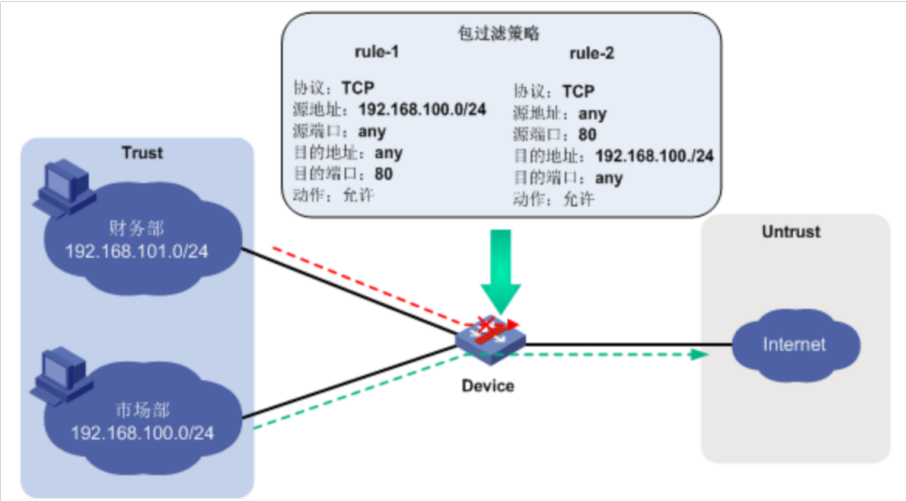
域间策略包括：包过滤、ASPF、对象策略和安全策略。管理员可以根据不同的应用场景，选择不同的域间策略对报文进行转发

控制。

1.2.1 包过滤策略

包过滤功能是根据报文的五元组（源IP地址、源端口号、目的IP地址、目的端口号、传输层协议）实现对报文在不同安全域之间的转发进行控制。

举例：若希望只允许市场部员工可以访问80端口，而财务部的员工不可以访问80端口，则需要在边界设备的Trust和Untrust安全域之间的两个方向上均应用包过滤策略。策略中需要配置两条规则rule-1和rule-2，保证市场部的员工可以访问80端口。默认策略可以禁止财务部员工访问80端口。



配置举例：

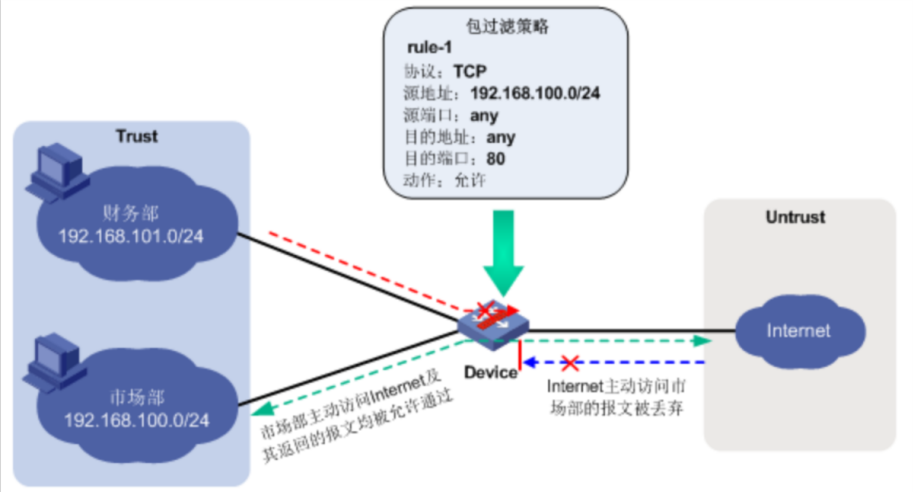
```
acl advanced 3000
  rule 0 permit tcp source 192.168.100.0 0.0.0.255 destination-port eq 80
acl advanced 3001
  rule 0 permit tcp destination 192.168.100.0 0.0.0.255 source-port eq 80
#
interface GigabitEthernet 1/0/1                    //外网接口
```

```
 packet-filter 3001 inbound
#
interface GigabitEthernet 1/0/2                    //内网接口
 packet-filter 3000 inbound
#
firewall default deny
```

1.2.2 ASPF策略

ASPF（Advanced Stateful Packet Filter，高级状态包过滤）可以对已放行报文进行信息记录，使已放行报文的回应报文在应用了包过滤策略的安全域之间可以正常通过。

举例：为了保护内部网络，可以在边界设备的Trust到Untrust安全域方向上应用包过滤策略和ASPF策略，只允许市场部的员工访问Internet网页，同时拒绝Untrust网络中的主机访问Trust网络。但是包过滤策略会将用户发起连接后返回的报文过滤掉，导致连接无法正常建立。利用ASPF功能可以解决此问题。默认策略可以禁止财务部员工访问80端口。



配置举例：

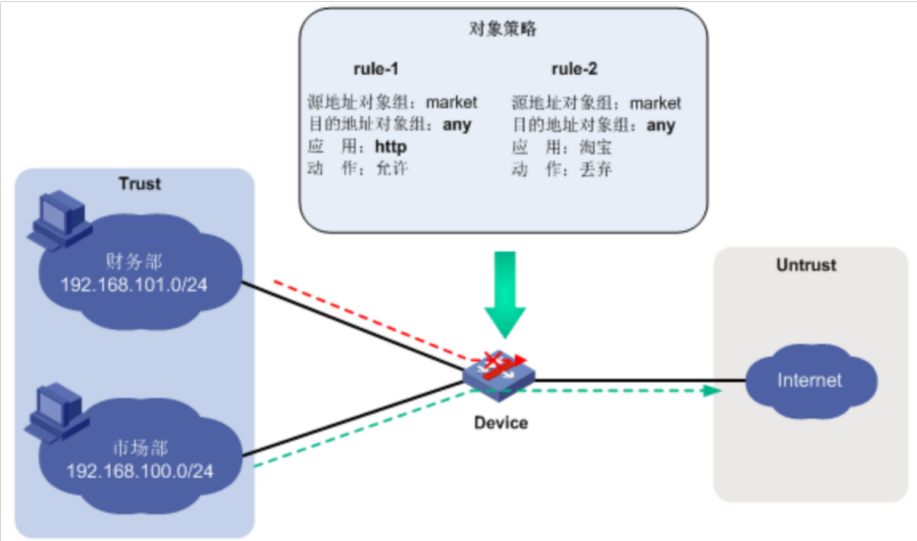
```
acl advanced 3000
 rule 0 permit tcp source 192.168.100.0 0.0.0.255 destination-
```

```
  port eq 80
#
zone-pair security source trust destination untrust
  packet-filter 3000
```

1.2.3 对象策略

对象策略基于全局进行配置，基于安全域间实例进行应用。在安全域间实例上应用对象策略可实现对报文的检查，并根据检查结果允许或拒绝其通过。

举例：若希望只允许市场部的员工可以访问80端口，但禁止其浏览淘宝网，则需要配置图1-4中的对象策略，并将对象策略应用在Trust到Untrust安全域间实例上。默认策略可以禁止财务部员工访问80端口。



配置举例：

```
object-group ip address market
 0 network subnet 192.168.100.0 255.255.255.0
#
object-policy ip market-1
 rule 0 pass source-ip market service http
```

rule 1 drop source-ip market application TaoBao

#

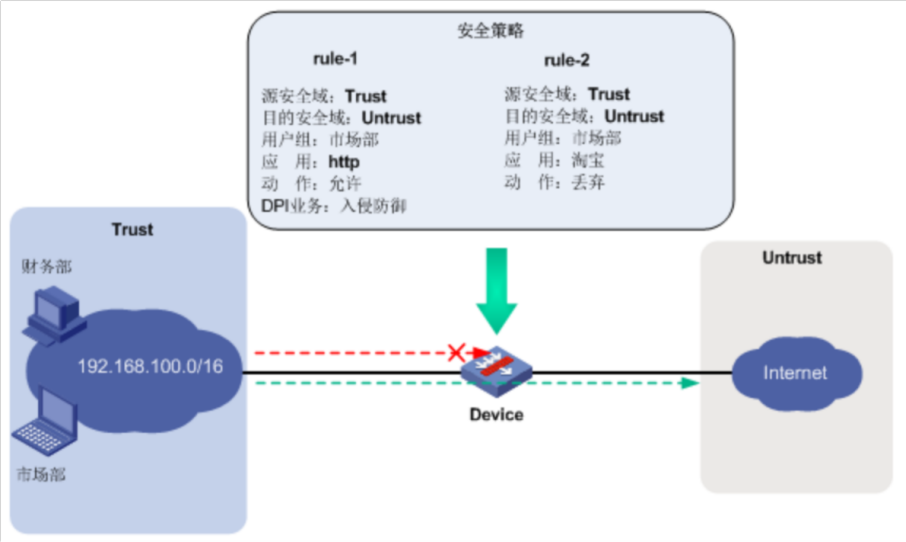
zone-pair security source trust destination untrust

object-policy apply ip market-1

1.2.4 安全策略

安全策略基于全局配置和全局生效，不需要被引用。安全策略不仅可以彻底替代包过滤和对象策略，还可以基于用户和应用对报文进行转发控制，并可以对符合过滤条件的报文进行DPI（Deep Packet Inspection，深度报文检测）检测。

举例：在安全策略中配置rule-1和rule-2基于用户和应用实现只允许市场部的员工可以访问80端口，但禁止其浏览淘宝网；并对市场部员工访问网页的内容进行深度检测，防止黑客入侵。默认策略可以禁止财务部员工访问80端口。



配置举例：

object-group ip address market

0 network subnet 192.168.100.0 255.255.255.0

#

app-group 8_IPv4

```
 description "User-defined application group"
#
security-policy ip
rule 0 name market
  action pass
  source-zone trust
  destination-zone untrust
  profile 8_IPv4
  source-ip market
  service http
rule 1 name market
  source-zone trust
  destination-zone untrust
  source-ip market
  application 淘宝
```

2 防火墙安全域

2.1.1 安全域介绍

防火墙基于安全域进行访问控制，将从接口的访问控制上升到基于安全域的访问控制。防火墙从体系结构上抛弃了传统防火墙的内外概念，各个域间的默认安全级别是一样的，之间的安全差异由用户来定制，具有极大的灵活性。防火墙可以根据企业的安全需求将不同网段划分成独立的安全域，通过在这些安全域间加载独立的访问控制策略来限制不同信任度网络之间的相互访问，也就是说，防火墙提供了更加细粒度的安全控制，这样即使某个低安全等级的区域出现了安全裂缝，但由于受到防火墙的控制，其它安全域也不会受其影响。

2.1.2 安全域分类

防火墙默认分为5个安全区域：untrust、dmz、trust、local、

management，安全域名称不同对应的功能也有区别：

untrust(不信任域):

通常用来定义Internet等不安全的网络，用于网络入口线的接入。

dmz(隔离区):

通常用来定义内部服务器所在网络，作用是把WEB,E-mail,等允许外部访问的服务器单独接在该区端口，使整个需要保护的内部网络接在信任区端口后，不允许任何访问，实现内外网分离，达到用户需求。DMZ可以理解为一个不同于外网或内网的特殊网络区域，DMZ内通常放置一些不含机密信息的公用服务器，比如Web、Mail、FTP等。这样来自外网的访问者可以访问DMZ中的服务，但不可能接触到存放在内网中的公司机密或私人信息等，即使DMZ中服务器受到破坏，也不会对内网中的机密信息造成影响。

trust(信任域):通常用来定义内部用户所在的网络，也可以理解为应该是防护最严密的地区。

local(本地):local就是防火墙本身的区域,比如ping指令等网际控制协议的回复，需要local域的权限，总结为以下两点：
1、凡是由防火墙主动发出的报文均可认为是从Local区域中发出
2、凡是需要防火墙响应并处理（而不是转发）的报文均可认为是由Local区域接收

management(管理):除了console控制接口对设备进行配置,如果防火墙设备可以通过web界面配置的话，需要一根双绞线连接到管理接口，键入用户名和密码进行配置。

2.1.3 安全域访问规则

缺省情况下（除management区域）所有安全域之间均不能互访、同安全区域间终端也无法互访，安全域之间互访必须使用安全策略来实现。

举例：现场设备已经放通了Any域到Any域的安全策略后发现trust域内用户无法互访？

```
zone-pair security source Any destination Any
packet-filter 3000
```

#
acl advanced 3000
rule 0 permit ip
.#
答案是Any域到Any域不包括trust域到trust域、trust域到local域、local域到trust域，因此需要放通同安全域间安全策略，放通同安全域安全策略有两种方法：
1、通过“security-zone intra-zone default permit”命令放通同安全域间的数据互访。
<H3C>system-view
[H3C]security-zone intra-zone default permit
2、配置同安全域间安全策略。
zone-pair security source trust destination trust
packet-filter 3000
#
acl advanced 3000
rule 0 permit ip
#

3 安全策略与对象策略

3.1 H3C 防火墙安全策略与域间策略

3.1.1 域间策略

1. 域间策略介绍

防火墙加入安全域的概念之后，安全管理员将安全需求相同的接口或IP地址进行分类（划分到不同的域），能够实现策略的分层管理，管理员只需要部署各域之间的域间策略即可。
域间策略是一种安全策略，应用于域间实例之间。域间实例用于

指定安全策略所需检测报文流的源安全域和目的安全域，即首个报文要进入的安全域和要离开的安全域。在域间实例上应用域间策略可实现对报文流的检查，并根据检查结果允许或拒绝其通过。域间策略通过配置域间策略规则实现。

一个域间策略中可以包含多条用于识别报文流的规则，称为域间策略规则。这里的规则是指通过指定对象组来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、服务类型等。设备依照这些规则识别出特定的报文，并根据设定的动作对其进行处理。

IPv4域间策略规则可以指定引用的对象，包括以下几种：

1、源IP地址对象：用于与报文的源IP地址进行匹配

2、目的IP地址对象：用于与报文的目的IP地址进行匹配

3、服务对象：用于与报文携带的服务类型进行匹配，如ICMP、TCP

4、VPN实例：用于与报文的VPN实例进行匹配

当一个域间策略中包含多条规则时，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。域间策略规则的匹配顺序与规则的创建顺序有关，先创建的规则优先进行匹配。域间策略规则的显示顺序与匹配顺序一致，从上到下依次匹配。同时可以通过命令移动规则位置来调整规则的匹配顺序。

2. 域间策略实现

NGFW防火墙上配置域间策略有两种方式，一种是基于ACL的包过滤策略，一种是基于对象组的对象策略。两者同时配置时对象策略的优先级高于包过滤策略。

1、基于ACL的包过滤策略：

```
zone-pair security source trust destination untrust
  packet-filter 3000
```

2、基于对象组的对象策略

```
 zone-pair security source trust destination untrust
```

```
object-policy apply ip market-1
```

3.1.2 安全策略

1. 安全策略介绍

与基于域间实例的包过滤策略、对象策略相比，安全策略具有如下优势：

1、与包过滤策略相比，安全策略不仅可以通过五元组对报文进行控制，还可以有效区分协议（如HTTP协议）上承载的不同应用（如基于网页的游戏、视频和购物），使网络管理更加精细和准确。

2、与对象策略相比，安全策略可以基于用户对报文进行控制，使网络管理更加灵活和可视。

3、安全策略的加速功能可用于提高安全策略规则的匹配速度。当有大量用户同时通过设备新建连接时，如果安全策略内包含大量规则，加速功能可以提高规则的匹配速度，保证网络通畅。

4、安全策略不再局限于一对一的域间实例下的引用，可以匹配一对多、多对一以及多对多等情况下安全域之间的访问。

H3C NGFW防火墙新Web版本支持安全策略，同时也仍然支持域间策略。当两种同样功能的策略同时存在时必然是有优先顺序：安全策略功能与对象策略功能在设备上不能同时使用，开启安全策略功能后，对象策略功能立即失效；当安全策略与包过滤策略同时配置时，由于安全策略对报文的处理在包过滤策略之前，报文与安全策略规则匹配成功后，不再进行包过滤处理。

2. 安全策略实现

安全策略配置举例：

```
security-policy ip
 rule 0 name market
   action pass
   source-zone trust
   destination-zone untrust
```

profile 8_IPv4
source-ip market
service http

3.2 H3C 防火墙安全策略与域间策略识别

3.2.1 安全策略和域间策略版本区别

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版本之后版本支持安全策略与域间策略共存。

查询防火墙版本方法：

1、查询到此台设备为D032版本：

<H3C>system-view

[H3C]probe

[H3C-probe]display system internal version

H3C SecPath F1070 V900R003B01D632SP20

Comware V700R001B64**D032**SP20

2、查询此板卡为D012版本：

[H3C-probe]display system internal version

H3C SecPath F1060 V900R003B01D612SP20

Comware V700R001B64**D012**SP20

3.2.2 安全策略和域间策略生效情况

安全策略与域间策略默认情况下只能一种生效，D022版本默认情况下域间策略生效，而在D032版本下则为安全策略生效。也可以通过命令查询当前设备生效的策略。

通过下面display命令查询：如果能查到命令“security-policy disable”则域间策略生效、没有查到任何命令则安全策略生效。

查询为域间策略生效：

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

security-policy disable

查询为安全策略生效：

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

3.3 H3C 防火墙安全策略与域间策略相互转换

3.3.1 安全策略与域间策略转换限制

1、 只有配置对象策略的域间策略才能转换为安全策略，使用包过滤策略域间策略不能转换为安全策略。

2、 当将对象策略转换为安全策略后，设备会强制将转换后的安全策略作为主启动文件，之前转换的对象策略配置文件还保存在设备中。

3、 对象策略转换为安全策略时，如果需要转换的对象策略配置文件不是设备正在运行的配置文件时，转换为安全策略后，日志提示需要重启设备，此时设备重启后的启动文件为转换后的安全策略配置文件，并不是转换前的下一次启动配置文件，

3.3.2 安全策略与域间策略转换方法

1、转换前一定要查看当前启动文件是否是需要转换的启动文件。

<H3C>dis startup

MainBoard:

Next main startup saved-configuration file: flash:/startup.cfg

2、配置对象策略到安全策略的转换命令

<H3C>system-view

[H3C]security-policy switch-from object-policy startup.cfg abc.cfg

Configuration switching begins...

Object policies in the specified configuration file have been switched to security policies.

Reboot the device to make the configuration take effect. Reboot now? [Y/N]:Y

注：startup.cfg为设备配置文件、abc.cfg为转换后的安全策略配置文件（其中abc可以自定义）

转换后设备会将包含安全策略的配置文件作为下次启动文件：

<H3C>dis startup

MainBoard:

Next main startup saved-configuration file: flash:/abc.cfg

4 域间策略与安全策略问题排查

4.1 包过滤策略排查方法

<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）

4.2 对象策略排查方法

<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.

4.3 安全策略排查方法

<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.