H3C SecPath AFC2000 开局指导书

目 录

1 特性简述

1.1 产品介绍

H3C SecPath AFC2000 系列异常流量检测系统和异常流量清洗系统是 H3C 依托专业的安全团队，凭借雄厚的研发实力，结合多年的技术积累和沉淀研发出来的专注于 DDoS 流量清洗过滤，实现对客户网络业务保护的一款产品。

1.2 外观介绍

H3C SecPath AFC2000 系列产品，主要包括两类产品，其中流量清洗设备款型为 AFC2020/2040/2100/2200，以及流量检测设备款型 AFC2100-D。在不区分具体型号时，后续章节统称为 AFC2000 系列设备。

图1-1 AFC2000 系列设备外观

AFC2020前后面板示意图

AFC2040前后面板示意图

AFC2100前后面板示意图

图1-2 AFC2000 系列设备外观（续）

AFC2200前后面板示意图

AFC2100-D前后面板示意图

1.3 系统登录

H3C SecPath AFC 2000 采用主流的 B/S 架构，设备支持 CLI（Command Line Interface，命令行接口）、Web 两种登录方式。

通过 CLI 登录设备后，可以直接输入命令行，来配置和管理设备。CLI 方式下又根据使用的登录接口以及登录协议不同，分为：通过 Console 口、Telnet、SSH 登录方式。

通过 Web 登录设备后，用户可以使用 Web 界面直观地管理和维护网络设备。Web 登录支持加密的 HTTPS 协议与便捷的 HTTP 协议远端管理方式，同时支持单用户多并发的账户机制。

用户首次登录设备时，可通过 Console 口、Web 或 SSH 进行登录，各登录方式下需要的最小配置详见下表：

表1-1 各种登录设备方式的最小配置描述表

登录方式	缺省情况最小配置描述
Console口本地登录设备	缺省情况下，Console口登录时用户名和密码均为admin。
SSH登录设备	配置设备 IP地址，并确保设备与 SSH 登录客户端间路由可达（缺省情况下，设备管理口eth0接口的 IP为 192.168.0.1/24，SSH登录时用户名和密码均为 admin）。
Web登录设备	配置设备 IP地址，确保设备与管理客户端间路由可达（缺省情况下，设备管理接口的 IP地址为 192.168.0.1/24）。 配置 Web 用户的用户名与密码（缺省情况下，用户名和密码均为 admin）

1.3.1 Web 登录方式

H3C SecPath AFC 2000 所有设备出厂时有固定的管理口 Eth0 口，其 IP 地址为 192.168.0.1，因此请将任意一台电脑的 IP 地址设置为与产品管理地址同一网段的 IP，并与管理接口相连。例如：在浏览器地址栏中输入 http://192.168.0.1 或 https://192.168.0.1 并回车，即可打开产品的登录界面，如下图 1-3 ~~图 1-3~~ 所示：

图1-3 系统登录界面

在设备的登录界面输入用户名账号和密码，点击<登录>按钮，进入系统 Web 管理界面。

在系统登录界面可以选择显示语言的种类目前支持的语言有“中文”和“English”两种。

在 Web 界面中可以对设备状态进行查看和配置。

成功登录后，<系统管理>→<设备管理>→选择“设备”中的接口→对应“地址、网关”变量框中填写正确参数值→<提交>参数值，可完成设备接口地址更改，如图 1-4 ~~图 1-4~~ 所示。

图1-4 Web 界面配置管理地址

在“设备管理”界面可以对设备系统的网卡接口的地址进行配置，输入项表示为设备的数据入口，输出项表示为设备的数据出口，数据输入口和数据输出口上的 IP 地址不可以作为管理地址；而其它项均为设备的配置接口，用户可更改这些网卡的 IP 地址，方便访问。同时，还可将某些网卡接入外网，并配置外网 IP 地址，这样就无须控制机的中转。

- 更改接口地址：

在“设备管理”列表底部，设备接口栏目填写，如下图：

图1-5 设备接口

图1-6 添加接口地址

图1-7 删除接口地址

- 链路聚合配置：

如果两个接口配置同样的 IP 地址，这两个接口就会默认聚合，从 CLI 命令行查看这两个接口将会生成一个新的相同的地址。如下图 1-8 ~~图 1-8~~ 所示：

图1-8 将接口地址改为相同

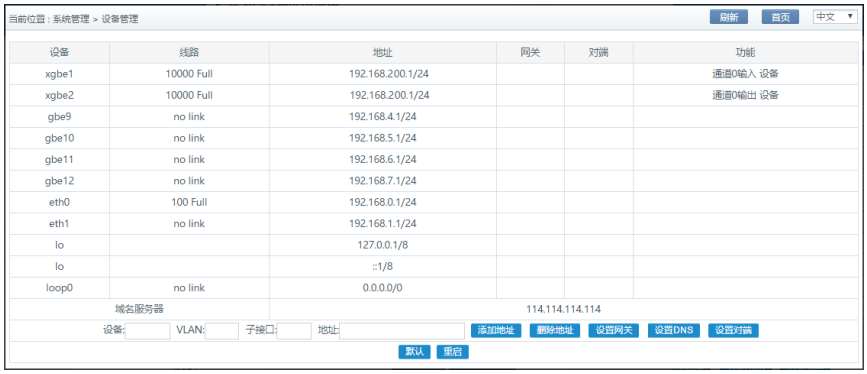
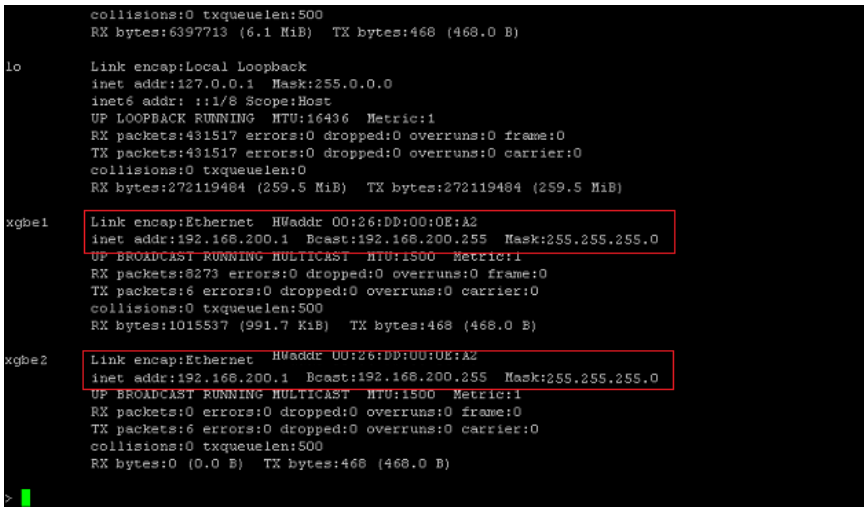


图1-9 通过 CLI 界面查看接口 MAC



1.3.2 SSH 登录设备

H3C SecPath AFC 2000 设备出厂时默认支持了 SSH 登录方式，无需单独的去配置，只需要 SSH Client 与设备管理地址直接路由可达即可登录到设备 CLI 界面，SSH 默认登录端口为 22。配置 SSH 登录环境如图 1-10 ~~图 1-10~~ 所示：

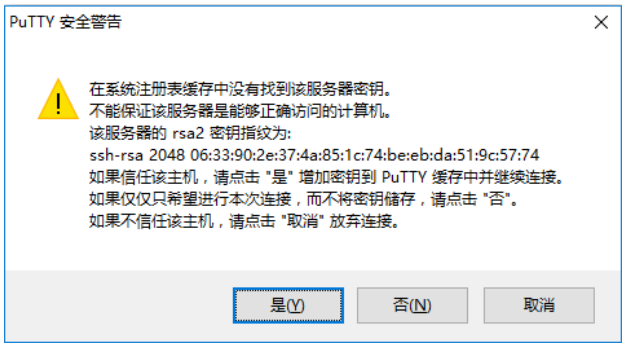
图1-10 SSH 登录环境

SSH 连接设备需要通过 PuTTY 、Xshell 等终端仿真程序，SSH 登录时提示用户输入用户名和密码，出现命令行提示符后即可键入命令来配置设备或查看设备运行状态，需要帮助可以随时键入“?”。这里我们采用的是 PuTTY，打开工具如下图所示：

图1-11 PuTTY 配置

选择连接类型“SSH”→选择“主机名称（或 IP 地址）(N)”填写设备 IP 地址→选择“端口（P)”填写设备 SSH 端口号→<打开>

图1-12 安全提示



选择<是>进入 SSH 登录界面。

图1-13 SSH 登录界面

输入账户信息→按<回车键>→输入对应密码→按<回车键>→进入 CLI 控制台。

图1-14 CLI 控制台配置界面

1.3.3 配置通过 Console 口本地登录设备

通过 Console 口进行本地登录是登录设备的基本方式之一，用户可以使用本地链路登录设备，便于系统维护。如图 1-15 ~~图 1-15~~所示，通过 Console 口登录设备时，请按照以下步骤进行操作：

(1) 准备好 RS-232 线缆（产品随机附带的配置口电缆）和 USB 口转串口转接线缆（需要用户自备）。

(2) 请先将 RS-232 线缆的 DB-9（孔）插头插入 USB 口转串口转接线缆的 9 芯（针）串口中，再将 RJ-45 插头端插入设备的 Console 口中，将 USB 口插入 PC 的 USB 口中。

图1-15 将设备与 PC 通过 Console 通信线缆进行连接

- 在通过 Console 口搭建本地配置环境时，需要通过超级终端或 PuTTY 等终端仿真程序与设备建立连接。打开终端仿真程序后，请按如下要求设置终端参数：
  - 波特率：115200
  - 数据位：8
  - 停止位：1
  - 奇偶校验：无
  - 流量控制：无
- 设备上电，终端上显示设备启动自检信息，自检结束后提示用户输入用户名和密码，出现命令行提示符后即可键入命令来配置设备或查看设备运行状态，需要帮助可以随时键入“?”。

  【注】：千兆设备的波特率为 38400，万兆设备的波特率为 115200。

2 AFC2000 的版本升级

2.1 版本升级前准备工作

更新软件版本要对设备进行重启才可生效，故客户谨慎选择业务不繁忙时升级，并提前发布系统升级公告。为了保障升级安全且高效完成，需客户提前做好如下准备工作步骤如下：

- 选择网络方便可供重启设备的升级时间；
- 提供设备远程管理地址，远程用户权限需属于 service 组；
- 提前接好设备 Console 口，如若远程重启设备后管理地址出现丢失时，可通过 Console 口重新配置管理；
- 机房有留守值班人员，以防止涉及需要本地协助处理事项。

2.2 AFC2000升级过程

2.2.1 登录设备

1. 设备已有 service 角色账号

在浏览器中输入设备管理地址 http://192.168.0.1，进入登录页面，登录设备账号权限使用“service”角色账号。

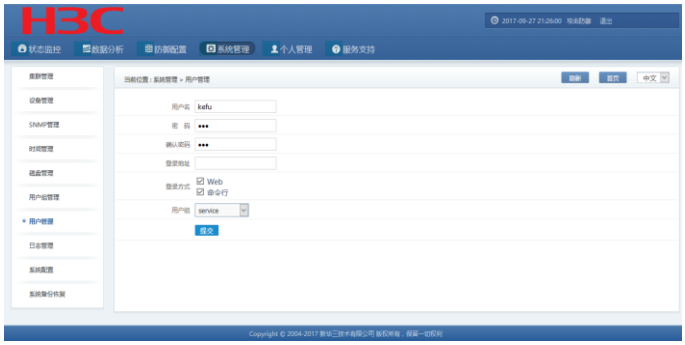
图2-1 登录页面

【注】：设备出厂默认只有一个 admin 帐户，service 组帐户需要自己创建。

2. 设备无 service 角色账号，新建 service 角色账号

操作步骤：“系统管理>用户管理”点击<添加>，根据如下编辑页面要求填写上所建账号用户名、密码、确认密码、登录方式（web、命令行）、用户组（service），点击<提交>。

图2-2 创建 service 角色账号



2.2.2 保存备份策略配置

升级过程中设备策略可直接进行保存，针对版本跨度比较大的产品，更新版本时可提前备份设备策略配置，如若策略配置出现丢失情况可及时恢复。

1. 保存策略配置

操作步骤：“系统管理>系统备份恢复>备份项目”中所有选项选择，点击<保存>并<确定>。设备默认识别最后一次保存动作，故在重启设备前，请选择保存所有项目。

图2-3 保存策略配置

2. 备份策略配置

操作步骤：“系统管理 > 系统备份恢复界面 > 备份项目”，除设备网络地址项目以外的其他 4 项目均选择，点击<导出>保存备份策略配置文档，此文档以 txt 形式保存。

图2-4 备份策略配置

【注】：下载备份时“设备网络地址”项不要选择，主要避免针对集群设备或者 ATCA 设备，每台设备接口的公网 IP 不一样；如若备份保存，升级版本完毕后集群同步恢复配置时，会导致所有的设备接口 IP 统一成一样，造成其他设备公网地址冲突无法登录。

【特别注意事项】：针对部署方式为旁路的防护设备，路由协议配置备份，需要在“路由协议”栏单独进行备份。

2.3 AFC2000软件版本更新

2.3.1 单台升级

(1) 导入升级包

请选择正确升级包，并导入升级包。

操作步骤：“服务支持>产品升级>系统升级>系统镜像”选择对应更新升级包文件，点击<提交>。

图2-5 导入升级包

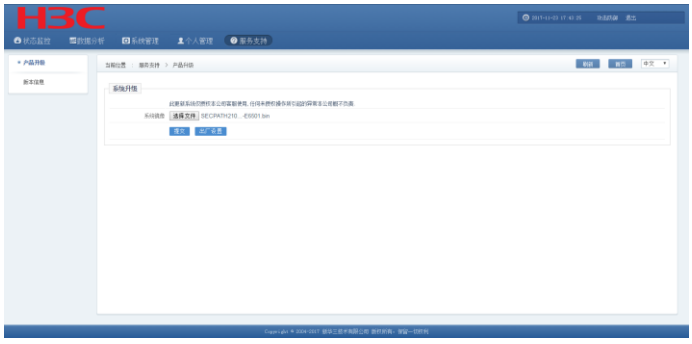


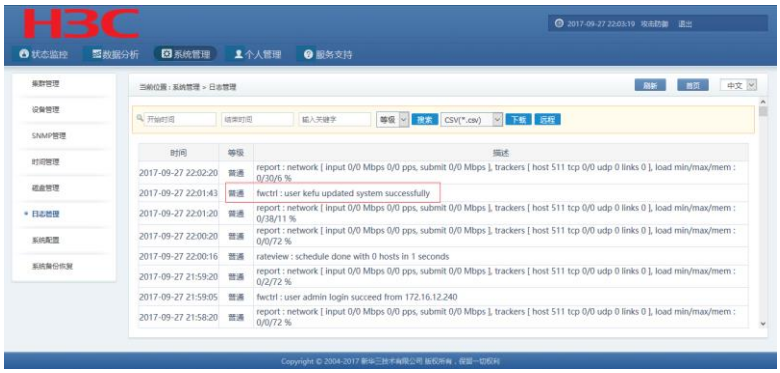
图2-6 确认提交

(2) 验证是否导入成功

升级包选择并提交后，请耐心等待，导入升级包需要几分钟。可通过如下几点来验证升级包是否导入成功。

- 导入完成会有“升级成功！在重启之后生效”提示字样。
- 日志记录中会出现 update system 操作日志。

图2-7 系统升级日志



- CLI 中查询版本构建日期是否为更新后对应版本号。

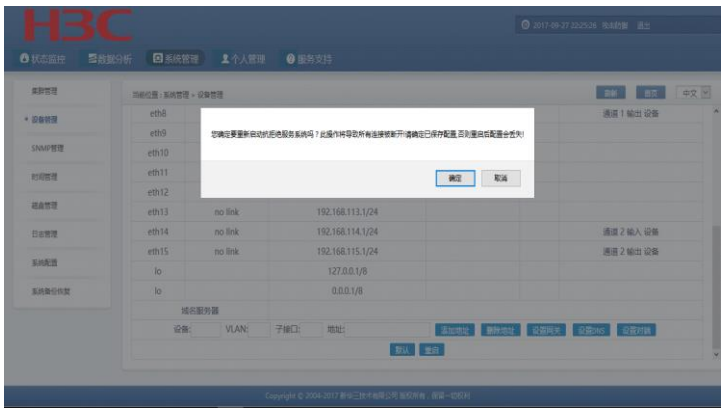
图2-8 更新后系统版本

```
> display system version
   version string : H3C SecPath AFC2040 Build #70,2017-09-23 17:00:08
```

(3) 重启设备

升级包验证已经正常导入成功，此时请重启设备，重启完成后则表示更新版本升级完毕。

图2-9 重启设备



2.3.2 先进的电信计算架构（ATCA）设备升级

(1) 使用 service 角色账号登录设备；

(2) 导入升级包，升级包导入提示成功后，请耐心等待 2 分钟左右；然后检查确认其他业务板单元版本是否同步更新成功。

【注】：切记 ATCA 设备所有业务板单元必须均更新成功后，方可 Web 界面重启设备，否则会造成系统崩溃。

(3) 确认设备所有业务板单元版本更新后，重启设备

【注】：切记 ATCA 设备只有在 WEB 界面重启，才会整机生效，在命令行重启只针对当前单元生效。

2.3.3 集群升级

(1) 确保设备集群同步正常；

(2) 集群中每台设备均需要使用统一的 service 角色账号登录设备（用户名、密码统一）；

(3) 集群同步情况下，只需在其中一台设备导入升级包，其他设备会同步更新。

(4) 导入升级包，并提示成功后，请耐心等待 1 分钟左右；然后检查确认其他设备版本是否同步更新成功。（验证升级包是否同步更新成功，可参照单台升级步骤中）

【注】：切记所有集群设备版本未更新成功时，不可重启设备，否则会造成系统崩溃。

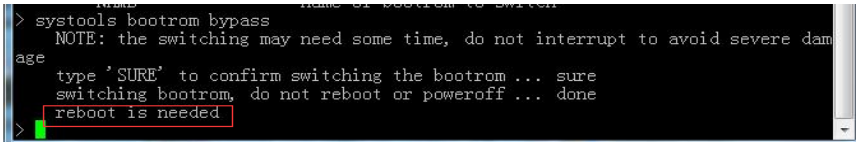
(5) 确认所有设备版本更新后，每台设备逐一通过 Web 界面重启。

2.3.4 串联切换旁路

(1) 登录 SSH 端口，使用命令：systools bootrom bypass

(2) 输入后请稍等 1 分钟左右，当出现 reboot is needed 表示切换成功，方可重启设备，建议通过 Web 界面重启设备。

图2-10 串联切换旁路



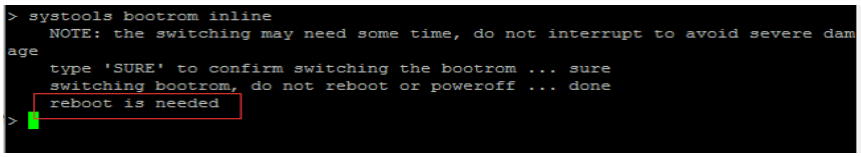
【注】：设备出厂版本为默认工作模式为串联模式，且旁路版本在升级后，其工作模式会变成串联模式，需要重新切换到旁路。

2.3.5 旁路切换串联

(1) 登录 ssh 端口，使用命令：systools bootrom inline

(2) 输入后请稍等 1 分钟左右，当出现 reboot is needed 表示切换成功，方可重启设备，建议通过 Web 界面重启设备。

图2-11 旁路切换串联



2.4 配置恢复

核验设备各项设置策略是否有丢失，如若出现丢失情况可把此前备份策略重新导入。

操作步骤：“系统管理>系统备份恢复>备份项目”，除设备网络地址项目外其余 4 项均选择，点击<浏览>选择此前备份 txt 备份配置文本，点击<导入>。

图2-12 配置导入

【注】：配置恢复时，所选择导入项目需要与备份配置时所下载项目保持一致。

2.5 注意事项

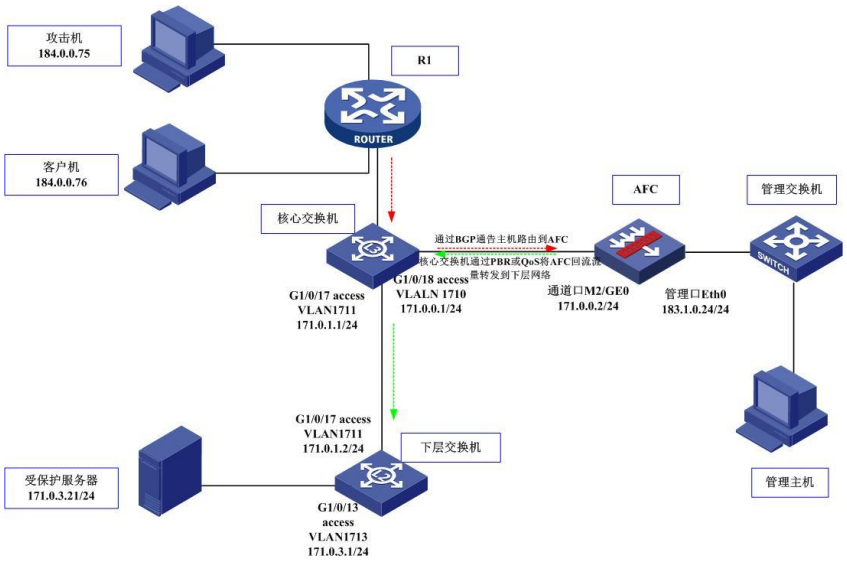
- 如若出现 Web 管理正常提交升级包后，Web 界面无法打开时。可通过 SSH 方式查验软件版本号是否正常更新，若版本号正常更新，直接通过 SSH 方式重启设备。
- 如若正常重启设备后，设备 Web 管理无法打开时。此时可通过 Console 口登录设备，查验设备管理是否恢复默认。
- 集群设备账号用户名、密码、角色类型均需统一。
- 同种型号集群部署设备可针对集群中一台设备提交升级包，其他集群设备会自动更新同步；设备需逐台重启。
- 配置导入时勾选项需要与下载时一一对应（例如只下载了“主机及配置参数”的配置，导入时只能勾选此项）。

3 单机组网之旁路 BGP 三层回注配置举例

3.1 组网需求

为实现对防护主机 171.0.3.21 的攻击流量的清洗，在核心交换设备处旁路部署一台异常流量清洗系统。核心交换机通过接口 G1/0/18 和 AFC 设备的接口 M2/GE0 连接建立 BGP 邻居，进行引流清洗。在核心交换机的 G1/0/18 接口的入方向配置策略路由或 QoS 实现清洗流量回流转发。组网如下图 3-1 ~~图 3-1~~ 所示。

图3-1 AFC 旁路部署三层回流模式配置组网图



具体实现如下：

- 主机路由发布：AFC 通过 M2/GE0 接口和核心交换机建立 BGP 邻居，AFC 将被保护 IP 的 32 位路由发布到核心交换机。
- 主机流量清洗：核心交换机将被保护主机流量牵引到 AFC，AFC 通过清洗策略对主机流量中异常流量进行清洗。
- 流量重定向：核心交换机配置策略路由或 QoS，并应用到在核心交换机与 AFC 连接的接口输入方向，实现清洗后的回流流量被转发到指定网络中。

3.2 配置思路

要实现 AFC 旁路部署 BGP 三层回流模式配置，可按照如下思路进行配置：

(1) 建立 BGP 路由

在 AFC 和核心交换机上分别启用 BGP 进程，并互为邻居关系。

(2) 核心交换机流量转发策略配置

通过在核心交换机上建立策略路由或 QoS 匹配 ACL 规则实现被保护主机流量转发，并将策略路由或 QoS 应用到核心交换机与 AFC 连接的接口入方向。

(3) AFC 路由牵引及流量清洗

发布受保护主机的路由下一跳到 AFC，AFC 根据防御策略对主机流量进行清洗，将清洗后的流量回送到核心交换机。

3.3 配置注意事项

要进行旁路组网部署，首先要确保 AFC 设备部署方式已经切换为旁路模式。

#切换 AFC 工作模式为：bypass

```
> systools bootrom bypass
    NOTE: the switching may need some time, do not interrupt to avoid severe damage
    type 'SURE' to confirm switching the bootrom ... sure
    switching bootrom, do not reboot or poweroff ... done
reboot is needed
```

要配置路由协议，还要确保 web 界面上静态路由协议已经开启。否则无法配置路由协议。

带格式的：字体：五号

提示

当前 AFC 支持旁路与串联切换，切换命令为:systool boot bypass|inline，其中 bypass 表示切换为旁路，inline 表示切换为串联。

3.4 配置步骤

1. 配置 AFC

#使用 SSH 方式登录 AFC CLI 配置视图：

```
> config startup-script channel_device 1 M2/GE0 M2/GE1
      modified the startup script with channel 1 devices
> config startup-script channel_device apply
      apply the channel device settings ? yes
      applying ... succeed
      applied the channel device settings
```

#登录 AFC 进入 Web 页面“系统管理 > 设备管理”查看此时通道状态，配置 M2/GE0 接口 IP 为 171.0.0.2/24，配置对端接口（即核心交换机 G1/0/18）IP 为 171.0.0.1

图3-2 配置 AFC 与核心交换连接的接口 IP

#配置 AFC BGP 路由

```
telnet 183.1.0.25 28065
Hello, this is Quagga (version 0.99.22).
Copyright 1996-2005 Kunihiro Ishiguro, et al.
User Access Verification
Password:
H3C>
```

```
H3C> enable
H3C# conf terminal
H3C(config)#router bgp 65534
H3C(config-router)#bgp router-id 171.0.0.2
H3C(config-router)#bgp scan-time 5
H3C(config-router)#neighbor 171.0.0.1 remote-as 65535
H3C(config-router)#neighbor 171.0.0.1 soft-reconfiguration inbound
H3C(config-router)#neighbor 171.0.0.1 route-map afc out
H3C(config)# route-map afc permit 10
H3C(config-route-map)# set community no-export no-advertise
H3C# write
Configuration saved to /mnt/storage/etc/dsfw/bgpd.conf
```

#查看配置

```
H3C# show running-config
Current configuration:
!
hostname H3C
password admin
log stdout
!
router bgp 65534
 bgp router-id 171.0.0.2
 bgp scan-time 5
 neighbor 171.0.0.1 remote-as 65535
 neighbor 171.0.0.1 soft-reconfiguration inbound
 neighbor 171.0.0.1 route-map afc out
!
route-map afc permit 10
 set community no-export no-advertise
!
line vty
!
end
```

提示

默认系统有一个 AS 号为 7675 的 BGP 进程，如果需要手动指定 AS 号，可以使用 no 命令删除默认的 AS 号为 7675 的 BGP 进程，并重新建立新的指定 AS 号的 BGP 进程。

#添加防护范围及回注方式

防护范围及回注方式，回注方式选择“默认”，回注参数留空。

图3-3 配置 AFC 防护范围及回注参数

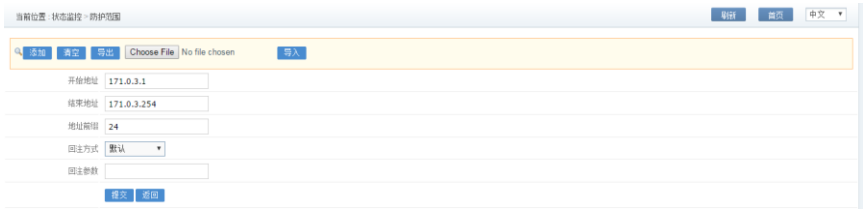


图3-4 配置 AFC 牵引主机 IP

提示

此时不要勾选主机配置中的“防护”，等对端路由进程配置完成后，勾选防护进行路由手动通告。

2. 配置核心交换机

#创建 VLAN

```
[L3SW1]vlan 1710 to 1711
```

#配置 VLAN IP

```
[L3SW1]interface Vlan-interface1710
[L3SW1-Vlan-interface1710]ip address 171.0.0.1 255.255.255.0
[L3SW1-Vlan-interface1710]quit
[L3SW1]interface Vlan-interface1711
[L3SW1-Vlan-interface1711]ip address 171.0.1.1 255.255.255.0
```

#将对应端口加入到对于 VLAN 中，将 G1/0/18 加入 VLAN 1710，将 G1/0/17 加入到 VLAN 1711

```
[L3SW1]interface GigabitEthernet1/0/17
[L3SW1-GigabitEthernet1/0/17]port link-mode bridge
[L3SW1-GigabitEthernet1/0/17]port access vlan 1711
[L3SW1-GigabitEthernet1/0/17]quit
interface GigabitEthernet1/0/18
[L3SW1-GigabitEthernet1/0/18]port link-mode bridge
[L3SW1-GigabitEthernet1/0/18]port access vlan 1710
[L3SW1-GigabitEthernet1/0/18]quit
```

#配置 BGP 进程

```
[L3SW1]#bgp 65535
```

```
[L3SW1-bgp]router-id 171.0.0.1
[L3SW1-bgp]undo synchronization
[L3SW1-bgp]peer 171.0.0.2 enable
[L3SW1-bgp]peer 171.0.0.2 as-number 65534
[L3SW1-bgp]peer 171.0.0.2 description afc2100
[L3SW1-bgp]peer 171.0.0.2 preferred-value 1
[L3SW1-bgp]peer 171.0.0.2 keep-all-routes
```

提示

如果配置的 BGP IPv6 协议，需要进入 BGP IPv6 单播视图。

#查看 BGP 对端

```
[L3SW1] display bgp peer

 BGP local router ID : 171.0.0.1
 Local AS number : 65535
 Total number of peers : 1        Peers in established state : 1
  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State
  171.0.0.2            65534        5        3    0       0 00:01:59 Established
```

#配置回流流量转发策略，实现将 AFC 清洗后的正常流量转发到下层网络

提示

AFC 旁路三层回流模式三层设备上转发策略有两种，一种是策略路由，一种是 QoS，在这里只介绍策略路由的配置，Qos 配置请参见《H3C 异常流量清洗系统旁路 BGP 三层回注配置案例》

策略路由 PBR：

#配置 ACL 匹配牵引 IP 地址段

```
[L3SW1]acl number 3003
[L3SW1-acl-adv-3003]rule 1 permit ip destination 171.0.3.0 0.0.0.255
[L3SW1-acl-adv-3003]quit
```

#创建策略路由

```
[L3SW1]policy-based-route p_afc_out permit node 5
[L3SW1]if-match acl 3003
[L3SW1]apply ip-address next-hop 171.0.1.2
```

#在三层接口应用策略路由

```
[L3SW1]interface Vlan-interface1710
[L3SW1-Vlan-interface1710]ip address 171.0.0.1 255.255.255.0
[L3SW1-Vlan-interface1710]ip policy-based-route p_afc_out
```

3. 配置下层交换机

#创建 VLAN

```
[L3SW2]vlan 1711
[L3SW2-vlan1711]quit
```

```
[L3SW2]vlan 1713
[L3SW2-vlan1713]quit
```

#配置 VLAN IP

```
[L3SW2]int Vlan-interface 1711
[L3SW2-Vlan-interface1711]ip address 171.0.1.2 24
[L3SW2-Vlan-interface1711]quit
[L3SW2]int Vlan-interface 1713
[L3SW2-Vlan-interface1711]ip address 171.0.3.1 24
[L3SW2-Vlan-interface1711]quit
[L3SW2]interface GigabitEthernet1/0/13
[L3SW2-GigabitEthernet1/0/13]port link-mode bridge
[L3SW2-GigabitEthernet1/0/13]port access vlan 1713
[L3SW2-GigabitEthernet1/0/13]quit
[L3SW2]interface GigabitEthernet1/0/17
 [L3SW2-GigabitEthernet1/0/17]port link-mode bridge
[L3SW2-GigabitEthernet1/0/17]port access vlan 1711
[L3SW2-GigabitEthernet1/0/17]quit
[L3SW2]ospf 1
[L3SW2-ospf-1]area 0
[L3SW2-ospf-1-area-0.0.0.0]network 171.0.1.0 0.0.0.255
[L3SW2-ospf-1-area-0.0.0.0]network 171.0.3.0 0.0.0.255
[L3SW2-ospf-1-area-0.0.0.0]quit
```

3.5 验证配置

(1) 验证核心交换机 L3SW1 与 AFC 通道输入口是否互通

```
 [L3SW1]ping -a 171.0.0.1 171.0.0.2
  PING 171.0.0.2: 56  data bytes, press CTRL_C to break
    Reply from 171.0.0.2: bytes=56 Sequence=1 ttl=64 time=3 ms
    Reply from 171.0.0.2: bytes=56 Sequence=2 ttl=64 time=3 ms
    Reply from 171.0.0.2: bytes=56 Sequence=3 ttl=64 time=3 ms
    Reply from 171.0.0.2: bytes=56 Sequence=4 ttl=64 time=3 ms
    Reply from 171.0.0.2: bytes=56 Sequence=5 ttl=64 time=3 ms
  --- 171.0.0.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/3/3 ms
```

(2) 验证核心交换机 L3SW1 与 AFC 路由牵引是否成功

未在 AFC 上启用主机配置“防护”时，查看 L3SW1 的 BGP 路由表

```
[L3SW1]display bgp routing-table
 Total Number of Routes: 0
```

在 AFC 上勾选保护主机的“防护”按钮

图3-5 在 AFC 上勾选保护主机的“防护”按钮进行主机路由牵引

查看核心交换机 L3SW1 的路由表

```
[L3SW1]display bgp routing-table
 Total Number of Routes: 1
 BGP Local router ID is 171.0.0.1
 Status codes: * - valid, ^ - VPNv4 best, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn
* >  171.0.3.21/32      171.0.0.2       0                     1       65534i
```

提示

如果需要牵引的主机是一个网段时，可以进入 AFC 命令行在路由协议下手动宣告网段路由。如果是连续某几个 IP，可以在“主机设置”中按照“171.0.3.1-171.0.3.254”勾选或取消后面的“防护”来进行 IP 段牵引。当与检测设备联动时可以实现自动牵引，而无需手动填写牵引 IP。

(3) 验证客户端与服务端是否互通

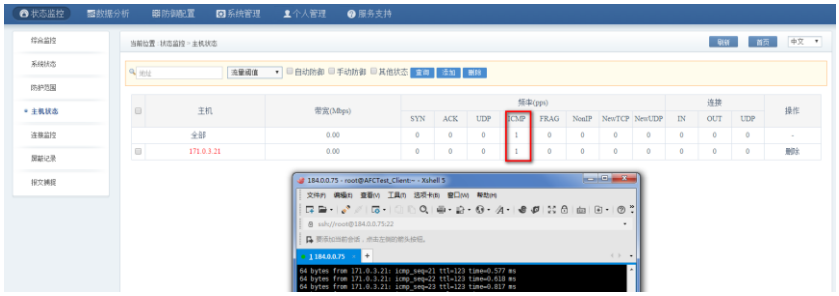
```
 [root@AFCTest_Client ~]# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0C:29:9D:1B:7A
          inet addr:184.0.0.75  Bcast:184.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe9d:1b7a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:257120 errors:0 dropped:0 overruns:0 frame:0
          TX packets:47273087 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:28882056 (27.5 MiB)  TX bytes:3460908912 (3.2 GiB)
[root@AFCTest_Client ~]# ping -c 5 171.0.3.21
PING 171.0.3.21 (171.0.3.21) 56(84) bytes of data.
64 bytes from 171.0.3.21: icmp_seq=1 ttl=124 time=0.799 ms
```

```
64 bytes from 171.0.3.21: icmp_seq=2 ttl=124 time=0.736 ms
64 bytes from 171.0.3.21: icmp_seq=3 ttl=124 time=0.862 ms
64 bytes from 171.0.3.21: icmp_seq=4 ttl=124 time=1.47 ms
64 bytes from 171.0.3.21: icmp_seq=5 ttl=124 time=1.02 ms
--- 171.0.1.21 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 0.736/0.977/1.470/0.266 ms
```

(4) 验证客户端与服务端通信是否进过 AFC

在客户端 ping 保护主机，查看 AFC 上主机状态，有 ICMP 报文过来

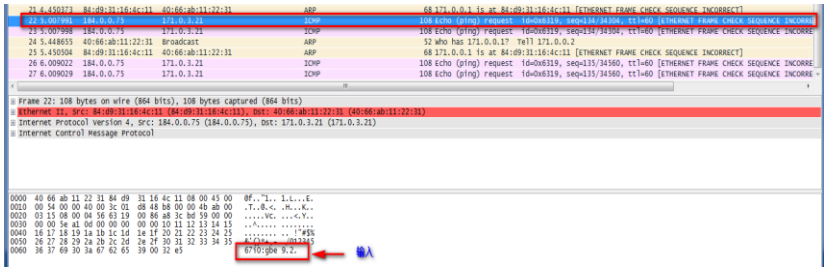
图3-6 客户端 ping 服务器



在 AFC 上抓取客户端到服务器的 ping 包。

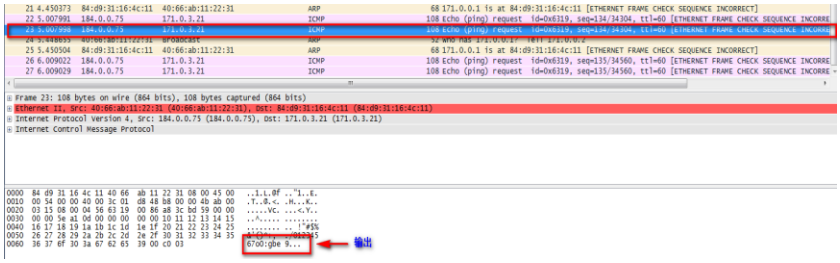
抓包分析，在 AFC 通道的输入口 M2/GE0 即 gbe9，可以看到客户端 184.0.0.75 到服务器 171.0.3.21 的 echo 包。

图3-7 在 AFC 上抓包，查看输入口报文



抓包分析，在 AFC 通道的输出口 M2/GE0 即 GBE9，可以看到客户端 184.0.0.75 到服务器 171.0.3.21 的 echo 包。

图3-8 在 AFC 上抓包，查看输出口报文

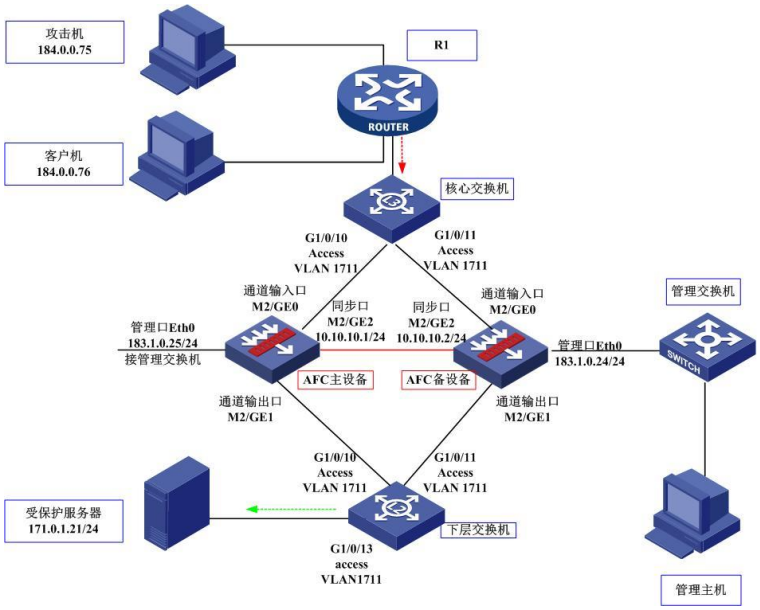


4 AFC2000 串联部署双机主备配置举例

4.1 组网需求

为实现对攻击被保护 IP 171.0.1.21 的流量的清洗，将 AFC 设备串联到客户网络中，将 AFC 主/备设备的输入口接上层交换机，将 AFC 主/备设备的输出口接下层交换机，AFC 对接收的混合流量进行检测过滤后转发到下层网络。组网如图 4-1 ~~图 4-1~~ 所示：

图4-1 AFC 串联部署双机主备配置组网图



具体实现如下：

- 接口连接：AFC 主/备设备的通道输入口 M2/GE0 接上层交换机 VLAN 1711，AFC 主/备设备通道输出口 M2/GE1 接下层交换机 VLAN 1711。
- 主机流量清洗：AFC 上配置防护范围及防护主机策略，通过策略实时对主机流量进行过滤检测。

表4-1 VLAN 分配列表

VLAN ID	作用描述	IP地址
1711	● 核心交换机与AFC通道输入口连接接口； ● 下层网络的网关地址 ● 上下层网络所在VLAN ID，受保护主机所在VLAN	171.0.1.1/24

提示

上下层交换机连接 AFC 主/备设备的接口 VLAN 号需要保持一致，否则会造成主备失败。

表4-2 AFC 接口 IP 分配列表

接口	作用描述	IP地址
M2/GE0	● 主/备设备的通道输入口，接上层网络 ● 串联模式下，无需配置，如果配置，需要与网络地址无冲突	
M2/GE1	● 主/备设备的通道输出口，接下层网络 ● 串联模式下，无需配置，如果配置，需要与网络地址无冲突	
M2/GE2	● 主/备设备同步接口	主设备：10.10.10.1/24 备设备：10.10.10.2/24
Eth0	● AFC管理口	主设备：183.1.0.24/24 备设备：183.1.0.25/24

提示

AFC 接口名称，由具体设备型号而定，此处只做指导参考。

4.2 配置思路

要实现 AFC 串联部署主备配置，可按照如下思路进行配置：

- 上下层交换机配置：配置上下层交换机与 AFC 相连的接口二层属性一致，比如同为 VLAN 1711，或者同为 Trunk 模式，且允许受保护主机 VLAN 通过。
- AFC 配置：修改 AFC 为串联模式，设置防护范围及防护主机，启用防护策略。

4.3 配置步骤

1. 配置 AFC

使用 SSH 方式登录 AFC CLI 配置视图，在 AFC 主/备设备上创建通道：

#修改 AFC 通道

```
> config startup-script channel_device 1 M2/GE0 M2/GE1
      modified the startup script with channel 1 devices
```

#应用通道配置

```
> config startup-script channel_device apply
      apply the channel device settings ? yes
      applying ... succeed
      applied the channel device settings
```

#配置 AFC 主/备设备接口

登录 AFC 进入 Web 页面“系统管理 > 设备管理”查看此时通道状态，确认通道已经创建成功。

图4-2 查看 AFC 通道口

提示

默认串联版本，通道口有默认 IP，在不与网络 IP 冲突的情况下不需要修改。

(1) AFC 主设备配置

设置设备号，删除无关地址，或保证地址不会冲突

进入 AFC CLI 命令行配置

#设置主设备的设备号

```
> conf startup-script init_address 1
```

提示

建议将 Master 设备的所有接口 IP 的尾数为 1,Backup 设备的所有接口 IP 的尾数为 2。

图4-3 设置 AFC 主设备同步口地址为 10.10.10.1/24

提示

保证 Master 设备与 Backup 设备同步口地址在一个网段。

填写 AFC 主设备集群管理，并点击下方的<保存>按钮，不是<开启>按钮。

图4-4 配置系统集群管理

提示

集群同步设备：即“设备管理”页面预先指定的同步接口；

集群同步地址：即 Master 与 Backup 设备在“设备管理”页面预先指定的同步接口 IP；

AFC 主设备配置完集群管理时，填写集群同步地址后，点击的是保存，而不是开启。

(2) AFC 备设备配置

设置设备号，删除无关地址，或保证地址不会冲突

进入 AFC CLI 命令行配置

#设置备设备的设备号

```
> conf startup-script init_address 2
```

提示

建议将 Master 设备的所有接口 IP 的尾数为 1,Backup 设备的所有接口 IP 的尾数为 2。

图4-5 设置 AFC 备设备同步口地址为 10.10.10.2/24

提示

保证 Master 设备与 Backup 设备同步口地址在一个网段。

填写 AFC 备设备集群管理，并点击下方的<保存>按钮，不是<开启>按钮。

图4-6 配置系统集群管理

提示

集群同步设备：即“设备管理”页面预先指定的同步接口；

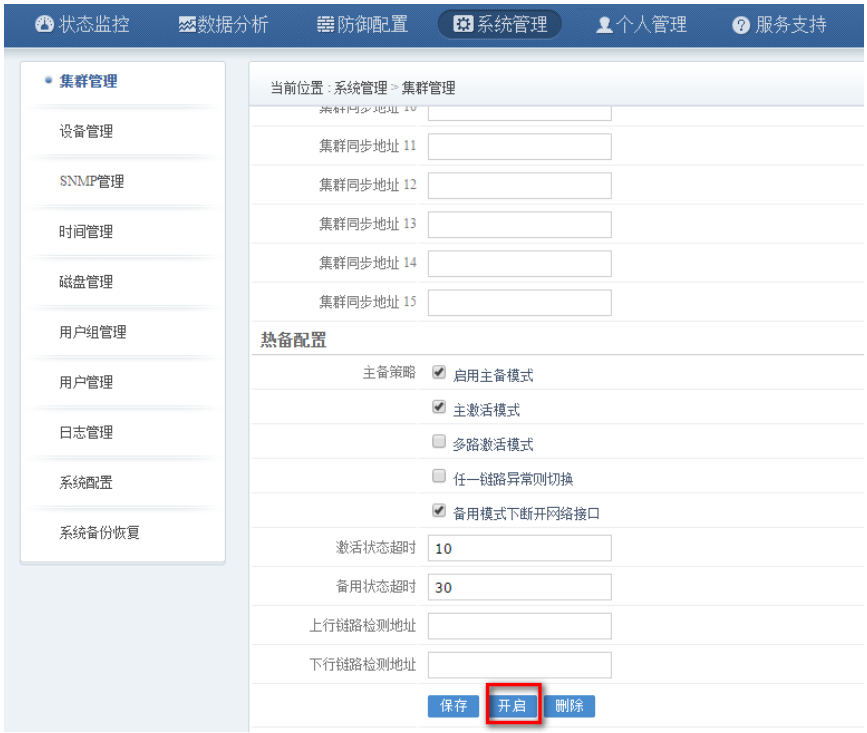
集群同步地址：即 Master 与 Backup 设备在“设备管理”页面预先指定的同步接口 IP；

AFC 主设备配置完集群管理时，填写集群同步地址后，点击的是保存，而不是开启。

(3) 启用 AFC 主/备设备热备配置

勾选 AFC 主设备：热备启用主备模式、主激活模式、备用模式下断开网络接口、激活状态超时和备用状态超时。

图4-7 AFC 主设备热备配置

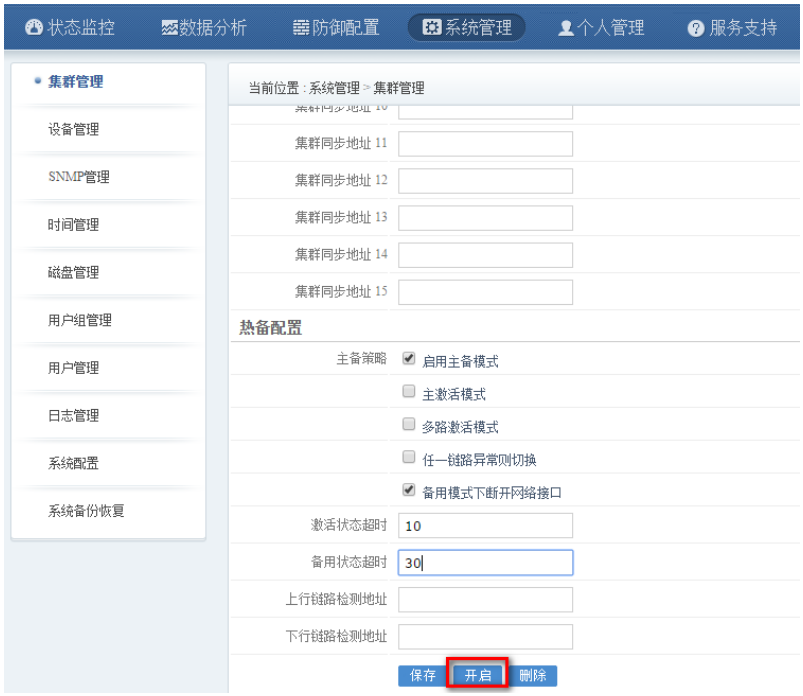


提示

热备配置，只有“开启”按钮，如果要关闭，将热备配置中的选项取消，再次点击“开启”即可关闭热备。当前“集群管理”中的保存按钮仅对“系统集群管理”生效。

勾选 AFC 备设备：热备启用主备模式、备用模式下断开网络接口、激活状态超时和备用状态超时。

图4-8 AFC 备设备热备配置



提示

启用主备配置：表示此设备为主备部署

主激活模式：表示当前设备为 Master 设备

备用模式下断开网络接口：表示设备处于 Backup 模式时自动关闭业务口

激活状态超时：系统处于激活模式时，设定时间（秒）内，没有检测到有效的数据或者测试地址间的回应，则切换为备份模式，默认 3 秒

备用状态超时：系统处于备份模式时，系统在设定时间（秒）内，无其他系统处于激活状态，则本系统进入激活状态以检测链路是否恢复。默认 30 秒。

2. 配置核心交换机

创建 1711， VLAN 1711 对应 171.0.1.0/24 网段，作用为保证 AFC 主/备设备的通道输入口和输出口在相同的 VLAN。

#创建 VLAN

```
[L3SW1]vlan 1711
[L3SW1]quit
```

#配置 VLAN IP

```
[L3SW1]interface Vlan-interface1711
[L3SW1-Vlan-interface1711]ip address 171.0.1.1 255.255.255.0
[L3SW1-Vlan-interface1711]quit
```

#将接口 G1/0/10 和 G1/0/11 加入到 VLAN 1711

```
[L3SW1]int GigabitEthernet 1/0/10
[L3SW1-GigabitEthernet1/0/10]port access vlan 1711
[L3SW1-GigabitEthernet1/0/10]quit
[L3SW1]int GigabitEthernet 1/0/11
[L3SW1-GigabitEthernet1/0/11]port access vlan 1711
[L3SW1-GigabitEthernet1/0/11]quit
```

3. 配置下层交换机

创建 VLAN 1711，作用为保证 AFC 主/备设备的通道输入口和输出口在相同的 VLAN。

#创建 VLAN

```
  [L2SW1]vlan 1711
```

#将交换机连接主机的接口加入 VLAN

```
[L2SW1]interface GigabitEthernet1/0/13
//连接被保护主机
[L2SW1-GigabitEthernet1/0/13]port link-mode bridge
[L2SW1-GigabitEthernet1/0/13]port access vlan 1711
[L2SW1-GigabitEthernet1/0/13]quit
```

#将接口 G1/0/10 和 G1/0/11 加入到 VLAN 1711

```
[L2SW1]int GigabitEthernet 1/0/10
[L2SW1-GigabitEthernet1/0/10]port access vlan 1711
[L2SW1-GigabitEthernet1/0/10]quit
[L2SW1]int GigabitEthernet 1/0/11
[L2SW1-GigabitEthernet1/0/11]port access vlan 1711
[L2SW1-GigabitEthernet1/0/11]quit
```

4. AFC 添加防护范围及启用 AFC 主备开关

#添加防护范围及回注方式

防护范围及回注方式，回注方式选择“默认”，回注参数留空

图4-9 配置 AFC 防护范围

【注】：当防护主机达到万级以上，建议添加防护范围的时候添加 24 位掩码。因为如果添加 16 位或者 8 位掩码，会导致主机列表加载地非常缓慢。

图4-10 配置 AFC 保护主机 IP

4.4 验证配置

4.4.1 验证 AFC 主设备和备设备接口状态

AFC 主设备的业务接口为激活状态。

图4-11 AFC 主设备接口状态

AFC 备设备的业务接口为关闭状态

图4-12 AFC 备设备接口状态

设备	线路	地址	网关	对端	功能
M0/XGE0	no link	1::2/64		1::1	通道 0 输入输出 设备
M0/XGE0		fe80::222:4fff:fe04:4154/64			
M0/XGE0		fe80::2255:b9ff:fec3:c516/64			
M1/XGE0	no link	0.0.0.0/0			
M2/GE0	no link	171.0.4.2/24			通道 1 输入 设备
M2/GE0		fe80::4266:abff:fe11:2631/64			
M2/GE1	no link	171.0.5.2/24			通道 1 输出 设备
M2/GE1		fe80::4266:abff:fe11:2731/64			
M2/GE2	1000 Full	10.10.10.2/24			同步设备

4.4.2 验证客户端与服务端通信是否经过 AFC

在客户端 ping 保护主机，查看 AFC 上主机状态，有 ICMP 报文过来

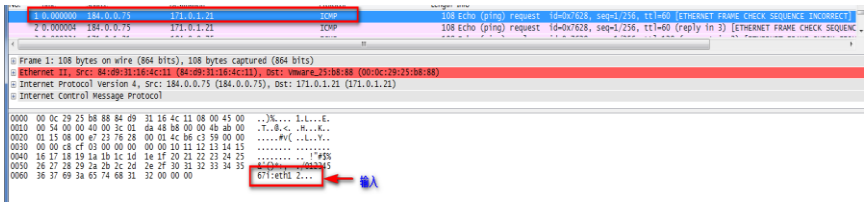
图4-13 客户端 ping 服务器

主机	带宽(Mbps)				频率(pps)								连接			操作
	IN	IN Pass	OUT	OUT Pass	SYN	ACK	UDP	ICMP	FRAG	NonIP	NewTCP	NewUDP	IN	OUT	UDP	
全部	99.74	6.98	0.00	0.00	0	0	13765	1	0	0	0	0	1	0	1064	-
171.0.1.21	0.00	0.00	0.00	0.00	0	0	0	1	0	0	0	0	0	0	0	删除

在 AFC 上抓取客户端到服务器的 ping 包

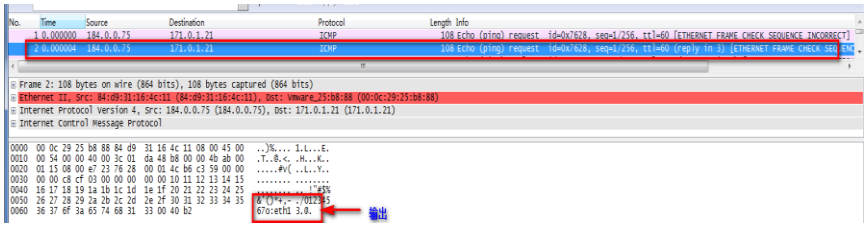
抓包分析，在AFC通道的输入口M2/GE0即Eth12，可以看到客户端184.0.0.75到服务器171.0.1.21的 echo 包

图4-14 在 AFC 上抓包，查看输入口报文



抓包分析，在AFC通道的输出口M2/GE1即Eth13，可以看到客户端184.0.0.75到服务器171.0.1.21的 echo 包。

图4-15 在 AFC 上抓包，查看输出口报文



4.5 注意事项

要进行串联组网部署，首先要确保 AFC 设备部署方式已经切换为串联模式。

通过 SSH 配置视图，切换 AFC 部署模式：

#切换 AFC 工作模式为：inline

```
> systools bootrom inline
    NOTE: the switching may need some time, do not interrupt to avoid severe damage
    type 'SURE' to confirm switching the bootrom ... sure
    switching bootrom, do not reboot or poweroff ... done
reboot is needed
```

提示

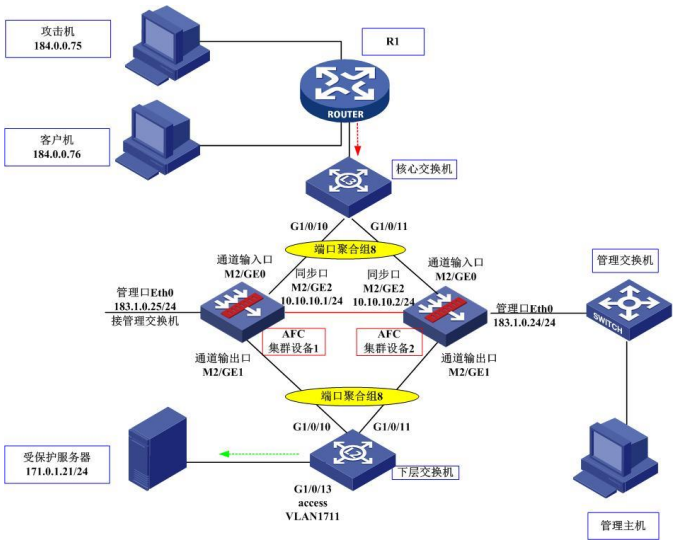
当前 AFC 支持旁路与串联切换，切换命令为:systool boot bypass|inline，其中 bypass 表示切换为旁路，inline 表示切换为串联。

5 AFC2000 串联部署双机集群配置举例

5.1 组网需求

为实现对防护主机 171.0.1.21 的攻击流量的清洗，将 AFC 设备串联到客户网络中，AFC 集群中设备的通道输入口接上层交换机端口聚合组，AFC 集群中所有设备的通道输出口接下层交换机端口聚合组，AFC 对接收的混合流量进行检测过滤后转发到下层网络。组网如图 5-1 ~~图 5-1~~ 所示。

图5-1 AFC 串联部署多通道设备配置组网图



具体实现如下：

- 接口连接：AFC 集群所有设备通道输入口接上层交换机端口聚合组 aggregation 8，AFC 集群设备所有通道输出口接下层交换机端口聚合组 aggregation 8。
- 主机流量清洗：AFC 上配置防护范围及防护主机策略，通过策略实时对主机流量进行过滤检测。

表5-1 VLAN 分配列表

VLAN ID	作用描述	IP地址
1711	● 核心交换机与AFC通道输入口连接接口； ● 上下层交换机聚合组所属VLAN ● 下层网络网关	171.0.1.1/24

表5-2 AFC 接口 IP 分配列表

接口	作用描述	IP地址
M2/GE0	● 集群所有设备的通道输入口，接上层网络 ● 串联模式下，无需配置，如果配置，需要与网络地址无冲突	
M2/GE1	● 集群所有设备的通道输出口，接下层网络 ● 串联模式下，无需配置，如果配置，需要与网络地址无冲突	

接口	作用描述	IP地址
M2/GE2	● 集群所有设备同步接口	设备1：10.10.10.1/24 设备2：10.10.10.2/24
Eth0	● AFC管理口	设备1：183.1.0.24/24 设备2: 183.1.0.25/24

提示

AFC 接口名称，由具体设备型号而定，此处只做指导参考。

5.2 配置思路

要实现 AFC 串联部署集群配置，可按照如下思路进行配置：

- 上下层交换机配置：上下交换机分别建立端口聚合组，且聚合组配置属性相同，如 VLAN 信息均属于 VLAN 1711；
- AFC 配置：修改 AFC 为串联模式，设置防护范围及防护主机，启用防护策略。将 AFC 集群所有设备通道输入口接入到上层交换机的聚合组，将 AFC 集群所有设备通道的输出口接入下层交换机的聚合组。

5.3 配置步骤

1. 配置 AFC

使用 SSH 方式登录 AFC CLI 配置视图：

#配置 AFC 集群设备 1 通道，并应用配置

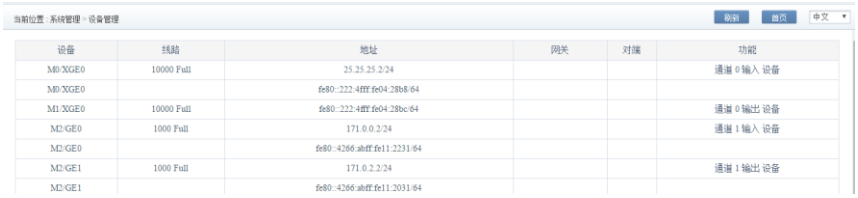
```
> config startup-script channel_device 1 M2/GE0 M2/GE1
      modified the startup script with channel 1 devices
> config startup-script channel_device apply
      apply the channel device settings ? yes
      applying ... succeed
      applied the channel device settings
```

#配置 AFC 集群设备 2 通道，并应用配置

```
> config startup-script channel_device 1 M2/GE0 M2/GE1
      modified the startup script with channel 1 devices
> config startup-script channel_device apply
      apply the channel device settings ? yes
      applying ... succeed
      applied the channel device settings
```

#配置 AFC 集群设备 1 接口

图5-2 查看 AFC 通道口



#配置 AFC 集群设备 2 接口

图5-3 查看 AFC 通道口

提示

默认串联版本，通道口有默认 IP，在不与网络 IP 冲突的情况下不需要修改。

启用 AFC 集群所有设备集群管理配置

#依次配置 AFC 集群设备同步口，本实例中均为 M2/GE2，分别为 10.10.10.1/24 和 10.10.10.2/24

图5-4 AFC 集群设备 1 同步口 IP

图5-5 AFC 集群设备 2 同步口 IP

提示

没有开启集群配置之前，所有 M2/GE2 功能未显示为“同步设备”

集群同步设备：即“设备管理”页面预先指定的同步接口

集群同步地址：即在“设备管理”页面预先指定的同步接口 IP，依次填写集群设备 1 到集群设备 N 的同步接口 IP（2≤N≤32），本次实验使用两台设备做集群。

在集群设备 1 上启用“系统集群配置”

图5-6 在集群设备 1 启用集群配置

查看集群设备 2，其接口 M2/GE2 已经变为“同步设备”

图5-7 集群设备 2 的 M2/GE1 状态

提示

在进行集群部署时，除了要保证所有集群设备型号一致，在进行同步口配置时，需要选择所有设备的相同接口作为同步口，比如这里的 M2/GE2.

集群设备 1，配置好系统集群管理中的集群同步设备及集群同步地址，点击下方“保存”，先不要点击“开启”。等其他设备均配置好同步接口 IP 后，且都接入同步交换机后，只需要在集群设备 1 上开启集群即可，集群设备 1 会将配置信息同步到集群所有设备上。

#添加防护范围及回注方式

防护范围及回注方式，回注方式选择“默认”，回注参数留空

图5-8 配置 AFC 防护范围

【注】：当防护主机达到万级以上，建议添加防护范围的时候添加 24 位掩码。因为如果添加 16 位或者 8 位掩码，会导致主机列表加载地非常缓慢。

图5-9 配置 AFC 保护主机 IP

2. 配置核心交换机

创建 1711， VLAN 1711 对应 171.0.1.0/24 网段，作用为保证所有 AFC 集群设备通道输入口和输出口在相同的 VLAN。

#创建 VLAN

```
[L3SW1]vlan 1711
[L3SW1]quit
```
#配置 VLAN IP
```
[L3SW1]interface Vlan-interface1711
[L3SW1-Vlan-interface1711]ip address 171.0.1.1 255.255.255.0
[L3SW1-Vlan-interface1711]quit
```
#创建端口聚合组
```
[L3SW1]int Bridge-Aggregation 8
[L3SW1-Bridge-Aggregation8]quit
```
#将接口 G1/0/10 和 G1/0/11 加入到聚合组
```
[L3SW1]int GigabitEthernet 1/0/10
[L3SW1-GigabitEthernet1/0/10]port link-aggregation group 8
[L3SW1-GigabitEthernet1/0/10]quit
[L3SW1]int GigabitEthernet 1/0/11
[L3SW1-GigabitEthernet1/0/11]port link-aggregation group 8
[L3SW1-GigabitEthernet1/0/11]quit
```
#配置聚合组 VLAN 信息
```
[L3SW1]int Bridge-Aggregation 8
[L3SW1-Bridge-Aggregation8]port access vlan 1711
[L3SW1-Bridge-Aggregation8]quit
```
#在此查看接口配置
```
[L3SW1]int GigabitEthernet 1/0/10
[L3SW1-GigabitEthernet1/0/10]dis this
#
interface GigabitEthernet1/0/10
 port link-mode bridge
 port access vlan 1711
 port link-aggregation group 8
[L3SW1-GigabitEthernet1/0/10]quit
[L3SW1]int GigabitEthernet 1/0/11
[L3SW1-GigabitEthernet1/0/11]dis this
#
interface GigabitEthernet1/0/11
 port link-mode bridge
 port access vlan 1711
 port link-aggregation group 8
```
#查看聚合组状态，默认为二层静态聚合
```
[L3SW1]display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired
Aggregation Interface: Bridge-Aggregation8
Aggregation Mode: Static
Loadsharing Type: Shar
```

```
  Port             Status    Oper-Key
--------------------------------------------------------------------------------
  GE1/0/10         S         1
  GE1/0/11         S         1
```

#查看负载方式，默认为目的/源 IP 负载分担

```
[L3SW1]display link-aggregation load-sharing mode interface
Bridge-Aggregation8 Load-Sharing Mode:
Layer 2 traffic: ingress-port,            destination-mac address,
                 source-mac address
Layer 3 traffic: destination-ip address,  source-ip address
```

3. 配置下层交换机

创建 VLAN 1711, 作用为保证所有 AFC 集群设备设备的通道输入口和输出口在相同的 VLAN。

#创建 VLAN

```
[L2SW1]vlan 1711
```

#将交换机连接主机的接口加入 VLAN

```
[L2SW1]interface GigabitEthernet1/0/13
//连接被保护主机
[L2SW1-GigabitEthernet1/0/13]port link-mode bridge
[L2SW1-GigabitEthernet1/0/13]port access vlan 1711
[L2SW1-GigabitEthernet1/0/13]quit
```

#聚合组配置

```
[L2SW1]interface Bridge-Aggregation 8
[L2SW1- Bridge-Aggregation 8]port access vlan 1711
```

#将接口 G1/0/10 和 G1/0/11 加入到聚合组

```
[L2SW1]int GigabitEthernet 1/0/10
[L2SW1-GigabitEthernet1/0/10]port link-aggregation group 8
[L2SW1-GigabitEthernet1/0/10]quit
[L2SW1]int GigabitEthernet 1/0/11
[L2SW1-GigabitEthernet1/0/11]port link-aggregation group 8
[L2SW1-GigabitEthernet1/0/11]quit
```

#配置聚合组 VLAN 信息

```
[L2SW1]int Bridge-Aggregation 8
[L2SW1-Bridge-Aggregation8]port access vlan 1711
[L2SW1-Bridge-Aggregation8]quit
```

#在此查看接口配置

```
[L2SW1]int GigabitEthernet 1/0/10
[L2SW1-GigabitEthernet1/0/10]dis this
#
interface GigabitEthernet1/0/10
 port link-mode bridge
 port access vlan 1711
 port link-aggregation group 8
[L2SW1-GigabitEthernet1/0/10]quit
[L2SW1]int GigabitEthernet 1/0/11
[L2SW1-GigabitEthernet1/0/11]dis this
```

```
#
interface GigabitEthernet1/0/11
 port link-mode bridge
 port access vlan 1711
 port link-aggregation group 8
#
return
```

#聚合状态查看

```
[L2SW1]display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregation Interface: Bridge-Aggregation8
Aggregation Mode: Static
Loadsharing Type: Shar
  Port             Status    Oper-Key
--------------------------------------------------------------------------------
  GE1/0/10         S         1
  GE1/0/11         S         1
```

#聚合负载方式查看

```
[L2SW1]display link-aggregation load-sharing mode interface

Bridge-Aggregation8 Load-Sharing Mode:
Layer 2 traffic: ingress-port,            destination-mac address,
                 source-mac address
Layer 3 traffic: destination-ip address,  source-ip address
```

提示

上下层交换机必须支持端口聚合。

5.4 验证配置

(1) 验证集群状态是否成功

查看所有集群设备的集群同步口功能是否变为“同步设备”，以集群设备 2 为例，如图 5-10 ~~图 5-10~~。

图5-10 集群设备 2 的 M2/GE1 状态

在所有集群设备上查看系统日志，可以看到关于激活集群配置的成功提示，见图 5-11 ~~图 5-11~~。

图5-11 集群同步日志

(2) 验证客户端与服务端通信是否经过 AFC

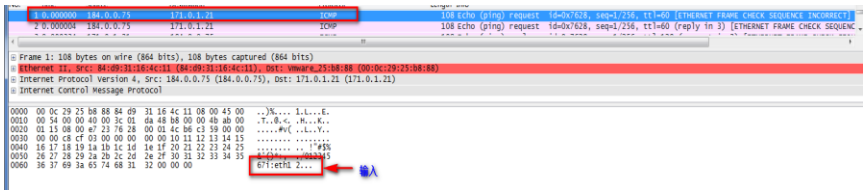
在客户端 ping 保护主机，查看 AFC 上主机状态，有 ICMP 报文过来。

图5-12 客户端 ping 服务器

在 AFC 上抓取客户端到服务器的 ping 包

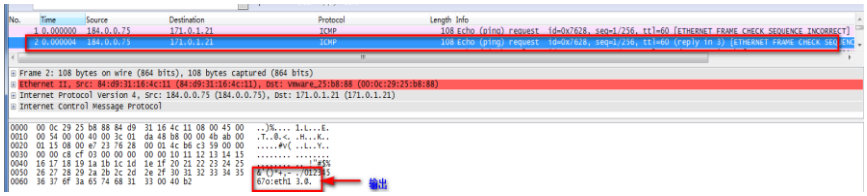
抓包分析，在AFC通道的输入口M2/GE0即eth12，可以看到客户端184.0.0.75到服务器171.0.1.21的 echo 包

图5-13 在 AFC 上抓包，查看输入口报文



抓包分析，在AFC通道的输出口M2/GE1即eth13，可以看到客户端184.0.0.75到服务器171.0.1.21的 echo 包。

图5-14 在 AFC 上抓包，查看输出口报文



提示

对于多通道设备，主机流量经过那个通道由上层设备负载方式来决定，此实例为客户端到服务器的 ping 数据包经过集群设备 1 的通道 1。

5.5 注意事项

要进行串联组网部署，首先要确保 AFC 设备部署方式已经切换为串联模式，将所有集群设备工作模式均切换为串联防护。

通过 SSH 配置视图，切换 AFC 部署模式：

#切换 AFC 工作模式为：inline

```
> systools bootrom inline
    NOTE: the switching may need some time, do not interrupt to avoid severe damage
    type 'SURE' to confirm switching the bootrom ... sure
    switching bootrom, do not reboot or poweroff ... done
reboot is needed
```

提示

当前 AFC 支持旁路与串联切换，切换命令为:systool boot bypass|inline，其中 bypass 表示切换为旁路，inline 表示切换为串联。

6 AFC2000 应对常见攻击的防御策略配置举例

6.1 手动防御

6.1.1 CC 攻击防护策略配置

1. 配置思路

要实现防御 CC 攻击的能力，可按照如下思路进行 AFC 配置：

- 把受保护服务器添加进 AFC 的防护范围；
- 开启针对 80 端口的 TCP 端口保护；
- 在端口上启用 web 插件，采用应用层源认证方式防御 CC 攻击。

2. 配置步骤

#添加防护主机

通过 http 或 https 方式登录 AFC Web 管理界面，如图 6-1 ~~图 6-1~~ 所示。

图6-1 系统登录界面

点击“防护范围 > 添加”，添加主机防护范围 ，添加的防护范围要包含受保护服务器 IP。以保护 200.2.0.100 这一台服务器为例。

图6-2 添加防护范围

【注】：当防护主机达到万级以上，建议添加防护范围的时候添加 24 位掩码。因为如果添加 16 位或者 8 位掩码，会导致主机列表加载地非常缓慢。

进入“主机状态”视图，点击<添加>按钮，添加被保护服务器 IP，如图 6-3 ~~图 6-3~~ 所示。

图6-3 添加防护主机

#添加 TCP 端口保护

进入“防御配置”视图，点击<TCP 端口保护>，点击<添加>，添加针对 80 端口的 TCP 端口保护。如下图所示。

图6-4 添加 TCP 端口保护

图6-5 配置 TCP 80 端口保护

3. 验证配置

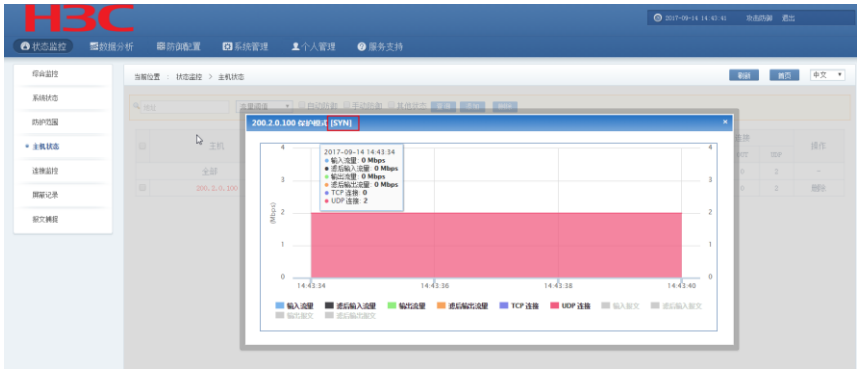
如下图所示，使用 Linux 下的攻击工具 webbench 向防护主机发送 CC 攻击，客户端超出连接数量限制设置值，客户端连接被屏蔽，AFC 只允许同一个客户端与 80 端口建立 30 个连接，因为模拟 10 个客户端所以只能建立 300 个连接；且攻击源地址被加入屏蔽列表，屏蔽原因是“系统连接保护”；且防护主机进入[SYN]保护状态。

图6-6 使用工具生成 CC 攻击

```
[root@localhost Desktop]# webbench -c 10 http://200.2.0.100/
Webbench - Simple Web Benchmark 1.5
Copyright (c) Radim Kolar 1997-2004, GPL Open Source Software.

Benchmarking: GET http://200.2.0.100/
10 clients, running 30 sec.

Speed=608 pages/min, 9310 bytes/sec.
Requests: 300 susceed, 4 failed.
[root@localhost Desktop]#
```

图6-7 攻击主机 IP 被屏蔽

图6-8 保护主机进入[SYN]防护状态



如下图所示，使用工具向防护主机发送 CC 攻击，攻击频率大于攻击检测频率设置值 10，防护主机进入[TCP]保护状态，web 插件自动开启。

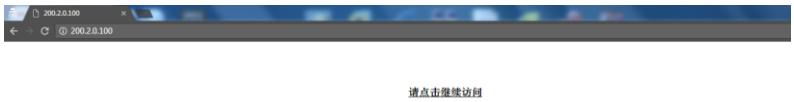
图6-9 使用工具产生 CC 攻击

```
[root@localhost Desktop]# webbench -c 10 http://200.2.0.100/
Webbench - Simple Web Benchmark 1.5
Copyright (c) Radim Kolar 1997-2004, GPL Open Source Software.

Benchmarking: GET http://200.2.0.100/
10 clients, running 30 sec.

Speed=28 pages/min, 602 bytes/sec.
Requests: 14 susceed, 0 failed.
```

图6-10 防护主机进入[TCP]防护状态

插件开启后，再访问受保护服务器的 80 端口就会出现如下图所示的源认证页面(当前不支持自定义)。因为正常用户是活动的，出现“手动点击继续”界面时用户会点击，但攻击机不具备此能力。

图6-11 防护网站启用 Web 插件



4. 注意事项

- 受保护服务器的 TCP 端口集要和端口保护设置集序号保持一致。
- Web 插件的开启有两种方式，自动开启和手动开启。如果想自动启用插件，您需要根据自己的现网流量情况根据经验设置“攻击频率检测”阈值。

6.1.2 DNS Query Flood 攻击防护策略配置

1. 配置思路

可以使用 UDP 端口保护-DNS 防护插件方式防御 DNS Query Flood，开启 DNS 插件后，客户端的 DNS 查询都会被强制使用 TCP 进行查询。

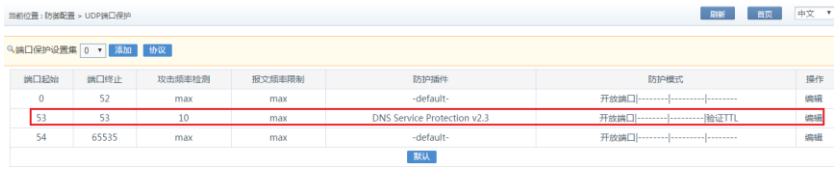
2. 配置步骤

(1) “防御配置 > UDP 端口保护”，设置端口保护设置集 0

(2) 设置 UDP 端口保护参数，选择针对 53 端口开启 DNS Service Protection 插件。

(3) 设置攻击频率检测参数如 10，防护模式同时勾选“开放端口”和另外一个防护模式的选项如“验证 TTL”，这样当 DNS QUERY 攻击报文频率超过 10 时，会自动启用该 DNS 插件。

图6-12 设置 UDP 端口保护参数



提示

仅仅只是“开放端口”不能启动 UDP 端口保护的，需要同时勾选一个其他的防护模式如验证 TTL。

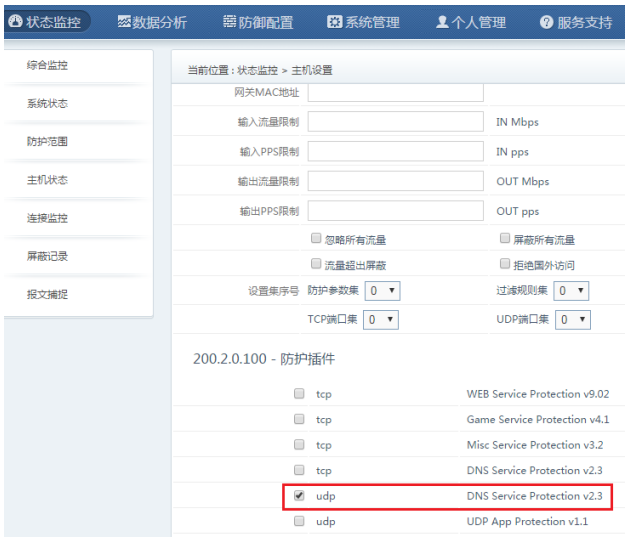
(4) 配置主机防护参数集为上一步设置的 UDP 端口集 0。

图6-13 设置主机 UDP 端口集

以上步骤 1-4 为 AFC 设备根据攻击报文自动开启 DNS 插件的情况，也可以手动开启 DNS 插件，方法如下：

在“状态监控 > 主机状态”，进入到主机设置中，手动勾选 UDP-DNS 插件，提交即可。

图6-14 手动开启 DNS 插件



3. 验证配置

(1) 通过 BPS 等测试仪向主机 200.2.0.100 发送大量的 UDP Query Flood 报文

(2) 登录 AFC 进入 Web 页面，“状态监控 > 主机状态”

- 可以看到该主机转发给 Server 的报文为 0 即 IN Pass 为 0，同时 AFC 作为代理设备给 Client 回复了 DNS Response 即 OUT Pass。

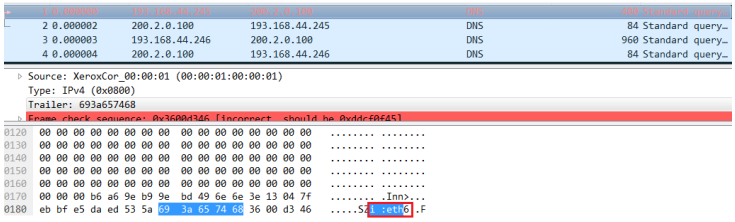
  【注】：由于 DNS Query 报文和 DNS Response 报文的大小不一致，所以下图中 IN 和 OUT Pass 大小不一致。

图6-15 主机状态

抓包情况如下：

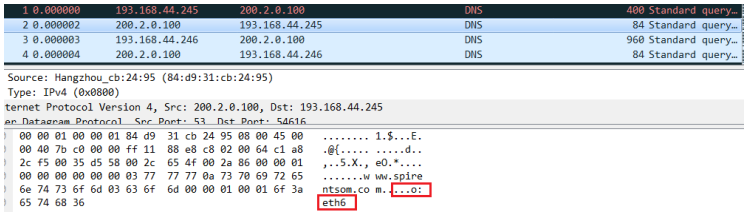
- 报文从 Eth6 进入 AFC

图6-16 DNS Query



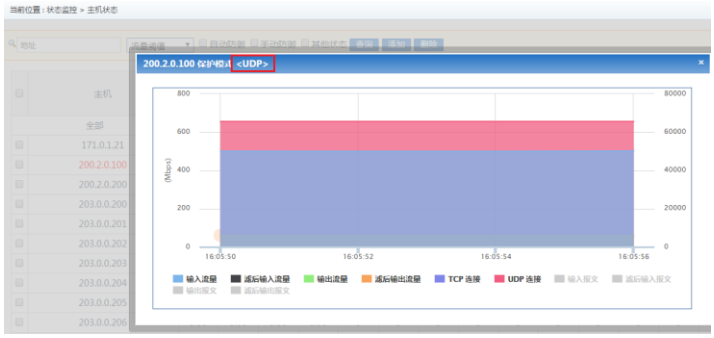
- AFC 做代理，回复 DNS Response，报文仍然从 Eth6 发出去到 Client，要求 Client 发 TCP 连接的 DNS 报文。

图6-17 DNS Response



- 点击主机可以看到该主机进入<UDP>保护状态

图6-18 UDP 保护状态



- “状态监控 > 综合监控”，可以观察到外网滤后流量为 0，内网有滤后流量。

图6-19 综合监控显示

6.2 自动防御

常见的 SYN Flood / ACK Flood / UDP Flood / ICMP Flood 等流量型攻击可以通过调整“防御配置 > 全局参数 > 流量防护策略”阈值来进行防护，配置简单，见下图。当用户网络受到流量型 DDOS 攻击时，这种防护策略可以有效地拦截攻击流量，放行正常客户流量。

图6-20 流量防护策略配置

7 故障诊断信息收集方法配置举例

7.1 报文捕捉

选择“状态监控 > 报文捕捉”进入“报文捕捉”界面，报文捕捉功能可以实时的捕获设备下某个主机 IP 或者客户端 IP 的数据，为管理人员提供故障排查的依据。在原有的报文捕捉的基础上，增加了捕获的协议内容和针对接口抓包功能。具体如下图所示：

图7-1 报文捕捉页面

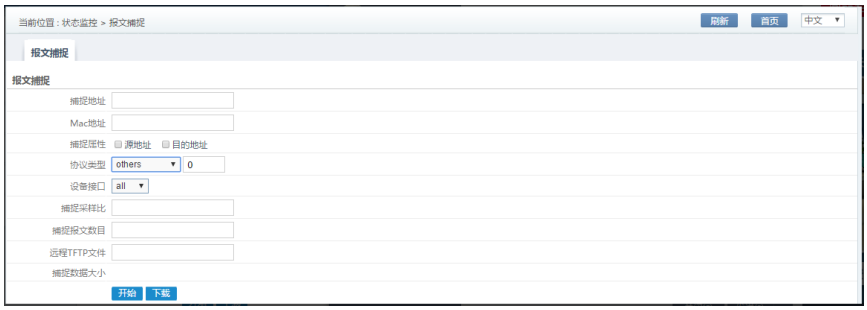


表7-1 报文捕捉相关参数

编号	功能	说明
1	捕捉地址	输入需要捕捉报文的主机地址，此地址可以是墙下主机IP也可以是客户端IP
2	MAC地址	输入要捕捉的MAC地址，可以是墙下主机MAC地址也可以是客户端MAC地址
3	捕捉属性	包括源地址和目的地址。 例如捕获地址填写的是墙下服务器的IP：192.168.59.10，并只选择了源地址，那么设备抓取数据包时，之后抓取该服务器为源IP的数据（即为该服务器对外发送的数据）
4	协议类型	设备可以针对协议类型进行抓包，协议类型目前支持 IP、TCP、UDP、ICMP、ICMPv6、IGMP 和 Others，选择 Others 时后面填写相应协议的端口号
5	设备接口	目前设备支持针对设备接口的抓包，all 表示对所有接口进行抓包
6	捕捉采样比	以采样比的形式进行抓包，比如采样比选择100，表示每100个包中随机采样一个数据包。
7	捕捉报文数目	输入想要捕捉报文的个数
8	远程TFTP文件	可以对捕捉的报文进行重命名，利于区分报文，另外可以输入TFTP地址，把捕捉好的包放入这个TFTP服务器；填写格式为 IP@文件名，例如1.1.1.1@捕捉报文 即TFTP远程地址为1.1.1.1，文件名称为捕捉报文。

7.2 Ping工具

组网时，时常会遇到从本地 ping 不同被保护服务器的问题，可以使用 AFC 自带的 ping 工具测试设备间的连通性，为管理人员提供故障排查的依据。先用 SSH 方式登录设备，方法参见 1.3.2 节，然后使用 ping 命令。

systools ping *IP_ADDR*

测试地址 192.168.2.1 的连通性。

```
> systools ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1): 56 data bytes
64 bytes from 192.168.2.1: seq=0 ttl=254 time=8.153 ms
64 bytes from 192.168.2.1: seq=1 ttl=254 time=1.822 ms
64 bytes from 192.168.2.1: seq=2 ttl=254 time=1.595 ms
```