H3C SecPath Web 应用防火墙

开局指导书

目　录

1 特性简介 1
1.1 产品介绍 1
1.2 前后面板介绍 1
1.2.1 W2000-AK415 1
1.2.2 W2000-G510 2
1.2.3 W2000-AK425 3
1.2.4 W2000-AK435 3
1.2.5 W2000-AK445 4
1.2.6 W2010-G2 5
1.2.7 W2020-G2 7
1.2.8 W2040-G2 8
1.2.9 W2080-G2 9
1.2.10 W2200-G2 10
1.3 指示灯介绍 11
2 硬件调测 11
2.1 设备上电 11
2.2 上电后检查 12
3 设备管理 12
3.1 设备管理方式 12
3.1.2 Console 口登录配置 12
3.1.3 Web 界面登录配置 13
3.2 系统默认账号说明 19
4 License 申请及导入 19
4.1 WAF License 的说明 19
4.2 License 查看 20
4.3 License 申请及激活 20
4.4 License 导入 22
5 升级 23
5.1 系统升级 23
5.2 规则库升级 31
6 WEB 应用防火墙部署 33
6.1 部署方式说明 33

6.2 部署模式推荐 37
6.3 设备上线流程 39
7 透明流模式部署配置举例 39
7.1 简介 39
7.2 配置前提 40
7.3 使用限制 40
7.4 适用产品和版本 40
7.5 组网需求 40
7.6 配置思路 40
7.7 配置步骤 41
7.8 验证配置 44
8 透明代理模式部署配置举例 46
8.1 简介 46
8.2 配置前提 46
8.3 使用限制 46
8.4 适用产品和版本 46
8.5 组网需求 47
8.6 配置思路 47
8.7 配置步骤 47
8.8 验证配置 54
9 串联反向代理模式部署配置举例 56
9.1 简介 56
9.2 配置前提 56
9.3 使用限制 56
9.4 适用产品和版本 56
9.5 组网需求 57
9.6 配置思路 57
9.7 配置步骤 57
9.8 验证配置 64
10 反向代理模式部署配置举例 66
10.1 简介 66
10.2 配置前提 66
10.3 使用限制 66
10.4 适用产品和版本 66
10.5 组网需求 66
10.6 配置思路 67

10.7 配置步骤 ····· 67
10.8 验证配置 ····· 74
11 旁路镜像检测模式部署配置举例 ····· 76
11.1 简介 ····· 76
11.2 配置前提 ····· 76
11.3 使用限制 ····· 76
11.4 适用产品和版本 ····· 76
11.5 组网需求 ····· 76
11.6 配置思路 ····· 77
11.7 配置步骤 ····· 77
11.8 验证配置 ····· 81
12 旁路镜像检测&阻断模式部署配置举例 ····· 83
12.1 简介 ····· 83
12.2 配置前提 ····· 84
12.3 使用限制 ····· 84
12.4 适用产品和版本 ····· 84
12.5 组网需求 ····· 84
12.6 配置思路 ····· 84
12.7 配置步骤 ····· 85
12.8 验证配置 ····· 91
13 透明代理双机模式部署配置举例 ····· 93
13.1 简介 ····· 93
13.2 配置前提 ····· 93
13.3 使用限制 ····· 93
13.4 适用产品和版本 ····· 93
13.5 组网需求 ····· 94
13.6 配置思路 ····· 94
13.7 配置步骤 ····· 94
13.8 验证配置 ····· 110
14 反向代理双机模式部署配置举例 ····· 112
14.1 简介 ····· 112
14.2 配置前提 ····· 113
14.3 使用限制 ····· 113
14.4 适用产品和版本 ····· 113
14.5 组网需求 ····· 113
14.6 配置思路 ····· 113

14.7 配置步骤 ····· 114
14.8 验证配置 ····· 124
15 链路聚合部署配置举例 ····· 125
15.1 简介 ····· 125
15.2 配置前提 ····· 126
15.3 使用限制 ····· 126
15.4 适用产品和版本 ····· 126
15.5 组网需求 ····· 126
15.6 配置思路 ····· 126
15.7 配置步骤 ····· 126
15.8 验证配置 ····· 129
16 Trunk 部署配置举例 ····· 130
16.1 简介 ····· 130
16.2 配置前提 ····· 130
16.3 使用限制 ····· 130
16.4 适用产品和版本 ····· 130
16.5 组网需求 ····· 130
16.6 配置思路 ····· 131
16.7 配置步骤 ····· 131
16.8 验证配置 ····· 134
17 常见故障处理 ····· 135
17.1 WAF 部署完毕查看无日志 ····· 135
17.2 WAF 部署完毕运行一段时间后，WAF 出现无法访问的状况 ····· 135
17.3 WAF 防护的网站出现无法访问或者卡顿的现象 ····· 135

1 特性简介

1.1 产品介绍

为了弥补目前安全设备，如防火墙对 Web 应用攻击防护能力的不足，我们需要一种新的工具用于保护重要信息系统不受 Web 应用攻击的影响。这种工具不仅仅能够检测目前复杂的 Web 应用攻击，而且必须在不影响正常业务流量的前提下对攻击流量进行实时阻断。这类工具相对于目前常见的安全产品，必须具备更细粒度的攻击检测和分析机制。

H3C SecPath WEB 应用防火墙，是基于自主知识产权的 H3C-OS 开发的新一代安全产品，作为网关设备，防护对象为 Web 服务器，其设计目标为：针对安全事件发生时序进行安全建模，分别针对安全漏洞、攻击手段及最终攻击结果进行扫描、防护及诊断，提供综合 Web 应用安全解决方案。

事前，产品提供 Web 应用漏洞扫描功能，检测 Web 应用程序是否存在 SQL 注入、跨站脚本漏洞。

事中，对黑客入侵行为、SQL 注入/跨站脚本等各类 Web 应用攻击、DDoS 攻击进行有效检测、阻断及防护。

产品提供了业界领先的 Web 应用攻击防护能力，通过多种机制的分析检测，能够有效的阻断攻击，保证 Web 应用的合法流量正常传输，这对于保障业务系统运行的连续性和完整性有着极为重要的意义。同时，针对当前的热点问题，如 SQL 注入攻击、网页挂马等，产品按照安全事件发生的时序考虑问题，优化最佳安全-成本平衡点，有效降低安全风险。

H3C SecPath WAF 产品包括 W2000-AK415、W2000-G510、W2000-AK425、W2000-AK435、W2000-AK445、W2010-G2、W2020-G2、W2040-G2、W2080-G2、W2200-G2 共 9 个型号，广泛适用于“金融、运营商、政府、公安、教育、能源、税务、工商、社保、卫生、电子商务”等所有涉及 Web 应用的各个行业。通过部署 H3C SecPath Web 应用防火墙产品，可以帮助用户解决目前所面临的各类网站安全问题。

1.2 前后面板介绍

1.2.1 W2000-AK415

图1-1 H3C SecPath W2000-AK415 前面板示意图

其中，2-3 为一对 Bypass 口，4-5 为一对 Bypass 口

图1-2 H3C SecPath W2000-AK415 后面板示意图

1.2.2 W2000-G510

图1-3 H3C SecPath W2000-G510 前面板示意图

其中，2-3 为一对 Bypass 口，4-5 为一对 Bypass 口

图1-4 H3C SecPath W2000-G510 后面板示意图

1.2.3 W2000-AK425

图1-5 H3C SecPath W2000-AK425 前面板示意图

其中，2-3 为一对 Bypass 口，4-5 为一对 Bypass 口

图1-6 H3C SecPath W2000-AK425 后面板示意图

1.2.4 W2000-AK435

图1-7 H3C SecPath W2000-AK435 前面板示意图

其中，0-1 为一对 Bypass 口，2-3 为一对 Bypass 口

图1-8 H3C SecPath W2000-AK435 后面板示意图

1.2.5 W2000-AK445

图1-9 H3C SecPath W2000-AK445 前面板示意图

其中，0-1 为一对 Bypass 口，2-3 为一对 Bypass 口

图1-10 H3C SecPath W2000-AK445 后面板示意图

1.2.6 W2010-G2

图1-11 H3C SecPath W2010-G2 前面板示意图

其中，0-1 为一对 Bypass 口，2-3 为一对 Bypass 口

图1-12 H3C SecPath WAF W2010-G2 后面板示意图

1.2.7 W2020-G2

图1-13 H3C SecPath W2020-G2 前面板示意图

图1-14 H3C SecPath W2020-G2 后面板示意图

1.2.8 W2040-G2

图1-15 H3C SecPath W2040-G2 前面板示意图

图1-16 H3C SecPath W2040-G2 后面板示意图

1.2.9 W2080-G2

图1-17 H3C SecPath W2080-G2 前面板示意图

图1-18 H3C SecPath W2080-G2 后面板示意图

1.2.10 W2200-G2

图1-19 H3C SecPath W2200-G2 前面板示意图

图1-20 H3C SecPath W2200-G2 后面板示意图

注意

WAF 插卡不支持热插拔，C236 平台（包括 SecPath W2000-AK435，SecPath W2000-AK445，SecPath W2010-G2）的卡槽 2，不支持 Bypass 插卡。

1.3 指示灯介绍

表1-1 H3C SecPath WAF 指示灯说明表

指示灯说明表		
指示灯	状态	含义
PWR灯	常亮	电源工作正常
	不亮	电源工作异常
HD灯	闪烁	硬盘工作正常
	不亮	硬盘工作异常
ALM 灯	常灭	设备正常或未上电
	红色常亮	设备有严重故障
	红色快闪	设备有故障，但仍可以运行
Bypass0/Bypass1灯	常亮	Bypass开启
	不亮	Bypass关闭

注意

关于 Bypass 灯的状态，若设备有电源输入，关机或强制 bypass，此时 Bypass 灯将常亮；若整机掉电，此时 Bypass 灯不亮。

关于 sys 灯：J1900 平台有 sys 灯不亮；C236 及单志强 ：没有 sys 灯；双至强：有 sys 灯且亮

2 硬件调测

2.1 设备上电

设备接上电源，然后正常开机。

2.2 上电后检查

设备在接上电源后即可开机，开机过程中 Power 指示灯常亮，HD 灯闪烁，一般系统启动时间为 4 分钟左右，使用笔记本配置 IP 为 192.168.0.0/24 网段，连接 WAF 的管理口，默认 IP 为 192.168.0.1，使用 Ping 探测尝试 WAF，ping 通后说明启动成功。

3 设备管理

3.1 设备管理方式

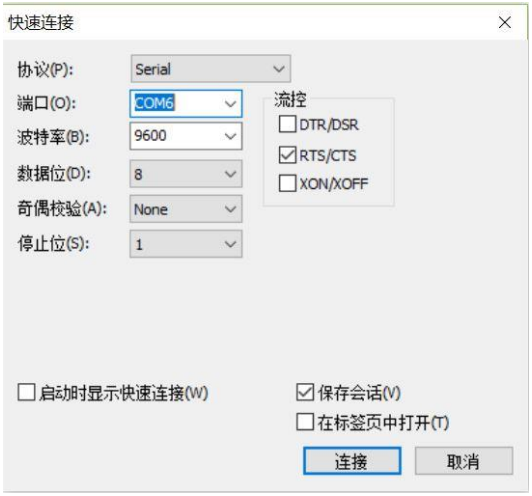
表3-1 管理方式表

IP 地址	登录方式	用户名	密码	描述
192.168.0.1	https	admin	admin	系统管理员，主要用于设备策略配置与下发；
192.168.0.1	https	account	account	账号管理员，主要用于账号的增，删等
192.168.0.1	https	audit	audit	审计管理员，主要用于审计日志查看
192.168.0.1	ssh（端口 60022）	admin	admjin	登录后台，版本升级等
-	console (波特率9600)	admin	admin	串口登录
网桥接口	管理口:设备出厂默认管理网桥为“MngtBridge”			
	业务口：设备出厂默认带“br2”网桥为业务接口，除管理口外的接口均在此桥下			

3.1.2 Console 口登录配置

可通过 Console 接口登录设备进行管理，默认 Console 登录用户名：admin；密码：admin。默认 Console 接口连接设置如图 3-1，端口可根据连接主机的具体 COM 接口选择，波特率：9600，其他保持默认设置即可。

图3-1 Console 接口设置



3.1.3 Web 界面登录配置

设备出厂默认带管理口所在网桥为“MngtBridge”，不同型号设备的默认管理口不同，见表 3-2，默认管理 IP 为:192.168.0.1。管理设备浏览器推荐使用推荐使用 Firefox56+及其以上版本浏览器，谷歌浏览器存在部分页面兼容性问题。

1. 管理口说明

- 对于如下型号的设备：SecPath W2000-AK415，SecPath W2000-G510，SecPath W2000-AK425，SecPath W2020-G2，SecPath W2040-G2，SecPath W2080-G2，SecPath W2200-G2，使用 GE0/0 接口作为管理口，需要使用管理口直连进行登录，通过界面配置管理 IP，并配置管理网段的路由；
- 对于如下型号的设备：SecPath W2000-AK435，SecPath W2000-AK445，SecPath W2010-G2，使用 GE0/7 接口作为管理口，需要使用管理口直连进行登录，通过界面配置管理 IP，并配置管理网段的路由。

表3-2 设备默认管理口表格

设备型号	默认管理口
J1900平台：SecPath W2000-AK415，SecPath W2000-G510，SecPath W2000-AK425	GE0/0
C236平台：SecPath W2000-AK435，SecPath W2000-AK445，SecPath W2010-G2	GE0/7
单志强平台：SecPath W2020-G2, SecPath W2040-G2	GE0/0
双志强平台：SecPath W2080-G2, SecPath W2200-G2	GE0/0

2. Web 界面管理口直连登录

WAF 默认管理口地址为 192.168.0.1，可在串口下使用如下命令配置 WAF 设备 IP 地址。

```
bridge -A -v MngtBridge -f 183.1.4.230 -m 255.255.255.0 -n y
```
（注意一定要加上-n y ，否则无法登陆该管理地址）

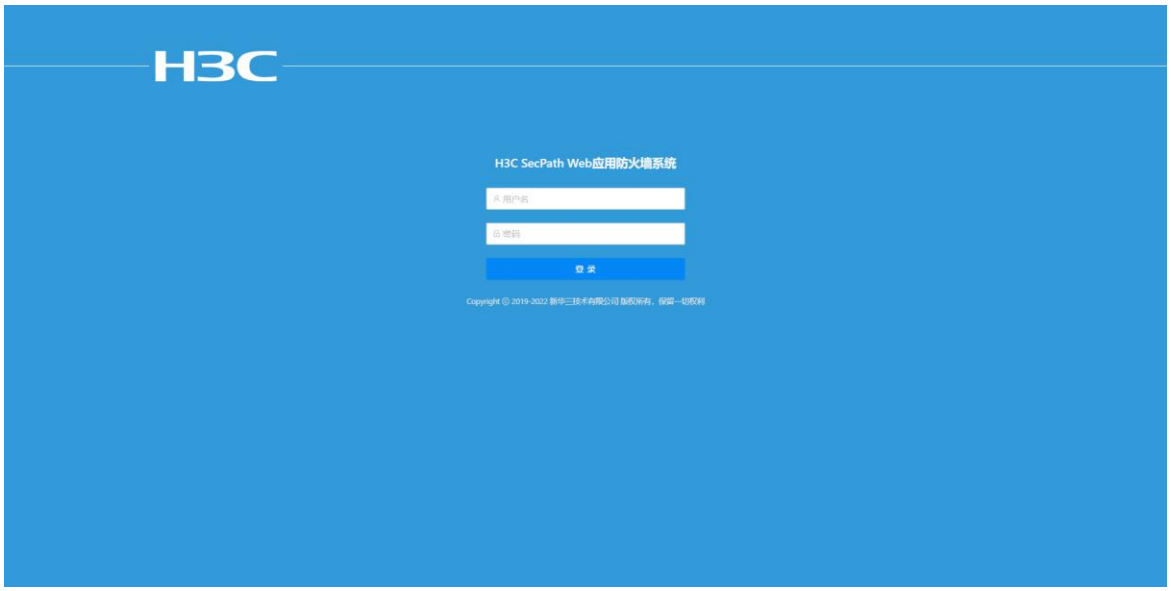
若使用默认 WAF 管理地址配置时，将电脑 IP 地址设置成 192.168.0.0/24 网段的 IP（如 IP 地址设置为 192.168.0.10，掩码 255.255.255.0），以保证与设备默认管理 IP 192.168.0.1 在同一网段，然后使用网线直接接在设备管理接口上，管理接口见表 3-2。

打开 Firefox 浏览器，在地址栏中输入 https://192.168.0.1 （注意是 https，不支持 http），按回车后，由于浏览器的安全性设置较高，非信任的根证书颁发机构颁发的证书使用时都会弹出不安全网站提示。

图3-2 浏览器提示举例图

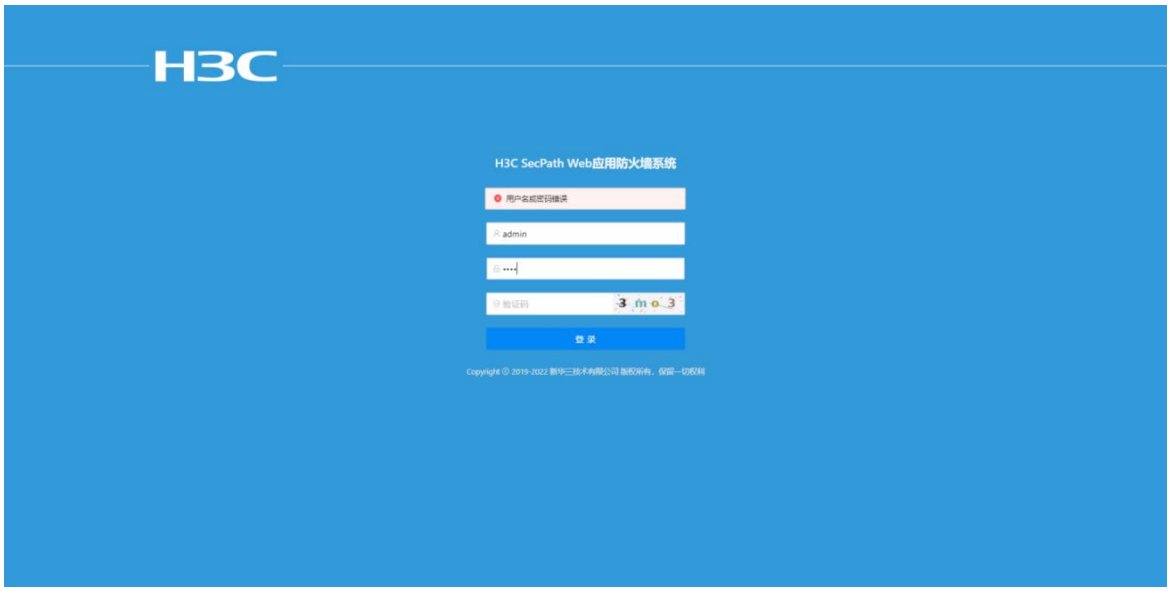
此时选择“继续转到网页”（注：其他浏览器也会弹出类似的窗口，选择 继续/添加例外等操作可登录），弹出系统登录框，输入用户名：admin 密码：admin 以系统管理员登录。

图3-3 登录界面



备注：若密码输入错误 2 次后，登录界面会弹出验证码条框，需输入用户名、密码和验证码后才可登录

图3-4 需输验证码信息登录界面

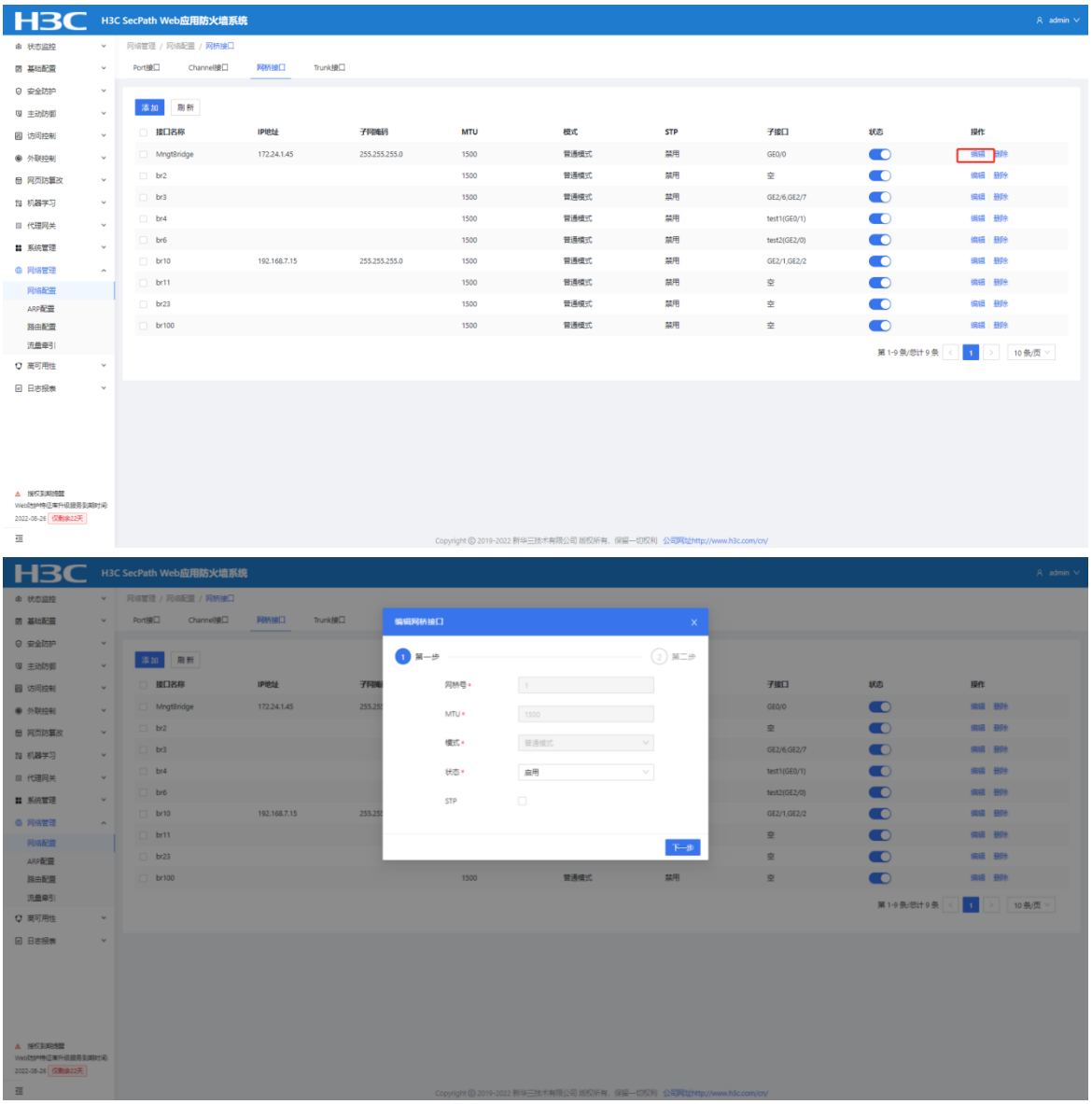


3. Web 界面配置管理地址

(1)　在管理桥 MngtBridge 下增加管理 IP

设备默认管理接口在 MngtBridge 桥下，点击左侧菜单栏，网络管理>网络配置>网桥接口如图 3-5，点击 “编辑”

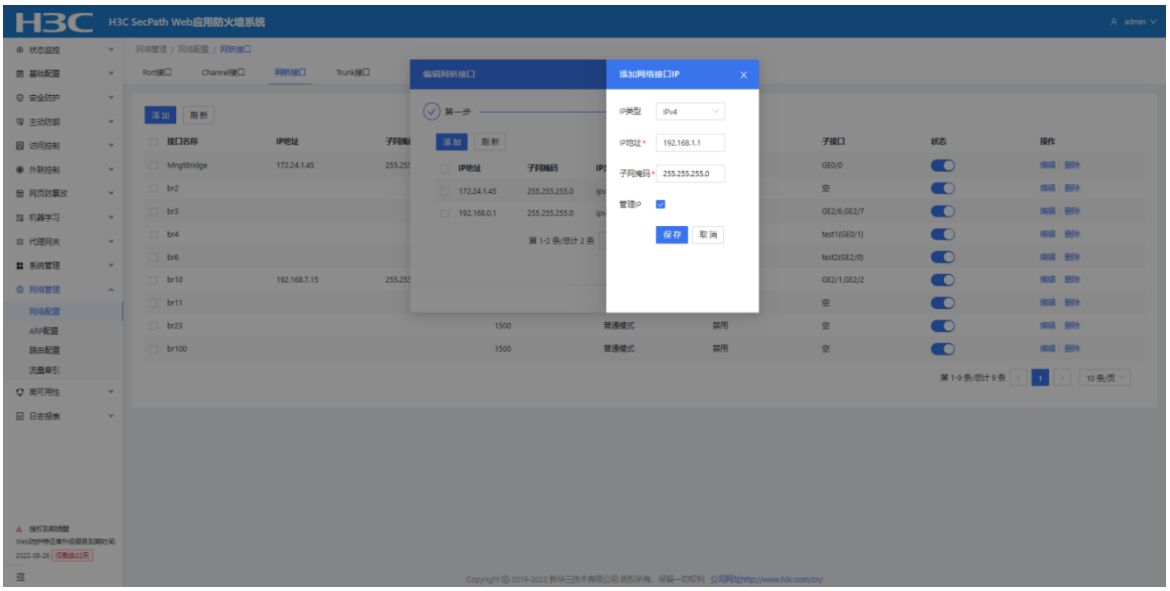
图3-5 网桥配置



是否勾选 STP 根据网络情况决定（若网络拓扑易引起环路，请勾选此项，具体网络情况请咨询客户网络工程师），点击下一步。

进入第二步之后，点击添加，可以添加新的 IP，是否勾选管理 IP，可以选择是否将添加的该 IP 设置为管理 IP，见图 3-6

图3-6 添加 IP



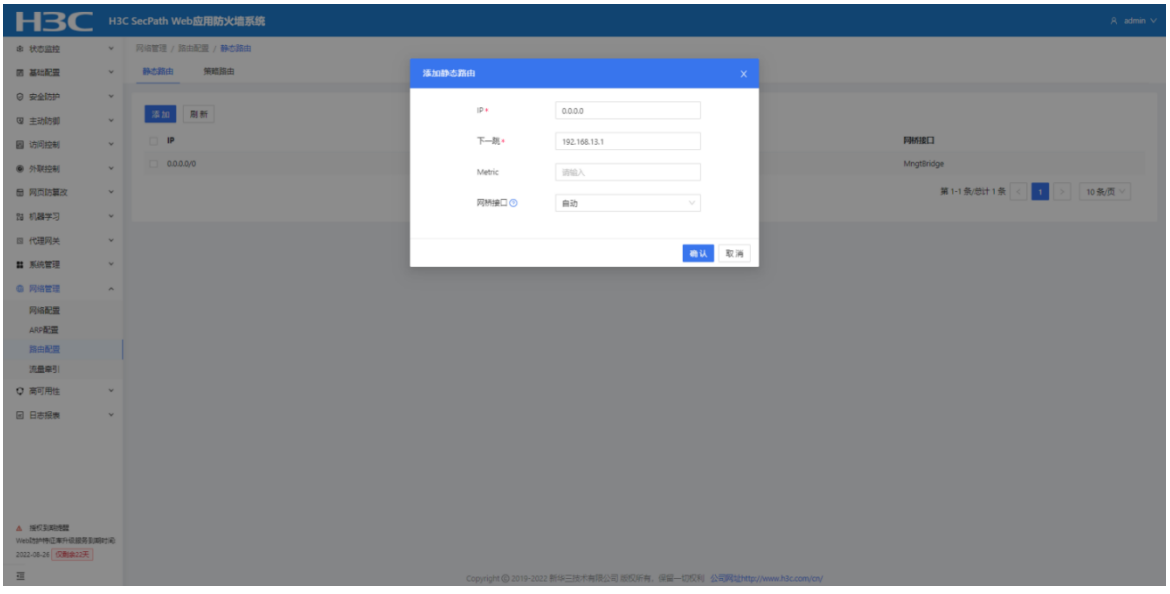
从图 3-6 可以看到已添加 IP：192.168.1.1 为一个管理 IP 地址，点击保存。

(2)　路由配置

管理 IP 配置完成后，配置路由信息。

网络管理>路由配置，点击增加，如图 3-7，配置路由信息（本例配置：IP 地址：0.0.0.0　子下一跳：192.168.13.1，Metric 可不填，选择网桥接口，默认会自动分配）

图3-7 路由配置



路由配置详细介绍如表 3-3

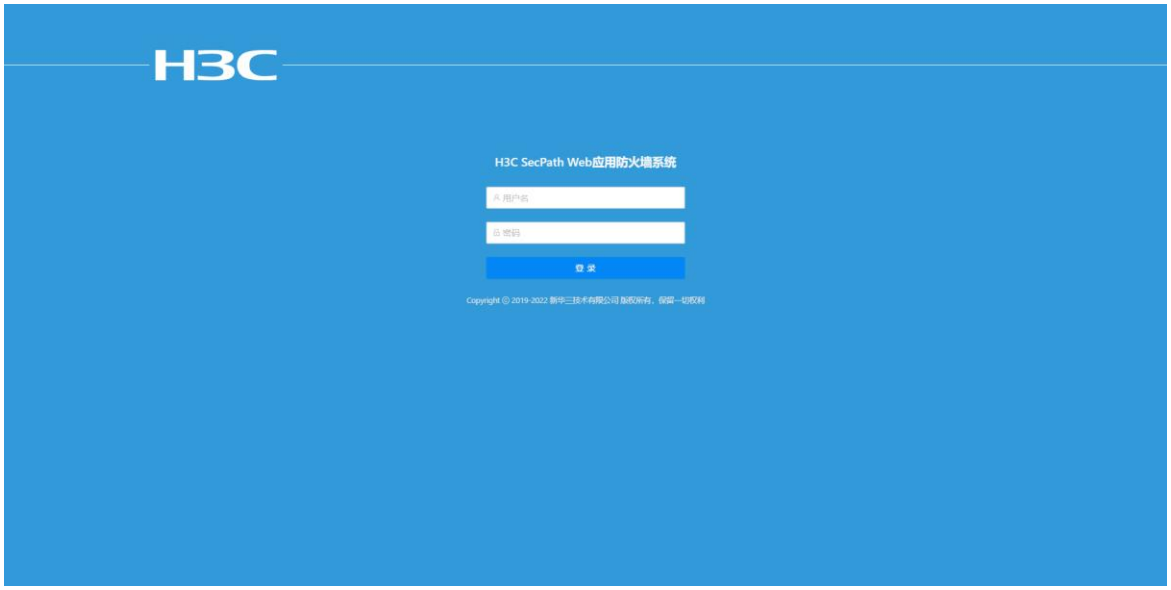
表3-3 路由配置

配置项	描述
IP地址	目的网络地址
下一跳	路由的下一跳，对端直连路由器的接口地址
Metric（非必填）	Metric：跳数，跳数用于指出路由的成本，通常情况下代表到达目标地址所需要经过的跳跃数量，一个跳数代表经过一个路由器。 跳数越低，代表路由成本越低，优先级越高。
网桥接口	选择要在哪个网桥下添加路由，默认会自动分配

点击保存，之后即可通过设置的管理地址进行访问，不需再直连设备进行访问。

管理 IP 与路由配置完成后，设备接入网络环境后，可直接通过浏览器访问配置的管理 IP 进行设备登录访问。

图3-8 登录界面



注意

首次登录后，建议用户修改登录密码，升级到 E6203 版本以上，首次登录系统会强制修改默认密码。

3.2 系统默认账号说明

表3-4 系统默认账号说明表

账号	初始密码	说明
admin	admin	系统管理员账号，主要用于设备的网络配置、系统配置、WAF策略配置与下发、攻击日志查看等；
account	account	账号管理员账号，主要用于账号的增、删、密码重置等；
audit	audit	审计管理员账号，主要用于审计日志查看；
注意：admin和audit账户密码忘记，使用account账户重置账户密码。account账户密码忘记联系H3C售后工程师进行后台重置密码。		

4 License 申请及导入

4.1 WAF License的说明

WAF 产品的授权分为“系统软件功能授权”、 “特征库升级授权”和“网页防篡改授权”三种。正式的系统软件功能授权包含永久的系统软件功能授权+一年期限的特征库升级授权+1 个 Linux 网页防篡改授权和 1 个 Windows 网页防篡改授权（若使用网页防篡改功能，则需要将 WAF 系统升级到 E6203 版本），当自带的一年有效期的特征库升级授权到期后，将无法进行 WAF 规则库的更新，需要进行特征库升级授权的扩容激活并导入设备，才能继续规则库的更新。

备注：WAF 产品支持临时授权，方便用户测试使用。

4.2 License查看

图4-1 系统许可信息查看（设备有授权的截图）

图4-2 系统许可信息查看（设备无授权的截图）

说明：许可证管理界面，“基本许可信息”中的许可有效期是指系统软件功能授权的剩余时间（备注：“无限制”代表系统软件功能是永久授权），“其他许可信息”中的规则库升级剩余时间是指特征库升级授权的剩余时间。

4.3 License申请及激活

激活 license 的步骤如下：

(1) 填写对应的需求数量并申请，获取对应的授权码。

(2) 访问 H3C 公司中文网站

(1) http://www.h3c.com/cn/Service/Policy_Trends/Authorize_License/Achieve_License/ 可进入如下图的“License 激活申请”页面，输入授权码。

需要注意的是，WAF 产品与其他硬件产品不同的是，“设备信息”需要填写两个信息，分别是“H3C 设备 S/N”和“机器码”。使用 admin/admin 账号登录 WAF 管理端，在授权管理可以看到如下字符串。

图4-1 在“授权管理”页面中获取“H3C 设备 S/N”和“机器码”

图4-2 输入 License 首次激活信息（示例）

(3) 步骤(1)的信息填写无误后，系统将提示如图 4-3 所示的对话框，并且对话框中附有已经申请下来的 License 激活文件的链接，点击并下载 License 激活文件到本地 PC。

图4-3 License 首次激活申请操作成功（示例）

注意

关于更多 WAF License 激活步骤和说明，可参考产品对应的《License 激活手册》

4.4 License导入

在 Web 应用防火墙“授权管理”页面，在升级许可处，点击上传文件，导入申请的 license 文件，并点击升级。

将激活文件导入设备，点击升级，升级成功后，可以查看许可有效期和特征库升级剩余时间。

图4-4 激活文件导入设备

注意

请妥善保管 License 文件，不要遗失。如果没有 License 文件激活系统，产品应用防护系统将不会进行安全检测工作而进入纯 IP 转发状态。如果您的 License 是一个试用版的 License，请在 License 有效期过后，向 H3C 购买正式 License；否则 License 有效期过后，系统将仅仅作为一个网络转发设备存在，没有任何安全保护功能。

5 升级

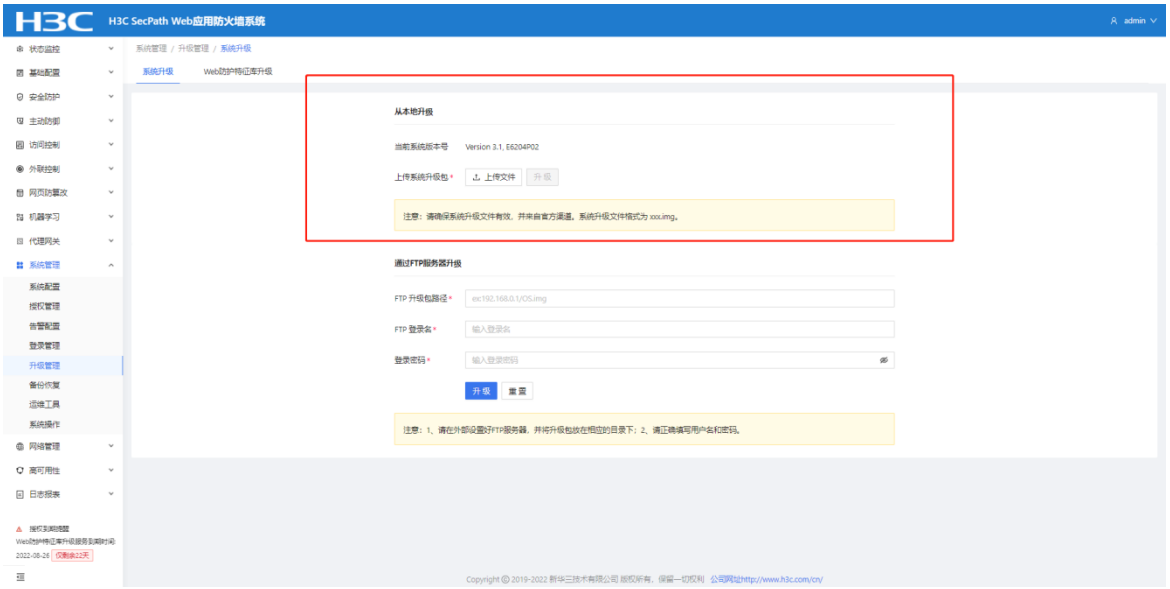
5.1 系统升级

系统升级分两种方式：系统升级包升级和FTP升级。因为浏览器上传升级包可能会有损坏或浏览器限制无法上传，推荐使用FTP方式升级。若采用本地系统包升级时，推荐使用火狐浏览器，同时保证本地PC预留3.5G以上的内存空间。

1. 从本地升级

选择“系统管理->升级管理->系统升级”进入系统升级管理界面，点击【选择】按钮选择本地的升级包后点击【升级】按钮升级系统。升级后系统会自动进行重启，请耐心等待 10—15 分钟。由于兼容性问题，不支持谷歌浏览器升级，使用火狐浏览器进行升级操作。

图5-1 从本地升级



2. 通过 FTP 服务器升级

在外部设置好 FTP 服务器，并将升级包放在相应目录下后，在界面中输入 FTP 升级路径、FTP 登录名和登录密码，点击【升级】按钮执行升级。升级后系统会自动进行重启，请耐心等待 10—15 分钟。

图5-2 通过 FTP 服务器升级

(1) 通过命令行进行 FTP 升级（推荐使用）

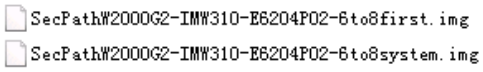
(1) 推荐使用此种升级方式，可在命令行下查看升级包升级进度。若硬件接串口线通过命令行升级可查看升级后重启过程，便于掌握升级进度。

(2) 在外部设置好 FTP 服务器（密码请不要包含特殊字符），并将升级包放在相应的目录下（路径中请勿含有中文字符），点击升级即可。

3. R6203P13 升级至 E6204P02 升级步骤

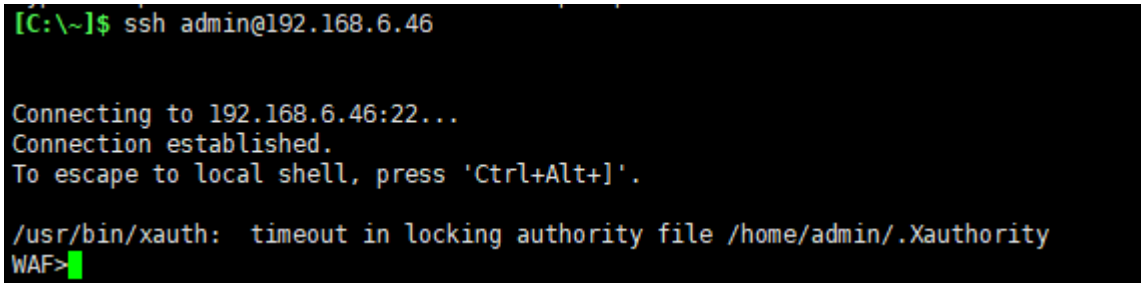
(2) 搭建 ftp 服务器，在 ftp 服务器目录放置 first 包和 system 升级包

图5-3 搭建 FTP 服务器目录下文件



(3) 使用 ssh 登陆 H3C SecPath Web 应用防火墙系统

图5-4 ssh 登陆后台系统



(4) 使用命令行先升级 first 包（保留网络配置）

注：如果不打 first，无法保留网络配置

图5-5 升级 first 文件

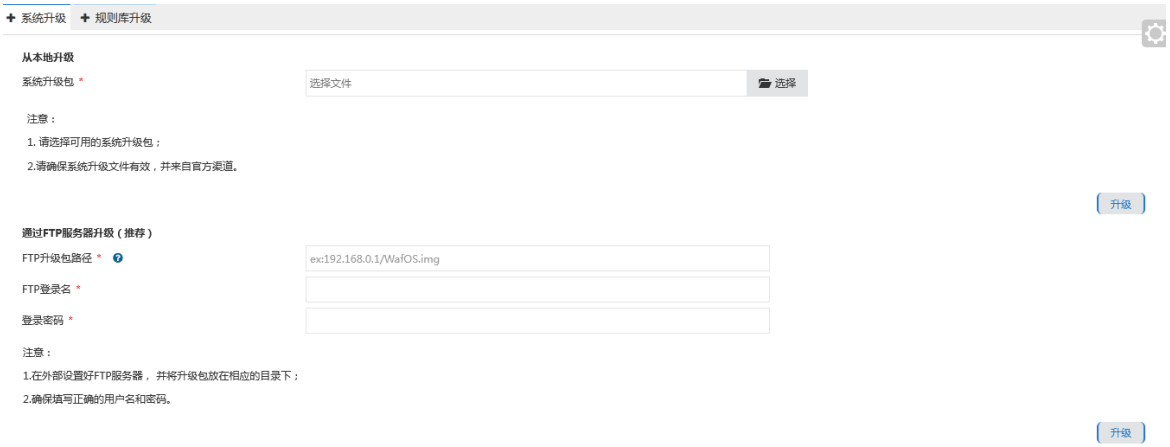
```
WAF>upgradepatch ftp://1:1@183.1.1.222:21/SecPathW2000G2-IMW310-E6204P02-6to8first.img
--2022-06-11 00:39:00--  ftp://1:*password*@183.1.1.222/SecPathW2000G2-IMW310-E6204P02-6to8first.img
           => `patch.img'
Connecting to 183.1.1.222:21... connected.
Logging in as 1 ... Logged in!
==> SYST ... done.    ==> PWD ... done.
==> TYPE I ... done.  ==> CWD not needed.
==> SIZE SecPathW2000G2-IMW310-E6204P02-6to8first.img ... 2000
==> PASV ... done.    ==> RETR SecPathW2000G2-IMW310-E6204P02-6to8first.img ... done.
Length: 2000 (2.0K) (unauthoritative)

100%[=============================================================================================================>]

2022-06-11 00:39:00 (3.10 MB/s) - `patch.img' saved [2000]

Upgrade Patch Successfully!
```

(5)　系统升级分两种方式：本地升级和 FTP 服务器升级。

- 本地升级

进入系统升级界面，点击系统升级包后【选择】按钮，选择本地的升级包后点击【升级】按钮升级系统。

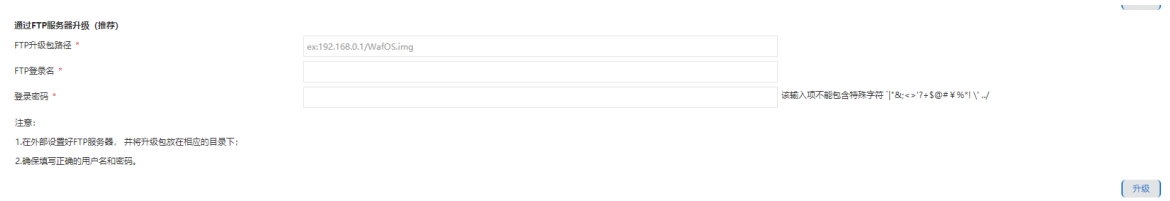
图5-6 本地升级图



- FTP 服务器升级（推荐此升级方式）

进入系统升级界面， 设置好 FTP 服务器，并将系统升级包放在相应目录下后，在界面中输入 FTP 升级路径、FTP 登录名和登录密码，点击【升级】按钮执行升级。

图5-7 FTP 服务器升级图




```
WAF>upgradesystem ftp://1:1@183.1.1.222:21/SecPathW2000G2-IMW310-E6204P02-6to8system.img
    Not Probe a hardware disk
Clean to upgrade file
--2022-06-11 00:41:30--  ftp://1:*password*@183.1.1.222/SecPathW2000G2-IMW310-E6204P02-6to8system.img
           => `SecPathW2000G2-IMW310-E6204P02-6to8system.img'
Connecting to 183.1.1.222:21... connected.
Logging in as 1 ... Logged in!
==> SYST ... done.    ==> PWD ... done.
==> TYPE I ... done.  ==> CWD not needed.
==> SIZE SecPathW2000G2-IMW310-E6204P02-6to8system.img ... 1350517344
==> PASV ... done.    ==> RETR SecPathW2000G2-IMW310-E6204P02-6to8system.img ... done.
Length: 1350517344 (1.3G) (unauthoritative)

100%[=============================================================================================>] 1,350,517,344 10.7M/s   in 2m 6s

2022-06-11 00:43:36 (10.2 MB/s) - `SecPathW2000G2-IMW310-E6204P02-6to8system.img' saved [1350517344]


****** Step 1: Prepare Upgrade ******

    Not Probe a hardware disk
Check image ...
Remove all other files ...

****** Step 2: Decrypt image ******


****** Step 3: Decompress image ******


****** Step 4: Image Check ******

System Version: 6.3.1.88162
Image Version:   8.1.6.23446-5fdad6df
This is a valid image, upgrade now ...

****** Step 5: Backup Current System ******


******  Step 6: Update Bootloader ******


Congratulations! New system installed successfully!

If there is problem, you can rollback the system!
```

(6)　升级成功后使用默认账户密码 admin/admin 进行登录

升级成功版本号为 E6204P02，如需进行其他升级，进入系统管理->系统升级界面，选择对应升级包后，直接升级即可

图5-8 界面

4. E6204 或者 E6204L01 升级至 E6204P02 升级步骤

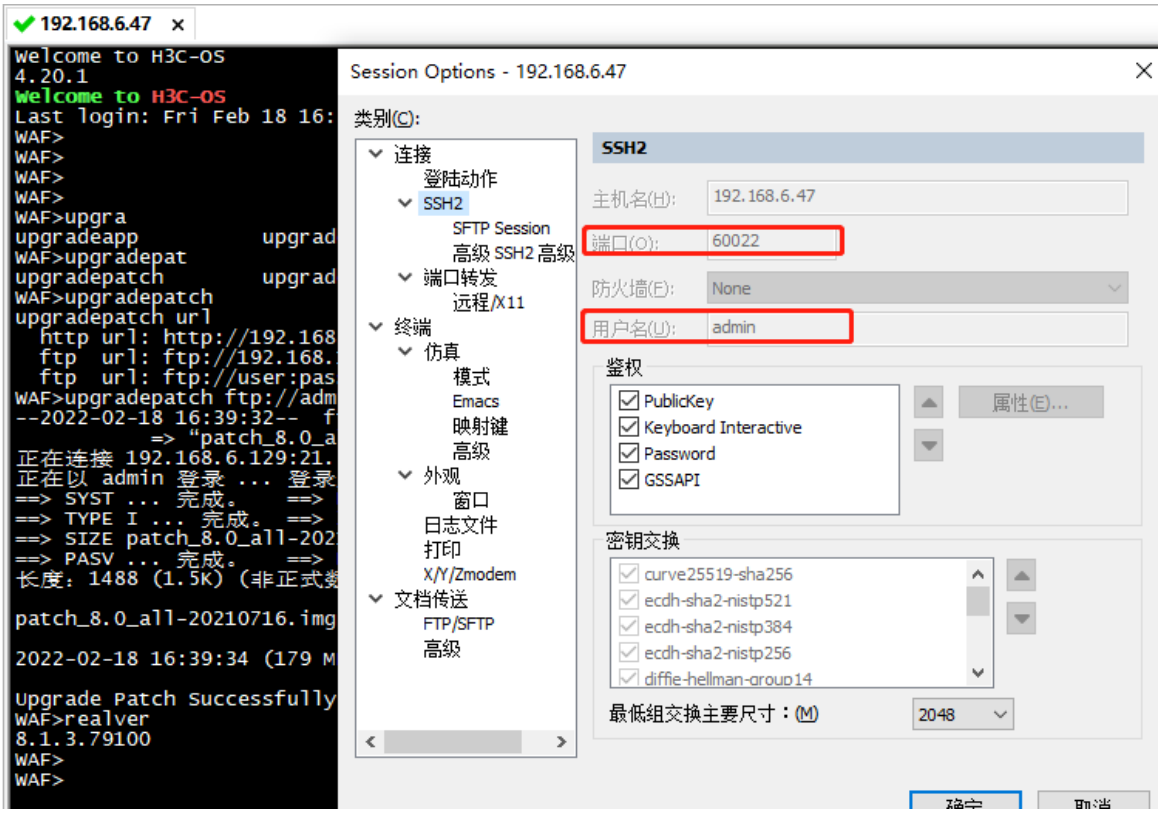
(7)　搭建 ftp 服务器，在 ftp 服务器目录放置 first 包和 system 升级包

图5-9 搭建 FTP 服务器目录下文件

(8)　使用 ssh 登陆 H3C SecPath Web 应用防火墙系统

图5-10 ssh 登陆后台系统

默认登录账号密码为 admin/WafAdmin!，如果已经修改使用修改后的密码



(9) 使用命令行先升级 first 包（保留网络配置）

命令行举例：

Upgradepatch ftp://admin:admin@101.1.15.2/6204P02/huiguiyi/SecPathW2000G2-IMW310-E6204P02-8to8first.img

图5-11 升级 patch

(10) 系统升级：本地升级和 FTP 服务器升级

- 本地升级

使用 admin 账号登录 H3C SecPath Web 应用防火墙系统， 系统管理>升级管理 。选择所需升级包后点击【升级】，跳出弹框警告“确保选择的升级包版本更新，否则可能出现未知问题”，点击【确认】。升级大致需要 30 分钟左右，请耐心等待，直至可 ping 通管理地址。

图5-12 本地升级图

- FTP 服务器升级（推荐使用）

推荐使用此种升级方式，可在命令行下查看升级包升级进度。若硬件接串口线通过命令行升级可查看升级后重启过程，便于掌握升级进度。命令 upgradeapp ftp://admin:admin@101.1.15.2/6204P02/huiguiyi/SecPathW2000G2-IMW310-E6204P02-8to8system.img (注意：admin:admin 分别指的是 FTP 服务器的用户名和密码，101.1.15.2 为 FTP 服务器的 IP 地址，后面跟升级包所在路径)

图5-13 FTP 升级


```
WAF>upgradeapp ftp://admin:admin@101.1.15.2/6204P02/huiguiyi/SecPathW2000G2-IMW310-E6204P02-8to8system.img
        Not Probe a hardware disk
--2022-06-11 10:18:46--  ftp://admin:*password*@101.1.15.2/6204P02/huiguiyi/SecPathW2000G2-IMW310-E6204P02-8to8system.img
           => "SecPathW2000G2-IMW310-E6204P02-8to8system.img"
正在连接 101.1.15.2:21... 已连接。
正在以 admin 登录 ... 登录成功!
==> SYST ... 完成。   ==> PWD ... 完成。
==> TYPE I ... 完成。  ==> CWD (1) /D:/WAF_G2/6204P02/huiguiyi ... 完成。
==> SIZE SecPathW2000G2-IMW310-E6204P02-8to8system.img ... 711461323
==> PASV ... 完成。    ==> RETR SecPathW2000G2-IMW310-E6204P02-8to8system.img ... 完成。
长度：711461323 (679M) (非正式数据)

SecPathW2000G2-IMW310-E6204P02-8to8system 100%[=============================================================================================>] 678.50M  13.3MB/s  用时 47s

2022-06-11 10:19:33 (14.5 MB/s) - "SecPathW2000G2-IMW310-E6204P02-8to8system.img" 已保存 [711461323]

parsing check header...
summary:
    md5sum:          e019f64c245a8e0c61d1e4a65f961e12
    product:         waf
    depends:
    current version: 8.1.3.79100

****** Step 1: Prepare Upgrade ******

Check image ...
Remove all other files ...

****** Step 2: Decrypt image ******


Congratulations! New system installed successfully!

Reboot to use the new system now...
WAF>
```

(11) 升级成功后使用默认账户密码 admin/admin 进行登录

升级成功版本号为 E6204P02，如需进行其他升级，进入系统管理->系统升级界面，选择对应升级包后，直接升级即可

图5-14 界面

a) 注意事项

a) 升级过程中保证设备不要断电。

- 升级过程中设备会重新启动。
- **如果使用到万兆光口，升级到 E6204P02 版本后，需要设备断电重启**

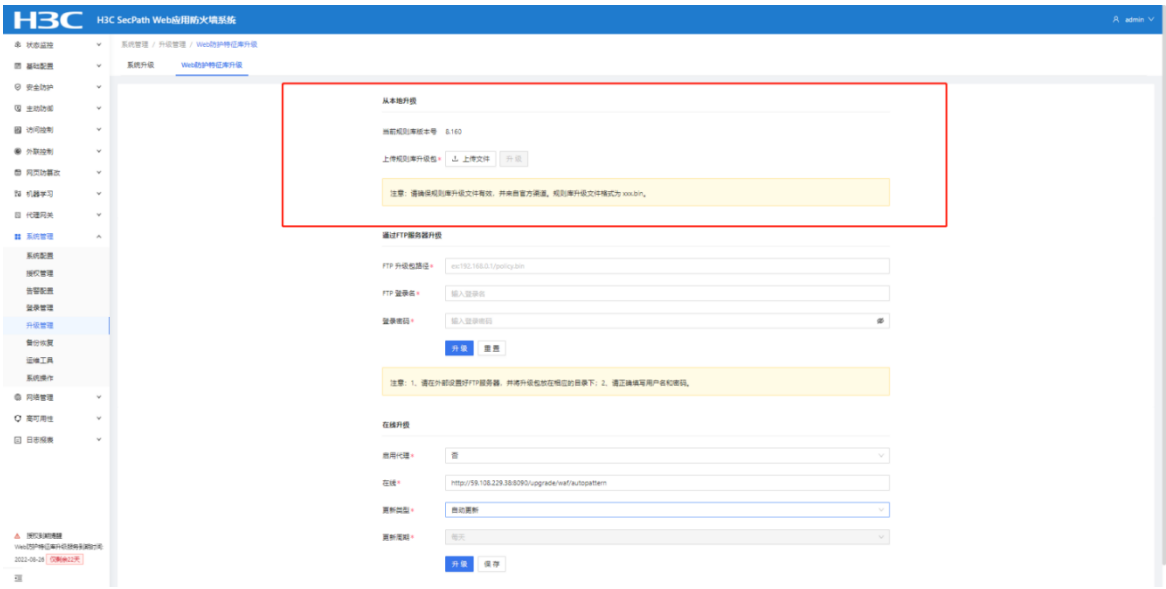
5.2 规则库升级

规则库升级分三种方式：规则库本地升级和规则库在线自动升级，以及通过 FTP 升级。

1. 规则库离线升级

选择“在线升级->规则库升级”进入规则库升级管理界面，点击【选择】按钮选择本地的规则库升级包后点击【升级】按钮升级规则库。

图5-1 规则库离线升级

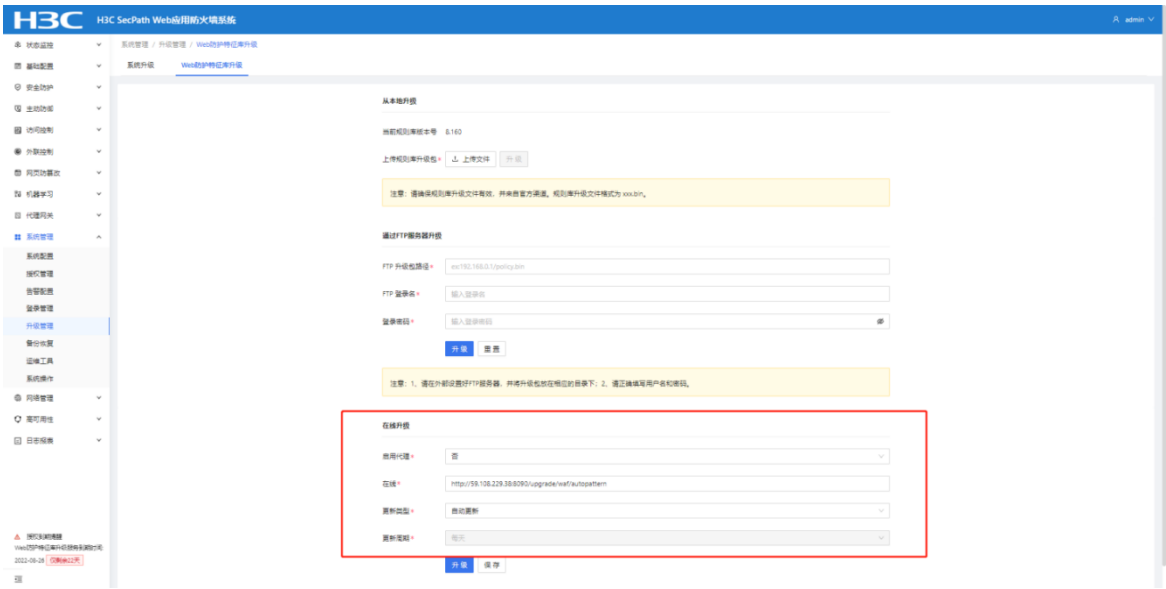


2. 规则库在线自动升级

支持互联网在线更新规则库，前提是所部署的 WAF 的管理 IP 允许访问互联网

使用默认的在线升级链接，手动点击【升级】按钮升级规则库或者按照默认周期在线自动升级

图5-2 规则库在线升级



3. 通过 FTP 服务器升级

图5-3 规则库在线升级

备注：在线自动升级是每天的凌晨 6 点 25 分自动连接升级服务器，获取最新的规则库

6 WEB 应用防火墙部署

6.1 部署方式说明

产品支持串联与旁路部署两种部署方式，6种工作模式。包括串联部署中的：透明流模式、透明代理模式、串联反向代理模式；旁路部署的：镜像检测模式、镜像检测&阻断模式、旁路反向代理模式（物理位置为旁路，实际逻辑位置为，需要配置代理服务器）。

1. 透明流模式

透明流模式是H3C SecPath Web应用防火墙在网站防护中常用的部署模式，设备串联在网络中，通过流检测引擎对数据流进行解析，匹配规则与自定义策略，进行安全防护。当检测到报文中有攻击流量时，WAF会分别向客户端和服务器发送了RST报文，断开TCP连接。

- 部署优点

  透明流模式部署简单，不改变拓扑结构，部署后网络无感知，支持软硬件 Bypass，保证高可用性，支持的防护功能较全面，可支持网段和多端口防护策略，性能高。

- 部署劣势

  1、不支持 HTTPS，因为不拆包，检测效果较透明代理要差一些。

  2、对被保护服务器没有隐藏能力，源服务器地址还是会被前端发现。

- 支持功能

  HTTP 协议校验、SQL 注入防护、XSS 防护、命令注入防护、组件漏洞防护、Web 扫描防护、XPATH 注入防护、XML 注入防护、SSI 注入防护、JSON 注入防护、LDAP 注入防护、Webshell 防护、Web 敏感信息防护、弱密码检测、CGI 安全防护、跨站请求伪造防护、业务流程控制、DDOS 攻击防护、爬虫陷阱、安全扫描。

- 支持协议

HTTP

- 特点

  Web 应用防火墙无需配置业务 IP，需配置管理 IP。

- 推荐场景

  对性能要求高且无 HTTPS 需求的场景

2. 透明代理模式

透明代理模式是H3C SecPath Web应用防火墙在网站防护中常用的部署模式，WAF串联在网络中，基于TCP数据包的检测，采用代理转发的技术，通过内部代理拆包解包，对应用层数据进行解析，并匹配安全策略，客户端访问真实服务器地址，数据包至WAF时记录访问的源地址，内部数据转发往服务器时，封装数据包为访问者的源地址，从而实现透明代理。当检测到报文中有攻击流量时，WAF向客户端返回HTTP响应码400，带有攻击语句的HTTP请求数据并未转发给服务器。

- 部署优势

  透明代理模式防护效果好，不改变拓扑结构，部署后客户端、服务器都无感知，支持软硬件 Bypass，保证高可用性，支持的防护功能全面，检测效果优于透明流模式，支持 HTTPS。

- 部署劣势

  1、性能较透明流低一些。

  2、对被保护服务器没有隐藏能力，源服务器地址还是会被前端发现。

- 支持功能

  HTTP 协议校验、SQL 注入防护、XSS 防护、命令注入防护、组件漏洞防护、Web 扫描防护、XPATH 注入防护、XML 注入防护、SSI 注入防护、JSON 注入防护、LDAP 注入防护、Webshell 防护、Web 敏感信息防护、中间件信息保护、数据库信息保护、隐私信息防护、弱密码检测、CGI 安全防护、会话安全防护、暴力破解防护、识别防护、跨站请求伪造防护、业务流程控制、DDOS 攻击防护、爬虫陷阱、虚拟补丁、安全扫描。

- 支持协议

  HTTP、HTTPS

- 特点

  Web 应用防火墙无需配置业务 IP，需配置管理 IP。

- 推荐场景

  对防护效果要求较高的场景。

3. 串联反向代理模式

WAF串联反向代理模式，需要将WAF串联到组网中，与透明代理的区别是，串联反向代理网桥上需要配置IP地址。当检测到报文中有攻击流量时，WAF向客户端返回HTTP响应码400，带有攻击语句的HTTP请求数据并未转发给服务器。

- 部署优势

  1、需要有一个业务 IP 与后端 server 通信。

  2、串联到用户网络，可实现硬件 bypass 功能。

- 部署劣势

需要配置代理服务器，客户端访问 WAF 的代理服务器地址。

- 支持功能

  HTTP 协议校验、SQL 注入防护、XSS 防护、命令注入防护、组件漏洞防护、Web 扫描防护、XPATH 注入防护、XML 注入防护、SSI 注入防护、JSON 注入防护、LDAP 注入防护、Webshell 防护、Web 敏感信息防护、中间件信息保护、数据库信息保护、隐私信息防护、弱密码检测、CGI 安全防护、会话安全防护、暴力破解防护、识别防护、跨站请求伪造防护、业务流程控制、DDOS 攻击防护、爬虫陷阱、虚拟补丁、安全扫描。

- 支持协议

  HTTP、HTTPS、。

- 特点

  Web 应用防火墙需配置业务 IP，需配置管理 IP。

- 推荐场景

串联环境下有 HTTPS 需求

4. 旁路反向代理模式

WAF 旁路在网络中，基于 TCP 数据包的检测，采用代理转发的技术。客户端访问地址为 WAF 的 IP 地址，请求至 WAF 后由 WAF 代理转发，以自身的 IP 地址向服务器发起请求，服务器回包时回给 WAF，由 WAF 再封装数据包，以 WAF 的 IP 地址回复客户端。当检测到报文中有攻击流量时，WAF 向客户端返回 HTTP 响应码 400，带有攻击语句的 HTTP 请求数据并未转发给服务器。

- 部署优势
  - 仅 HTTP/HTTPS 流量上 WAF，不影响其他流量。
  - 支持 HTTPS 防护。
- 部署劣势

  串联反向代理存在单点故障问题，一旦 WAF 出现故障会影响服务器正常访问。

- **支持功能**

  HTTP 协议校验、SQL 注入防护、XSS 防护、命令注入防护、组件漏洞防护、Web 扫描防护、XPATH 注入防护、XML 注入防护、SSI 注入防护、JSON 注入防护、LDAP 注入防护、Webshell 防护、Web 敏感信息防护、中间件信息保护、数据库信息保护、隐私信息防护、弱密码检测、CGI 安全防护、会话安全防护、暴力破解防护、识别防护、跨站请求伪造防护、业务流程控制、DDOS 攻击防护、爬虫陷阱、虚拟补丁、安全扫描。

- 支持协议

  HTTP、HTTPS。

- 特点

  Web 应用防火墙需配置业务 IP，需配置管理 IP。

- 推荐场景

有 HTTPS 需求，混合流量中除 HTTP 外其他流量较大的场景。

5. 旁路镜像检测模式

旁路镜像检测模式是 H3C SecPath Web 应用防火墙在网站防护中常用的部署模式，设备旁路部署在网络中，通过流检测引擎对数据流进行解析，匹配规则与自定义策略进行安全检测，旁路镜像检测模式只进行检测，不对攻击进行处理。

- 部署优势

  不改变网络拓扑结构，部署最方便快捷，只需将交换机进/出口双向流量镜像给 WAF 设备进行攻击检测不参与业务数据流转发，因此设备故障对业务无影响。

- 部署劣势
  - 无法对攻击进行阻断。
  - 不支持 HTTPS。
- 支持检测功能
- HTTP 协议校验、SQL 注入防护、XSS 防护、命令注入防护、组件漏洞防护、Web 扫描防护、XPATH 注入防护、XML 注入防护、SSI 注入防护、JSON 注入防护、LDAP 注入防护、Webshell 防护、Web 敏感信息防护、数据库信息保护、弱密码检测、CGI 安全防护、跨站请求伪造防护、业务流程控制、DDOS 攻击防护、安全扫描。
- 支持协议

  HTTP。

- 特点

  Web 应用防火墙无需配置业务 IP，需配置管理 IP。

- 使用场景

  旁路镜像场景。

6. 旁路镜像检测&阻断模式

旁路镜像检测&阻断模式是H3C SecPath Web应用防火墙在网站防护中常用的部署模式，设备旁路部署在网络中，通过流检测引擎对数据流进行解析，匹配规则与自定义策略进行安全防护。当检测到报文中有攻击流量时，WAF分别以服务器的地址向客户端，以客户端地址向服务器发送RST报文，断开连接。

- 部署优势

  旁路镜像检测&阻断模式部署简单，不改变拓扑结构，部署后网络无感知，支持的防护功能较全面，可支持网段和多端口防护策略，性能高。

- 部署劣势
  - 由于发送 reset 报文滞后性，无法达到 100%阻断。
  - 不支持 HTTPS。
- 支持功能
- HTTP 协议校验、SQL 注入防护、XSS 防护、命令注入防护、组件漏洞防护、Web 扫描防护、XPATH 注入防护、XML 注入防护、SSI 注入防护、JSON 注入防护、LDAP 注入防护、Webshell 防护、Web 敏感信息防护、数据库信息保护、弱密码检测、CGI 安全防护、跨站请求伪造防护、业务流程控制、DDOS 攻击防护、安全扫描。
- **支持协议**

  HTTP

- 特点

  Web 应用防火墙无需配置通信 IP，需配置管理 IP。

- 推荐场景

旁路镜像并提供一定的防护能力，但此场景防护效果不能达到百分百。

7. 关于串联反向代理模式与透明代理模式的不同点的说明

- 网络配置上，透明代理模式不需要在业务桥上配置业务 ip，而串联反向代理模式需要在业务桥上配置业务 ip；
- 服务器配置上，透明代理模式下，“客户端 IP 还原”选择“是”，意思是，WAF 以客户端 IP 与防护服务器建链接通信；串联反向代理模式下，“客户端 IP 还原”选择“否”，意思是 WAF 以自身的业务 IP 与防护服务器建链接，防护服务器看不到客户端的地址。
- 原理上，透明代理模式下，WAF 分别与客户端、服务器建链接，其中 WAF 伪装成服务器地址与客户端建链接，WAF 伪装成客户端地址与服务器建链接；串联反向代理模式下，WAF 分别与客户端、服务器建链接，其中 WAF 伪装成服务器地址与客户端建链接，WAF 以自身的业务地址与服务器建链接；
- 功能支持度上，各个模式支持的防护功能或其他功能有所差异，具体内容详见规格表描述。

6.2 部署模式推荐

- 如果防护站点不涉及 HTTPS 站点时，串联组网一般推荐透明流，部署简单，并且支持网段防护；
- 其次是代理模式，理由是防护效果好，稳定性好；
- 如果防护站点含有 HTTPS 时，串联组网下，可以使用透明代理或串联反向代理模式；
- 旁路组网一般推荐旁路反向代理模式，该模式也支持防护 HTTPS 和 ipv6 站点；
- 旁路镜像检测模式仅具有检测功能，无防护功能；
- 串联组网下，推荐使用成对的 Bypass 口；
- 旁路镜像检测&阻断模式具有检测和防护功能，但防护级别低，无法实现 100%阻断；

表6-1 部署模式推荐表

部署模式		支持功能	支持协议	部署优势	部署劣势	推荐场景
串联部署	透明流模式	HTTP协议校验、SQL注入防护、XSS防护、命令注入防护、组件漏洞防护、Web扫描防护、XPATH注入防护、XML注入防护、SSI注入防护、JSON注入防护、LDAP注入防护、Webshell防护、Web敏感信息防护、弱密码检测、CGI安全防护、跨站请求伪造防护、业务流程控制、DDOS攻	HTTP	1、性能高 2、支持软硬件Bypass 3、支持网段防护	1、不支持HTTPS 2、因为不拆包，检测效果较透明代理差一些	对性能要求高且无HTTPS需求的场景。

		击防护、爬虫陷阱、安全扫描。				
	透明代理	HTTP协议校验、SQL注入防护、XSS防护、命令注入防护、组件漏洞防护、Web扫描防护、XPATH注入防护、XML注入防护、SSI注入防护、JSON注入防护、LDAP注入防护、Webshell防护、Web敏感信息防护、弱密码检测、CGI安全防护、会话安全防护、暴力破解防护、识别防护、跨站请求伪造防护、业务流程控制、DDOS攻击防护、负载均衡、爬虫陷阱、虚拟补丁、安全扫描。	HTTP/HTTPS	检测效果最好 2、支持软硬件Bypass	1、性能较透明流低一些	对防护效果要求高的场景
	串联反向代理	扫描防护、HTTP协议校验、HTTP 访问控制、特征防护、威胁情报、爬虫 、防盗链、CSRF、虚拟补丁防护、弱密码检测、访问顺序、文件上传、文件下载、敏感信息、敏感词防护、负载均衡、数据压缩、高速缓存、Cookie加密、cookie加固、DDoS防护	HTTP/HTTPS	支持软硬件Bypass 2、支持HTTPS 3、支持主备HA	1、需要有一个业务IP与后端server通信 2、需要配置代理服务器，客户端访问的为WAF代理服务器地址 3、对server来说，看到的client IP为WAF的IP,可在访问日志或攻击日志中查看XFF字段来溯源。 4、由于仅数量有限的代理IP与server通信，若server侧开启了DDoS策略，会造成阻断	适合串联环境下需求IPv6和HTTPS的环境 防护效果好，单台高可靠性（硬件bypass）的场景
旁路部署	旁路反向代理	扫描防护、HTTP协议校验、HTTP 访问控制、特征防护、威胁情报、爬虫 、防盗链、CSRF、虚拟补丁防护、弱密码检测、访问顺序、文件上	HTTP/HTTPS	1、仅HTTP/HTTPS流量上WAF，不影响其他流量 2、支持HTTPS和IPv6防护	旁路反向代理存在单点故障问题，一旦WAF出现故障会影响服务器正常访问	有HTTPS需求，混合流量中除HTTP外其他流量较大的场景

		传、文件下载、敏感信息、敏感词防护、负载均衡、数据压缩、高速缓存、Cookie加密、cookie加固、DDoS防护		3、支持主备HA		
	镜像检测	HTTP协议校验、HTTP访问控制、特征防护、防盗链、防跨站请求伪造、文件上传、文件下载、弱密码检测、访问顺序、敏感词防护	HTTP	1、仅需镜像流量 2、支持网段防护	1、 无法对攻击进行阻断 2、 不支持HTTPS	旁路镜像场景
	镜像阻断	HTTP 协议校验、HTTP 访问控制、特征防护、防盗链、防跨站请求伪造、文件上传、文件下载、弱密码检测、访问顺序、敏感词防护	HTTP	1、仅需镜像流量，并能实现一定的阻断效果 2、支持网段防护	1、由于发送 reset 报文滞后性，无法达到100%阻断 2、不支持 HTTPS	防护效果无法达到100%。

6.3 设备上线流程

- 收集客户需求。如是否需要 HTTPS、IPv6、主备等场景。
- 确定设备部署位置，推荐部署位置尽可能靠近服务端
- 配置好管理口地址，默认管理 IP 为 192.168.0.1，如需更改管理，可通过 console 口更改管理地址，再登录设备。
- 根据需求搭建组网，确保路由正常，客户端至 WAF，WAF 至 server 均路由可达，请求和响应双向流量均经过 WAF。
- 将新上线的 WAF 升级到现网发布最新版本，确保设备是最新版本之后配置功能。
- 先配置防护站点，确定部署模式，再对防护站点配置防护策略，可以选择低级规则或监控规则。
- 可以参照匹配到的日志，根据客户需求调整防护策略，可以先试运行一段时间，如果怕影响业务可以将防护策略选择监控规则。
- 可以观察日志，然后判断是否影响业务的策略，如果有，通过分析日志，调整相应的策略，具体可以参照对外测试手册，将对应的策略动作例外放行或者关闭策略，或者加入黑白名单，实在不确认可以抓取报文，联系华三技术人员处理，分析是否是误报等。

7 透明流模式部署配置举例

7.1 简介

透明流模式是 H3C SecPath Web 应用防火墙在网站防护中常用的部署模式，设备串联在网络中，通过流检测引擎对数据流进行解析，匹配规则与自定义策略，进行安全防护。

透明流模式部署简单，不改变拓扑结构，部署后网络无感知，支持软硬件 Bypass，保证高可用性，支持的防护功能较全面，可支持网段和多端口防护策略，性能高。

支持防护功能：协议合规检测、web 攻击防护、web 业务控制、web 敏感信息防护、web 业务加固（部分支持，仅支持弱密码检测、CGI 安全防护、跨站请求防护及业务流程控制）、DDOS 防护、爬虫陷阱。

支持协议：HTTP。

特点：WAF 无须配置通信 IP，需配置管理 IP。

7.2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

7.3 使用限制

WAF 接入网络过程中会造成短暂断网，需提前划分好网桥和网络接口。

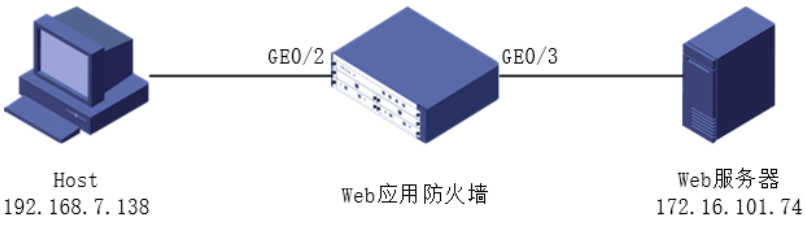
7.4 适用产品和版本

E6204P02 及以后版本。

7.5 组网需求

如下图所示，WAF 部署在核心交换机和服务器区交换机之间，串联接入网络，对 Web 服务器进行防护。

图7-1 组网图



7.6 配置思路

按照组网图组网。

(1)　登录 WAF。

(2) 创建新的网桥，并把接入网络的两个 port 口划分到新网桥中。

(3) 配置部署模式。

(4) 配置防护资产，引用防护策略。

7.7 配置步骤

1. 登录 WAF

如下图所示，使用 https 的方式登录 WAF，输入用户名和密码 admin/admin，并点击<登录>按钮。

注意：首次登录强制修改密码。

图7-2 登录 WAF

2. 创建新的网桥，并把接入网络的两个 port 口划分到新网桥中

如下图所示，在“网络管理>网络配置>网桥接口”中，点击增加，创建网桥“br10”。

图7-3 新建网桥-br10

如下图所示，网桥 br10 中不需要配置 IP 地址，点击保存。

图7-4 保存网桥配置

如下图所示，在“网络管理>网络配置>Port 接口”中编辑 port 接口，接口 GE0/2 和 GE0/3 的“网桥接口”选择 br10。

图7-5 port 口划分到新网桥

3. 配置部署模式

如下图所示，选择菜单“基础配置>部署模式”进入部署模式配置页面，选择“串联”部署模式，选择完成后保存配置。

图7-6 选择串联部署模式

4. 配置防护资产，引用防护策略

如下图所示，选择菜单“基础配置>防护资产”进入防护资产配置页面，点击添加，新建防护资产，配置资产的同时即可引用对应的防护资产。

图7-7 创建防护资产

在防护模块部分，根据需要进行防护策略的配置，配置完成后点击保存。

图7-8 配置安全防护策略

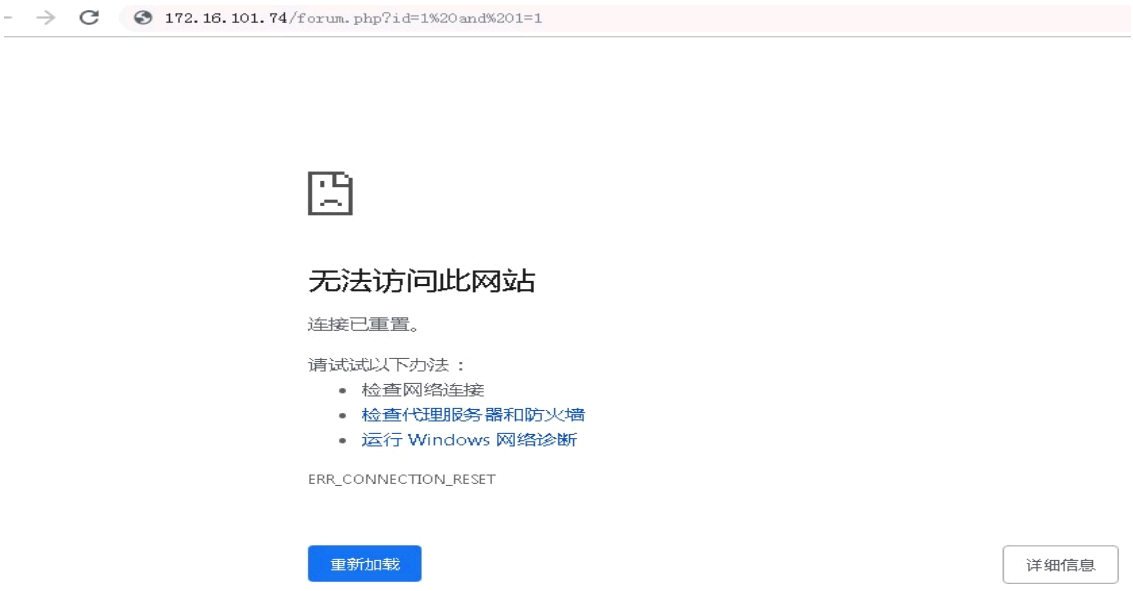
7.8 验证配置

(1) 访问受保护的网站，URL 为 http://172.16.101.74，可以正常访问。

图7-9 网站可以访问

(2) 加上攻击参数再次访问网站，URL 为 http://172.16.101.74/forum.php?id=1 and 1=1，网站不能访问。

图7-10 网站无法访问



(3) 选择"日志报表>防护日志"，查看攻击日志，可以看到攻击拦截的详细信息，证明 WAF 已经正常防护。

图7-11 拦截信息

8 透明代理模式部署配置举例

8.1 简介

透明代理模式是 H3C SecPath Web 应用防火墙在网站防护中常用的部署模式，WAF 串联在网络中，基于 TCP 数据包的检测，采用代理转发的技术，通过内部代理拆包解包，对应用层数据进行解析，并匹配安全策略，客户端访问真实服务器地址，数据包至 WAF 时记录访问的源地址，内部数据转发往服务器时，封装数据包为访问者的源地址，从而实现透明代理。

透明代理模式防护效果好，不改变拓扑结构，部署后客户端、服务器都无感知，支持软硬件 Bypass，保证高可用性，支持的防护功能全面，检测效果优于透明流模式。

支持功能：协议合规检测、web 攻击防护、web 业务控制、web 敏感信息防护、web 业务加固、DDOS 防护、爬虫陷阱、虚拟补丁。

支持协议：HTTP、HTTPS。

特点：WAF 无须配置通信 IP，需配置管理 IP。

8.2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

8.3 使用限制

WAF 接入网络过程中会造成短暂断网，需提前划分好网桥和网络接口。

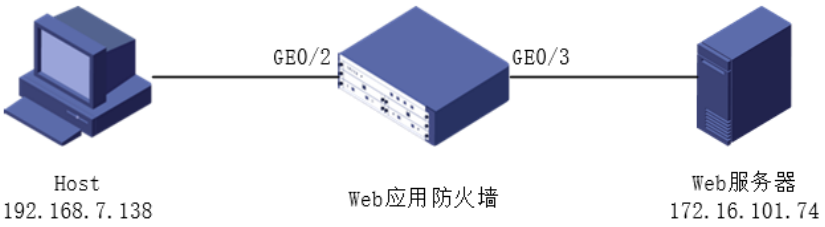
8.4 适用产品和版本

E6204P02 及以后版本。

8.5 组网需求

如下图所示，WAF 部署在核心交换机和服务器区交换机之间，串联接入网络，对 Web 服务器进行防护。

图8-1 组网图



8.6 配置思路

按照组网图组网。

(1) 登录 WAF。

(2) 创建新的网桥，并把接入网络的两个 port 口划分到新网桥中。

(3) 配置部署模式。

(4) 配置防护资产，引用防护策略。

(5) 配置代理网关规则。

8.7 配置步骤

1. 登录 WAF

如下图所示，使用 https 的方式登录 WAF，输入用户名和密码 admin/admin，并点击<登录>按钮。

注意：首次登录强制修改密码。

图8-2 登录 WAF

2. 创建新的网桥，并把接入网络的两个 port 口划分到新网桥中

如下图所示，在“网络管理>网络配置>网桥接口”中，点击增加，创建网桥 br10。

图8-3 新建网桥-br10

如下图所示，网桥 br10 中不需要配置 IP 地址，点击保存。

图8-4 保存网桥配置

如下图所示，在“网络管理>网络配置>Port 接口”中编辑 port 接口。接口 GE0/2 和 GE0/3 的“网桥接口”选择 br10。

图8-5 port 口划分到新网桥

3. 配置部署模式

如下图所示，选择菜单“基础配置>部署模式”进入部署模式配置页面，选择“串联”部署模式，选择完成后保存配置。

图8-6 选择串联部署模式

4. 配置防护资产，引用防护策略

如下图所示，选择菜单“基础配置>防护资产”进入防护资产配置页面，点击添加，新建防护资产，配置资产的同时即可引用对应的防护资产。

图8-7 创建防护资产

在防护模块部分，根据需要进行防护策略的配置，配置完成后点击保存。

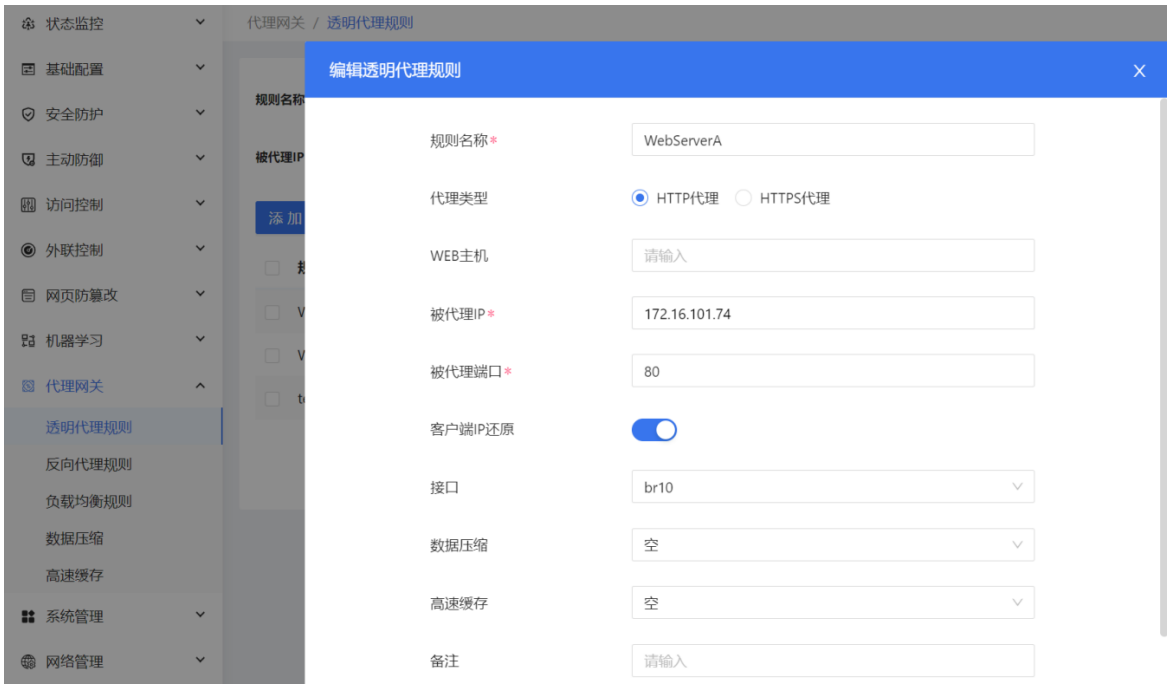
图8-8 配置安全防护策略

5. 配置代理网关规则

A.HTTP 配置

如下图所示，选择“代理网关>透明代理规则”进入透明代理规则配置页面，点击添加，新建透明代理规则，接口选择业务网桥 br10，客户端 IP 还原功能开启，具体配置如下：

图8-9 配置透明代理网关

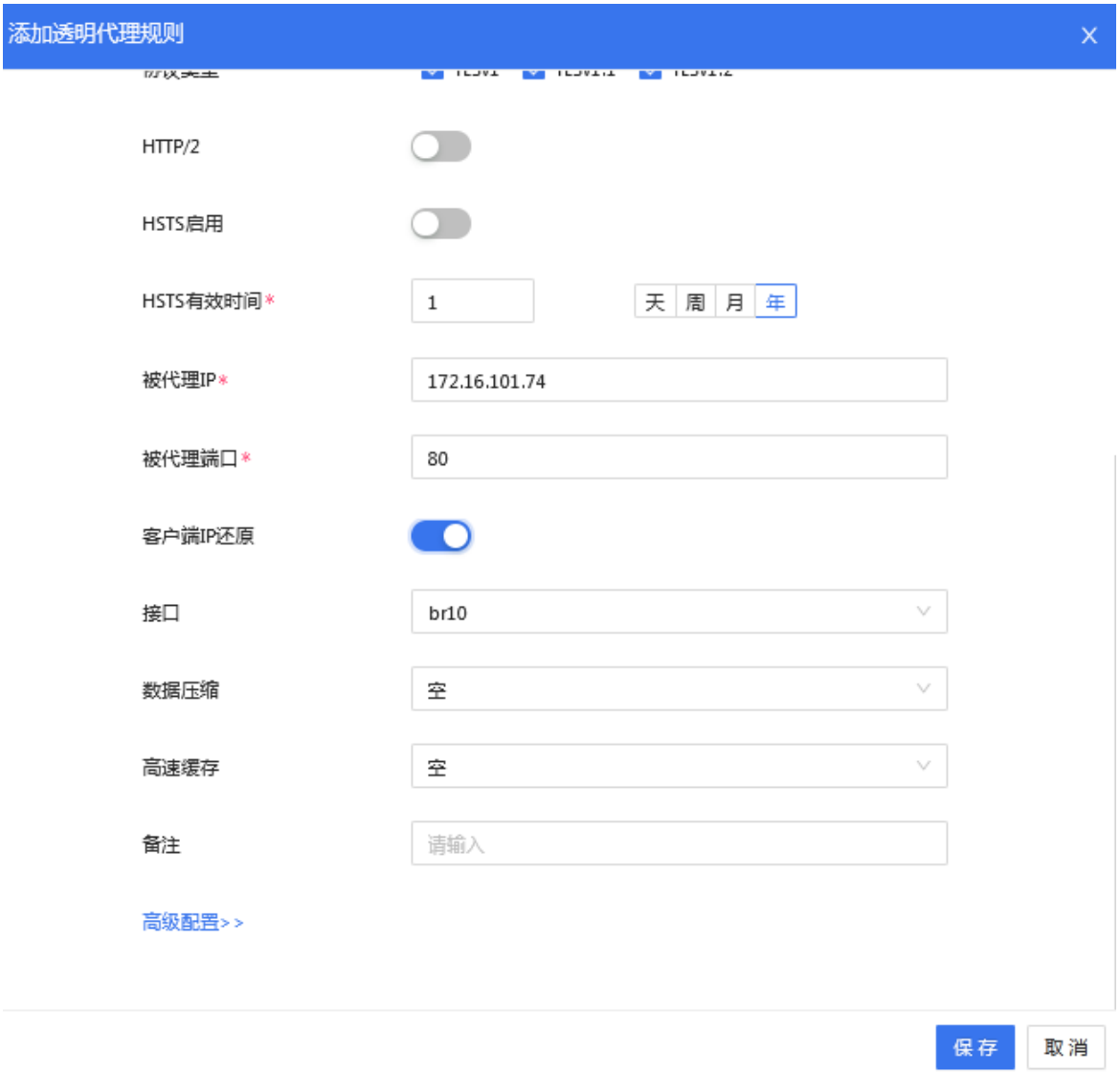


B.HTTPS 配置

如下图所示，选择“代理网关>透明代理规则”进入透明代理规则配置页面，点击添加，新建透明代理规则，接口选择业务网桥 br10，客户端 IP 还原功能开启，如果不设置域名，则对配置的 ip 地址进行防护，以及 IP 地址相关域名也可以防护；如果配置域名，则仅对域名进行防护。针对一个 Web 服务器绑定多个域名的场景，可以根据需求在域名类型中配置“单域名”或者“多域名”，上传对应的证书即可。此时，WAF 只防护配置中的域名，当客户端使用其他域名或使用 ip 访问/攻击时，不进行检测防护，具体配置如下：

图8-10 配置信息


添加透明代理规则
规则名称*
WebServerA
代理类型
HTTP代理
HTTPS代理
域名类型
单域名
多域名
WEB主机
请输入
证书格式
PEM
DER
PKCS12
ssl站点密钥（.key）*
上传文件
xbtest.key
ssl站点证书*
上传文件
（证书常用后缀：.pem .crt .cer）
xbtest.crt
协议类型
TLSv1
TLSv1.1
TLSv1.2
HTTP/2
HSTS启用
HSTS有效时间*
1
天
周
月
年
保存
取消



8.8 验证配置

(1) 以 http 为例，访问受保护的网站，URL 为 http://172.16.101.74，可以正常访问。

图8-11 网站可以访问

(2) 加上攻击参数再次访问网站，URL 为 http://172.16.101.74/forum.php?id=1 and 1=1，网站不能访问。

图8-12 网站无法访问

(3) 选择"日志报表>防护日志"，查看攻击日志，可以看到攻击拦截的详细信息，证明 WAF 已经正常防护。

图8-13 拦截信息

9 串联反向代理模式部署配置举例

9.1 简介

串联反向代理模式是 H3C SecPath Web 应用防火墙在网站防护中常用的部署模式，WAF 串联在网络中，基于 TCP 数据包的检测，采用代理转发的技术，通过内部代理拆包解包，对应用层数据进行解析并匹配安全策略。

客户端访问地址为真实服务器地址，当请求流经 WAF 时由 WAF 代理转发，服务器响应时首先回给 WAF，由 WAF 再封装数据包，以真实服务器地址转发给客户端，从而实现客户端请求服务器时的无感知透明转发。

串联反向代理模式防护效果好，不改变拓扑结构，部署后客户端无感知，支持软硬件 Bypass，保证高可用性，支持的防护功能全面，检测效果优于透明流模式。

支持功能：协议合规检测、web 攻击防护、web 业务控制、web 敏感信息防护、web 业务加固、DDOS 防护、爬虫陷阱、虚拟补丁。

支持协议：HTTP、HTTPS。

特点：WAF 配置通信 IP，需配置管理 IP。

9.2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

9.3 使用限制

WAF 接入网络过程中会造成短暂断网，需提前划分好网桥和网络接口。

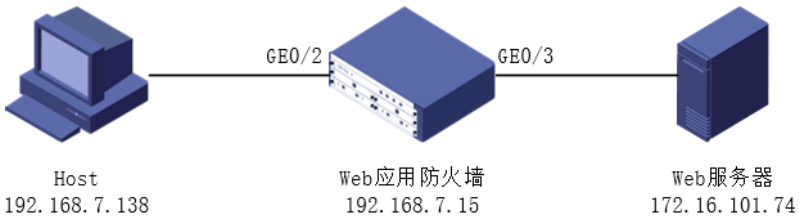
9.4 适用产品和版本

E6204P02 及以后版本。

9.5 组网需求

如下图所示，WAF 部署在核心交换机和服务器区交换机之间，串联接入网络，对 Web 服务器进行防护。

图9-1 组网图



9.6 配置思路

按照组网图组网。

(1) 登录 WAF。

(2) 创建新的网桥，并把接入网络的两个 port 口划分到新网桥中，配置 WAF 业务 IP 和路由。

(3) 配置部署模式。

(4) 配置防护资产，引用防护策略。

(5) 配置代理网关规则。

9.7 配置步骤

1. 登录 WAF

如下图所示，使用 https 的方式登录 WAF，输入用户名和密码 admin/admin，并点击<登录>按钮。

注意：首次登录强制修改密码。

图9-2 登录 WAF

2. 创建新的网桥，并把接入网络的两个 port 口划分到新网桥中。

如下图所示，在“网络管理>网络配置>网桥接口”中，点击增加，创建网桥 br10。

图9-3 新建网桥-br10

如下图所示，在创建网桥 br10 中增加业务 IP 地址。

图9-4 增加业务 IP 地址

如下图所示，在“网络管理>路由配置”中增加路由，保证和客户端和服务端路由均可达。

图9-5 增加路由

如下图所示，在“网络管理>网络配置>Port 接口”中编辑 port 接口。接口 GE0/2 和 GE0/3 的“网桥接口”选择 br10。

图9-6 port 口划分到新网桥

3. 配置部署模式

如下图所示，选择菜单“基础配置>部署模式”进入部署模式配置页面，选择“串联”部署模式，选择完成后保存配置。

图9-7 选择串联部署模式

4. 配置防护资产，引用防护策略

如下图所示，选择菜单“基础配置>防护资产”进入防护资产配置页面，点击添加，新建防护资产，配置资产的同时即可引用对应的防护资产。

图9-8 创建防护资产

在防护模块部分，根据需要进行防护策略的配置，配置完成后点击保存。

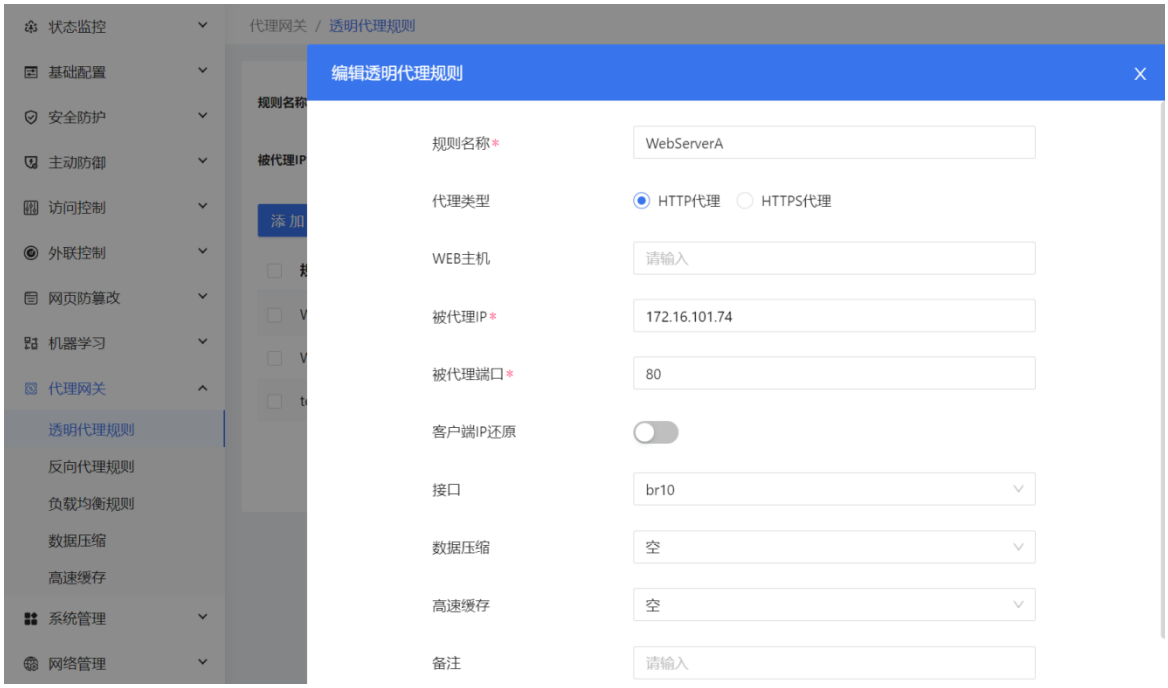
图9-9 配置安全防护策略

5. 配置代理网关规则

A.HTTP 配置

如下图所示，选择“代理网关>透明代理规则”进入透明代理规则配置页面，点击添加，新建透明代理规则，接口选择业务网桥 br10，客户端 IP 还原功能关闭，具体配置如下：

图9-10 配置串联反向代理网关

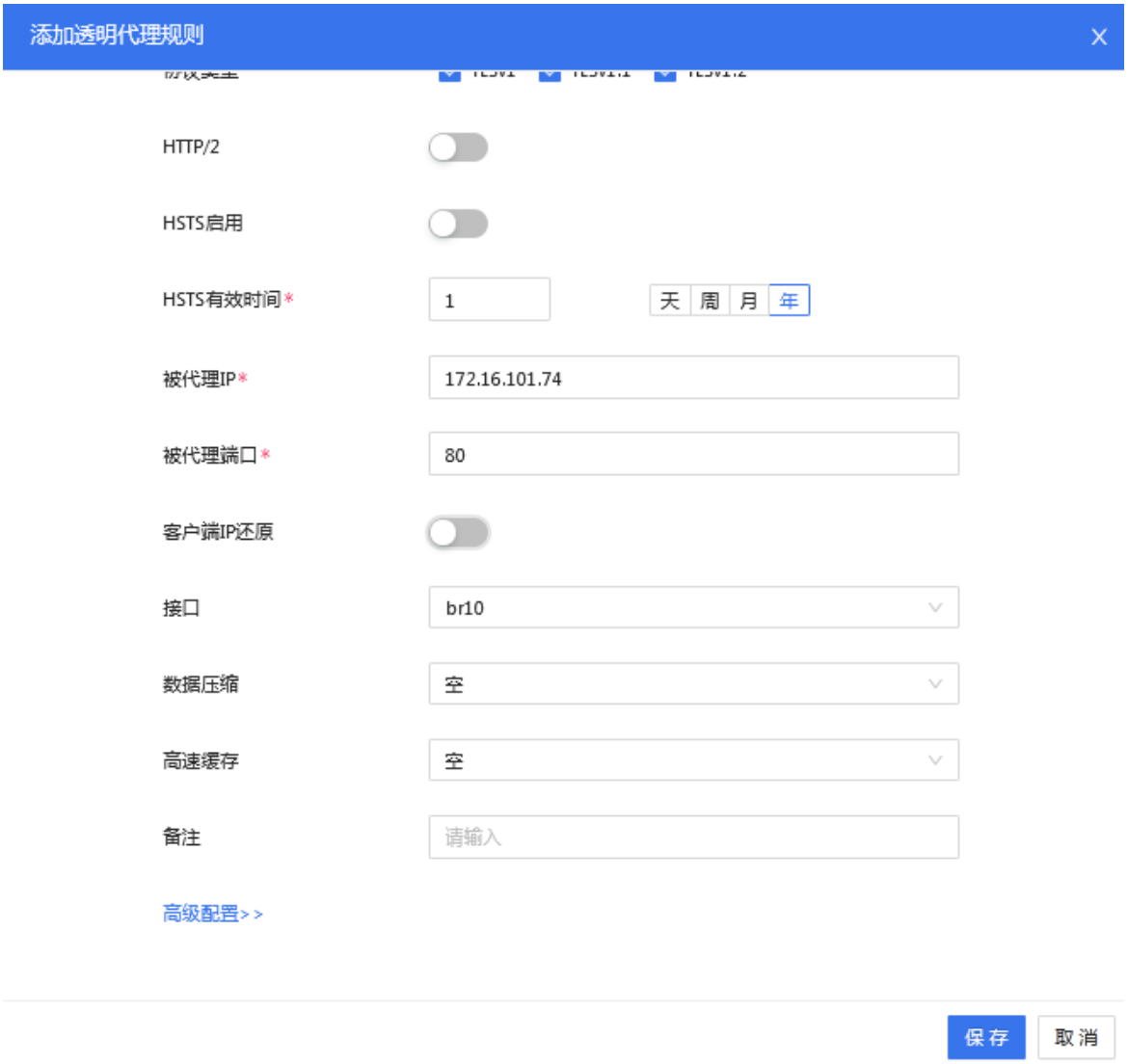


B.HTTPS 配置

如下图所示，选择“代理网关>透明代理规则”进入透明代理规则配置页面，点击添加，新建透明代理规则，接口选择业务网桥 br10，客户端 IP 还原功能关闭，如果不设置域名，则对配置的 ip 地址进行防护，以及 IP 地址相关域名也可以防护；如果配置域名，则仅对域名进行防护。针对一个 Web 服务器绑定多个域名的场景，可以根据需求在域名类型中配置“单域名”或者“多域名”，上传对应的证书即可。此时，WAF 只防护配置中的域名，当客户端使用其他域名或使用 ip 访问/攻击时，不进行检测防护，具体配置如下：

图9-11 代理规则


添加透明代理规则
规则名称*
WebServerA
代理类型
HTTP代理
HTTPS代理
域名类型
单域名
多域名
WEB主机
请输入
证书格式
PEM
DER
PKCS12
ssl站点密钥（.key）*
上传文件
xbtest.key
ssl站点证书*
上传文件
（证书常用后缀：.pem .crt .cer）
xbtest.crt
协议类型
TLSv1
TLSv1.1
TLSv1.2
HTTP/2
HSTS启用
HSTS有效时间*
1
天
周
月
年
保存
取消



9.8 验证配置

(1) 以 http 为例，访问受保护的网站，URL 为 http://172.16.101.74，可以正常访问。

图9-12 网站可以访问

(2) 加上攻击参数再次访问网站，URL 为 http://172.16.101.74?id=1 and 1=1，网站不能访问。

图9-13 网站无法访问

(3) 选择"日志报表>防护日志"，查看攻击日志，可以看到攻击拦截的详细信息，证明 WAF 已经正常防护。

图9-14 拦截信息

10 反向代理模式部署配置举例

10.1 简介

WAF 旁路在网络中，基于 TCP 数据包的检测，采用代理转发的技术。客户端访问地址为 WAF 的 IP 地址，请求至 WAF 后由 WAF 代理转发，以自身的 IP 地址向服务器发起请求，服务器回包时回给 WAF，由 WAF 再封装数据包，以 WAF 的 IP 地址回复客户端。

支持功能：协议合规检测、web 攻击防护、web 业务控制、web 敏感信息防护、web 业务加固、DDOS 防护、爬虫陷阱、虚拟补丁。

支持协议：HTTP、HTTPS。

特点：WAF 需配置通信 IP，需配置管理 IP。

10.2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

10.3 使用限制

WAF 接入网络过程中会造成短暂断网，需提前划分好网桥和网络接口。

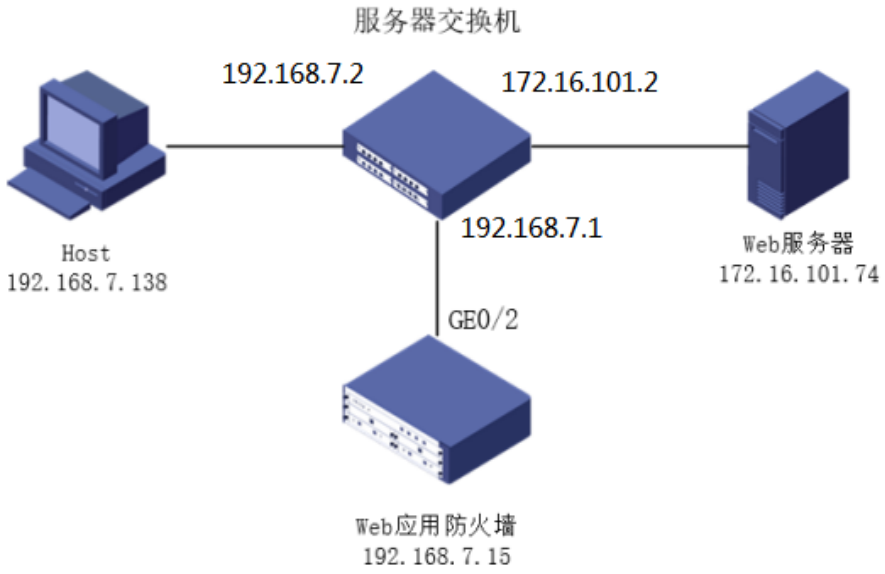
10.4 适用产品和版本

E6204P02 及以后版本。

10.5 组网需求

如下图所示，WAF 旁路部署在服务器区交换机上，对 Web 服务器进行防护。

图10-1 组网图



10.6 配置思路

按照组网图组网。

(1) 登录 WAF。

(2) 创建新的网桥，并把接入网络的两个 port 口划分到新网桥中，配置 WAF 业务 IP 和路由。

(3) 配置部署模式。

(4) 配置防护资产，引用防护策略。

(5) 配置代理网关规则。

10.7 配置步骤

1. 登录 WAF

如下图所示，使用 https 的方式登录 WAF，输入用户名和密码 admin/admin，并点击<登录>按钮。

注意：首次登录强制修改密码。

图10-2 登录 WAF

2. 创建新的网桥，并把接入网络的两个 port 口划分到新网桥中。

如下图所示，在“网络管理>网络配置>网桥接口”中，点击增加，创建网桥 br10。

图10-3 新建网桥-br10

如下图所示，在创建网桥 br10 中增加业务 IP 地址。

图10-4 增加业务 IP 地址

如下图所示，在“网络管理>路由配置”中增加路由。

图10-5 增加路由

如下图所示，在“网络管理>网络配置>Port 接口”中编辑 port 接口。接口 GE0/2 和 GE0/3 的“网桥接口”选择 br10。

图10-6 port 口划分到新网桥

3. 配置部署模式

如下图所示，选择菜单“基础配置>部署模式”进入部署模式配置页面，选择“串联”部署模式，选择完成后保存配置。

注：反向代理模式为物理旁路，逻辑串联的部署模式，因此部署模式选择串联。

图10-7 选择串联部署模式

4. 配置防护资产，引用防护策略

如下图所示，选择菜单“基础配置>防护资产”进入防护资产配置页面，点击添加，新建防护资产，配置资产的同时即可引用对应的防护资产。

图10-8 创建防护资产

在防护模块部分，根据需要进行防护策略的配置，配置完成后点击保存。

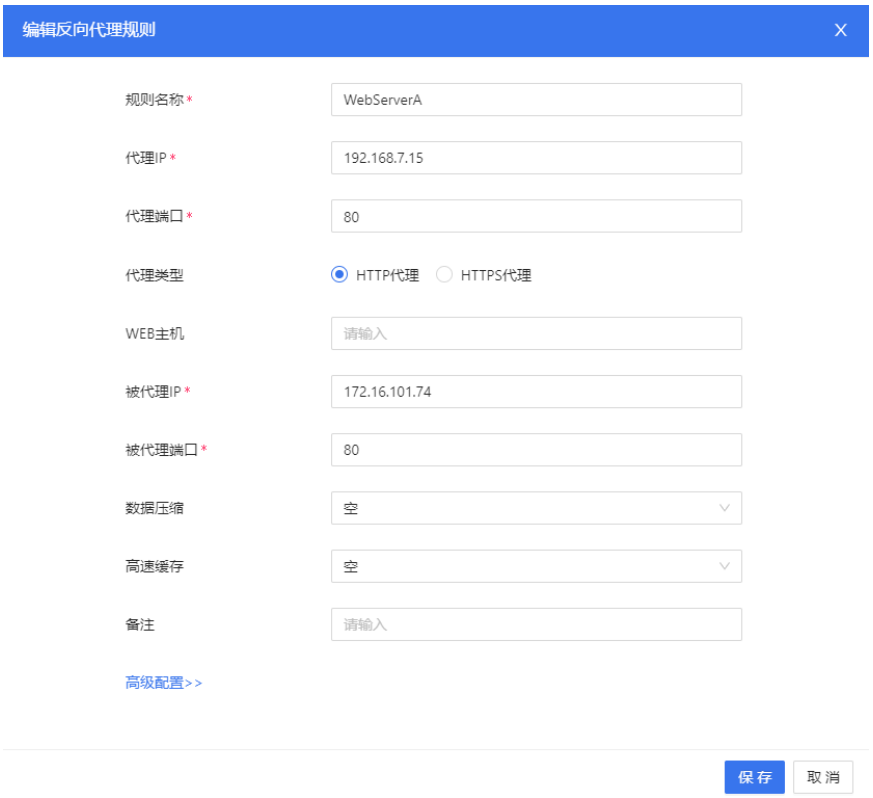
图10-9 配置安全防护策略

5. 配置代理网关规则

A.HTTP

如下图所示，选择“代理网关>反向代理规则”进入反向代理规则配置页面，点击添加，新建反向代理规则，代理 IP 选择 WAF 上配置的业务 IP，被代理 IP 填写后端真实服务器 IP，具体配置如下：

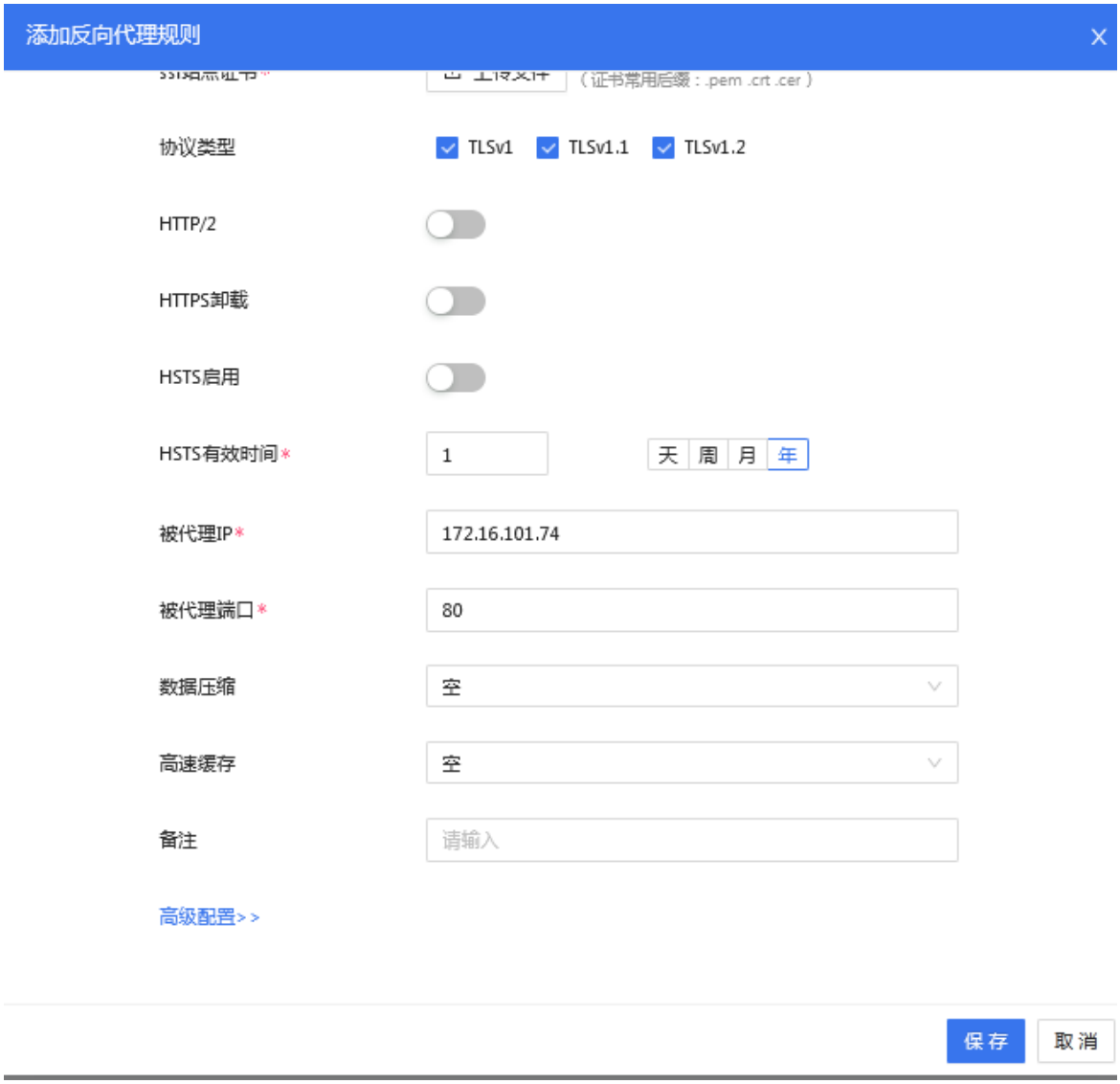
图10-10 配置反向代理网关



B.HTTPS

如下图所示，选择“代理网关>反向代理规则”进入反向代理规则配置页面，点击添加，新建反向代理规则，代理 IP 选择 WAF 上配置的业务 IP，被代理 IP 填写后端真实服务器 IP，如果不设置域名，则对配置的 ip 地址进行防护，以及 IP 地址相关域名也可以防护；如果配置域名，则仅对域名进行防护。针对一个 Web 服务器绑定多个域名的场景，可以根据需求在域名类型中配置“单域名”或者“多域名”，上传对应的证书即可。此时，WAF 只防护配置中的域名，当客户端使用其他域名或使用 ip 访问/攻击时，不进行检测防护，具体配置如下：

图10-11 反向代理规则



10.8 验证配置

(1) 访问 WAF 的 IP 地址，URL 为 http://192.168.7.15，可以正常访问。

图10-12 网站可以访问

(2) 加上攻击参数再次访问网站，URL 为 http://192.168.7.15/forum.php?id=1 and 1=1，网站不能访问。

图10-13 网站无法访问

(3) 选择"日志报表>防护日志"，查看攻击日志，可以看到攻击拦截的详细信息，证明 WAF 已经正常防护。

图10-14 拦截信息

11 旁路镜像检测模式部署配置举例

11.1 简介

旁路镜像检测模式是 H3C SecPath Web 应用防火墙在网站防护中常用的部署模式，设备旁路部署在网络中，通过流检测引擎对数据流进行解析，匹配规则与自定义策略进行安全检测，旁路镜像检测模式只进行检测，不对攻击进行处理。

旁路检测模式部署简单，不改变拓扑结构，部署后网络无感知。

支持检测功能：协议合规检测、web 攻击防护、web 业务控制、web 敏感信息防护（部分支持，仅支持数据库信息保护、敏感词防护）、web 业务加固（部分支持，仅支持弱密码检测、CGI 安全防护、跨站请求防护及业务流程控制）、DDOS 防护。

支持协议：HTTP。

特点：WAF 无须配置通信 IP，需配置管理 IP。

11.2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

11.3 使用限制

WAF 需要接入交换机镜像口，需提前划分好镜像口流量，用户交换机须镜像双向流量。

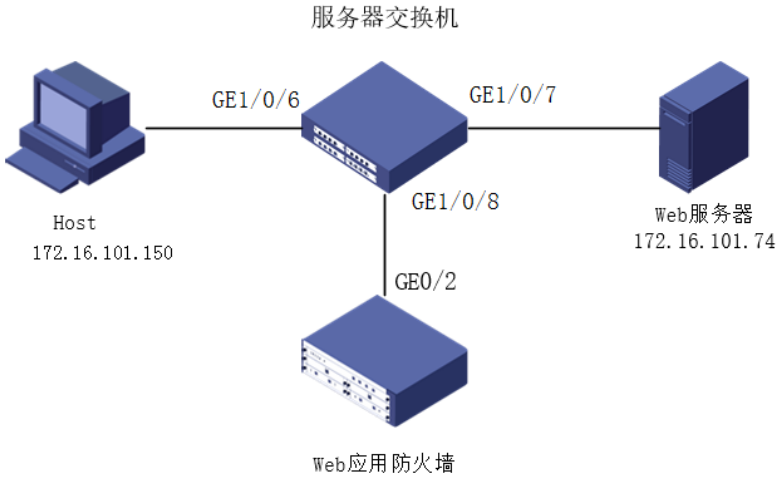
11.4 适用产品和版本

E6204P02 及以后版本

11.5 组网需求

如下图所示，WAF 旁路部署在服务器区交换机上，旁路接入网络，对 Web 服务器流量进行检测。

图11-1 组网图



11.6 配置思路

按照组网图组网。

(1) 交换机镜像和监听接口配置。

(2) 登录 WAF。

(3) 创建新的网桥，并把接入网络的 port 口划分到新网桥中。

(4) 配置部署模式。

(5) 配置防护资产，引用防护策略。

11.7 配置步骤

1. 交换机镜像和监听接口配置

登录服务器区交换机，如下图所示，将 GE1/0/6 和 GE1/0/7 划分到同一 VLAN 中。

图11-2 将两个镜像口划分到同一 VLAN 中

```
[SWUP_For_AUG_NewWAF]vlan 102          创建vlan102
[SWUP_For_AUG_NewWAF-vlan102]port GigabitEthernet 1/0/6 将GE1/0/6和GE1/0/7划入vlan102
[SWUP_For_AUG_NewWAF-vlan102]port GigabitEthernet 1/0/7
```

创建镜像组，如下图所示，将 GE1/0/6 和 GE1/0/7 配置为双向镜像口，GE1/0/8 配置为监听口。

图11-3 交换机上的镜像组配置

```
[SWUP_For_AUG_NewWAF]mirroring-group 2 local
[SWUP_For_AUG_NewWAF]mi
[SWUP_For_AUG_NewWAF]mirroring-group 2 mi
[SWUP_For_AUG_NewWAF]mirroring-group 2 mirroring-port g1/0/6 both
[SWUP_For_AUG_NewWAF]mi
[SWUP_For_AUG_NewWAF]mirroring-group 2 mi
[SWUP_For_AUG_NewWAF]mirroring-group 2 mirroring-port g1/0/7 bo
[SWUP_For_AUG_NewWAF]mirroring-group 2 mirroring-port g1/0/7 both
[SWUP_For_AUG_NewWAF]mi
[SWUP_For_AUG_NewWAF]mirroring-group 2 mo
[SWUP_For_AUG_NewWAF]mirroring-group 2 monitor-p
[SWUP_For_AUG_NewWAF]mirroring-group 2 monitor-port g1/0/8
[SWUP_For_AUG_NewWAF]dis mi
[SWUP_For_AUG_NewWAF]dis mirroring-group 2
Mirroring group 2:
    Type: Local
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/6  Both
        GigabitEthernet1/0/7  Both
    Monitor port: GigabitEthernet1/0/8
```

创建镜像组2

配置GE1/0/6、GE1/0/7为镜像口，镜像双向流量至监听口GE1/0/8。

配置GE1/0/8为监听口，监听GE1/0/6和GE1/0/7端口流量。

查看创建的镜像组信息。

2. 登录 WAF

如下图所示，使用 https 的方式登录 WAF，输入用户名和密码 admin/admin，并点击<登录>按钮。

注意：首次登录强制修改密码。

图11-4 登录 WAF

3. 创建新的网桥，并把接入网络的接口划分到新网桥中。

如下图所示，在“网络管理>网络配置>网桥接口”中，点击增加，创建网桥 br10

图11-5 新建网桥-br10

如下图所示，在“网络管理>网络配置>Port 接口”中编辑 port 接口。接口 GE0/2 的“网桥接口”选择 br10。

图11-6 port 口划分到新网桥

4. 配置部署模式。

如下图所示，选择菜单“基础配置>部署模式”进入部署模式配置页面，选择“旁路”部署模式，选择完成后保存配置。

图11-7 配置旁路部署模式

5. 配置防护资产，引用防护策略

如下图所示，选择菜单“基础配置>防护资产”进入防护资产配置页面，点击添加，新建防护资产，配置资产的同时即可引用对应的防护资产。

图11-8 创建防护资产

在防护模块部分，根据需要进行防护策略的配置，配置完成后点击保存。

图11-9 配置安全防护策略

11.8 验证配置

(1) 访问受保护的网站，URL 为 http://172.16.101.74，可以正常访问。

图11-10 网站可以访问

(2) 加上攻击参数再次访问网站，URL 为 http://172.16.101.74/forum.php?id=1 and 1=1，网站可以访问，WAF 上记录攻击日志。

图11-11 网站可以访问

(3) 选择"日志报表>防护日志"，查看攻击日志，可以看到攻击拦截的详细信息，证明 WAF 已经正常检测到攻击流量。

图11-12 拦截信息

12 旁路镜像检测&阻断模式部署配置举例

12.1 简介

旁路镜像检测&阻断模式是 H3C SecPath Web 应用防火墙在网站防护中常用的部署模式，设备旁路部署在网络中，通过流检测引擎对数据流进行解析，匹配规则与自定义策略进行安全防护。

旁路镜像检测&阻断模式部署简单，不改变拓扑结构，部署后网络无感知，支持的防护功能较全面，可支持网段和多端口防护策略，性能高。

支持防护功能：协议合规检测、web 攻击防护、web 业务控制、web 敏感信息防护（部分支持，仅支持数据库信息保护、敏感词防护）、web 业务加固（部分支持，仅支持弱密码检测、CGI 安全防护、跨站请求防护及业务流程控制）、DDOS 防护。

支持协议：HTTP。

特点：WAF 须配置通信 IP，需配置管理 IP。

12.2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

12.3 使用限制

WAF 需要接入交换机镜像口，需提前划分好镜像口流量，用户交换机须镜像双向流量。

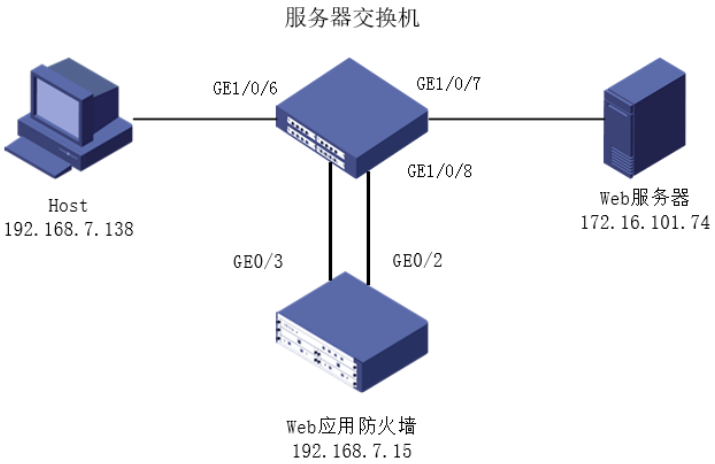
12.4 适用产品和版本

E6204P02 及以后版本

12.5 组网需求

如下图所示，WAF 旁路部署在服务器区交换机上，旁路接入网络，对 Web 服务器进行检测和阻断。

图12-1 组网图



12.6 配置思路

按照组网图组网。

(1) 交换机镜像和监听接口配置。

(2) 登录 WAF。

(3) 创建新的网桥，并把接入网络的 port 口划分到新网桥中。

(4) 配置部署模式。

(5) 配置防护资产，引用防护策略。

12.7 配置步骤

1. 交换机镜像和监听接口配置

登录服务器区交换机，如下图所示，将 GE1/0/6 和 GE1/0/7 划分到同一 VLAN 中。

图12-2 将两个镜像口划分到同一 VLAN 中

```
[SWUP_For_AVG_NewWAF]vlan 102
[SWUP_For_AVG_NewWAF-vlan102]port GigabitEthernet 1/0/6
[SWUP_For_AVG_NewWAF-vlan102]port GigabitEthernet 1/0/7
```

创建vlan102

将GE1/0/6和GE1/0/7划入vlan102

创建镜像组，如下图所示，将 GE1/0/6 和 GE1/0/7 配置为双向镜像口，GE1/0/8 配置为监听口。

图12-3 交换机上的镜像组配置

```
[SWUP_For_AVG_NewWAF]mirroring-group 2 local
[SWUP_For_AVG_NewWAF]mi
[SWUP_For_AVG_NewWAF]mirroring-group 2 mi
[SWUP_For_AVG_NewWAF]mirroring-group 2 mirroring-port g1/0/6 both
[SWUP_For_AVG_NewWAF]mi
[SWUP_For_AVG_NewWAF]mirroring-group 2 mi
[SWUP_For_AVG_NewWAF]mirroring-group 2 mirroring-port g1/0/7 bo
[SWUP_For_AVG_NewWAF]mirroring-group 2 mirroring-port g1/0/7 both
[SWUP_For_AVG_NewWAF]mi
[SWUP_For_AVG_NewWAF]mirroring-group 2 mo
[SWUP_For_AVG_NewWAF]mirroring-group 2 monitor-p
[SWUP_For_AVG_NewWAF]mirroring-group 2 monitor-port g1/0/8
[SWUP_For_AVG_NewWAF]dis mi
[SWUP_For_AVG_NewWAF]dis mirroring-group 2
Mirroring group 2:
    Type: Local
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/6  Both
        GigabitEthernet1/0/7  Both
    Monitor port: GigabitEthernet1/0/8
```

创建镜像组2

配置GE1/0/6、GE1/0/7为镜像口，镜像双向流量至监听口GE1/0/8。

配置GE1/0/8为监听口，监听GE1/0/6和GE1/0/7端口流量。

查看创建的镜像组信息。

2. 登录 WAF

如下图所示，使用 https 的方式登录 WAF，输入用户名和密码 admin/admin，并点击<登录>按钮。

注意：首次登录强制修改密码。

图12-4 登录 WAF

3. 创建新的网桥，并把接入网络的两个 port 口划分到新网桥中。

如下图所示，在“网络管理>网络配置>网桥接口”中，点击增加，创建网桥 br10

图12-5 新建网桥-br10

如下图所示，在“网络管理>网络配置>网桥接口”中，点击增加，创建网桥 br11。

图12-6 新建网桥-br11

如下图所示，在网桥 br11 中增加业务 IP 地址。

图12-7 增加业务 IP 地址

如下图所示，在“网络管理>路由配置”中增加路由。

图12-8 增加路由

如下图所示，在“网络管理>网络配置>Port 接口”中编辑 port 接口。接口 GE0/2 的“网桥接口”选择 br10，接口 GE0/3 的“网桥接口”选择 br11，使用 GE0/3 接口进行阻断。

图12-9 port 口划分到新网桥

4. 配置部署模式。

如下图所示，选择菜单“基础配置>部署模式”进入部署模式配置页面，选择“旁路”部署模式，配置对端设备的 MAC 地址，选择完成后保存配置。

图12-10 配置旁路检测阻断部署模式

5. 配置防护资产，引用防护策略

如下图所示，选择菜单“基础配置>防护资产”进入防护资产配置页面，点击添加，新建防护资产，配置资产的同时即可引用对应的防护资产。

图12-11 创建防护资产

在防护模块部分，根据需要进行防护策略的配置，配置完成后点击保存。

图12-12 配置安全防护策略

12.8 验证配置

(1) 访问受保护的网站，URL 为 http://172.16.101.74，可以正常访问。

图12-13 网站可以访问

(2) 加上攻击参数再次访问网站，URL 为 http://172.16.101.74/forum.php?id=1 and 1=1，网站不能访问。

图12-14 网站不能访问

404 Not Found

(3) 选择"日志报表>防护日志"，查看攻击日志，可以看到攻击拦截的详细信息，证明 WAF 已经正常防护。

图12-15 拦截信息

13 透明代理双机模式部署配置举例

13.1 简介

透明代理双机模式是 H3C SecPath Web 应用防火墙在网站防护中常用的部署模式，两台 WAF 串联在网络中，基于 TCP 数据包的检测，采用代理转发的技术，通过内部代理拆包解包，对应用层数据进行解析并匹配安全策略。

透明代理双机模式防护效果好，不改变拓扑结构，部署后客户端无感知，支持软硬件 Bypass 保证高可用性，支持的防护功能全面，检测效果优于透明流模式。

透明代理双机模式可支持主备模式。

支持功能：协议合规检测、web 攻击防护、web 业务控制、web 敏感信息防护、web 业务加固防护、爬虫陷阱、虚拟补丁。

支持协议：HTTP、HTTPS。

特点：WAF 须配置通信 IP，需配置管理 IP。

13.2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

13.3 使用限制

WAF 接入网络过程中会造成短暂断网，需提前划分好网桥和网络接口。

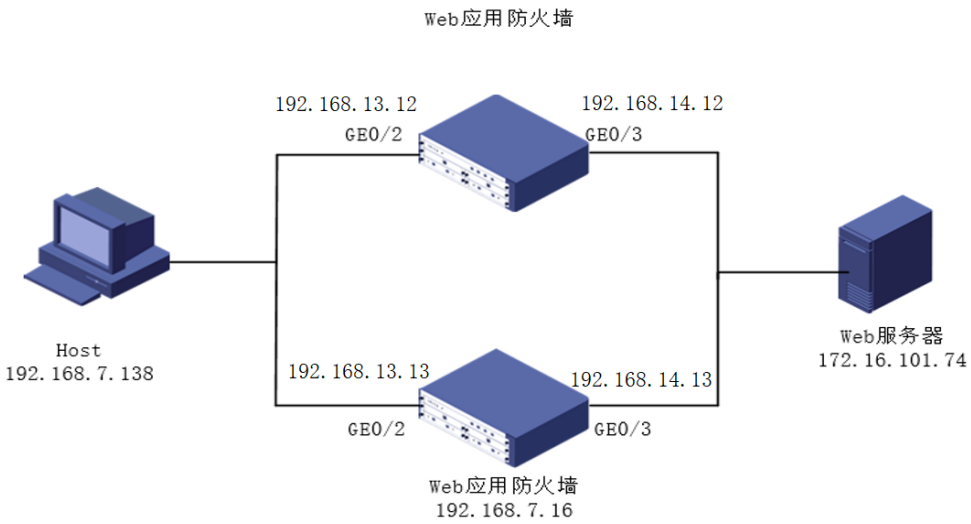
13.4 适用产品和版本

E6204P02 及以后版本

13.5 组网需求

如下图所示，WAF 部署在核心交换机和服务器区交换机之间，串联接入网络，对 Web 服务器进行防护。

图13-1 组网图



13.6 配置思路

按照组网图组网。

(1) 登录 WAF。

(2) 创建两个新的网桥，并把接入网络的两个 port 口分别划分到新网桥中。

(3) 配置部署模式。

(4) 配置防护资产，引用防护策略。

(5) 配置代理网关规则。

(6) 配置 VRRP 策略。

13.7 配置步骤

1. 登录 WAF

如下图所示，使用 https 的方式登录 WAF，输入用户名和密码 admin/admin，并点击<登录>按钮。

注意：首次登录强制修改密码。

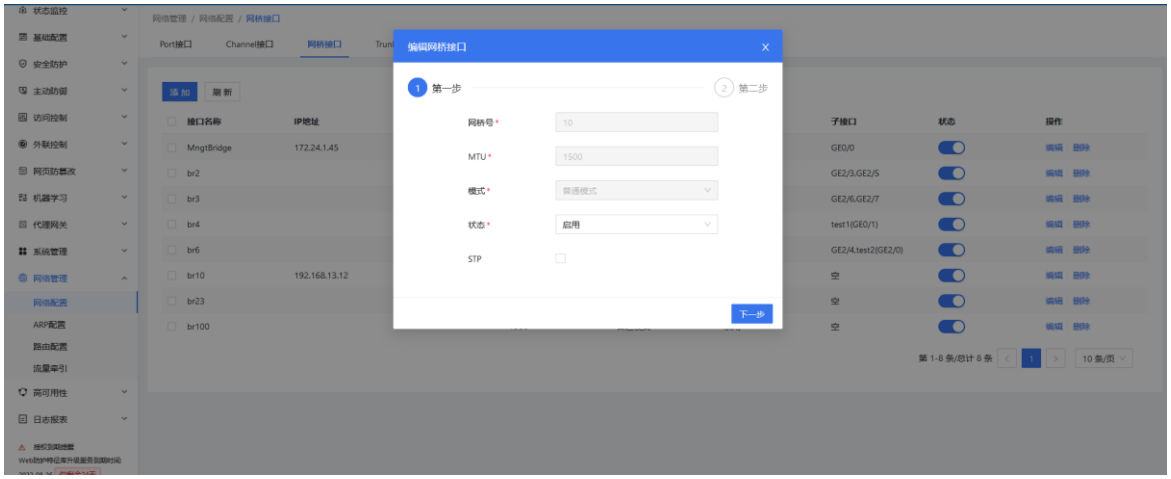
图13-2 登录 WAF

2. 创建新的网桥，并把接入网络的两个 port 口划分到新网桥中。

如下图所示，在“网络管理>网络配置>网桥接口”中，点击增加，创建网桥 br10

注：备机配置网桥 IP 地址和主机不同，为“192.168.13.13 和 192.168.14.13”其他配置和主机一样

图13-3 新建网桥-br10

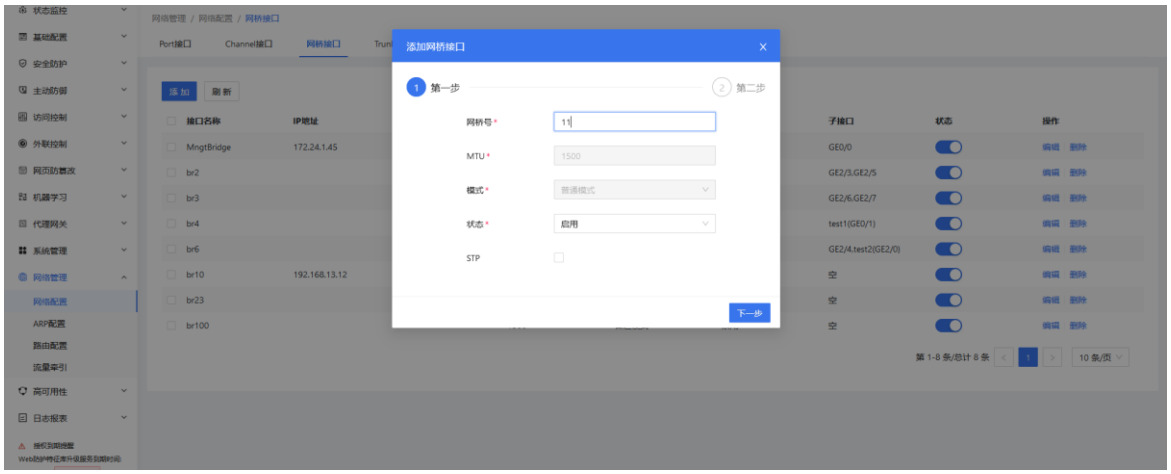


如下图所示，在桥 br10 上添加业务 IP，主机地址是“192.168.13.12”。备机上地址是“192.168.13.13”

图13-4 添加业务 IP-br10

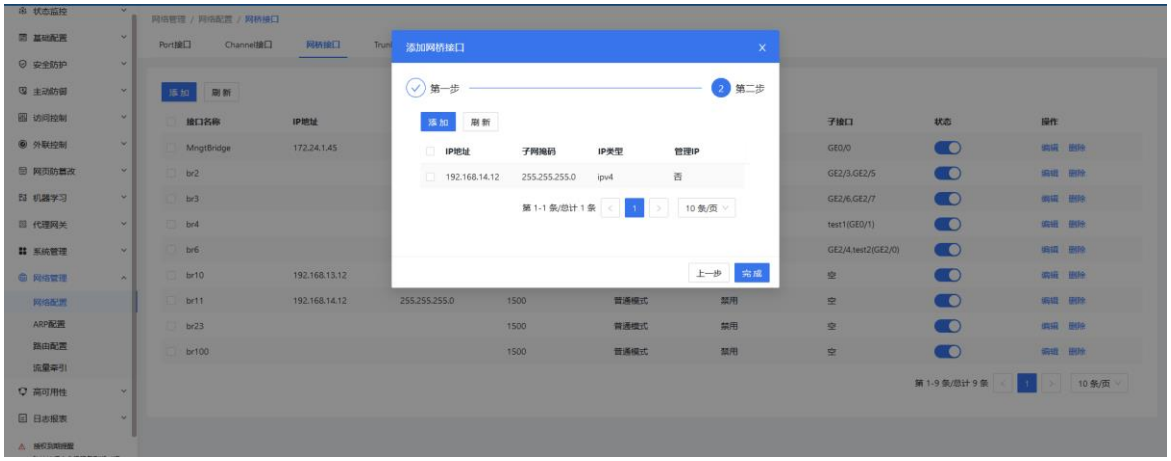
如下图所示，在“网络管理>网络配置>网桥接口”中，点击增加，创建网桥 br11。

图13-5 新建网桥-br11



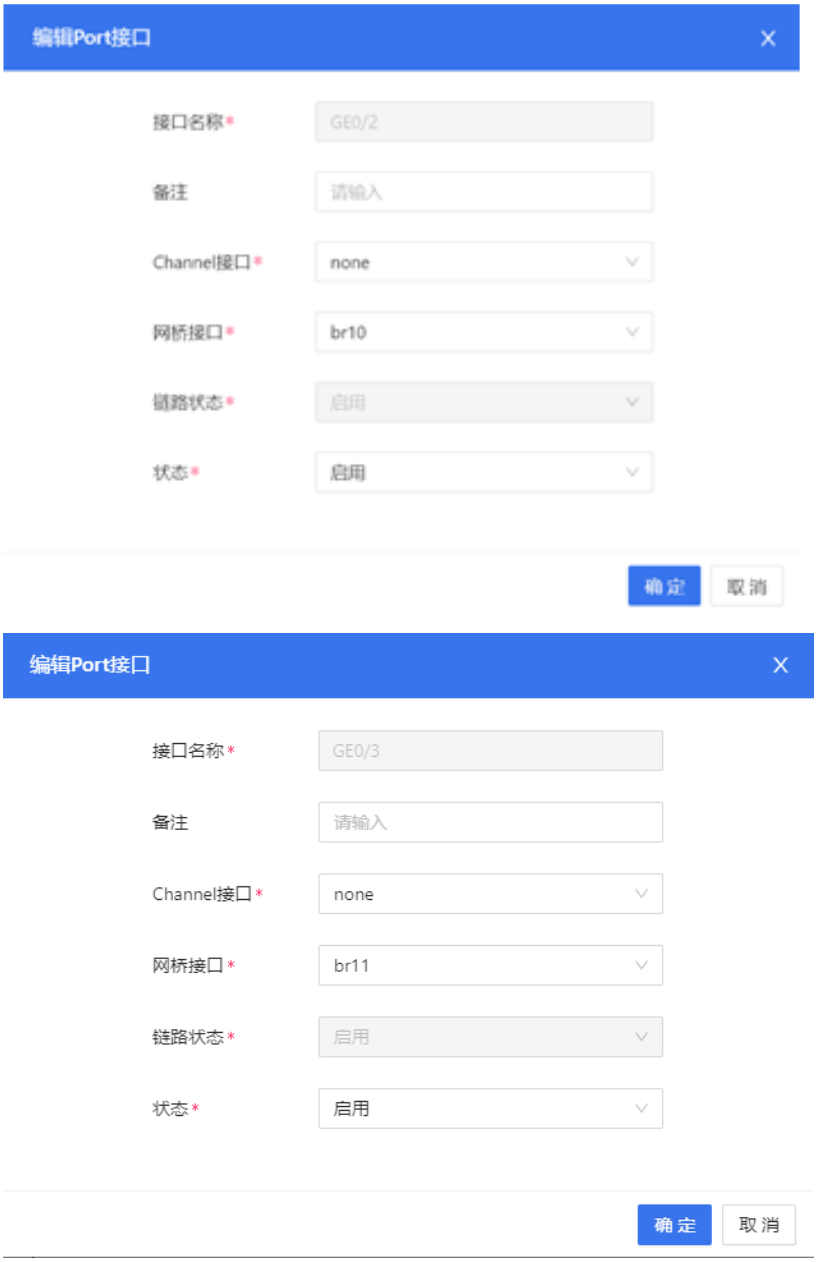
如下图所示，在桥 br11 上添加业务 IP，主机地址是“192.168.14.12”，备机上地址是“192.168.14.13”。

图13-6 添加业务 IP-br11



如下图所示，在“网络管理>网络配置>Port 接口”中编辑 port 接口。接口 GE2/0 的“网桥接口”选择 br10，GE0/3 的“网桥接口”选择 br11。

图13-7 port 口划分到新网桥



3. 配置部署模式

如下图所示，选择菜单“基础配置>部署模式”进入部署模式配置页面，选择“串联”部署模式，选择完成后保存配置。

注：备机配置和主机相同

图13-8 选择串联部署模式

4. 配置防护资产，引用防护策略

如下图所示，选择菜单“基础配置>防护资产”进入防护资产配置页面，点击添加，新建防护资产，配置资产的同时即可引用对应的防护资产。

注：备机配置和主机相同

图13-9 创建防护资产

在防护模块部分，根据需要进行防护策略的配置，配置完成后点击保存。

注：备机配置和主机相同

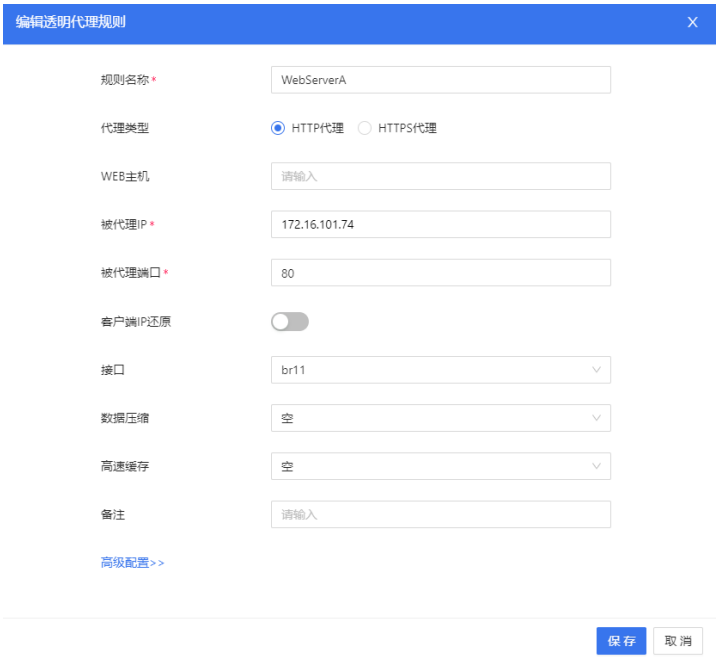
图13-10 配置安全防护策略

5. 配置代理网关规则

如下图所示，选择“代理网关>透明代理规则”进入透明代理规则配置页面，点击添加，新建透明代理规则，接口选择业务网桥 br11，客户端 IP 还原功能关闭，具体配置如下：

注：备机配置和主机相同

图13-11 配置透明代理网关



6. 添加 VRRP 策略，配置双机模式

A.主机配置

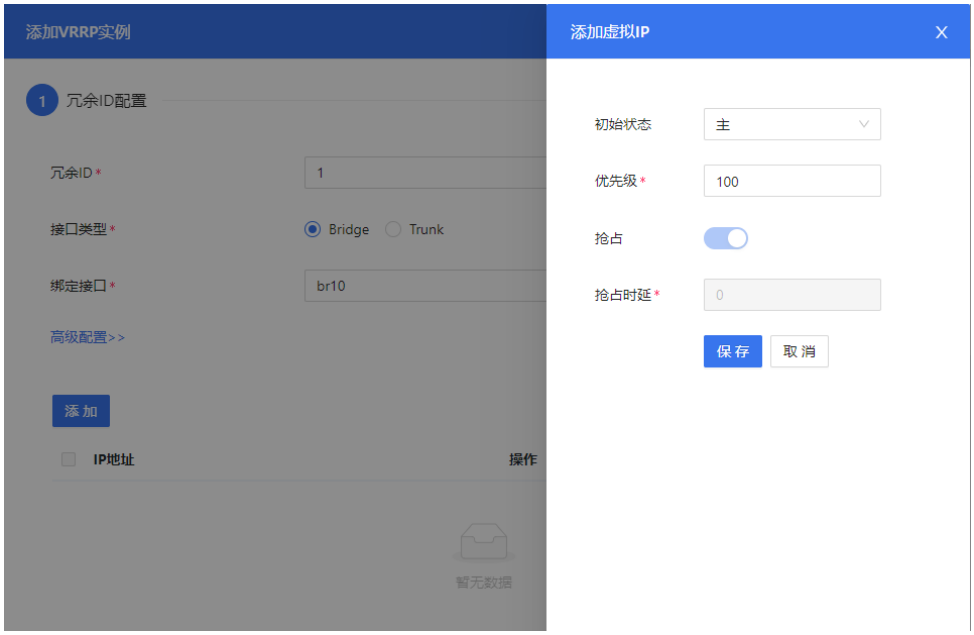
选择菜单“高可用性>HA 管理>VRRP 实例”进入 VRRP 配置页面，点击添加，新增 VRRP 实例，串联模式下需要添加两组 VRRP 实例。

设备状态为主时，流量会优先到主机上，由主机进行检测，当主机出现故障时，流量可实时切换到备机上进行检测，不会影响客户网络中的业务。

如下图所示，第一步配置冗余 ID 及设备初始状态，“冗余 ID”为 1，绑定接口选择上联接口“br10”，点击高级配置，初始状态为“主”，优先级为 100，点击保存。

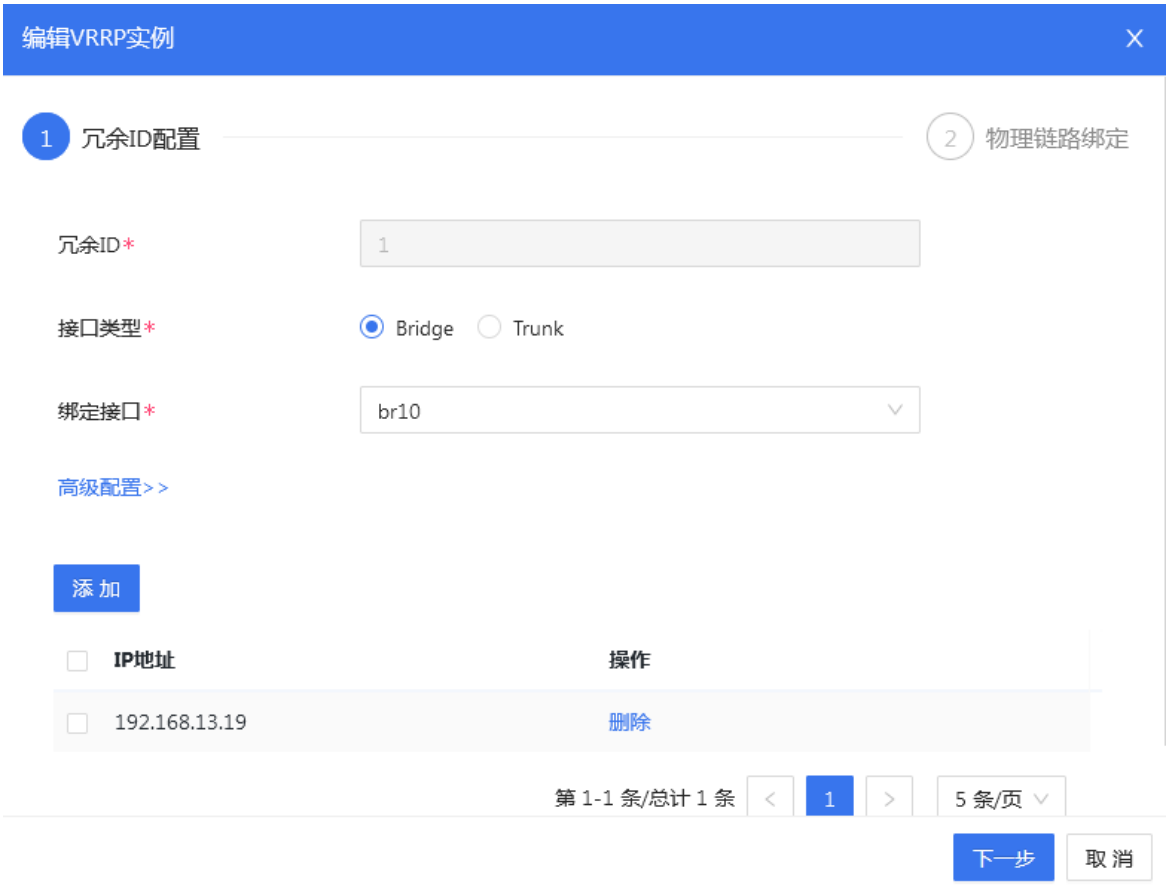
注：配置备机时保持与主机“冗余 ID”相同，“优先级”低于 100，“初始状态”为备。

图13-12 创建 VRRP 实例-主 1



如下图所示，第二步添加 IP，点击添加，输入 IP，此部分的 IP 为客户预先分配的 VRRP 虚拟冗余 IP。

图13-13 创建 VRRP 实例-主 2

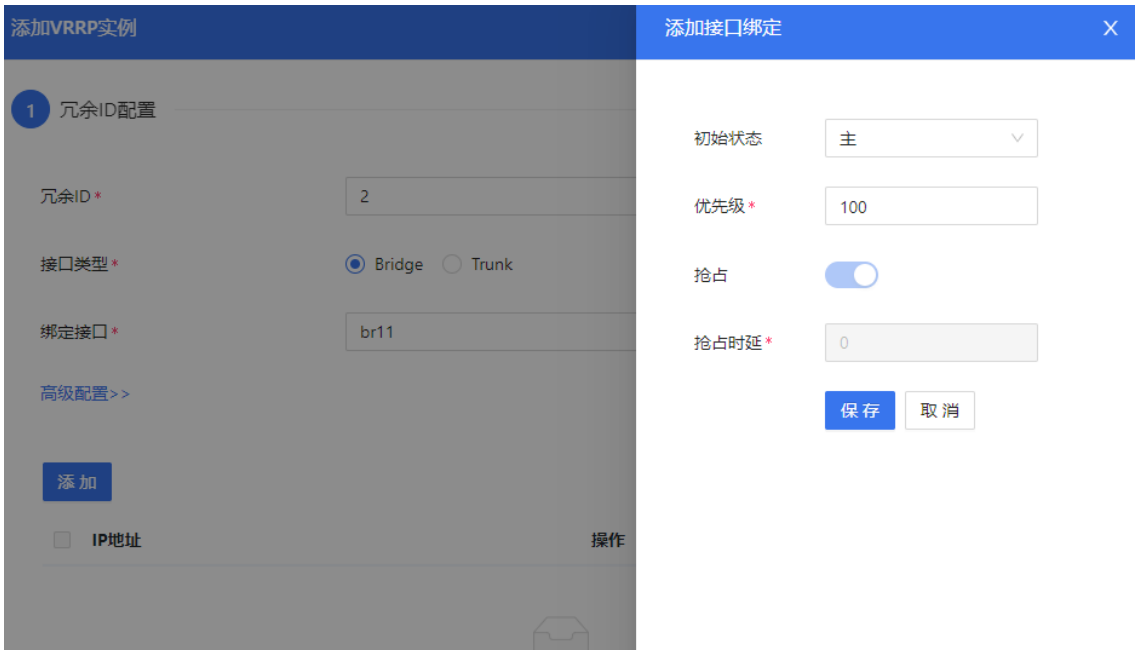


点击下一步，如下图所示，第三步配置物理链路绑定接口，点击增加，新增物理接口，选择分配到 br10 的接口 GE0/2，配置完成点击保存。

图13-14 创建 VRRP 实例-主 3

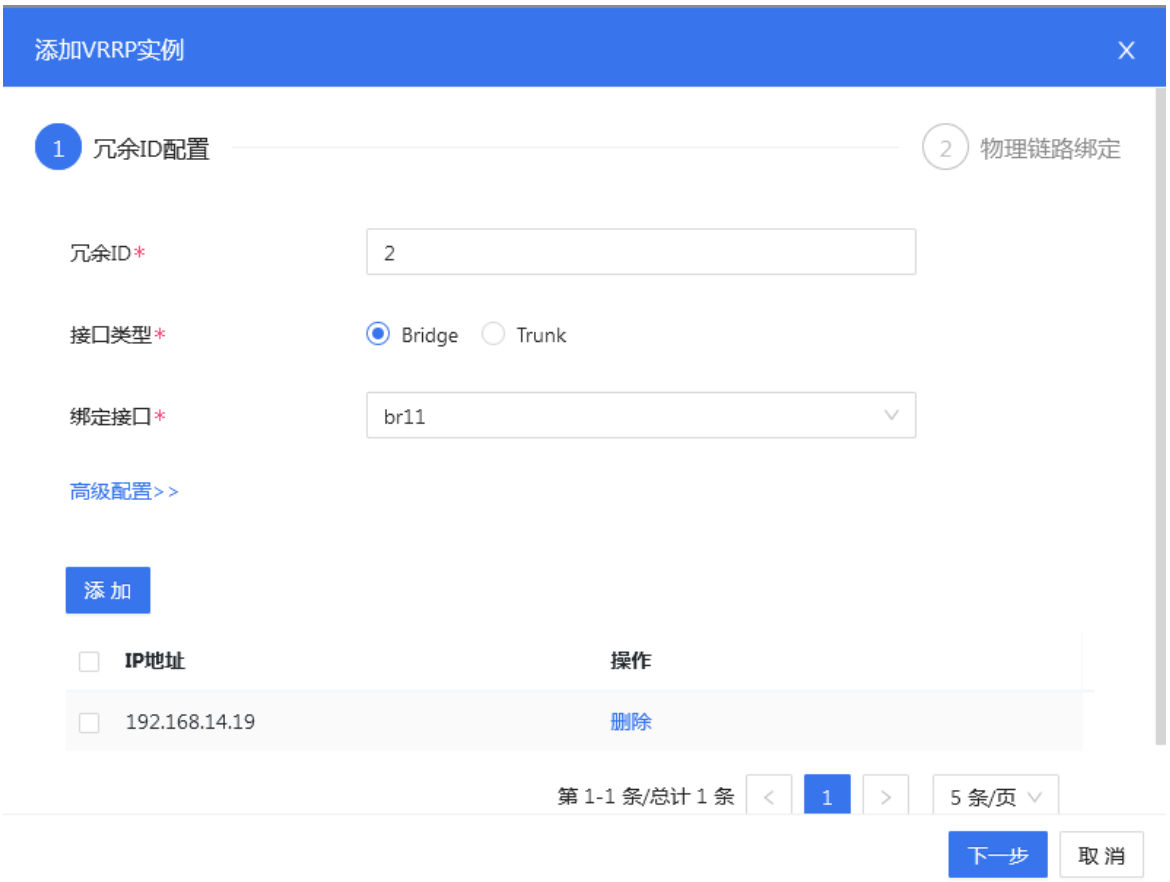
如下图所示，第四步添加第二组 VRRP 实例，“冗余 ID”为 2，“绑定接口”选择下联接口“br11”，其余配置与“冗余 ID”1 的配置相同，配置完成点击下一步，高级配置，初始状态为主，优先级为 100。

图13-15 创建 VRRP 实例-主 4



如下图所示，第五步配置 IP，点击添加，编辑增加 IP，此部分的 IP 为客户预先分配的 VRRP 虚拟冗余 IP。

图13-16 创建 VRRP 实例-主 5



点击下一步，如下图所示，第六步配置物理链路绑定接口，点击增加，新增物理接口，选择分配到 br11 的接口 GE0/3，配置完成点击保存。

图13-17 创建 VRRP 实例-主 6

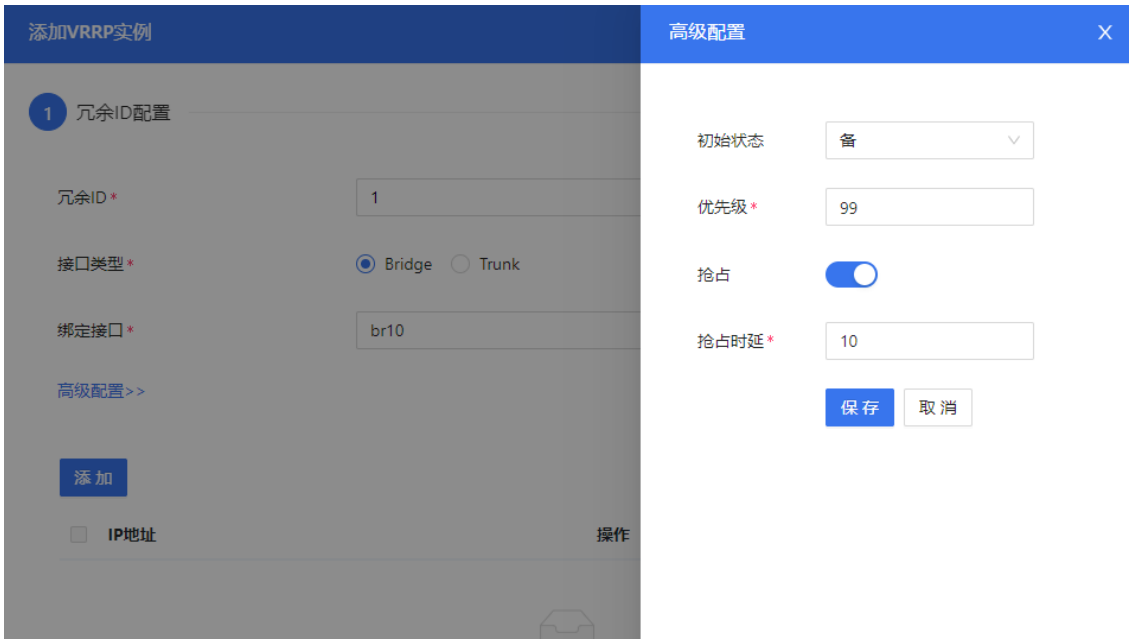
如下图所示，配置完 VRRP 实例后，需要将两组 VRRP 实例添加进 VRRP 组中，在菜单“VRRP 组”中点击增加，创建 VRRP 组，将上面创建好的 VRRP 实例勾选进 VRRP 组，点击保存。

图13-18 创建 VRRP 组-主

B.备机配置

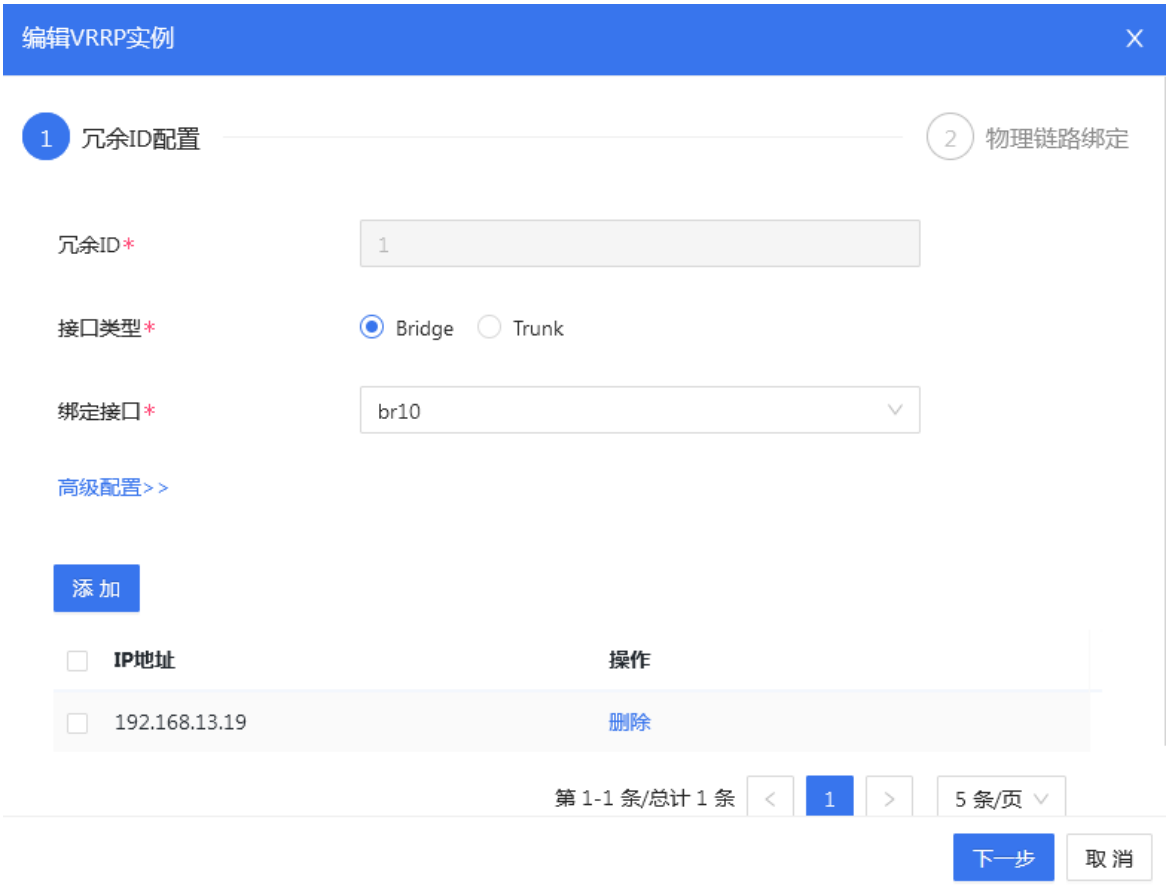
第一步配置冗余 ID 及设备初始状态，“冗余 ID”为 1，绑定接口选择上联接口“br10”,初始状态为“备”，高级配置中，初始状态是备、优先级是 99，配置完成点击下一步。

图13-19 创建 VRRP 实例-备 1



如下图所示，第二步添加 IP，点击添加，输入 IP，此部分的 IP 为客户预先分配的 VRRP 虚拟冗余 IP。

图13-20 创建 VRRP 实例-备 2

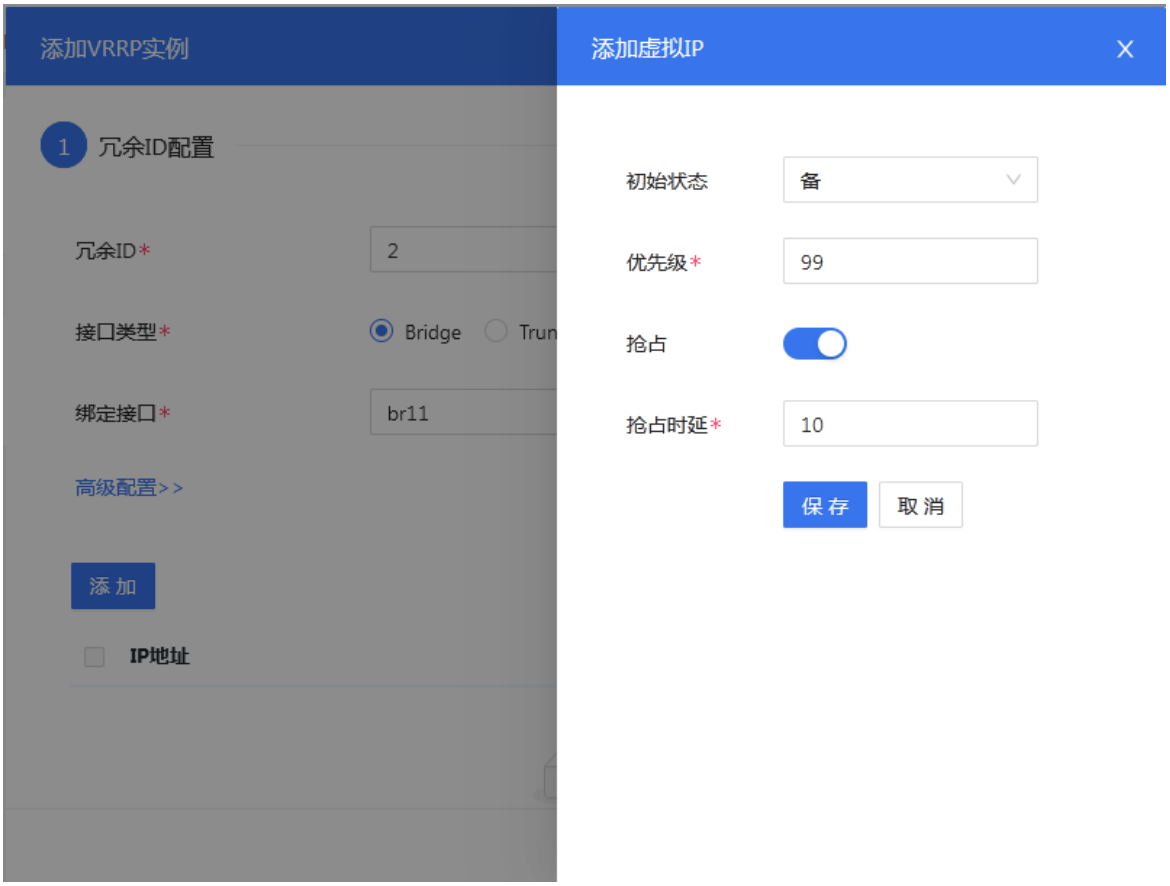


如下图所示，第三步配置物理链路绑定接口，点击增加，新增物理接口，选择分配到 br10 的接口 GE0/2，配置完成点击保存。

图13-21 创建 VRRP 实例-备 3

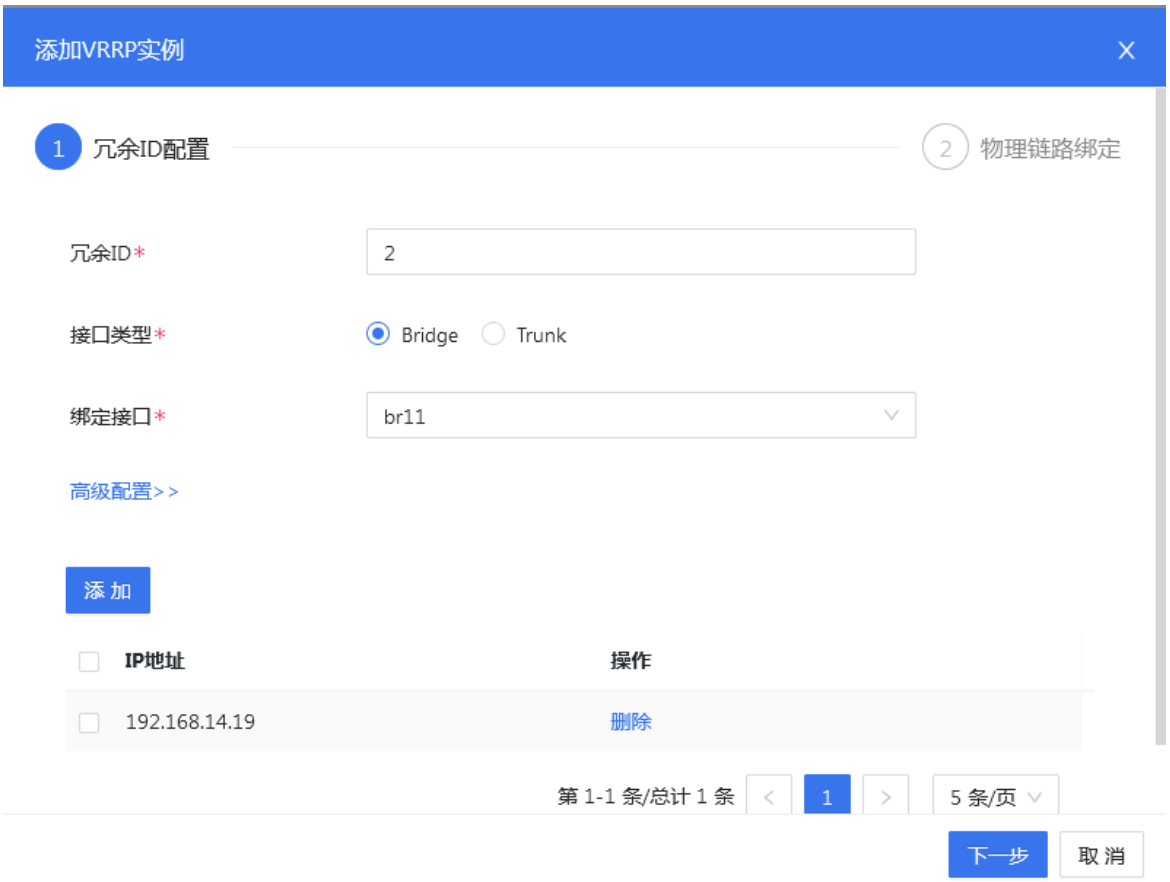
如下图所示，第四步添加第二组 VRRP 实例，“冗余 ID”为 2，“绑定接口”选择下联接口“br11”，高级配置中，初始状态是备、优先级是 99，配置完成点击下一步。

图13-22 创建 VRRP 实例-备 4



如下图所示，第五步配置 IP，点击添加，编辑增加 IP，此部分的 IP 为客户预先分配的 VRRP 虚拟冗余 IP。

图13-23 创建 VRRP 实例-备 5



点击下一步，如下图所示，第六步配置物理链路绑定接口，点击增加，新增物理接口，选择分配到 br11 的接口 GE0/3，配置完成点击保存。

图13-24 创建 VRRP 实例-备 6

如下图所示，配置完 VRRP 实例后，需要将两组 VRRP 实例添加进 VRRP 组中，在菜单“VRRP 组”中点击增加，创建 VRRP 组，将上面创建好的 VRRP 实例勾选进 VRRP 组。

图13-25 创建 VRRP 组-备

此时，HA 创建成功。

13.8 验证配置

(1) 访问受保护的网站，URL 为 http://172.16.101.74，可以正常访问。

图13-26 网站可以访问

(2) 加上攻击参数再次访问网站，URL 为 http://172.16.101.74/forum.php?id=1 and 1=1，网站不能访问。

图13-27 网站不能访问

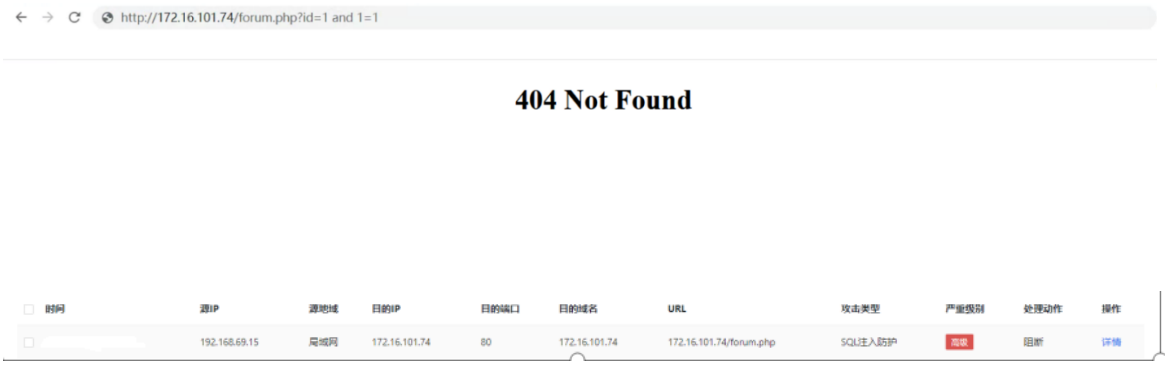
404 Not Found

(3) 选择"日志报表>防护日志"，查看攻击日志，可以看到攻击拦截的详细信息，证明 WAF 已经正常防护。

图13-28 拦截信息

(4) 将链路中的主机手动关机或断电，加上攻击参数再次访问网站，URL 为 http://172.16.101.74/forum.php?id=1 and 1=1，网站不能访问。

图13-29 网站不能访问



(5) 在备机上查看攻击日志，证明流量已切换至备机。

图13-30 攻击日志

14 反向代理双机模式部署配置举例

14.1 简介

WAF 旁路在网络中，基于 TCP 数据包的检测，采用代理转发的技术。客户端访问地址为 WAF 的 IP 地址，请求至 WAF 后由 WAF 代理转发，以自身的 IP 地址向服务器发起请求，服务器回包时回给 WAF，由 WAF 再封装数据包，以 WAF 的 IP 地址回复客户端。

反向代理双机模式可支持主备模式。

支持的防护功能较全面，可支持网段和多端口防护策略，性能高。

支持功能：协议合规检测、web 攻击防护、web 业务控制、web 敏感信息防护、web 业务加固防护、爬虫陷阱、虚拟补丁。

支持协议：HTTP、HTTPS。

特点：WAF 须配置通信 IP，需配置管理 IP。

14.2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

14.3 使用限制

WAF 接入网络过程中会造成短暂断网，需提前划分好网桥和网络接口。

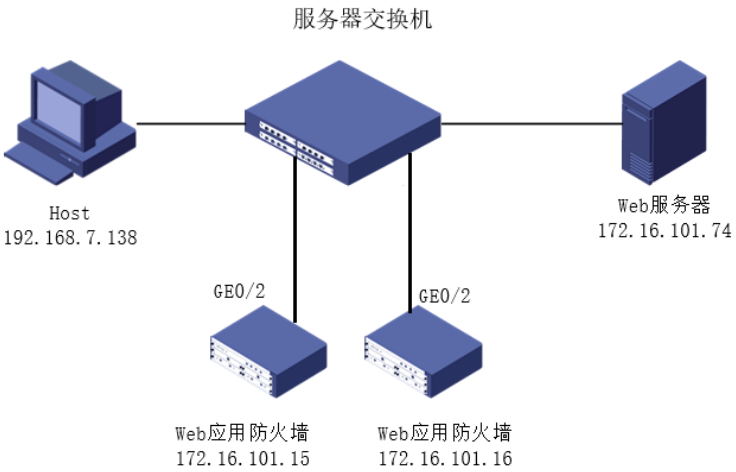
14.4 适用产品和版本

E6204P02 及以后版本

14.5 组网需求

如下图所示，两台 WAF 旁路部署在服务器区交换机上，对 Web 服务器进行防护。

图14-1 组网图



14.6 配置思路

按照组网图组网。

(1) 登录 WAF。

(2) 创建新的网桥，并把接入网络的 port 口划分到新网桥中。

(3) 配置部署模式。

(4) 配置防护资产，引用防护策略。

(5) 配置代理网关规则。

(6) 添加 VRRP 策略，配置双机模式。

14.7 配置步骤

1. 登录 WAF

如下图所示，使用 https 的方式登录 WAF，输入用户名和密码 admin/admin，并点击<登录>按钮。

注意：首次登录强制修改密码。

图14-2 登录 WAF

2. 创建新的网桥，并把接入网络的两个 port 口划分到新网桥中。

如下图所示，在“网络管理>网络配置>网桥接口”中，点击添加，创建网桥 br10。

图14-3 新建网桥-br10

如下图所示，在网桥 br10 上添加业务 IP。

注：主机地址是 172.16.101.15，备机网桥配置地址是 172.16.101.16

图14-4 添加业务 IP-br10

如下图所示，在“网络管理>网络配置>Port 接口”中编辑 port 接口。接口 GE0/1 的“网桥接口”选择 br10。

图14-5 port 口划分到新网桥

3. 配置部署模式

如下图所示，选择菜单“基础配置>部署模式”进入部署模式配置页面，选择“旁路”部署模式，选择完成后保存配置。

注：主机备机配置相同

图14-6 选择旁路部署模式

4. 配置防护资产，引用防护策略

如下图所示，选择菜单“基础配置>防护资产”进入防护资产配置页面，点击添加，新建防护资产，配置资产的同时即可引用对应的防护资产。

注：主机备机配置相同

图14-7 创建防护资产

在防护模块部分，根据需要进行防护策略的配置，配置完成后点击保存。

注：主机备机配置相同

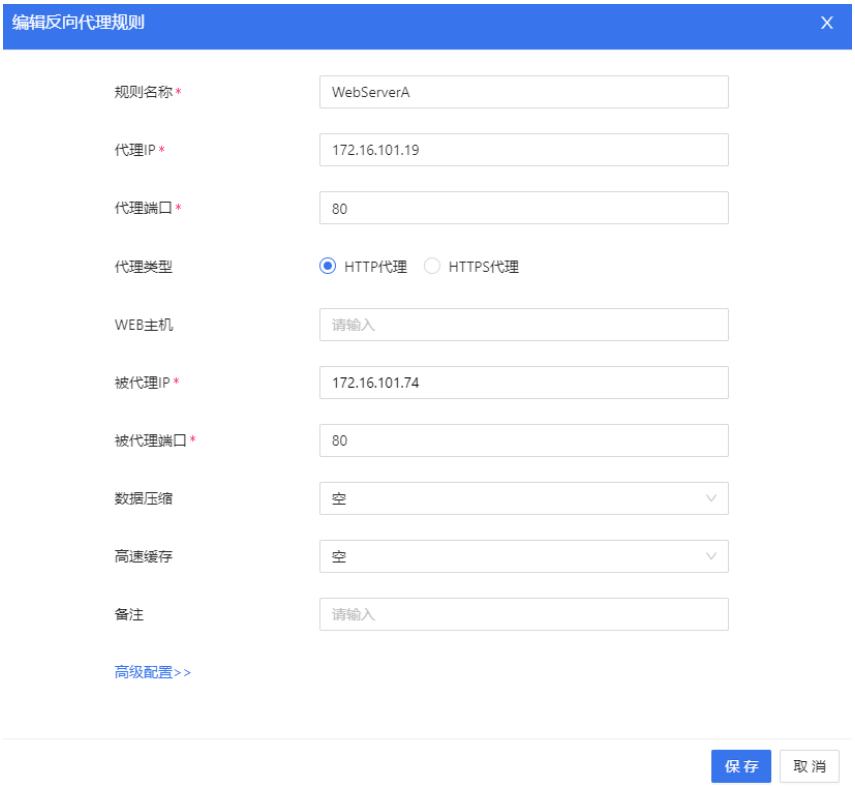
图14-8 配置安全防护策略

5. 配置代理网关规则

如下图所示，选择“代理网关>反向代理规则”进入反向代理规则配置页面，点击添加，新建反向代理规则，**代理 IP 选择 WAF 上配置的虚拟冗余 IP**，被代理 IP 填写后端真实服务器 IP，具体配置如下：

注：主机备机配置相同

图14-9 配置反向代理网关



6. 添加 VRRP 策略，配置双机模式。

选择菜单“高可用性>HA 管理>VRRP 实例”进入 VRRP 配置页面，点击添加，新增 VRRP 实例，旁路反向代理模式下需要添加一组 VRRP 实例。

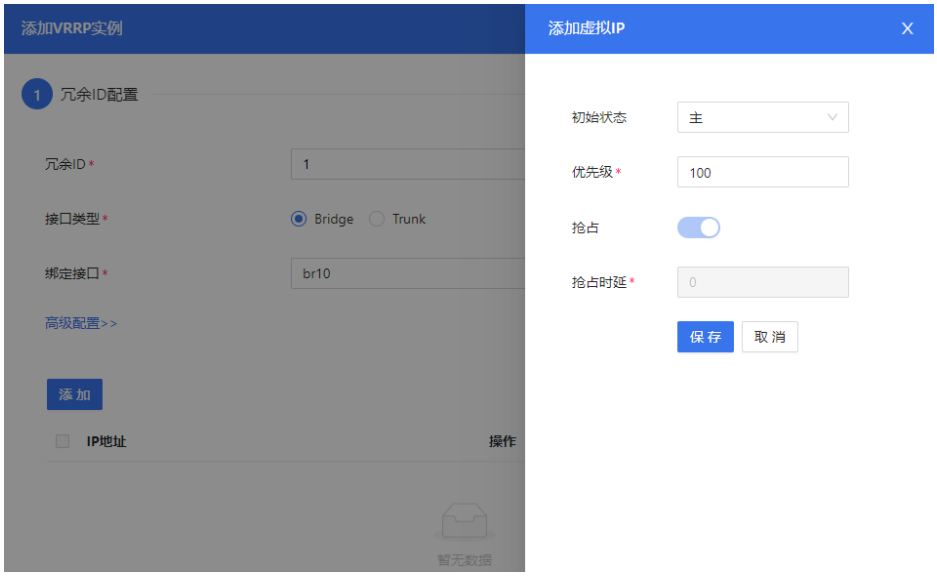
设备状态为主时，流量会优先到主机上，由主机进行检测，当主机出现故障时，流量可实时切换到备机上进行检测，不会影响客户网络中的业务。

A.主机配置

如下图所示，第一步配置冗余 ID 及设备初始状态，“冗余 ID”为 1，绑定接口选择上联接口“br10”，点击高级配置，初始状态为“主”，优先级为 100，保存配置完成。

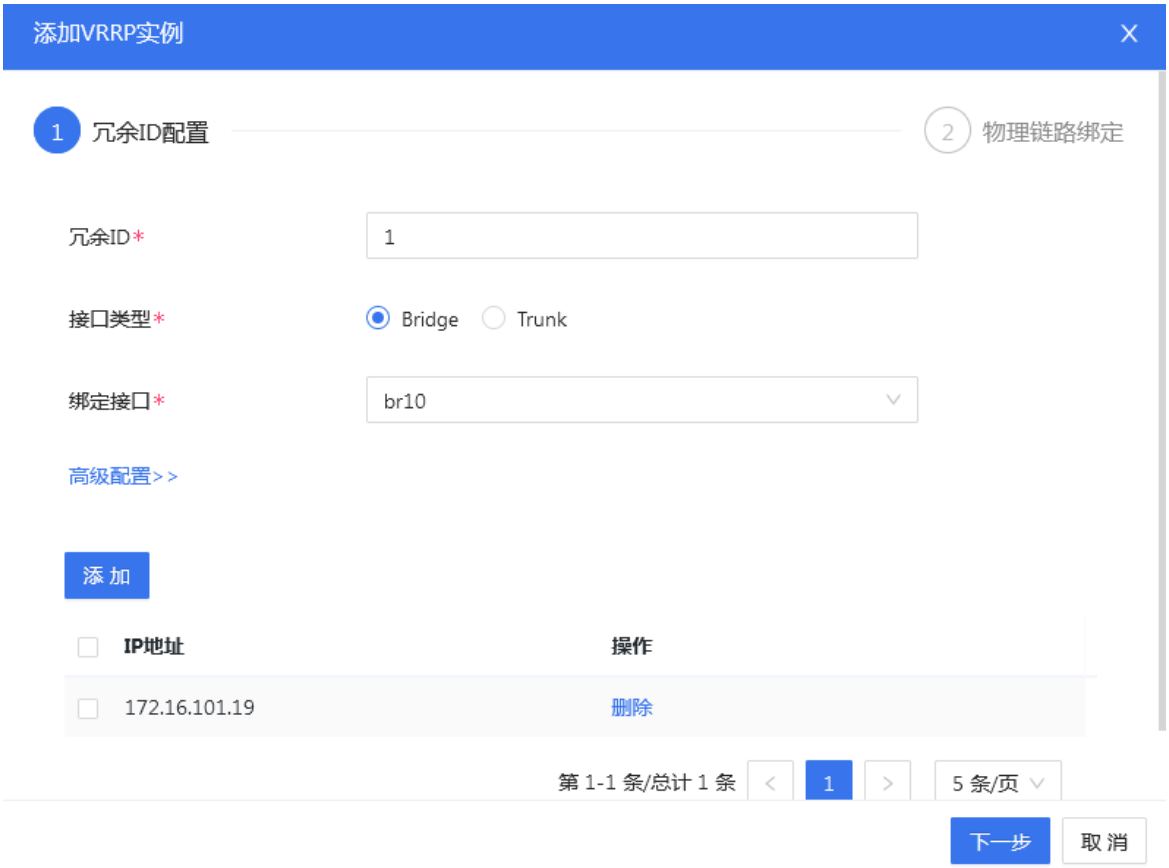
注：配置备机时保持与主机“冗余 ID”相同，“优先级”低于 100，“初始状态”为备。

图 8-9 创建 VRRP 实例-主 1



如下图所示，第二步添加 IP，点击添加，输入 IP，此部分的 IP 为客户预先分配的 VRRP 虚拟冗余 IP。

图 8-10 创建 VRRP 实例-主 2



然后点击下一步如下图所示，第三步配置物理链路绑定接口，点击增加，新增物理接口，选择分配到 br10 的接口 GE0/2，配置完成点击保存。

图 8-11 创建 VRRP 实例-主 3

创建完成以后，如下图：

图 8-12 创建 VRRP 实例-主 4

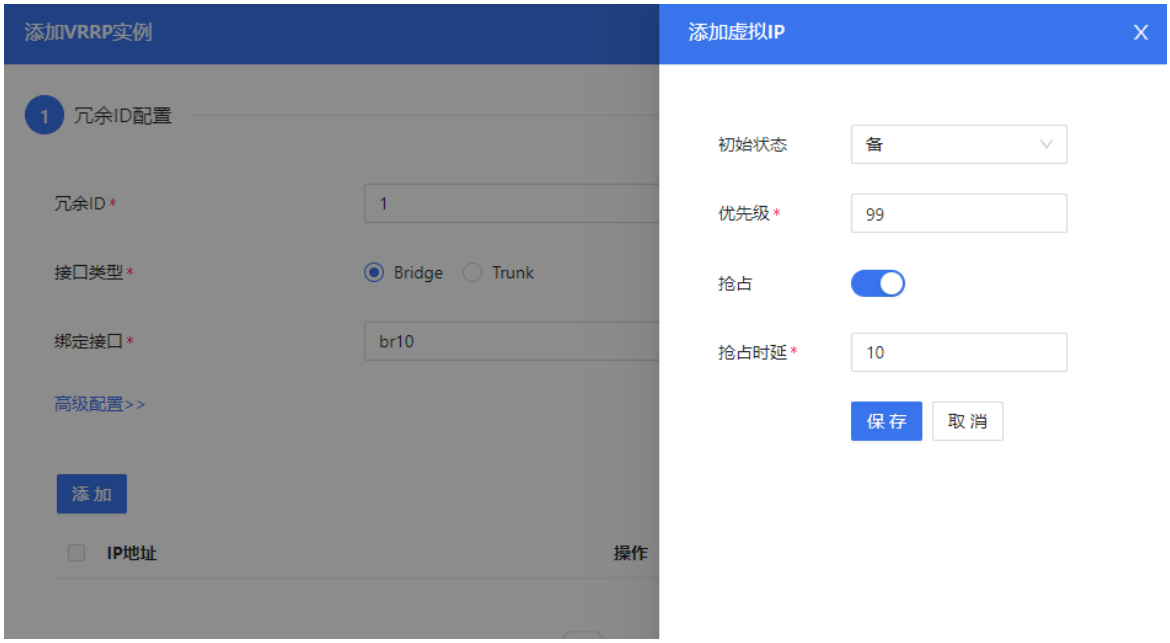
然后，配置完 VRRP 实例后，需要将一组 VRRP 实例添加进 VRRP 组中，在菜单“VRRP 组”中点击增加，创建 VRRP 组。

图 8-13 创建 VRRP 组-主

B.备机配置

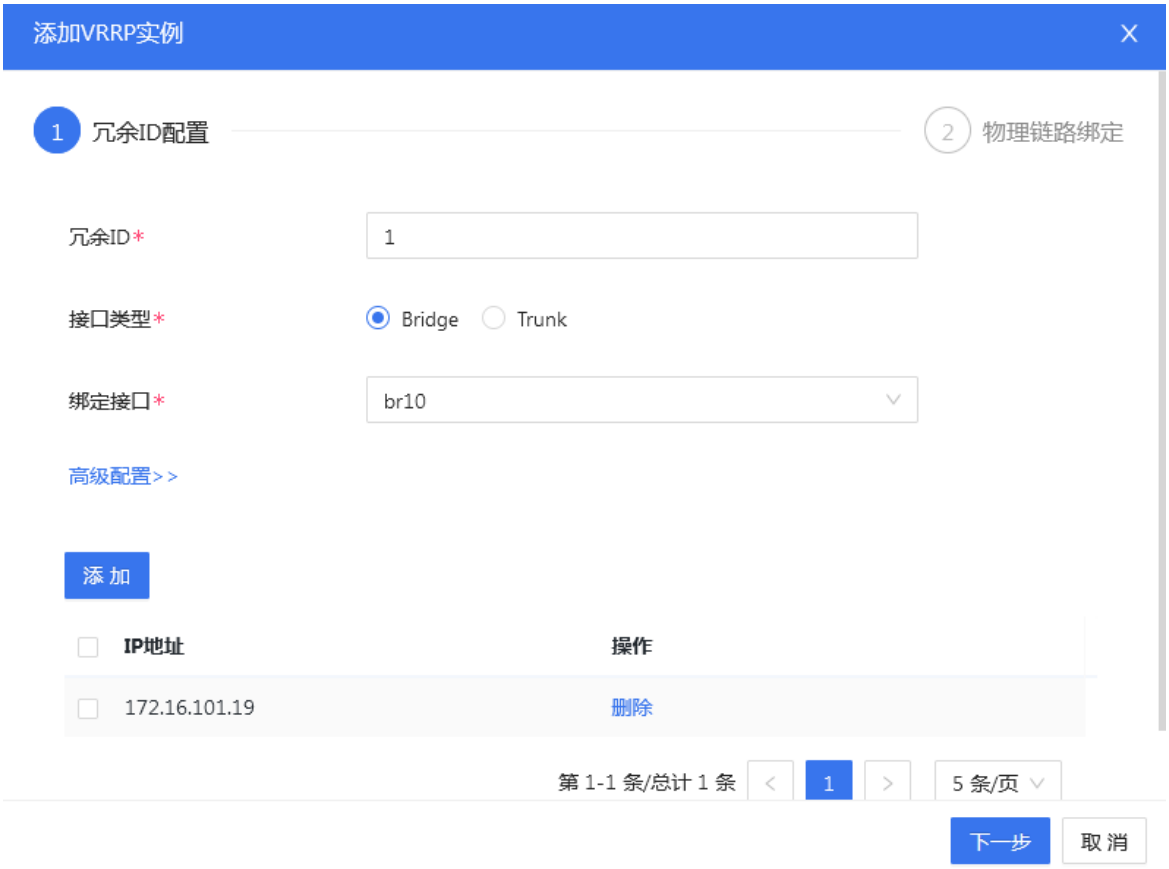
第一步配置冗余 ID 及设备初始状态，“冗余 ID”为 1，绑定接口选择上联接口“br10”,初始状态为“备”，具体配置参数如下，配置完成点击下一步。

图 8-9 创建 VRRP 实例-备 1



如下图所示，第二步添加 IP，点击添加，输入 IP，此部分的 IP 为客户预先分配的 VRRP 虚拟冗余 IP。

图 8-10 创建 VRRP 实例-备 2



点击下一步，如下图所示，第三步配置物理链路绑定接口，点击增加，新增物理接口，选择分配到 br10 的接口 GE0/2，配置完成点击保存。

图 8-11 创建 VRRP 实例-备 3

如下图所示，配置完 VRRP 实例后，需要将一组 VRRP 实例添加进 VRRP 组中，在菜单“VRRP 组”中点击增加，创建 VRRP 组。

图 8-15 创建 VRRP 组-备

此时 HA 成功部署成功。

14.8 验证配置

(1) 访问受保护的网站，URL 为 http://172.16.101.19，可以正常访问。

图14-10 网站可以访问

(2) 加上攻击参数再次访问网站，URL 为 http://172.16.101.19/forum.php?id=1 and 1=1，网站不能访问。

图14-11 网站无法访问

(3) 选择"日志报表>防护日志"，查看攻击日志，可以看到攻击拦截的详细信息，证明 WAF 已经正常防护。

图14-12 拦截信息

(4) 将链路中的主机手动关机或断电，加上攻击参数再次访问网站，URL 为 http://172.16.101.19/forum.php?id=1 and 1=1，网站不能访问。

图14-13 网站不能访问

(5) 在备机上查看攻击日志，证明流量已切换至备机。

图14-14 攻击日志

15 链路聚合部署配置举例

15.1 简介

链路聚合是指将多个物理端口汇聚在一起，形成一个逻辑端口，以实现出/入流量吞吐量在各成员端口的负荷分担。

15.2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

15.3 使用限制

WAF 接入网络过程中会造成短暂断网，需提前划分好网桥和网络接口。

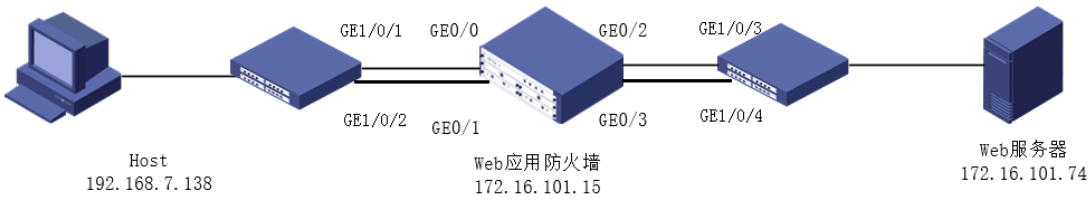
15.4 适用产品和版本

E6204P02 及以后版本。

15.5 组网需求

如下图所示，WAF 配置 channel 模式部署在交换机中，对 Web 服务器进行防护。

图15-1 组网图



15.6 配置思路

(1) 交换机配置链路聚合

(2) 登录 WAF。

(3) 创建网桥，

(4) 创建聚合接口。

(5) 把 port 接口划分到聚合接口中。

15.7 配置步骤

1. 交换机配置链路聚合

靠近客户端的交换机配置链路聚合，将接口 GE1/0/1 和 GE1/0/2 加入到聚合组 1 中。将接口 GE1/0/3 和 GE1/0/4 加入到聚合组 2 中。

2. 登录 WAF

如下图所示，使用 https 的方式登录 WAF，输入用户名和密码 admin/admin，并点击<登录>按钮。

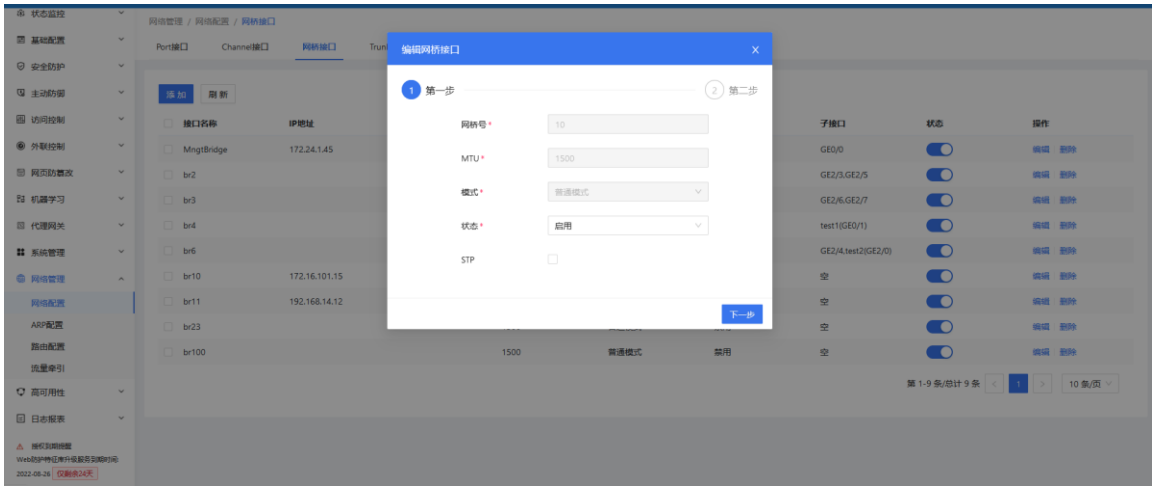
注意：首次登录强制修改密码。

图15-2 登录 WAF

3. 创建新的网桥

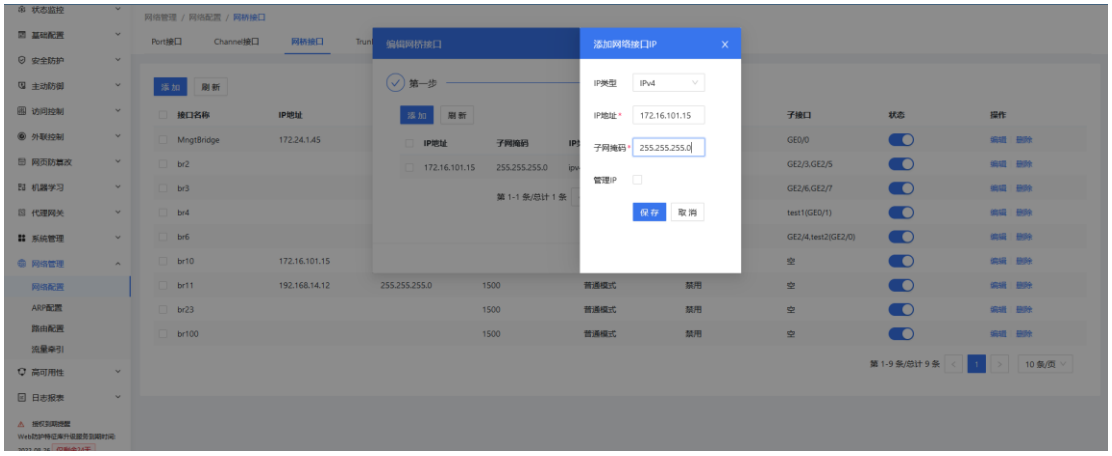
如下图所示，在“网络管理>网络配置>网桥接口”中，点击增加，创建网桥 br10。

图15-3 新建网桥-br10



如下图所示，根据部署模式，部分部署模式需要添加业务 IP 时，给网桥 br10 增加业务 IP 地址。

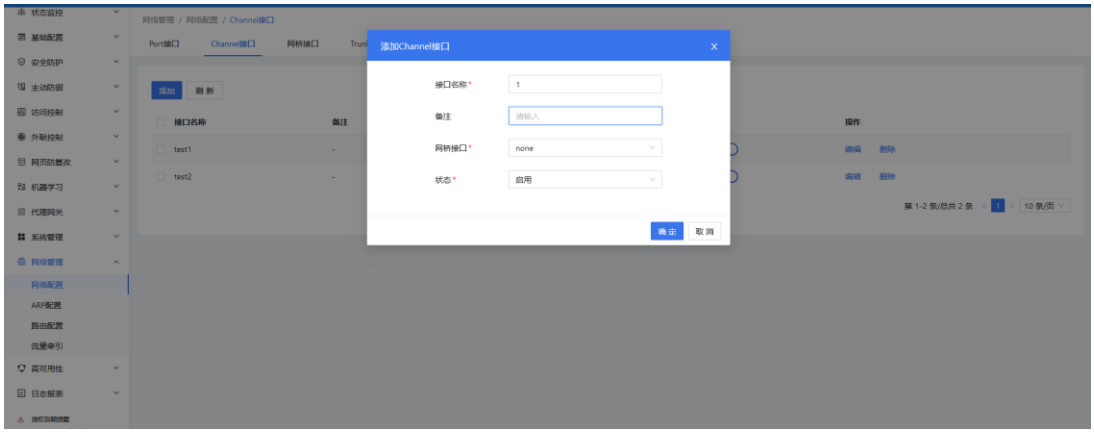
图15-4 增加业务 IP 地址



4. 创建聚合接口

如下图所示，在“网络管理>网络接口>channel 接口”中增加聚合接口 1 和 2。

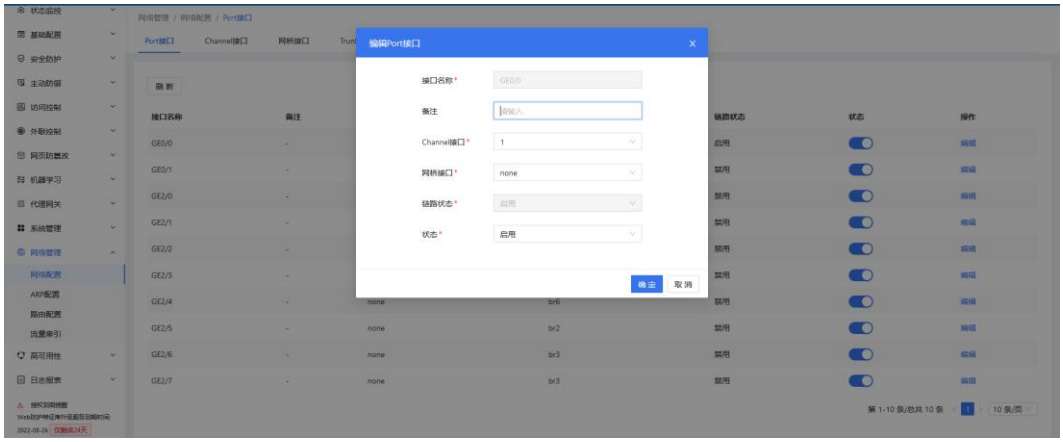
图15-5 增加聚合接口



5. 把 port 接口划分到聚合接口中

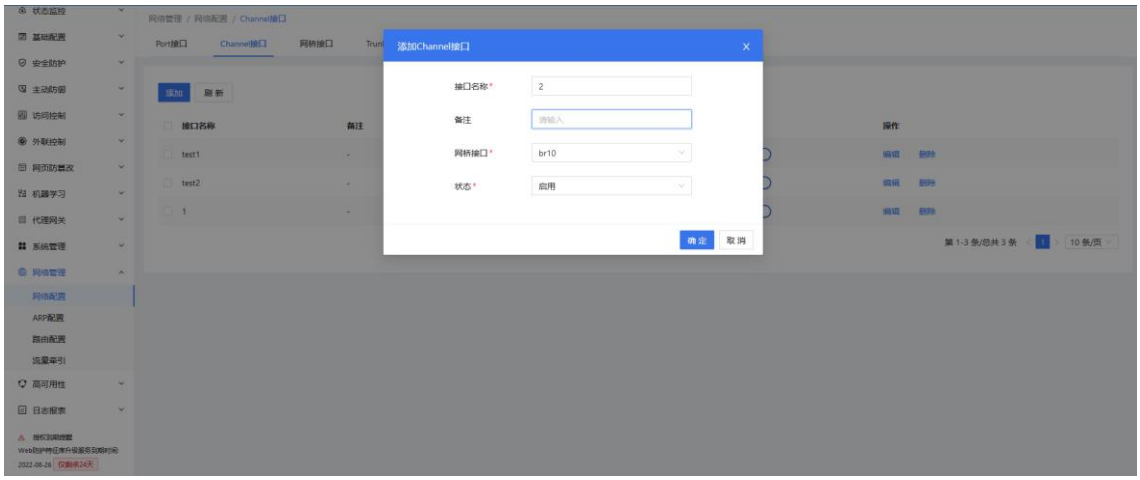
如下图所示，在“网络管理>网络配置>Port 接口”中编辑 port 接口。接口 GE0/0 和 GE0/1 的“channel 接口”选择 1。接口 GE0/2 和 GE0/3 的“channel 接口”选择 2。

图15-6 Port 接口配置聚合接口



如下图所示，在“网络管理>网络配置>channel 接口”中把 channel 接口的 1 和 2 接口的“网桥接口”选择 br10。

图15-7 聚合口划分到网桥中



15.8 验证配置

(1) port 接口验证，接口 GE0/0 和 GE0/1 在 channel 接口 1 中，接口 GE0/2 和 GE0/3 在 channel 接口 2 中。

图15-8 接口信息

接口名称	备注	Channel接口	网桥接口	链路状态	状态	操作
GE0/0	-	1	none	启用		编辑
GE0/1	-	1	none	禁用		编辑
GE0/2	-	2	none	禁用		编辑
GE0/3	-	2	none	禁用		编辑

(2) channel 接口验证，channel 接口中 1 接口和 2 接口在网桥 br10 中。

图15-9 接口信息

(3) 网桥接口验证，网桥接口 br10 中配置 IP 地址。

图15-10 网桥接口验证

16 Trunk 部署配置举例

16.1 简介

Trunk 模式适用网络部署中存在不同局域网的情况，部署时需要在交换机中添加 Trunk 接口，通过在 Trunk 接口上设置允许的 VLAN 来实现 H3CSecPathWeb 应用防火墙系统对不同局域网中的服务器进行防护的功能。

16.2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

16.3 使用限制

WAF 接入网络过程中会造成短暂断网，需提前划分好网桥和网络接口。一个 Trunk 接口当前仅支持配置一个 VLAN 标签，如果需要检测多 VLAN 流量即需要配置多个 VLAN 标签，需要添加多个 Trunk 接口。

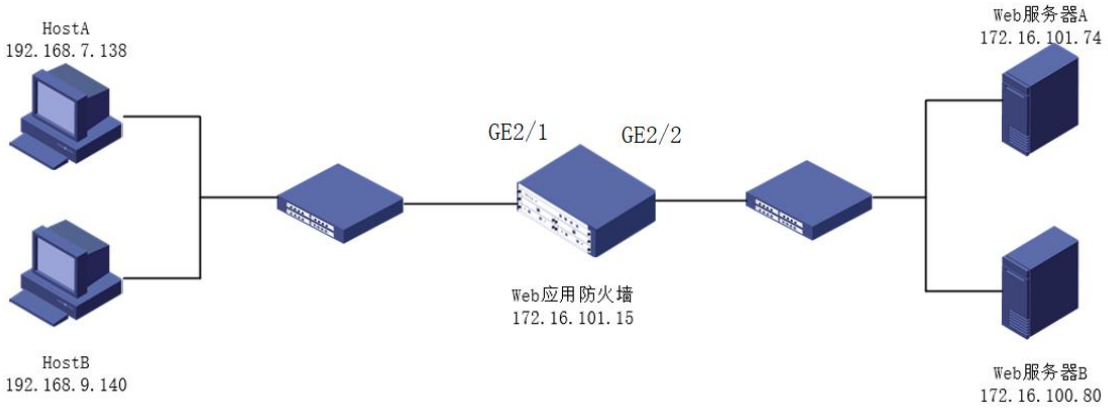
16.4 适用产品和版本

E6204P02 及以后版本。

16.5 组网需求

如下图所示，WAF 配置 trunk 模式部署在交换机中，对 Web 服务器进行防护。

图16-1 组网图



16.6 配置思路

(1) 登录 WAF。

(2) 创建网桥，把 port 接口划分到新建网桥中。

(3) 创建 trunk 接口。

16.7 配置步骤

1. 登录 WAF

如下图所示，使用 https 的方式登录 WAF，输入用户名和密码 admin/admin，并点击<登录>按钮。

注意：首次登录强制修改密码。

图16-2 登录 WAF

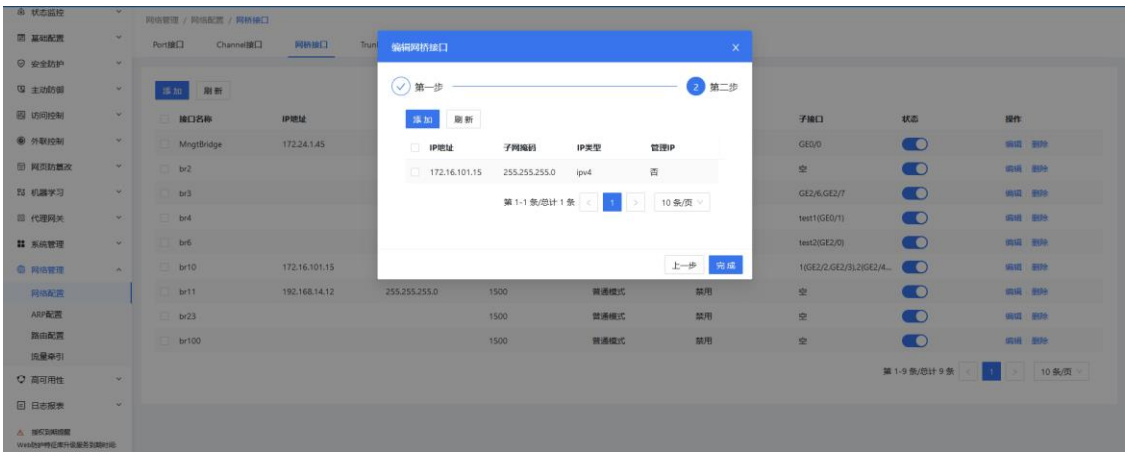
2. 创建新的网桥。

如下图所示，在“网络管理>网络配置>网桥接口”中，点击添加，创建网桥 br10。

图16-3 新建新的网桥

如下图所示，根据服务器部署模式，部分部署模式需要添加业务 IP 时，给网桥 br10 增加业务 IP 地址。

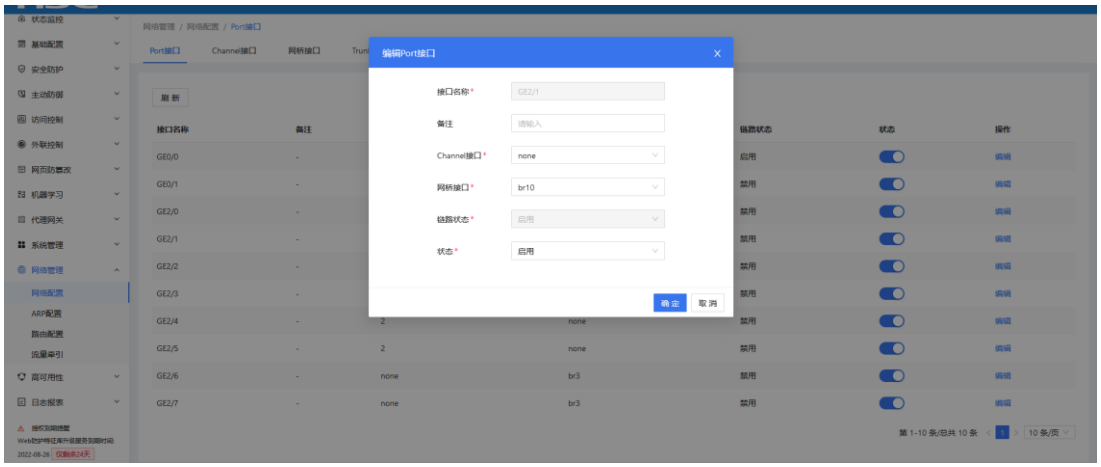
图16-4 增加业务 IP 地址



3. 把 port 接口划分到网桥中

如下图所示，在“网络管理>网络配置>Port 接口”中编辑 port 接口。接口 GE2/1、GE2/2 网桥接口选择新创建的网桥 10。

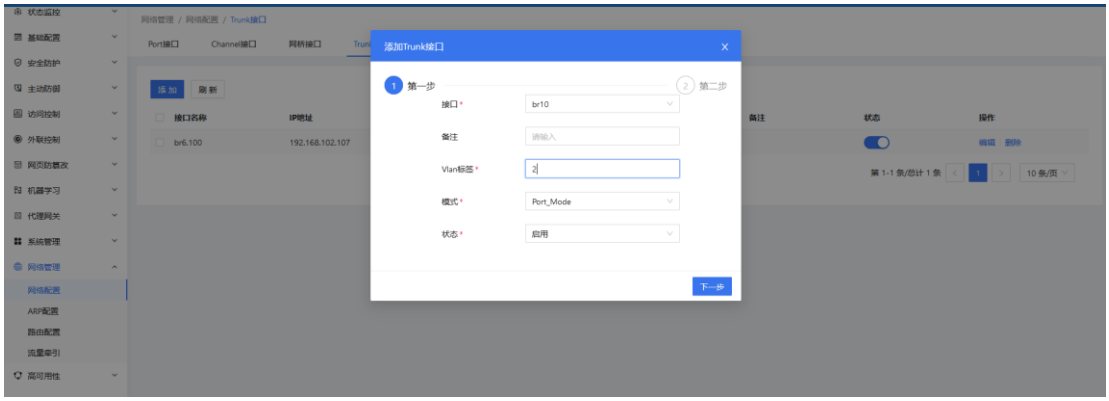
图16-5 Port 接口配置



4. 创建 trunk 接口

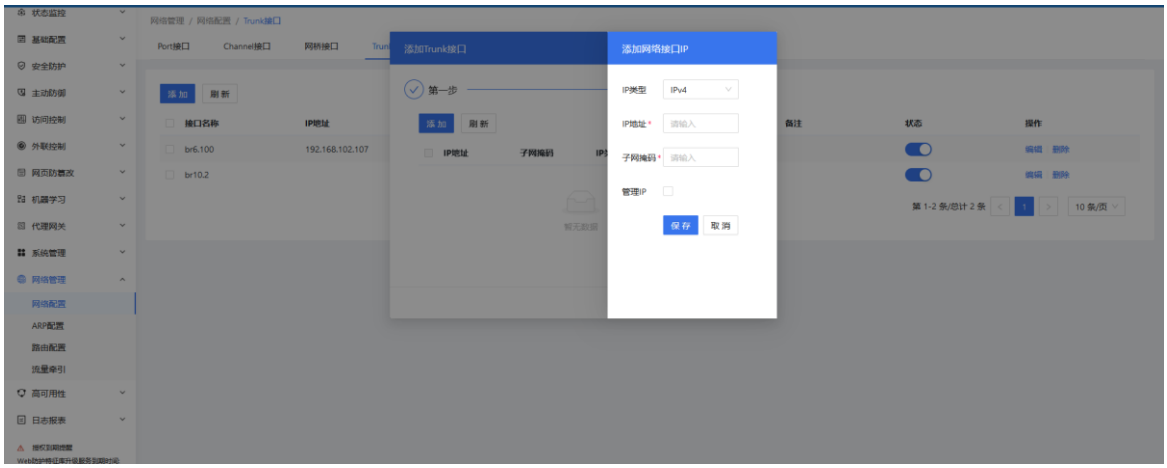
如下图所示，在网络管理>网络配置>channel 接口中增加 trunk 接口，配置允许的 vlan 标签，配置完成点击下一步。

图16-6 增加 trunk 接口



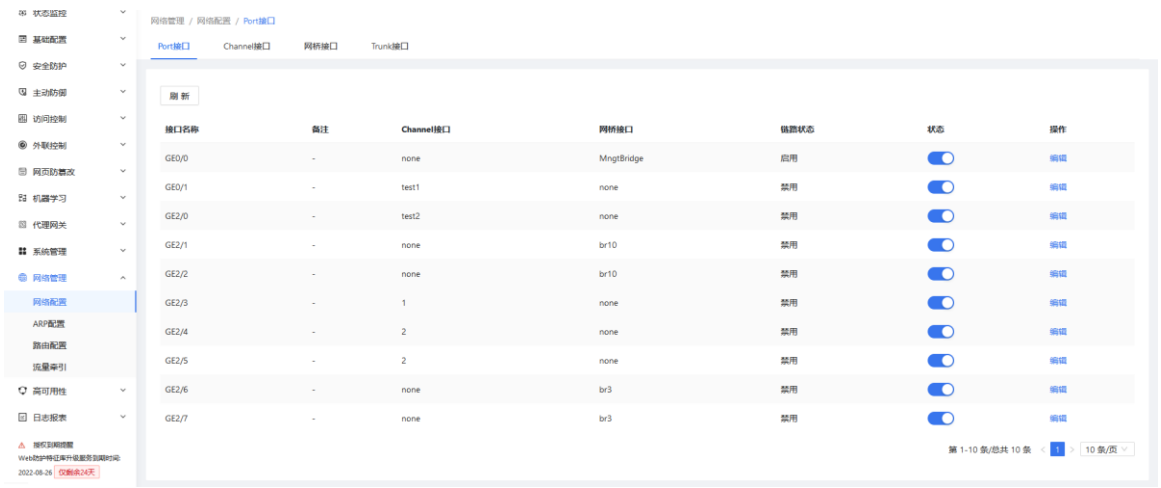
如下图所示，如需配置 IP 可添加业务 IP，无需配置 IP 时点击保存。

图16-7 保存 trunk 配置



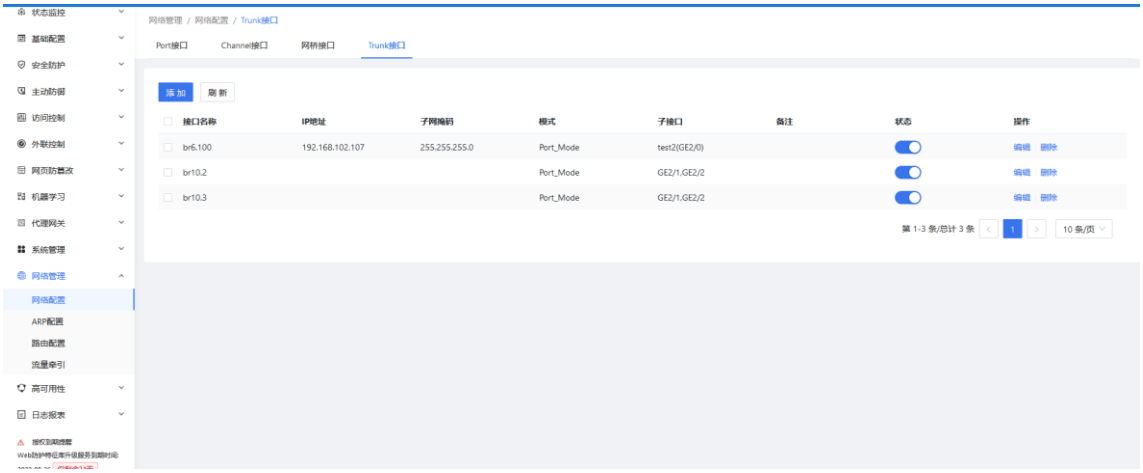
16.8 验证配置

(1) port 接口验证，GE2/1 接口和 GE2/2 接口在网桥 br10 中。



接口名称	备注	Channel接口	网桥接口	链路状态	状态	操作
GE0/0	-	none	MngtBridge	启用		编辑
GE0/1	-	test1	none	禁用		编辑
GE2/0	-	test2	none	禁用		编辑
GE2/1	-	none	br10	禁用		编辑
GE2/2	-	none	br10	禁用		编辑
GE2/3	-	1	none	禁用		编辑
GE2/4	-	2	none	禁用		编辑
GE2/5	-	2	none	禁用		编辑
GE2/6	-	none	br3	禁用		编辑
GE2/7	-	none	br3	禁用		编辑

(2) trunk 接口验证，br10.2 和 br10.3 子接口均为 GE2/1 接口和 GE2/2。



17 常见故障处理

17.1 WAF部署完毕查看无日志

- 首先，抓包，确认双向流量都经过了 WAF 才可以
- 如果报文带有 vlan tag，WAF 在对应 trunk 接口中需配置对应 vlan，这样才可以识别产生日志
- 开启访问日志开关查看是否有报文，有的话，证明配置无误，建议关闭访问日志开关，以免影响性能

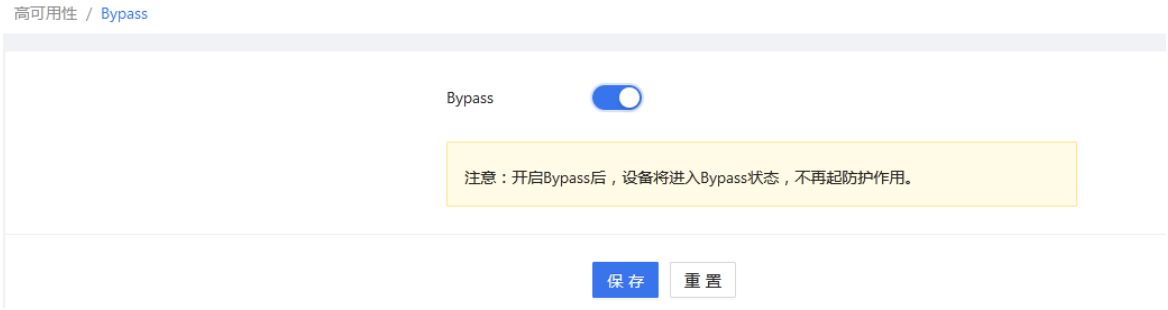
17.2 WAF部署完毕运行一段时间后，WAF出现无法访问的状况

如果遇到 WAF 无法访问，先 ping 管理口 IP 地址，如果无法连通，先联系管理员排查网络线路问题，再通过串口进行排查，如无法解决请联系新华三技术支持人员。

17.3 WAF防护的网站出现无法访问或者卡顿的现象

此类问题可能由于本身负载过高或者规则误拦截等问题造成，此时首要任务是使被保护站点恢复正常访问，保证业务的正常运作。情况紧急时，透明部署组网下，应将 WAF 切换到硬件 bypass 状态。待问题原因查明及解决了，再禁用硬件 Bypass，将 WAF 切换到正常模式。

图17-1 硬件 Bypass



如果确认是由于 WAF 规则引起业务问题，可在攻击日志模块中找到对应服务器 IP 的攻击日志，点击排除规则将其排除或者在防护策略中不启用误报的规则，确保业务正常。

注意

关于更多 WAF 故障处理说明，可参考产品对应的《故障处理手册》