UNIS W2000-G 系列 Web 应用防火墙

典型配置举例

目录

1 透明流模式部署配置举例

1.1 简介

透明流模式是 UNIS 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。

支持功能：扫描防护、HTTP 协议校验、特征防护、爬虫防护、防盗链、防跨站请求伪造、文件上传、文件下载、敏感信息检测、弱密码检测、虚拟补丁、访问顺序、敏感词防护、DDoS 防护、威胁情报。

支持协议：HTTP。

特点：Web 应用防火墙无须配置通信 IP，需配置管理 IP。

1.2 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。

1.3 使用限制

Web 应用防火墙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。

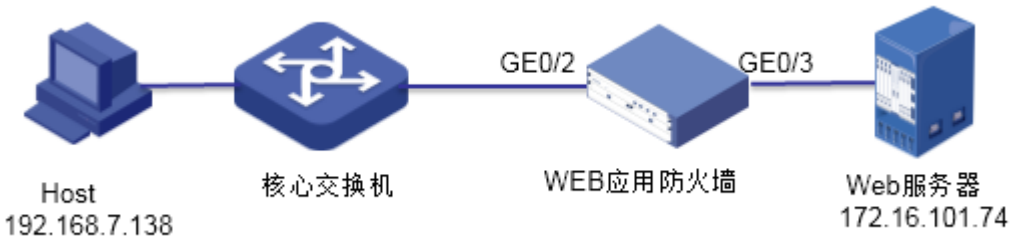
1.4 适用产品和版本

此配置举例在 E6713 版本上验证。

1.5 组网需求

如下图所示，Web 应用防火墙部署在核心交换机和 Web 服务器之间，串联接入网络，对 Web 服务器进行防护。

图1-1 组网图



1.6 配置思路

按照组网图组网。

(1) 创建新的网桥，并把接入网络的两个 port 口划分到新网桥中。

(2) 创建 HTTP 服务器，配置安全防护策略，对 Web 服务器进行防护。

1.7 配置步骤

1. 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>网络接口>网桥接口”中，点击增加，创建网桥“br10”。

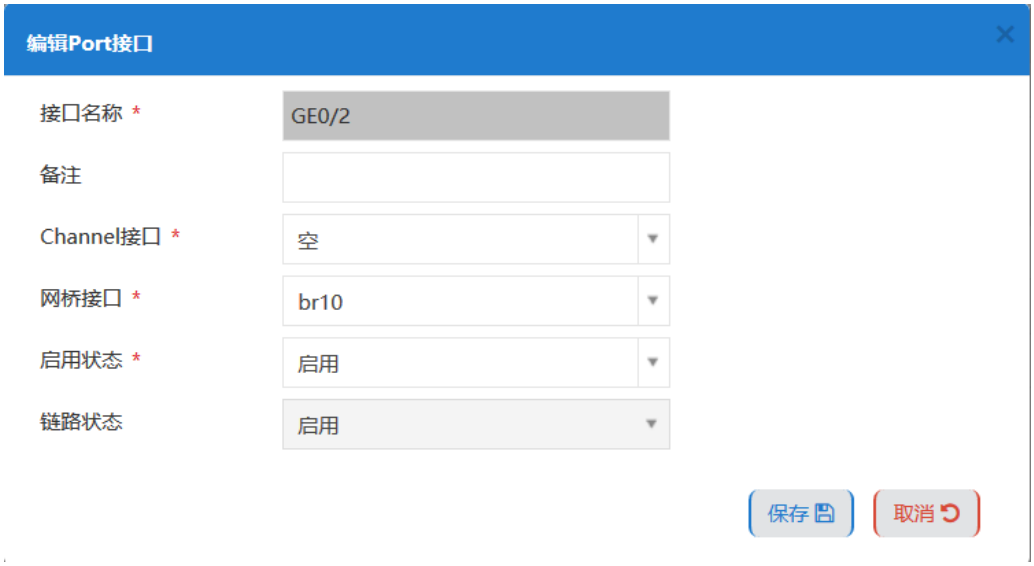
图1-2 新建网桥-br10

如下图所示，网桥 br10 中不需要配置 IP 地址，点击保存。

图1-3 保存网桥配置

如下图所示，在网络管理>网络接口>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1-4 port 口划分到新网桥



2. 创建 HTTP 服务器，对 Web 服务器进行防护。

如下图所示，选择菜单“服务器管理>普通服务器管理”进入普通服务器配置页面，点击增加，新建 HTTP 服务器，具体参数配置如下，防护模式选择流模式。配置完成后点击保存。

图1-5 创建 HTTP 服务器

如下图所示，选择“应用安全防护>Web 防护策略”，进入 Web 防护策略管理界面。点击增加，新增 Web 防护策略。在“服务器”中选择“test”服务器，根据需要进行防护策略的配置，配置完成后点击保存。

图1-6 配置安全防护策略

1.8 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。

(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。

(3) 选择"日志系统>攻击日志"，查看攻击日志，可以看到攻击拦截的详细信息，证明 Web 应用防火墙已经正常防护。

2 透明代理模式部署配置举例

2.1 简介

透明代理模式是 UNIS 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：扫描防护、HTTP 协议校验、特征防护、爬虫防护、防盗链、防跨站请求伪造、文件上传、文件下载、敏感信息检测、弱密码检测、虚拟补丁、访问顺序、敏感词防护、DDoS 防护、威胁情报。

支持协议：HTTP。

特点：Web 应用防火墙无须配置通信 IP，需配置管理 IP。

2.2 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。

2.3 使用限制

Web 应用防火墙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。

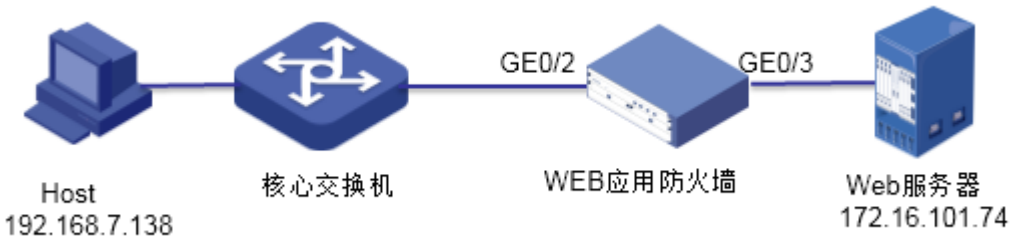
2.4 适用产品和版本

此配置举例在 E6713 版本上验证。

2.5 组网需求

如下图所示，Web 应用防火墙部署在核心交换机和 Web 服务器之间，串联接入网络，对 Web 服务器进行防护。

图2-1 组网图



2.6 配置思路

按照组网图组网。

(1) 创建新的网桥，并把接入网络的两个 port 口划分到新网桥中。

(2) 创建 HTTP 服务器，配置安全防护策略，对 Web 服务器进行防护。

2.7 配置步骤

1. 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>网络接口>网桥接口”中，点击增加，创建网桥 br10。

图2-2 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2-3 保存网桥配置

如下图所示，在网络管理>网络接口>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2-4 port 口划分到新网桥

2. 创建 HTTP 服务器，对 Web 服务器进行防护。

如下图所示，选择菜单“服务器管理>普通服务器管理”进入普通服务器配置页面，点击增加，新建 HTTP 服务器，具体参数配置如下，防护模式选择代理模式，客户端 IP 还原选择是。配置完成后点击保存。

图2-5 创建 HTTP 服务器

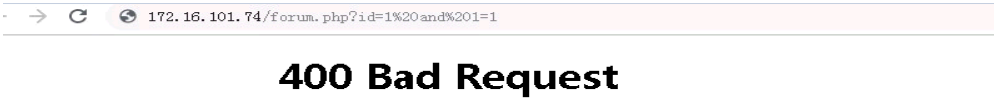
如下图所示，选择“应用安全防护>Web 防护策略”进入 Web 防护策略管理界面。点击增加，新增 Web 防护策略。在“服务器”中选择“test”服务器，根据需要进行防护策略的配置，配置完成后点击保存。

图2-6 配置安全防护策略

2.8 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。

(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



400 Bad Request

(3) 选择"日志系统>攻击日志"，查看攻击日志，可以看到攻击拦截的详细信息，证明 Web 应用防火墙已经正常防护。

3 透明反向代理模式部署配置举例

3.1 简介

透明反向代理模式是 UNIS 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。

透明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：扫描防护、HTTP 协议校验、特征防护、爬虫防护、防盗链、防跨站请求伪造、文件上传、文件下载、敏感信息检测、弱密码检测、虚拟补丁、访问顺序、敏感词防护、DDoS 防护、威胁情报。

支持协议：HTTP、HTTPS。

特点：Web 应用防火墙需配置通信 IP，需配置管理 IP。

3.2 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。

3.3 使用限制

Web 应用防火墙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。

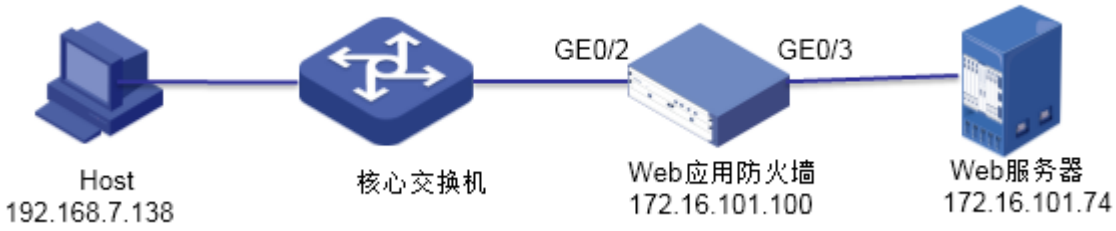
3.4 适用产品和版本

此配置举例在 E6713 版本上验证。

3.5 组网需求

如下图所示，Web 应用防火墙部署在核心交换机和 Web 服务器之间，串联接入网络，对 Web 服务器进行防护。

图3-1 组网图



3.6 配置思路

按照组网图组网。

(1) 创建新的网桥，并把接入网络的两个 port 口划分到新网桥中，配置网桥 IP 地址。

(2) 创建 HTTP 服务器，配置安全防护策略，对 Web 服务器进行防护。

3.7 配置步骤

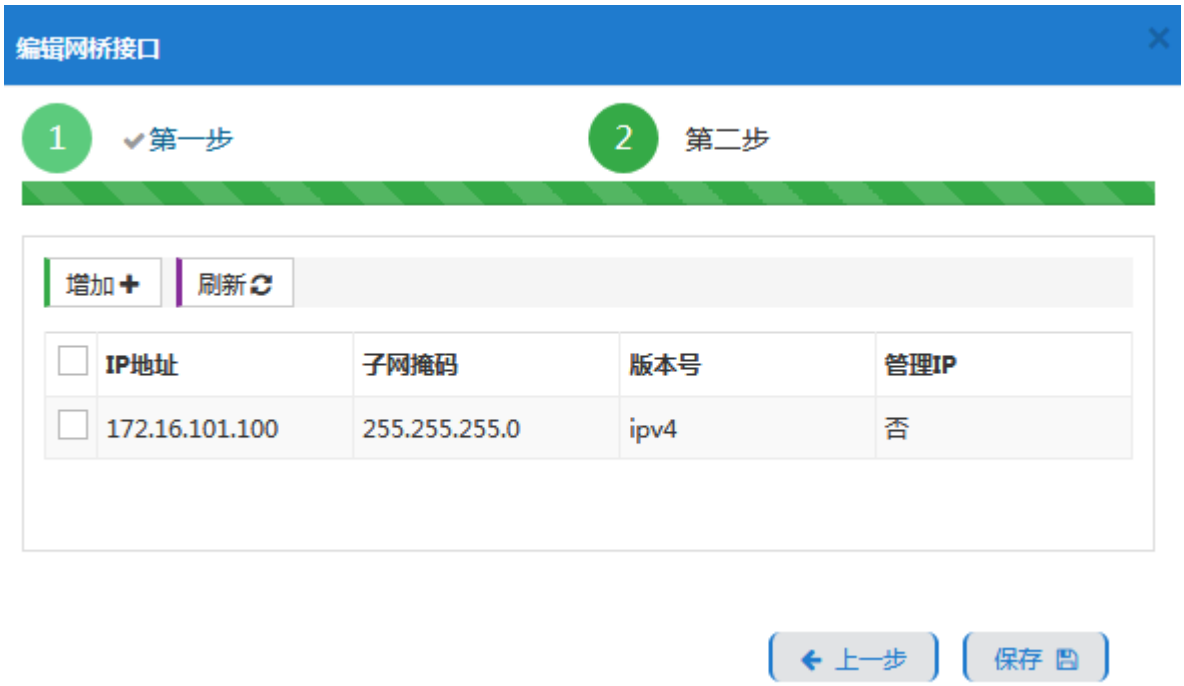
1. 创建新的网桥，并把接入网络的两个 port 口划分到新网桥中。

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

图3-2 新建网桥-br10

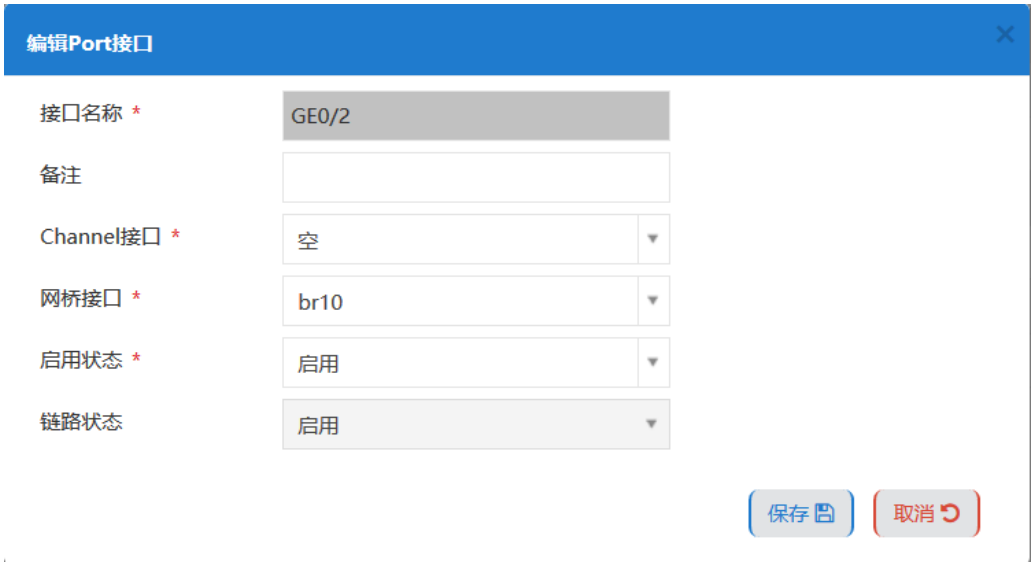
如下图所示，在创建网桥 br10 中增加业务 IP 地址。

图3-3 增加业务 IP 地址



如下图所示，在网络管理>网络接口>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3-4 port 口划分到新网桥



2. 创建 HTTP 服务器，对 Web 服务器进行防护。

如下图所示，选择菜单“服务器管理>普通服务器管理”进入普通服务器配置页面，点击“添加”HTTP 服务器，具体参数配置如下，客户端 IP 还原选择否。配置完成后点击保存。

图3-5 创建 HTTP 服务器（HTTPS 服务器需要上传证书和密钥）

如下图所示，选择“应用安全防护>Web 防护策略”进入 Web 防护策略管理界面。点击增加，新增 Web 防护策略。在“服务器”中选择“test”服务器，根据需要进行防护策略的配置，配置完成后点击保存。

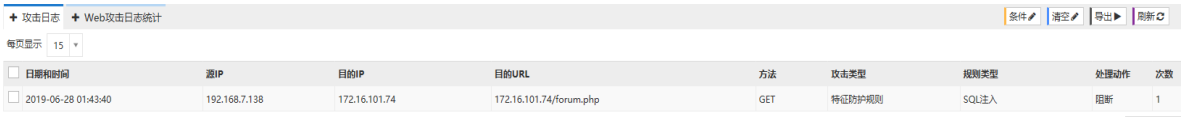
图3-6 配置安全防护策略

3.8 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。

(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。

(3) 选择"日志系统>攻击日志"，查看攻击日志，可以看到攻击拦截的详细信息，证明 Web 应用防火墙已经正常防护。



4 反向代理模式部署配置举例

4.1 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：扫描防护、HTTP 协议校验、特征防护、爬虫防护、防盗链、防跨站请求伪造、文件上传、文件下载、敏感信息检测、弱密码检测、虚拟补丁、访问顺序、敏感词防护、DDoS 防护、威胁情报。

支持协议：HTTP、HTTPS。

特点：Web 应用防火墙需配置通信 IP，需配置管理 IP。

4.2 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。

4.3 使用限制

Web 应用防火墙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。

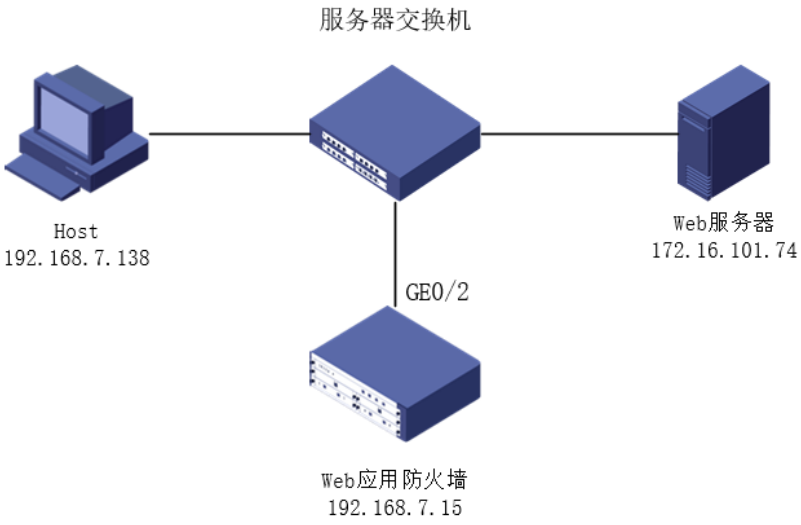
4.4 适用产品和版本

此配置举例在 E6713 版本上验证。

4.5 组网需求

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

图4-1 组网图



4.6 配置思路

按照组网图组网。

(1) 创建新的网桥，并把接入网络的接口划分到新网桥中。配置 WAF 业务 IP 和路由。

(2) 创建 HTTP 服务器，配置安全防护策略，对 Web 服务器进行防护。

4.7 配置步骤

1. 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>网络接口>网桥接口”中，点击增加，创建网桥 br10。

图4-2 新建网桥-br10

如下图所示，在网桥 br10 中增加业务 IP 地址。

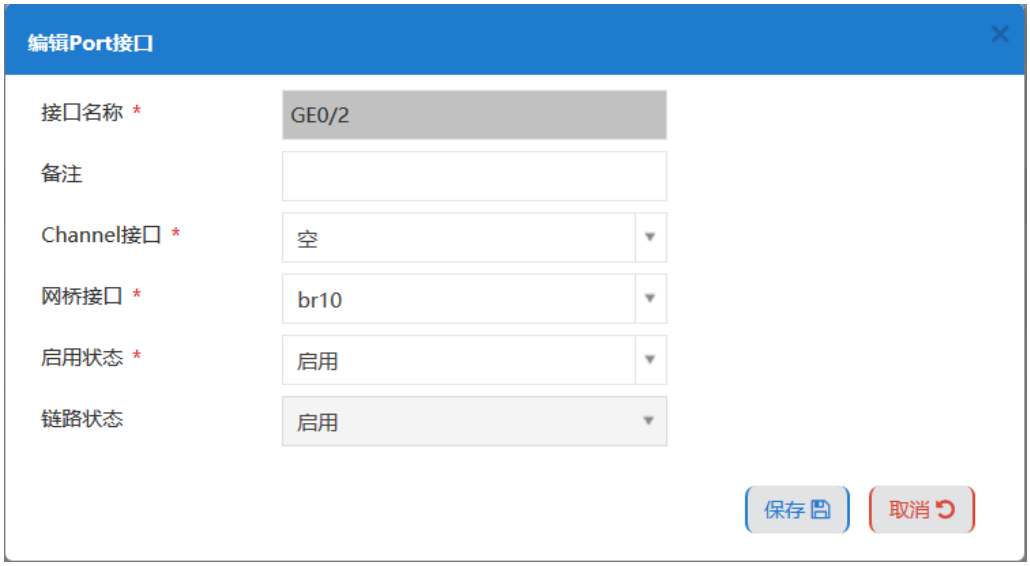
图4-3 增加业务 IP 地址

如下图所示，在网络管理>路由配置中增加路由。

图4-4 增加路由

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

图4-5 port 口划分到新网桥



2. 创建 HTTP 服务器，对 Web 服务器进行防护。

如下图所示，选择菜单“服务器管理>普通服务器管理”进入普通服务器配置页面，点击增加，新建 HTTP 服务器，具体参数配置如下，防护模式选择代理模式，客户端 IP 还原选择否。配置完成后点击保存。

图4-6 创建 HTTP 服务器（HTTPS 服务器需要上传证书和密钥）

如下图所示，选择菜单“服务器管理>代理服务器管理”，进入代理服务器配置页面，点击增加，新建 HTTP 代理服务器，IP 地址填写 Web 应用防火墙业务 IP 地址，具体参数配置如下。配置完成后点击保存。

图4-7 增加代理服务器

如下图所示，选择“应用安全防护>Web 防护策略”进入 Web 防护策略管理界面。点击增加，新增 Web 防护策略。在“服务器”中选择“test”服务器，根据需要进行防护策略的配置，配置完成后点击保存。

图4-8 配置安全防护策略

4.8 验证配置

(1) 访问 Web 应用防火墙的 IP 地址，URL 为 http://192.168.7.15，可以正常访问。

(1) 选择"日志系统>攻击日志"，查看攻击日志，可以看到攻击拦截的详细信息，证明 Web 应用防火墙已经正常防护。

(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。

5 反向代理模式 HTTPS 服务器部署配置举例

5.1 简介

在反代模式下支持 HTTPS 协议的解密，解密需要上传服务器 HTTPS 证书及密钥文件，HTTPS 解密需要耗费大量性能。

5.2 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。

5.3 使用限制

Web 应用防火墙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。

仅在反向代理模式下支持 HTTPS 解密。

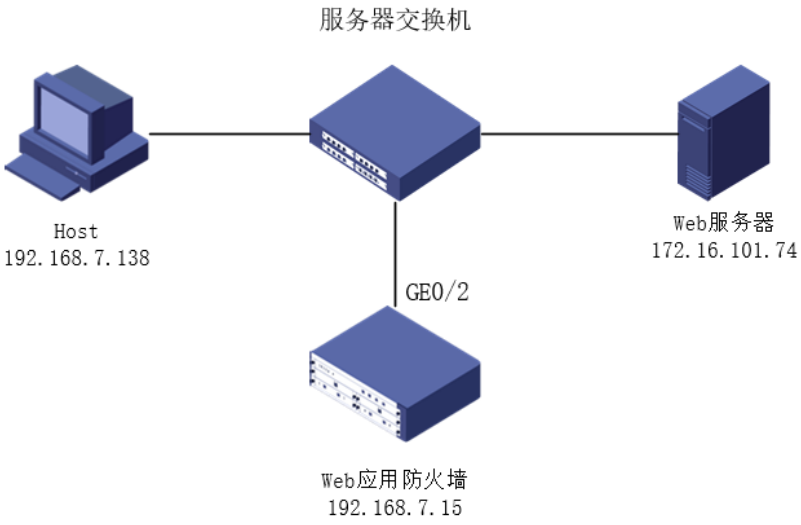
5.4 适用产品和版本

此配置举例在 E6713 版本上验证。

5.5 组网需求

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

图5-1 组网图



5.6 配置思路

按照组网图组网。

(1) 创建新的网桥，并把接入网络的接口划分到新网桥中。配置 WAF 业务 IP 和路由；

(2) 创建 HTTPS 服务器，需上传服务器证书和 key 文件；

(3) 创建 HTTPS 代理服务器，同样需上传服务器证书和 key 文件；

(4) 配置安全防护策略，对 Web 服务器进行防护。

5.7 配置步骤

1. 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>网络接口>网桥接口”中，点击增加，创建网桥 br10。

图5-2 新建网桥-br10

如下图所示，在网桥 br10 中增加业务 IP 地址。

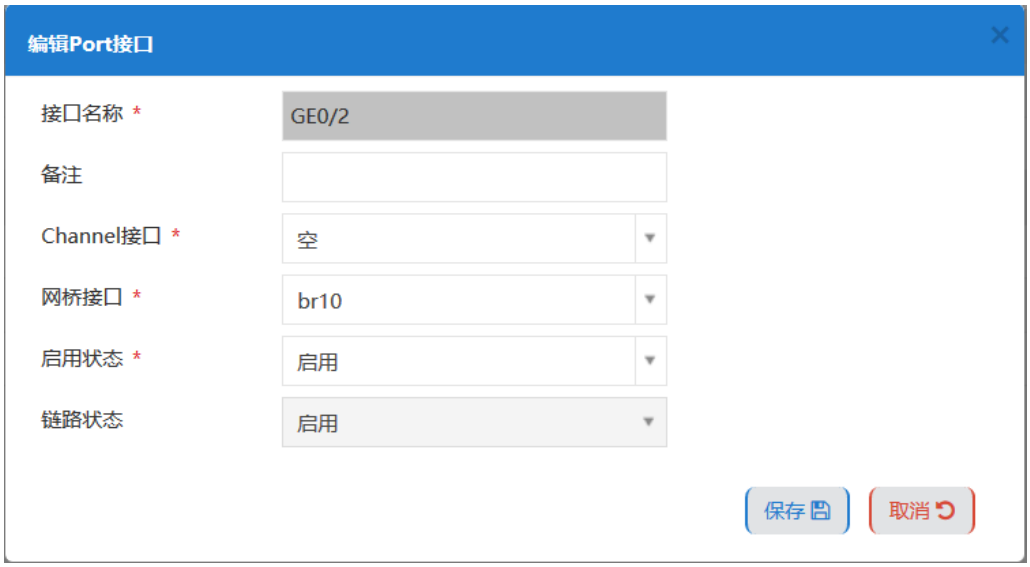
图5-3 增加业务 IP 地址

如下图所示，在网络管理>路由配置中增加路由。

图5-4 增加路由

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

图5-5 port 口划分到新网桥



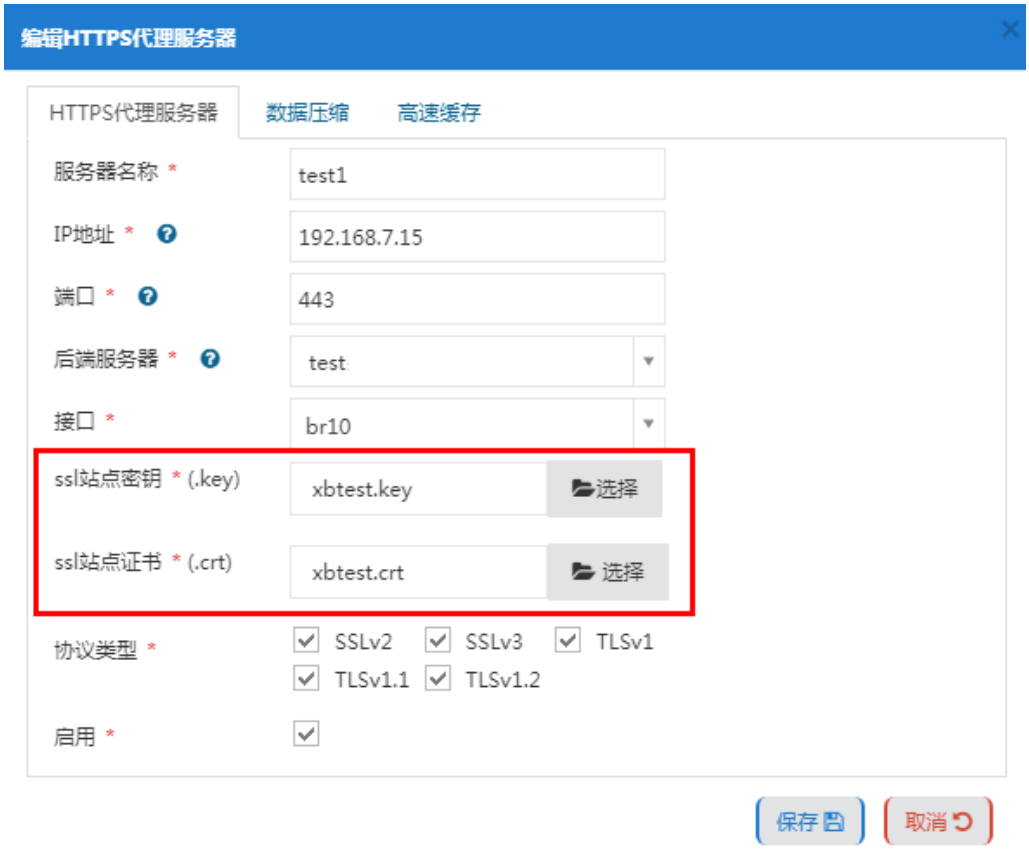
2. 创建 HTTP 服务器，对 Web 服务器进行防护。

如下图所示，选择菜单“服务器管理>普通服务器管理>HTTPS 服务器”进入 HTTPS 服务器配置页面，点击增加，新建 HTTPS 服务器，具体参数配置如下，防护模式选择代理模式，客户端 IP 还原选择否。配置完成后点击保存。

图5-6 创建 HTTPS 服务器

如下图所示，选择菜单“服务器管理>代理服务器管理>HTTPS 代理服务器”，进入代理服务器配置页面，点击增加，新建 HTTPS 代理服务器，IP 地址填写 WAF 业务 IP 地址，具体参数配置如下。配置完成后点击保存。

图5-7 增加 HTTPS 代理服务器



如下图所示，选择“应用安全防护>Web 防护策略”进入 Web 防护策略管理界面。点击增加，新增 Web 防护策略。在“服务器”中选择“test”服务器，根据需要进行防护策略的配置，配置完成后点击保存。

图5-8 配置安全防护策略

5.8 验证配置

(1) 访问 Web 应用防火墙的 IP 地址，URL 为 https://192.168.7.15，可以正常访问。

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

400 Bad Request

(3) 选择"日志系统>攻击日志"，查看攻击日志，可以看到攻击拦截的详细信息，证明 Web 应用防火墙已经正常防护。

6 旁路镜像检测模式部署配置举例

6.1 简介

旁路镜像检测模式是UNIS 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。

支持功能：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。

支持协议：HTTP。

特点：Web 应用防火墙无须配置通信 IP，需配置管理 IP。

6.2 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。

6.3 使用限制

交换机要保证镜像双向流量。

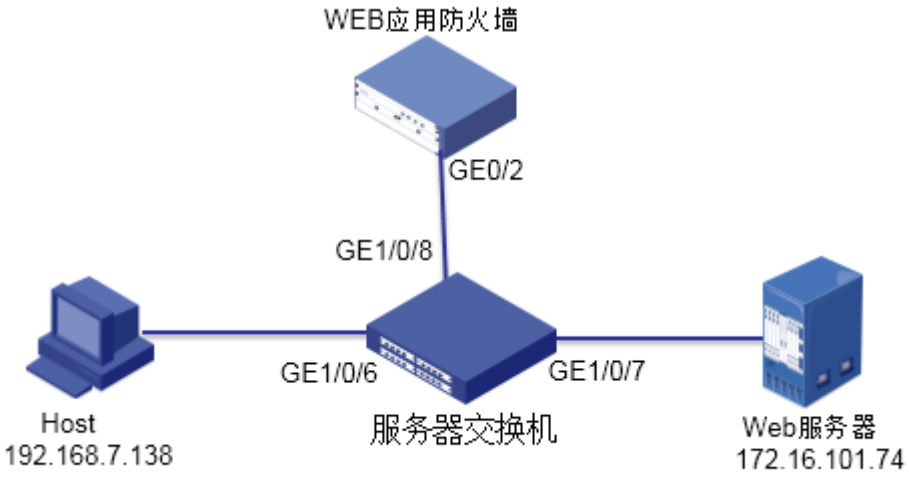
6.4 适用产品和版本

此配置举例在 E6713 版本上验证。

6.5 组网需求

如下图所示，Web 应用防火墙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6-1 组网图



6.6 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) 创建新的网桥，并把接入网络的 port 口划分到新网桥中。

(3) 创建 HTTP 服务器，配置安全防护策略，对 Web 服务器进行防护。

6.7 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，创建 vlan101 和 vlan102，并配置 IP 地址，分别作为客户端和服务器网关。

图6-2 将两个镜像口划分 VLAN 并配置 IP 地址。

```
[SWUP_For_AVG_NewWAF]vlan 101
[SWUP_For_AVG_NewWAF-vlan101]port GigabitEthernet 1/0/6        创建vlan101，将GE1/0/6口划入该vlan
[SWUP_For_AVG_NewWAF-vlan101]vlan 102
[SWUP_For_AVG_NewWAF-vlan102]port GigabitEthernet 1/0/7        创建vlan102，将GE1/0/7口划入该vlan
[SWUP_For_AVG_NewWAF]int vlan 101
[SWUP_For_AVG_NewWAF-Vlan-interface101]ip address 192.168.7.1 24
[SWUP_For_AVG_NewWAF-Vlan-interface101]int vlan 102            为vlan配置IP地址，作为客户端
[SWUP_For_AVG_NewWAF-Vlan-interface102]ip address 172.16.101.1 24   和服务器网关地址。
[SWUP_For_AVG_NewWAF-Vlan-interface102]quit
```

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

图6-3 交换机上的镜像组配置

```
[SWUP_For_AVG_NewWAF]mirroring-group 2 local                    创建镜像组2
[SWUP_For_AVG_NewWAF]mirroring-group 2 mirroring-port GigabitEthernet 1/0/7 both
[SWUP_For_AVG_NewWAF]mirroring-group 2 monitor-port GigabitEthernet 1/0/8
[SWUP_For_AVG_NewWAF]dis mirroring-group 2          将GE1/0/7双向流量镜像至监听口GE1/0/8
Mirroring group 2:
  Type: Local
  Status: Active
  Mirroring port:
    GigabitEthernet1/0/7 Both
  Monitor port: GigabitEthernet1/0/8
```

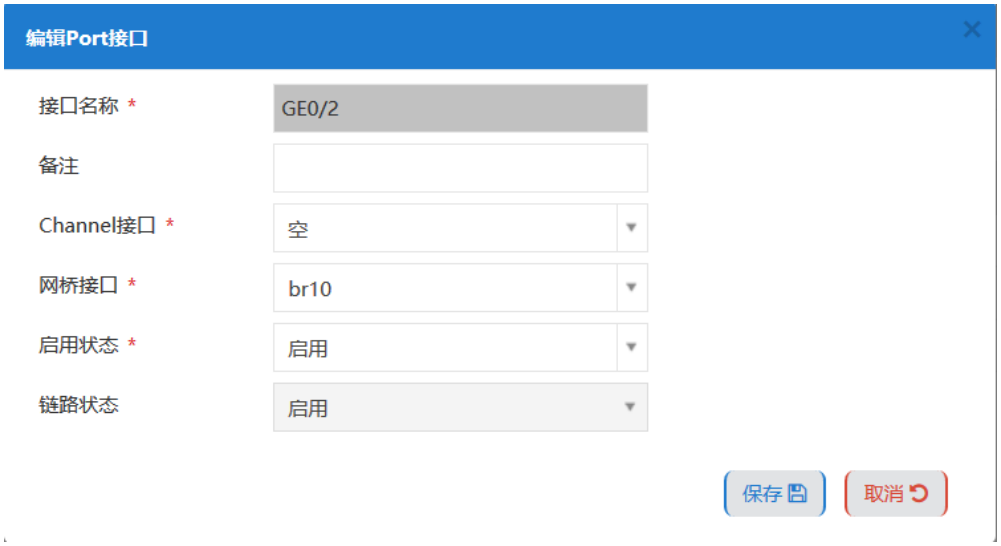
2. 创建新的网桥，并把接入网络的接口划分到新网桥中。

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

图6-4 新建网桥-br10

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

图6-5 port 口划分到新网桥



3. 创建 HTTP 服务器，对 Web 服务器进行防护。

如下图所示，选择菜单“服务器管理>普通服务器管理”进入普通服务器配置页面，点击增加，新建 HTTP 服务器，具体参数配置如下，部署模式选择旁路，防护模式为流模式。配置完成后点击保存。

图6-6 创建 HTTP 服务器

如下图所示，选择“应用安全防护>Web 防护策略”进入 Web 防护策略管理界面。点击增加，新增 Web 防护策略。在“服务器”中选择“test”服务器，根据需要进行防护策略的配置，配置完成后点击保存。

图6-7 配置安全防护策略

6.8 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。

(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，Web 应用防火墙上记录攻击日志。

(3) 选择"日志系统>攻击日志"，查看攻击日志，可以看到攻击拦截的详细信息，证明 Web 应用防火墙已经正常检测到攻击流量。

7 旁路镜像检测&阻断模式部署配置举例

7.1 简介

旁路镜像检测&阻断模式是 UNIS 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。

支持功能：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。

支持协议：HTTP。

特点：Web 应用防火墙无须配置通信 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

交换机须镜像连接服务器接口的双向流量，否则阻断效果很差。

旁路阻断模式下 Web 应用防火墙的部署需要尽可能接近服务器。

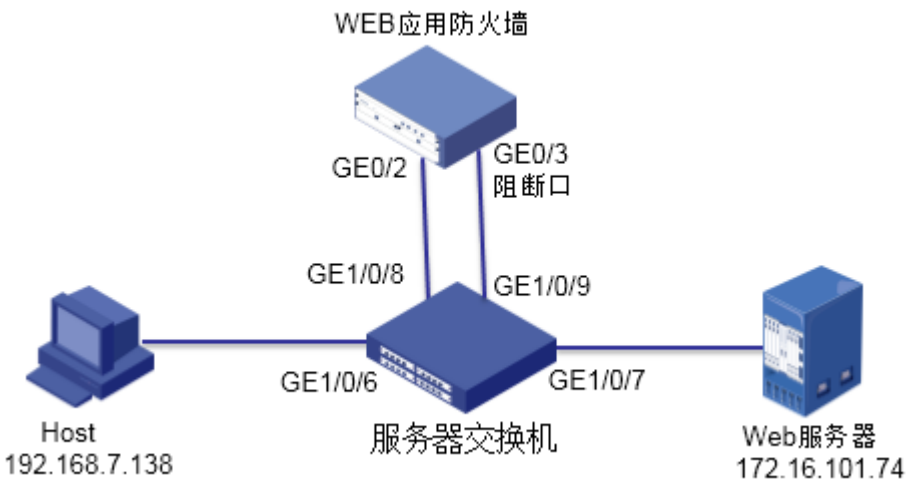
7.4 适用产品和版本

此配置举例在 E6713 版本上验证。

7.5 组网需求

如下图所示，Web 应用防火墙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7-1 组网图



7.6 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) 创建新的网桥，并把接入网络的 port 口划分到新网桥中。

(3) 创建 HTTP 服务器，配置安全防护策略，对 Web 服务器进行防护。

7.7 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，创建 vlan101 和 vlan102，并配置 IP 地址，分别作为客户端和服务器网关。

图7-2 将两个镜像口划分 VLAN 并配置 IP 地址。

```
[SWUP_For_AVG_NewWAF]vlan 101
[SWUP_For_AVG_NewWAF-vlan101]port GigabitEthernet 1/0/6        创建vlan101，将GE1/0/6口划入该vlan
[SWUP_For_AVG_NewWAF-vlan101]vlan 102
[SWUP_For_AVG_NewWAF-vlan102]port GigabitEthernet 1/0/7        创建vlan102，将GE1/0/7口划入该vlan
[SWUP_For_AVG_NewWAF]int vlan 101
[SWUP_For_AVG_NewWAF-Vlan-interface101]ip address 192.168.7.1 24
[SWUP_For_AVG_NewWAF-Vlan-interface101]int vlan 102            为vlan配置IP地址，作为客户端
[SWUP_For_AVG_NewWAF-Vlan-interface102]ip address 172.16.101.1 24   和服务器网关地址。
[SWUP_For_AVG_NewWAF-Vlan-interface102]quit
```

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

图7-3 交换机上的镜像组配置

```
[SWUP_For_AVG_NewWAF]mirroring-group 2 local                    创建镜像组2
[SWUP_For_AVG_NewWAF]mirroring-group 2 mirroring-port GigabitEthernet 1/0/7 both
[SWUP_For_AVG_NewWAF]mirroring-group 2 monitor-port GigabitEthernet 1/0/8
[SWUP_For_AVG_NewWAF]dis mirroring-group 2                      将GE1/0/7双向流量镜像至监听口GE1/0/8
Mirroring group 2:
   Type: Local
   Status: Active
   Mirroring port:
      GigabitEthernet1/0/7 Both
   Monitor port: GigabitEthernet1/0/8
```

交换机接 WAF 的监听口 GE1/0/8 配置为默认 vlan1，交换机接 WAF 阻断口 GE1/0/9vlan 配置为服务器侧 vlan，即 vlan102。

```
[SWUP_For_AVG_NewWAF]int GigabitEthernet 1/0/9
[SWUP_For_AVG_NewWAF-GigabitEthernet1/0/9]port link-type access
[SWUP_For_AVG_NewWAF-GigabitEthernet1/0/9]port access vlan 102
```

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>网络接口>网桥接口”中，点击增加，创建网桥 br10。

图7-4 新建网桥-br10

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

图7-5 新建网桥-br11

如下图所示，在网络管理>网络接口>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7-6 port 口划分到新网桥

3. 创建 HTTP 服务器，对 Web 服务器进行防护。

如下图所示，选择菜单“服务器管理>普通服务器管理”进入普通服务器配置页面，点击增加，新建 HTTP 服务器，具体参数配置如下，部署模式选择旁路，阻断接口选择 GE0/3。配置完成后点击保存。

图7-7 创建 HTTP 服务器

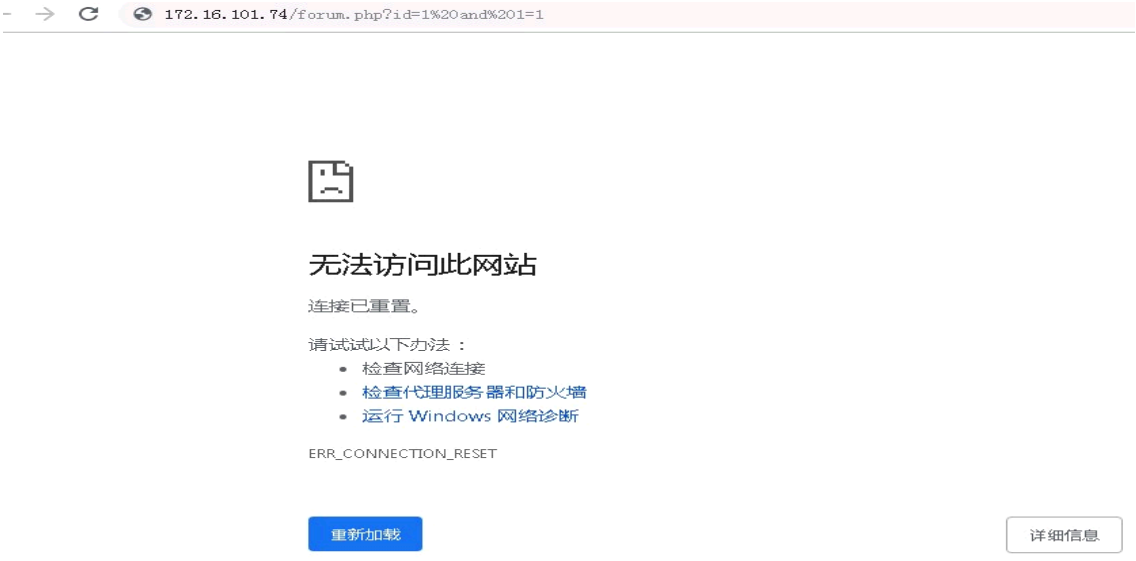
如下图所示，选择“应用安全防护>Web 防护策略”进入 Web 防护策略管理界面。点击增加，新增 Web 防护策略。在“服务器”中选择“test”服务器，根据需要进行防护策略的配置，配置完成后点击保存。

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。

(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。



(3) 选择"日志系统>攻击日志"，查看攻击日志，可以看到攻击拦截的详细信息，证明 Web 应用防火墙已经正常防护。

8 透明代理双机模式部署配置举例

8.1 简介

透明代理双机模式是 UNIS Web 应用防火墙在网站防护中常用的部署模式，两台 Web 应用防火墙串联在网络中，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。

透明代理双机模式仅支持主备模式。

支持功能：扫描防护、HTTP 协议校验、特征防护、爬虫防护、防盗链、防跨站请求伪造、文件上传、文件下载、敏感信息检测、弱密码检测、虚拟补丁、访问顺序、敏感词防护、DDoS 防护、威胁情报。

支持协议：HTTP。

特点：Web 应用防火墙需配置通信 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

Web 应用防火墙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。

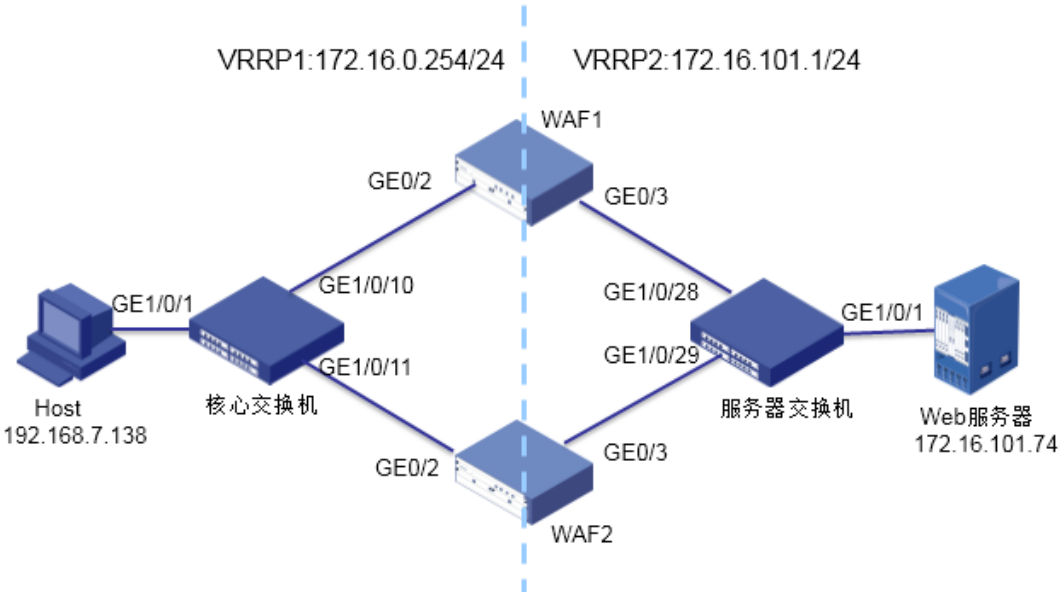
8.4 适用产品和版本

此配置举例在 E6713 版本上验证。

8.5 组网需求

如下图所示，Web 应用防火墙部署在核心交换机和服务器区交换机之间，核心交换机作为三层设备，客户端网关配置在该交换机上，交换机到服务端通过静态路由指向 VRRP1 地址，服务器交换机作为二层交换机，只做报文转发，服务器网关直接指向 VRRP2 地址。两台 WAF 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) 配置核心交换机和服务器交换机。

(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) 添加 HA 管理的 VRRP 配置，配置双机主备部署。

(4) 创建 HTTP 服务器，配置安全防护策略，对 Web 服务器进行防护。

8.7 配置步骤

1. 配置核心交换机

创建 vlan101 和 vlan172，并配置 IP 地址，作为客户端网关及 vlan172 接口地址。

[SWUP_For_AVG_NewWAF]vlan 101

[SWUP_For_AVG_NewWAF-vlan101]port GigabitEthernet 1/0/1

[SWUP_For_AVG_NewWAF-vlan101]vlan 172

[SWUP_For_AVG_NewWAF-vlan172]port GigabitEthernet 1/0/10

[SWUP_For_AVG_NewWAF-vlan172]port GigabitEthernet 1/0/11

[SWUP_For_AVG_NewWAF-vlan172]int vlan 101

[SWUP_For_AVG_NewWAF-Vlan-interface101]ip address 192.168.7.1 24

[SWUP_For_AVG_NewWAF-Vlan-interface101]int vlan 172

[SWUP_For_AVG_NewWAF-Vlan-interface172]ip address 172.16.0.1 24

[SWUP_For_AVG_NewWAF-Vlan-interface172]quit

添加交换机到 WAF 的静态路由

[SWUP_For_AVG_NewWAF]ip route-static 172.16.101.0 24 172.16.0.254

2. 配置服务器交换机

创建 vlan102，将 GE1/0/1、GE1/0/28、GE1/0/29 划入该 vlan。

[SWDown_For_AVG_NewWAF]vlan 102

[SWDown_For_AVG_NewWAF-vlan102]port GigabitEthernet 1/0/1

[SWDown_For_AVG_NewWAF-vlan102]port GigabitEthernet 1/0/28

[SWDown_For_AVG_NewWAF-vlan102]port GigabitEthernet 1/0/29

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（以 WAF1 为例，WAF2 对比进行配置）。

如下图所示，在“网络管理>网络接口>网桥接口”中，点击增加，创建网桥 br100。

图8-2 新建网桥-br100

如下图所示，在桥 br100 上添加业务 IP。

图8-3 添加业务 IP-br100

如下图所示，在“网络管理>网络接口>网桥接口”中，点击增加，创建网桥 br200。

图8-4 新建网桥-br200

如下图所示，在桥 br200 上添加业务 IP。

图8-5 添加业务 IP-br200

如下图所示，在网络管理>网络接口>Port 接口中编辑 port 接口。接口 GE0/2 的“网桥接口”选择 br100，GE0/3 的“网桥接口”选择 br200。

图8-6 port 口划分到新网桥

4. 添加 VRRP 策略，配置双机模式。

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

如下图所示，第一步配置冗余 ID 及设备状态，“冗余 ID”为 1，绑定接口选择上联接口“br100”，具体配置参数如下，配置完成点击下一步。

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。

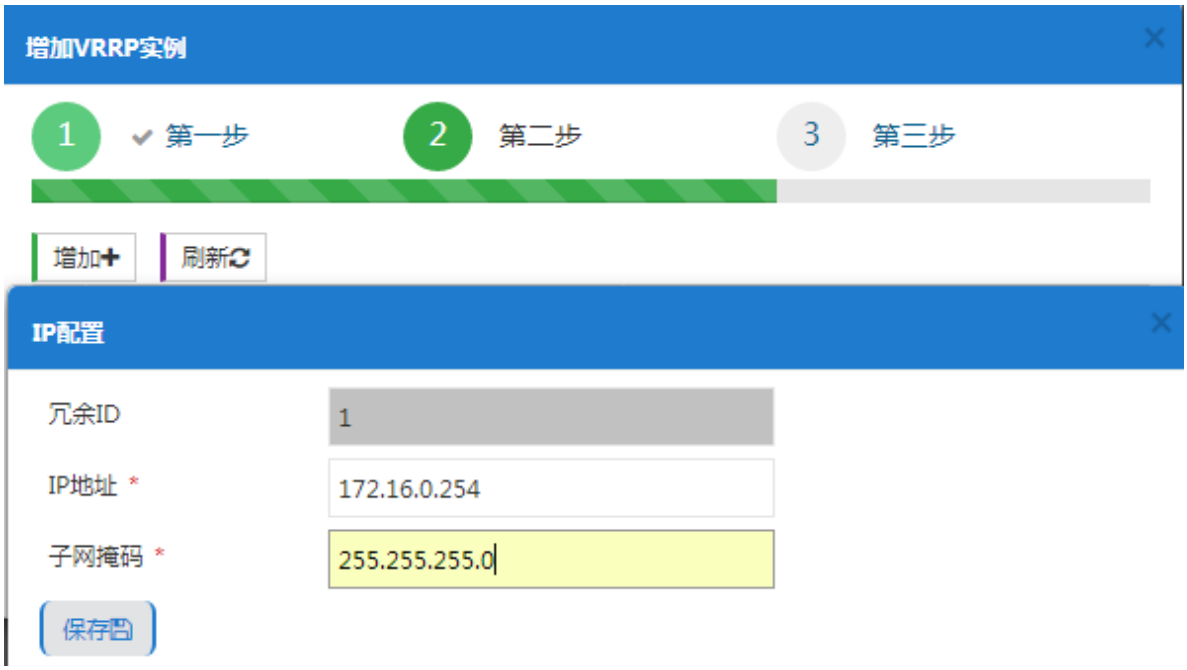
注：配置备机时保持与主机“冗余 ID”相同，“优先级”低于 100，“状态”为备。

下面截图以配置主机为例：

图8-7 创建 VRRP 实例-1

如下图所示，第二步配置虚拟 IP，点击增加，新增虚拟 IP，此处注意备机与主机冗余 IP 相同，配置完成点击下一步。

图8-8 创建 VRRP 实例-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 br100 的接口 GE0/2，配置完成点击保存。

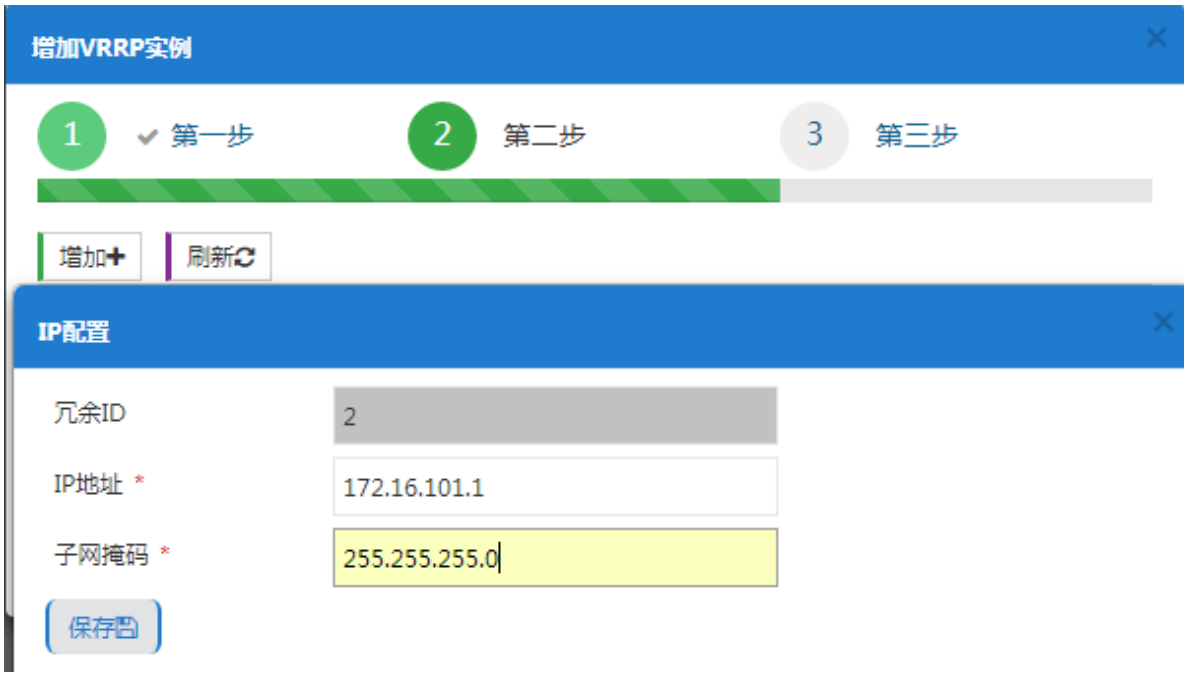
图8-9 创建 VRRP 实例-3

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“br200”，其余配置与“冗余 ID”1 的配置相同，配置完成点击下一步。

图8-10 创建 VRRP 实例-4

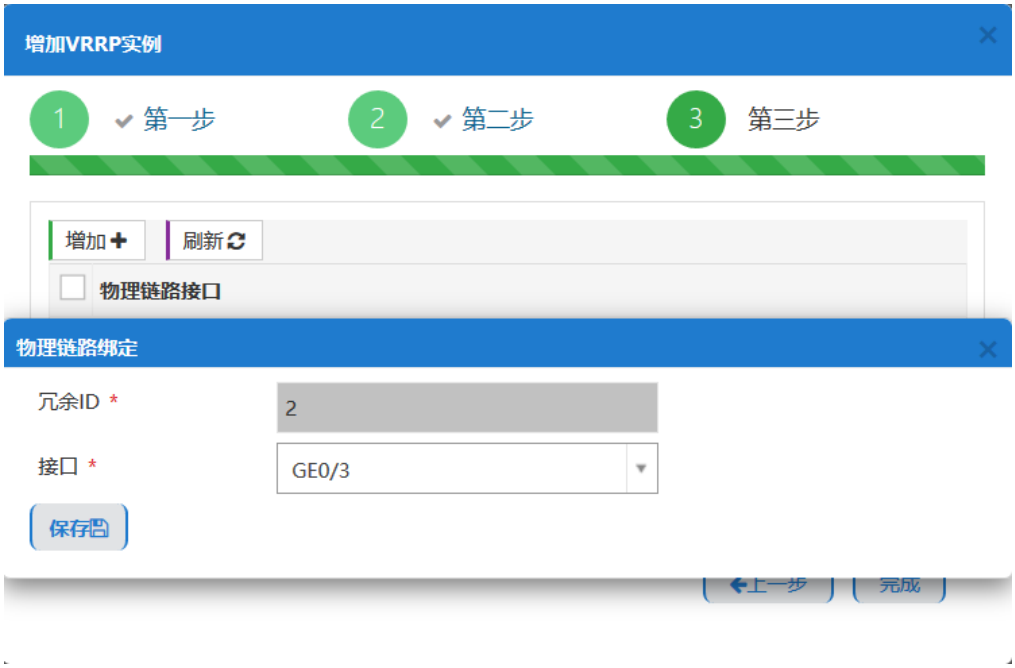
如下图所示，第五步配置虚拟 IP，点击增加，新增虚拟 IP，此处注意备机与主机冗余 IP 相同，配置完成点击下一步。

图8-11 创建 VRRP 实例-5



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 br200 的接口 GE0/3，配置完成点击保存。

图8-12 创建 VRRP 实例-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。

图8-13 创建 VRRP 组

如下图所示，应用添加完成的“test”VRRP 组。

图8-14 应用 VRRP

5. 创建 HTTP 服务器，对 Web 服务器进行防护（此处 WAF1 和 WAF2 配置相同）。

如下图所示，选择菜单“服务器管理>普通服务器管理”进入普通服务器配置页面，点击增加，新建 HTTP 服务器，具体参数配置如下，防护模式选择代理模式。配置完成后点击保存。

图8-15 创建 HTTP 服务器

如下图所示，选择“应用安全防护>Web 防护策略”进入 Web 防护策略管理界面。点击增加，新增 Web 防护策略。在“服务器”中选择“test”服务器，根据需要进行防护策略的配置，配置完成后点击保存。

图8-16 配置安全防护策略

8.8 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。

(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。

(3) 选择"日志系统>攻击日志"，查看攻击日志，可以看到攻击拦截的详细信息，证明 Web 应用防火墙已经正常防护。

(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。

(5) 在备机上查看有攻击日志，证明流量已切换至备机。

9 反向代理双机模式部署配置举例

9.1 简介

Web 应用防火墙旁路在网络中，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 Web 应用防火墙的 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。

反向代理双机模式仅支持主备模式。

支持功能：扫描防护、HTTP 协议校验、特征防护、爬虫防护、防盗链、防跨站请求伪造、文件上传、文件下载、敏感信息检测、弱密码检测、虚拟补丁、访问顺序、敏感词防护、DDoS 防护、威胁情报。

支持协议：HTTP、HTTPS。

特点：Web 应用防火墙需配置通信 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

Web 应用防火墙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，确保客户端、服务端和 Web 应用防火墙网络可达。

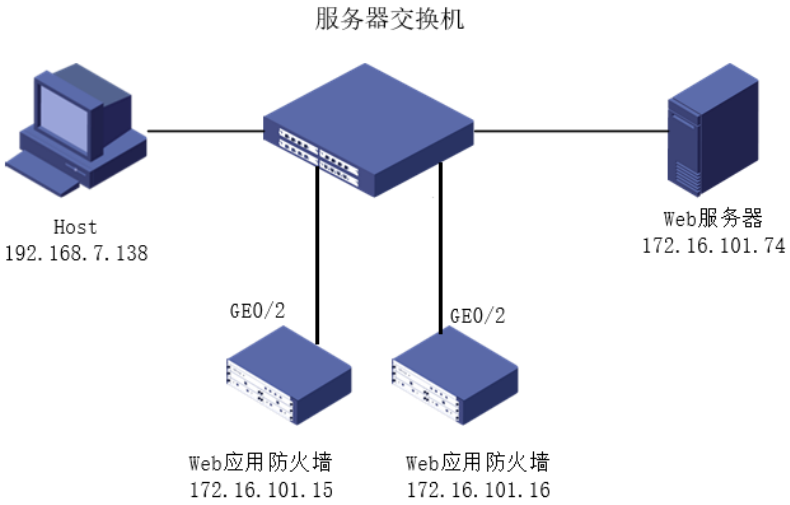
9.4 适用产品和版本

此配置举例在 E6713 版本上验证。

9.5 组网需求

如下图所示，两台 Web 应用防火墙旁路部署在服务器区交换机上，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) 创建新的网桥，并把接入网络的 port 口划分到新网桥中。

(2) 添加 HA 管理的 VRRP 配置，配置双机主备部署。

(3) 创建 HTTP 服务器，配置安全防护策略，对 Web 服务器进行防护。

9.7 配置步骤

1. 创建新的网桥，并把接入网络的 port 口划分到新网桥中。

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

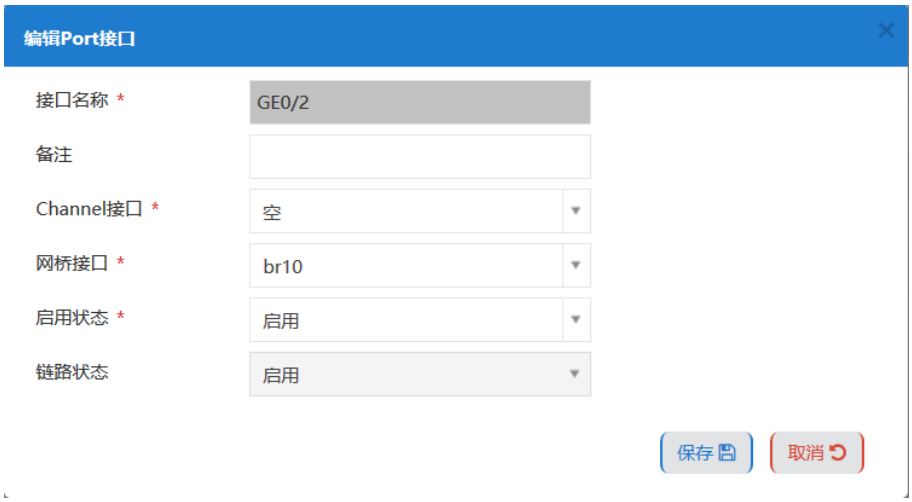
图9-2 新建网桥-br10

如下图所示，在网桥 br10 上添加业务 IP（另外一台 Web 应用防火墙 br10 上业务 IP 为 172.16.101.16）。

图9-3 添加业务 IP-br10

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

图9-4 port 口划分到新网桥



2. 添加 VRRP 策略，配置双机模式。

选择菜单“HA 管理>VRRP 配置”进入 VRRP 配置页面，点击增加，新增 VRRP 实例。

如下图所示，第一步配置冗余 ID 及设备状态，“冗余 ID”为 1，绑定接口选择接口“br10”,具体配置参数如下，配置完成点击下一步。

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。

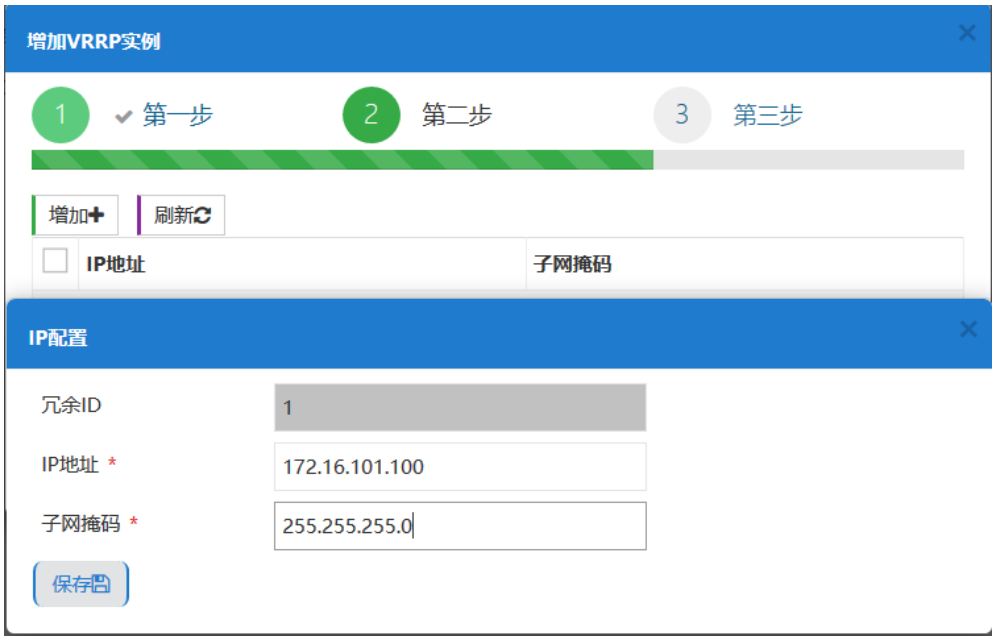
注：配置备机时保持与主机“冗余 ID”相同，“优先级”低于 100，“状态”为备。

下面截图以主设备为例：

图9-5 创建 VRRP 实例-1

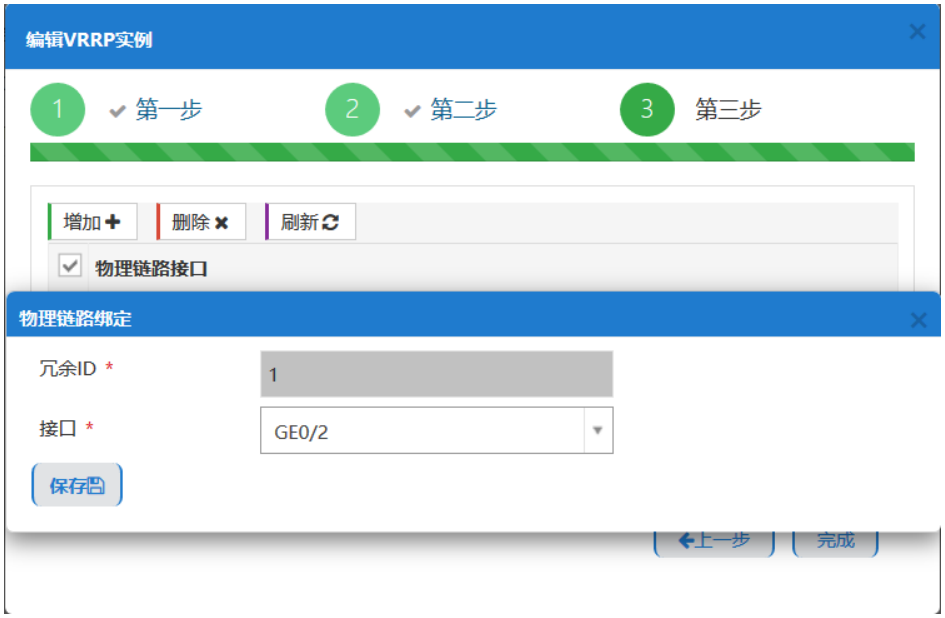
如下图所示，第二步配置虚拟 IP，点击增加，新增虚拟 IP，此处注意备机与主机冗余 IP 相同，配置完成点击下一步。

图9-6 创建 VRRP 实例-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9-7 创建 VRRP 实例-3



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。

图9-8 创建 VRRP 组

如下图所示，应用添加完成的“test”VRRP 组。

图9-9 应用 VRRP

3. 创建 HTTP 服务器，对 Web 服务器进行防护。

如下图所示，选择菜单“服务器管理>普通服务器管理”进入普通服务器配置页面，点击增加，新建 HTTP 服务器，具体参数配置如下，其中 IP 地址和端口为真实服务器的 IP 和端口，防护模式选择代理模式。配置完成后点击保存。

图9-10 创建 HTTP 服务器

如下图所示，选择菜单“服务器管理>代理服务器管理”进入代理服务器配置页面，点击“增加”，新建 HTTP 代理服务器，IP 地址填写 Web 应用防火墙配置 VRRP 的虚 IP，具体参数配置如下，后端服务器选择“test”。配置完成后点击保存。

图9-11 创建代理服务器

如下图所示，选择“应用安全防护>Web 防护策略”进入 Web 防护策略管理界面。点击增加，新增 Web 防护策略。在“服务器”中选择“test”服务器，根据需要进行防护策略的配置，配置完成后点击保存。

图9-12 配置安全防护策略

9.8 验证配置

(1) 访问受保护的网站，URL 为 http://172.16.101.100，可以正常访问。

(2) 加上攻击参数再次访问网站，URL 为 http://172.16.101.100/forum.php?id=1 and 1=1，网站不能访问。

(3) 选择"日志系统>攻击日志"，查看攻击日志，可以看到攻击拦截的详细信息，证明 Web 应用防火墙已经正常防护。

(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://172.16.101.100/forum.php?id=1 and 1=1，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。

10 链路聚合部署配置举例

10.1 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。

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

Web 应用防火墙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。

Web 应用防火墙默认支持静态聚合，如需配置动态链路聚合，需在命令行执行 channel -M -m 4 命令开启动态模式，执行完命令后需在重启 Web 应用防火墙后配置生效。

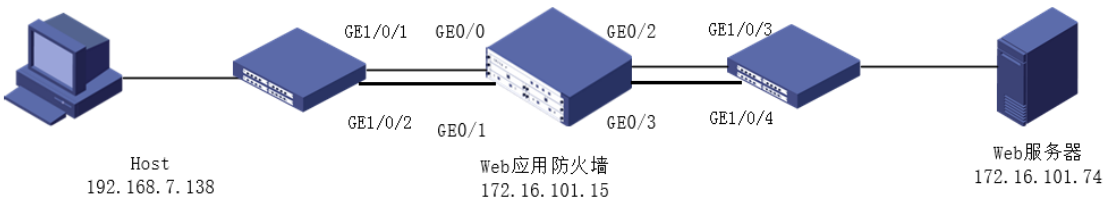
10.4 适用产品和版本

此配置举例在 E6713 版本上验证。

10.5 组网需求

如下图所示，web 应用防火墙配置 channel 模式串联部署在交换机中，对 Web 服务器进行防护。

图10-1 组网图



10.6 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。

10.7 配置步骤

1. 交换机配置链路聚合

如下图所示，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。

图10-2 交换机链路聚合配置-1

```
[SWUP_For_AUG_NewWAF]interface Bridge-Aggregation 1     创建聚合组1
[SWUP_For_AUG_NewWAF-Bridge-Aggregation1]quit
[SWUP_For_AUG_NewWAF]interface GigabitEthernet 1/0/1
[SWUP_For_AUG_NewWAF-GigabitEthernet1/0/1]port link-aggregation group 1  将接口GE1/0/1加入到聚合组1
[SWUP_For_AUG_NewWAF]interface GigabitEthernet 1/0/2
[SWUP_For_AUG_NewWAF-GigabitEthernet1/0/2]port link-aggregation group 1  将接口GE1/0/2加入到聚合组1
```

如下图所示，靠近服务器端的交换机配置链路聚合，将接口 GE1/0/3 和 GE1/0/4 加入到聚合组 2 中。

图10-3 交换机链路聚合-2

```
[SWUP_For_AVG_NewWAF]interface Bridge-Aggregation 2
[SWUP_For_AVG_NewWAF-Bridge-Aggregation2]quit
[SWUP_For_AVG_NewWAF]interface GigabitEthernet 1/0/3
[SWUP_For_AVG_NewWAF-GigabitEthernet1/0/3]port link-aggregation group 2
[SWUP_For_AVG_NewWAF]interface GigabitEthernet 1/0/4
[SWUP_For_AVG_NewWAF-GigabitEthernet1/0/4]port link-aggregation group 2
```

创建聚合组2

将接口GE1/0/3加入到聚合组2

将接口GE1/0/4加入到聚合组2

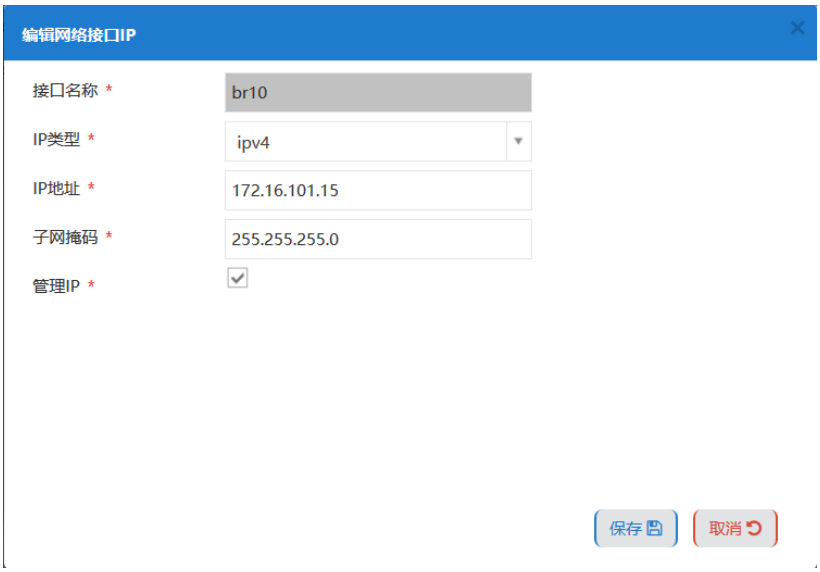
2. 创建新的网桥

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

图10-4 新建网桥-br10

如下图所示，根据服务器部部署模式，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。

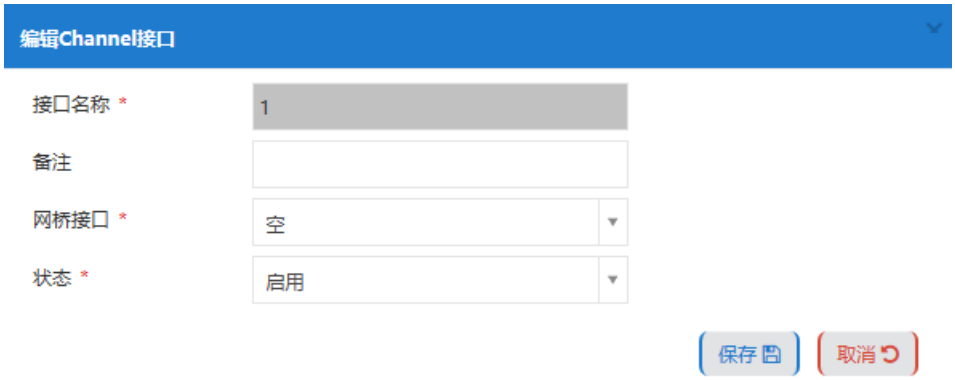
图10-5 增加业务 IP 地址



3. 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10-6 增加聚合接口



4. 把 port 接口划分到聚合接口中

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

图10-7 Port 接口配置聚合接口

如下图所示，在网络管理>网络接口>channel 接口中把 channel 接口的 1 和 2 接口的“网桥接口”选择 br10。

图10-8 聚合口划分到网桥中

10.8 验证配置

客户端访问服务端，断开 Web 应用防火墙的聚合口中的一个物理接口，不影响正常访问。

11 Trunk 部署配置举例

11.1 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 UNIS Web 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。

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

Web 应用防火墙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。

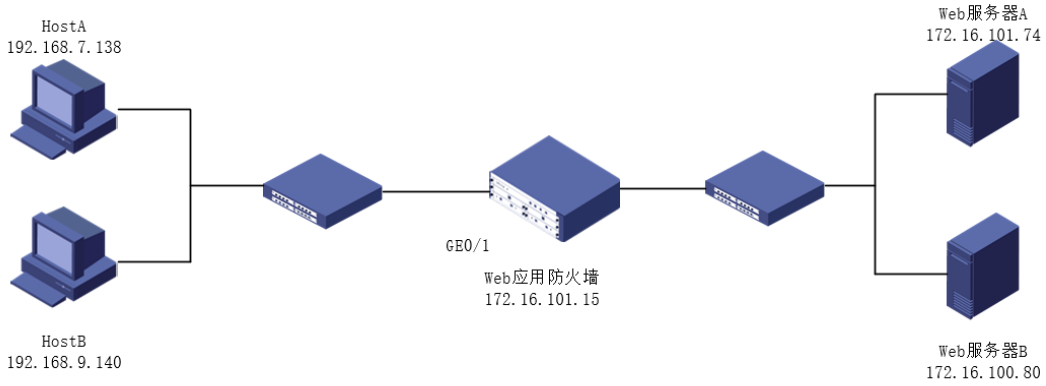
11.4 适用产品和版本

此配置举例在 E6713 版本上验证。

11.5 组网需求

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

图11-1 组网图



11.6 配置思路

(1) 创建网桥，把 port 接口划分到新建网桥中。

(2) 创建 trunk 接口。

11.7 配置步骤

1. 创建新的网桥

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

图11-2 新建新的网桥

点击下一步，进行第二步配置，如下图所示，点击保存即可。

图11-3 增加网桥第二步配置

2. 把 port 接口划分到网桥中

如下图所示，在网络管理>网络接口>Port 接口中编辑 port 接口，将接口 GE0/0、GE0/1 加入到网桥 10。

图11-4 Port 接口配置

3. 创建 trunk 接口

在网络管理>网络接口>trunk 接口中，点击增加弹出 Trunk 接口配置，接口选择 br10，VLAN 标签填写 2，配置完成点击下一步。

图11-5 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11-6 保存 trunk 配置

12 网页防篡改配置举例

说明 暂不支持网页防篡改功能

12.1 简介

网页防篡改是一种防止攻击者修改 Web 页面的技术，可以有效的阻止攻击者对网站内容进行破坏，尤其是在攻击者突破 Web 应用防火墙的防护后，依然可以有效的保护网站。

网页防篡改采用目前先进的系统驱动级文件保护技术（第三代防篡改技术），基于事件触发式监测机制。相比轮询检测、内嵌技术等传统类防护技术，第三代防篡改技术具有响应速度快、判断准确、资源占用少及部署灵活等特点。

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

部署防篡改客户端时需要重启服务器，因此部署时需要协调好部署时间，以防在部署时重启服务器影响业务。

保证 Web 应用防火墙与防篡改的服务端互通。

12.4 适用产品和版本

Windows 防篡改端支持在 Windows server 2003 32 位、Windows server 2008 32/64 位、Windows server 2012 64 位、Windows server 2016 64 位系统上安装。

Linux 防篡改端支持在 Debian/Ubuntu/CentOS/Redhat 等主流 Linux 系统的 32 位及其 64 位系统安装。

12.5 组网需求

组网需求按照 Web 应用防火墙需求模式部署即可。

12.6 配置思路

(1) 按照客户服务器版本需求下载防篡改客户端。

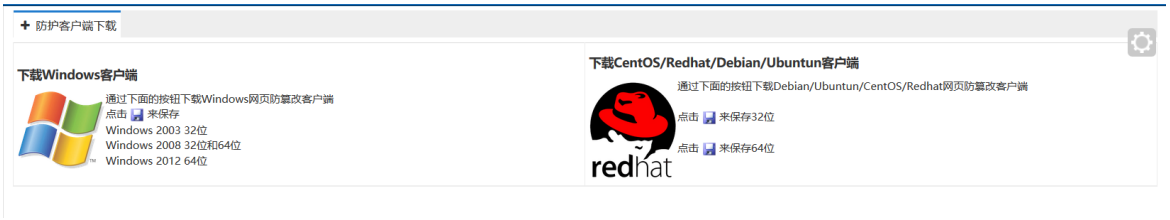
(2) 在 WAF 上探测防护端。

(3) 点击探测到的防护端配置防护策略。

12.7 配置步骤

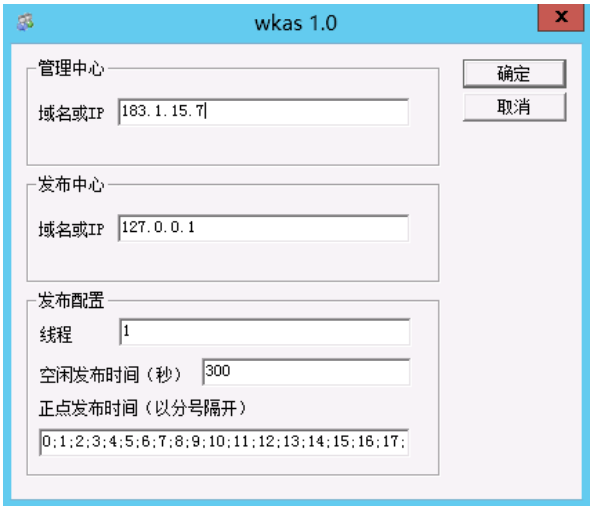
1. 按照客户服务器版本需求下载防篡改客户端

本配置以 Windows 2012 为例，在防护的服务器上，通过浏览器登录 Web 应用防火墙，在网页防篡改->防护客户端下载中按需求下载客户端软件，如下图所示。



下载客户端后，进行安装，安装最后一步，需要填写管理中心 IP（即 Web 应用防火墙的地址），如下图所示。

注意：只需配置管理中心 IP，其他保持默认配置。安装完成后需要重启服务器。



2. 在 WAF 上探测防护端

在网页防篡改>防护服务器探测中，查看探测到的服务器信息，点击生成配置，完成相关配置，配置完成后，服务器信息会自动转存到网页防篡改配置中，可在网页防篡改配置中再次对服务器进行配置修改。

图12-1 网页防篡改探测

第一步，基本配置，详细参数如下，配置完点击下一步

Web 名称：填写策略名称；

主机名：服务器主机名，不可修改；

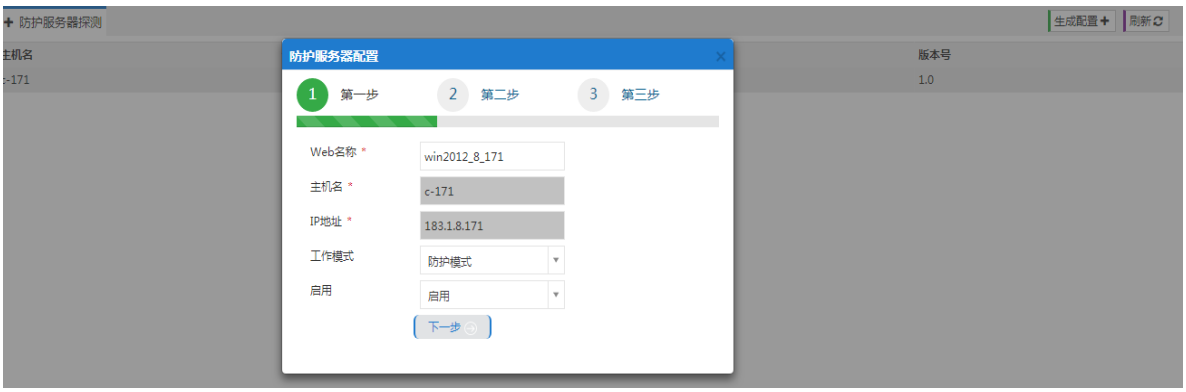
IP 地址：服务器 IP 地址；

是否启用：是否启用策略，选择 是；

工作模式：可选防护模式或监控模式；

注意：工作模式分为防护模式和监控模式，默认是防护模式，防护模式下对防护目标起防护作用并记录日志。监控模式下对防护目标保持监控状态，只报警不防护，并通过报警日志作为优化防护策略的参考，此模式下可大大降低部署防篡改时因策略不恰当导致的误防护情况。优化策略后再改变工作模式为防护模式即可。

图12-2 配置选项 1



第二步，细节配置，详细参数如下，配置完点击下一步

操作系统类型：选择操作系统类型；

Web 根目录：输入 Web 根目录的绝对目录；

例外目录/文件：添入例外目录/文件的相对路径，添加的目录/文件将不会被保护，（此处要求填相对目录）；

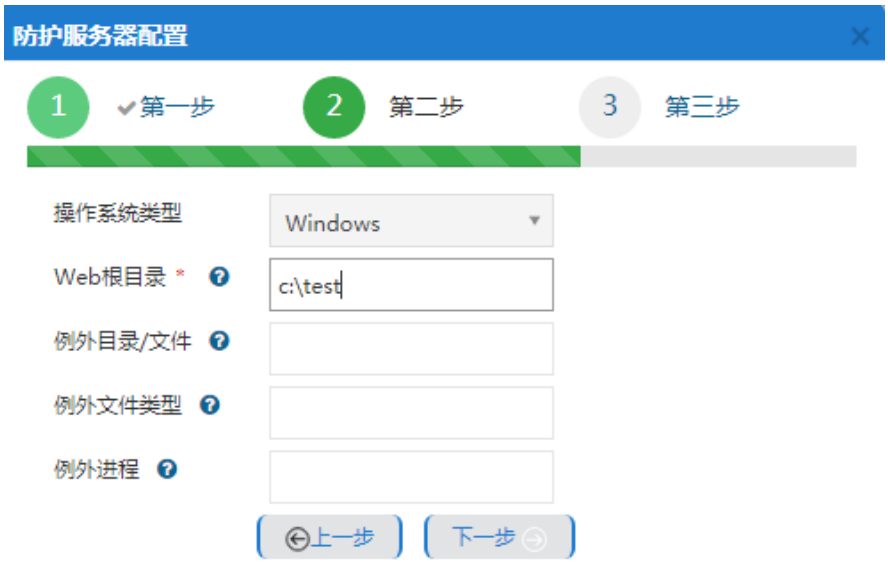
说明：通常网站中有部分文件夹是客户内部管理用于上传文件的，需要设置成例外。还有如网站管理平台周期性写入的 log 文件等。

例外文件类型：可以是*.txt、*.xml 等文件类型，这些文件类型将不会被保护；

例外进程：例外进程可以对 Web 根目录下的文件进行修改。

说明：用于网站后台同步数据的进程也需要设置成例外。

图12-3 配置选项 2



注意：

1、web 根目录是需要防护的网页目录文件夹，保护的是目录内的文件，图片，文档等信息不被进行非法操作。防篡改不能对数据库等动态文件起防护作用。

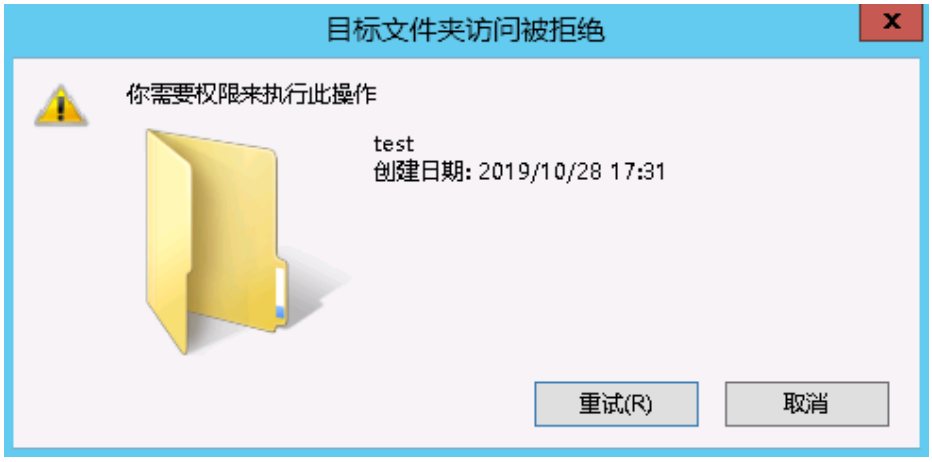
2、数据库应该不在防护目录之下，尽量与防护目录同级目录或不再同一磁盘下。

3、若数据库在防护目录内，可在例外目录/文件选择数据库目录对数据库目录例外，例外后不对该例外目录起防护效果。

第三步，无需配置，点击完成即可。

12.8 验证配置

(1) 在防护目录中新增文件。



(2) 查看防篡改日志。

13 IPV6 反向代理配置举例

13.1 简介

因 IPV4 地址的局限性，IPV6 地址取代 IPV4 是大势所趋。本次配置举例主要介绍在 WAF 上如何配置，使得 IPV4 客户端可以访问 IPV6 服务器（简称 IPV4 反代 IPV6），以及使得 IPV6 客户端能够访问 IPV4 服务器（简称 IPV6 反代 IPV4）。

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

Web 应用防火墙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。

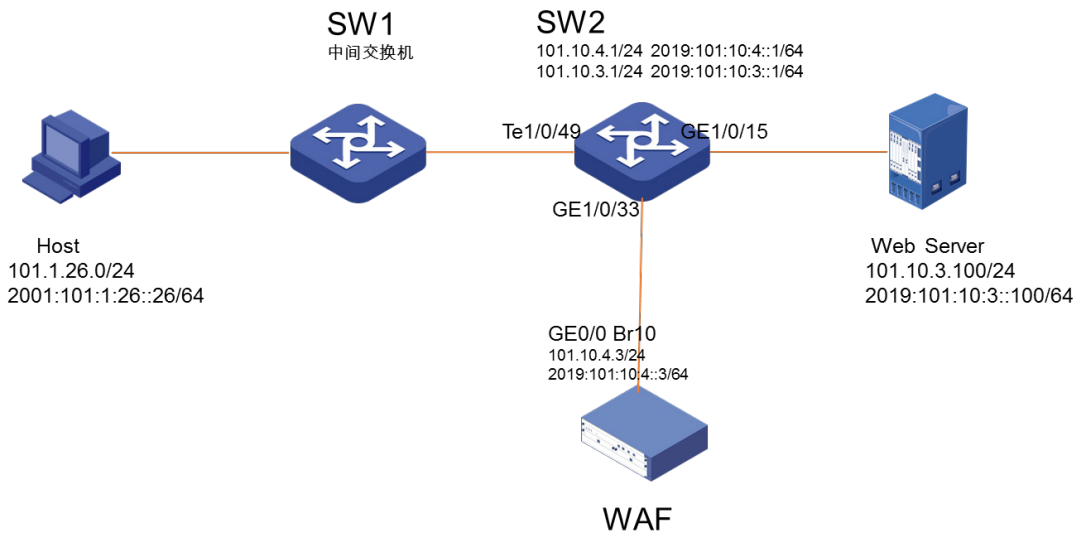
旁路反代模式下支持 IPV6 配置。

13.4 适用产品和版本

此配置举例在 E6713 版本上验证。

13.5 组网需求

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



13.6 配置思路

按照组网图组网。

(1) 创建网桥，配置 WAF 业务 IP 和路由。

(2) 创建 HTTP 服务器，配置安全防护策略，对 Web 服务器进行防护。

13.7 配置步骤

1. 创建网桥，配置 WAF 业务 IP 和路由

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

图13-1 新建网桥-br10

如下图所示，在网桥 br10 中增加业务 IP 地址。

注意：IPV4 反代 IPV6，或者 IPV6 反代 IPV4，必须在同一个桥接口下同时配置 IPV4 地址和 IPV6 地址。

图13-2 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13-3 增加 IPV4 路由

图13-4 增加 IPV6 路由

如下图所示，在网络管理>网络接口>Port 接口中编辑 port 接口。接口 GE0/0 的“网桥接口”选择 br10。

图13-5 port 口划分到新网桥

2. 创建 HTTP 服务器，对 Web 服务器进行防护。

如下图所示，选择菜单“服务器管理>普通服务器管理”进入普通服务器配置页面，点击增加，新建 HTTP 服务器，具体参数配置如下，防护模式选择代理模式，客户端 IP 还原选择否。配置完成后点击保存。

图13-6 创建 IPV4 HTTP 服务器

图13-7 创建 IPV6 HTTP 服务器

如下图所示，选择菜单“服务器管理>代理服务器管理”，进入代理服务器配置页面，点击增加，新建 HTTP 代理服务器，IP 地址填写 Web 应用防火墙业务 IP 地址，具体参数配置如下。配置完成后点击保存。

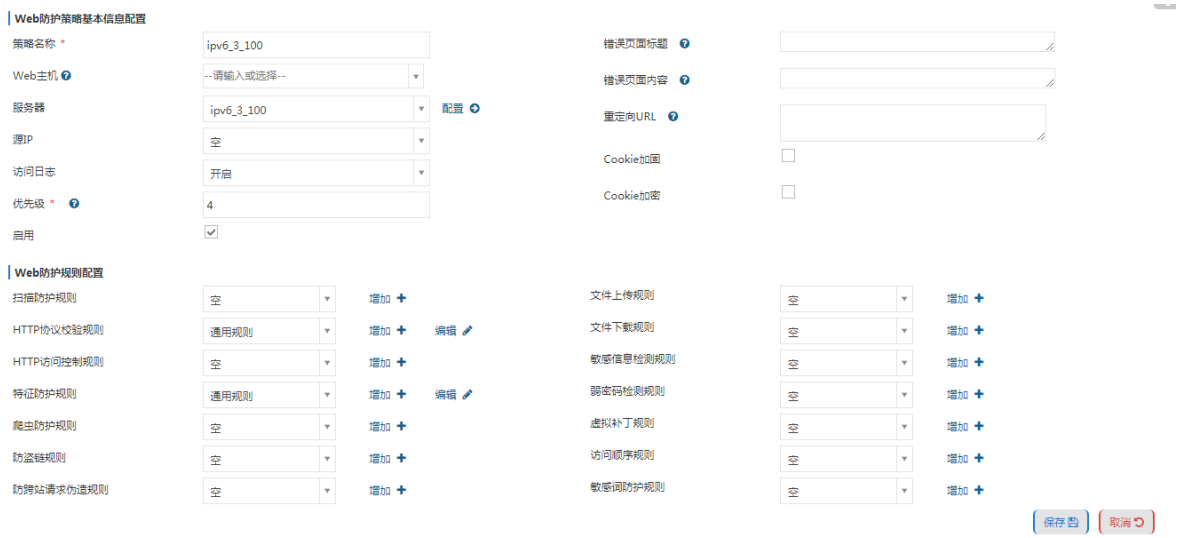
图13-8 增加 IPV4 反代 IPV6 的代理服务器

图13-9 增加 IPV6 反代 IPV4 的代理服务器

如下图所示，选择“应用安全防护>Web 防护策略”进入 Web 防护策略管理界面。点击增加，新增 Web 防护策略。在“服务器”中分别选择 IPV4 和 IPV6 服务器，根据需要进行防护策略的配置，配置完成后点击保存。

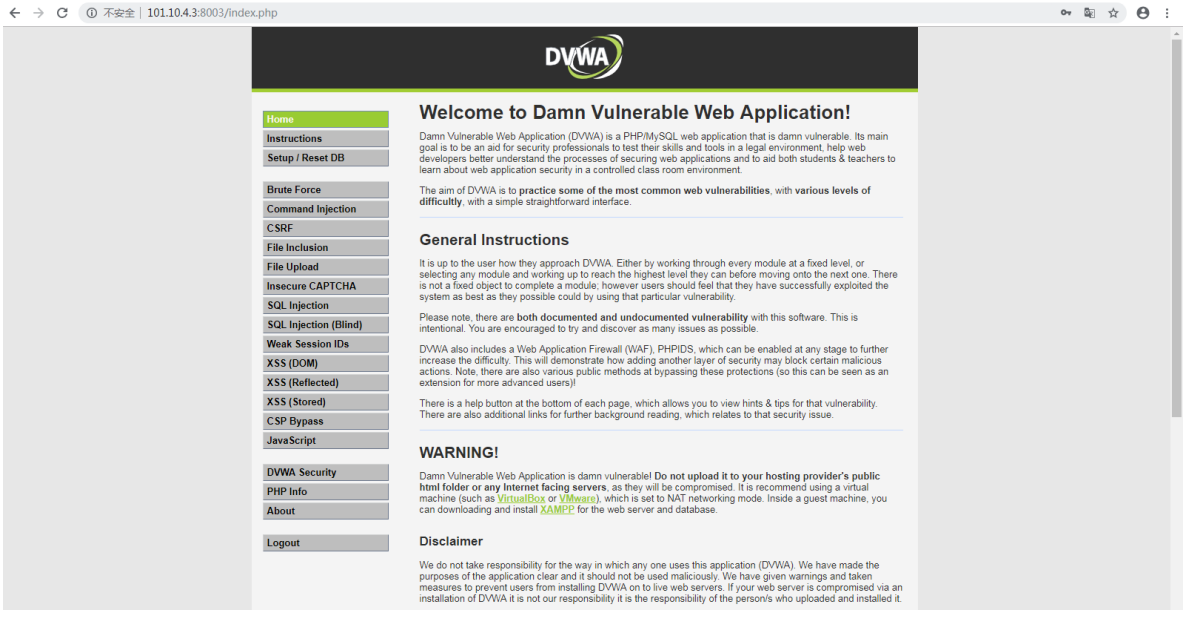
图13-10 配置 IPV4 服务器安全防护策略

图13-11 配置 IPV6 服务器安全防护策略



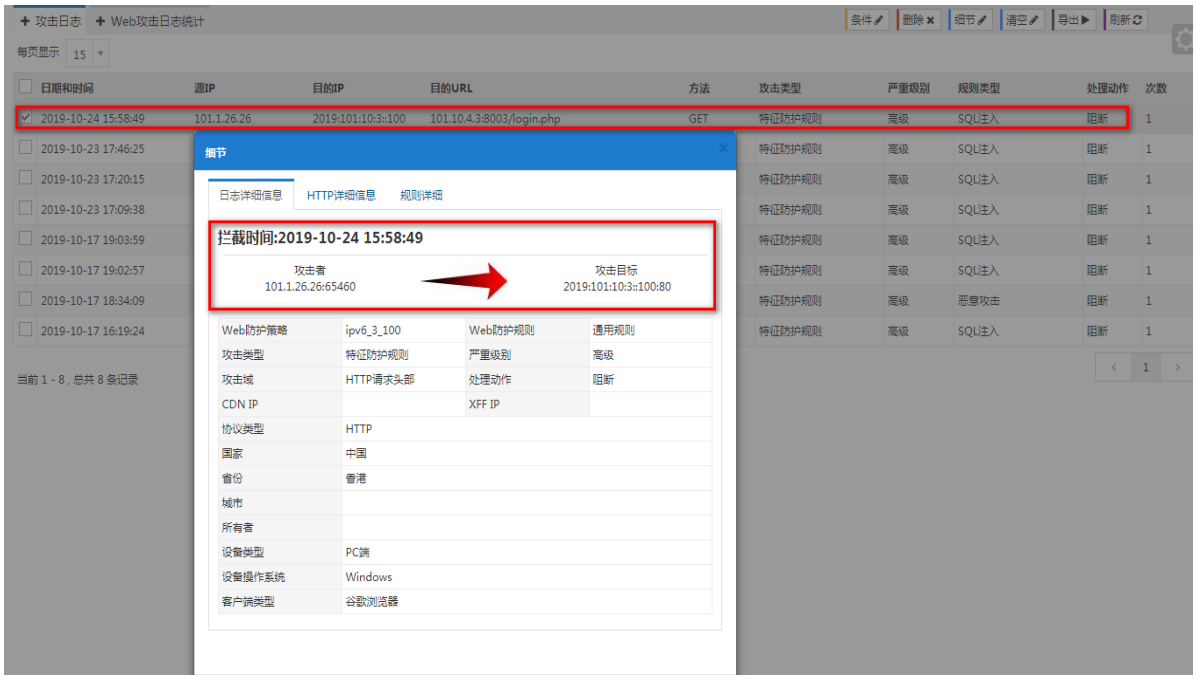
13.8 IPV4反代IPV6的验证配置

(1) 客户端访问 IPV4 的反代 IP 地址和端口，URL 为 http://101.10.4.3:8003，可以正常访问。



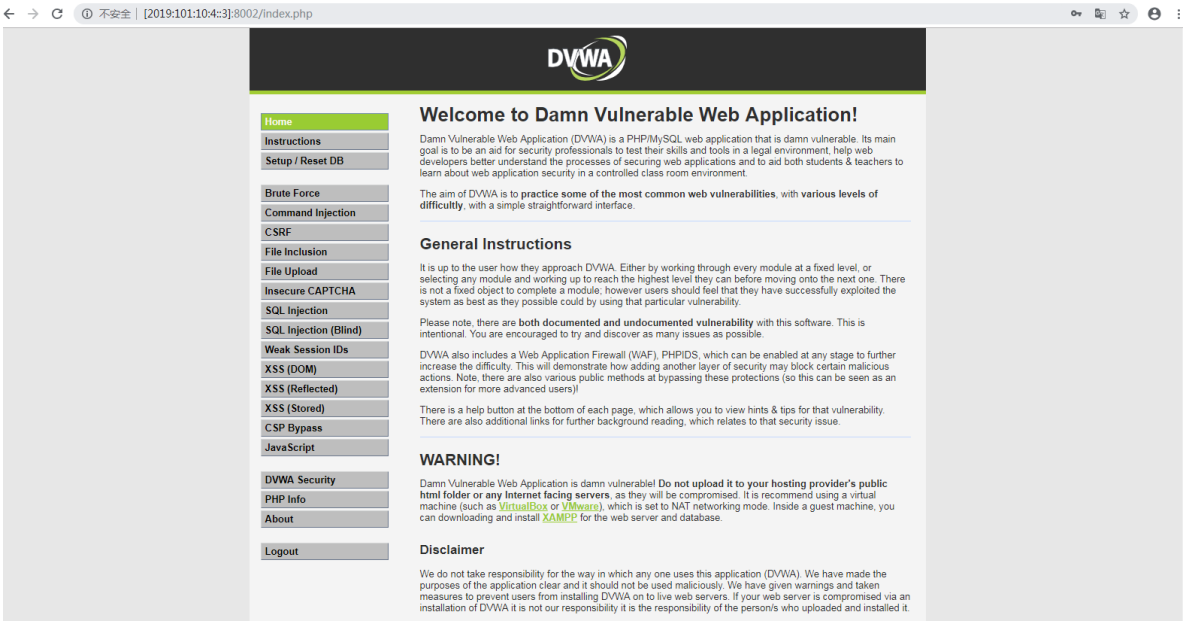
(2) 加上攻击参数再次访问网站，URL 为 http://101.10.4.3:8003/login.php?id=1 and 1=1，网站不能访问。

(3) 选择"日志系统>攻击日志"，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，且后端服务器为 IPV6 地址。



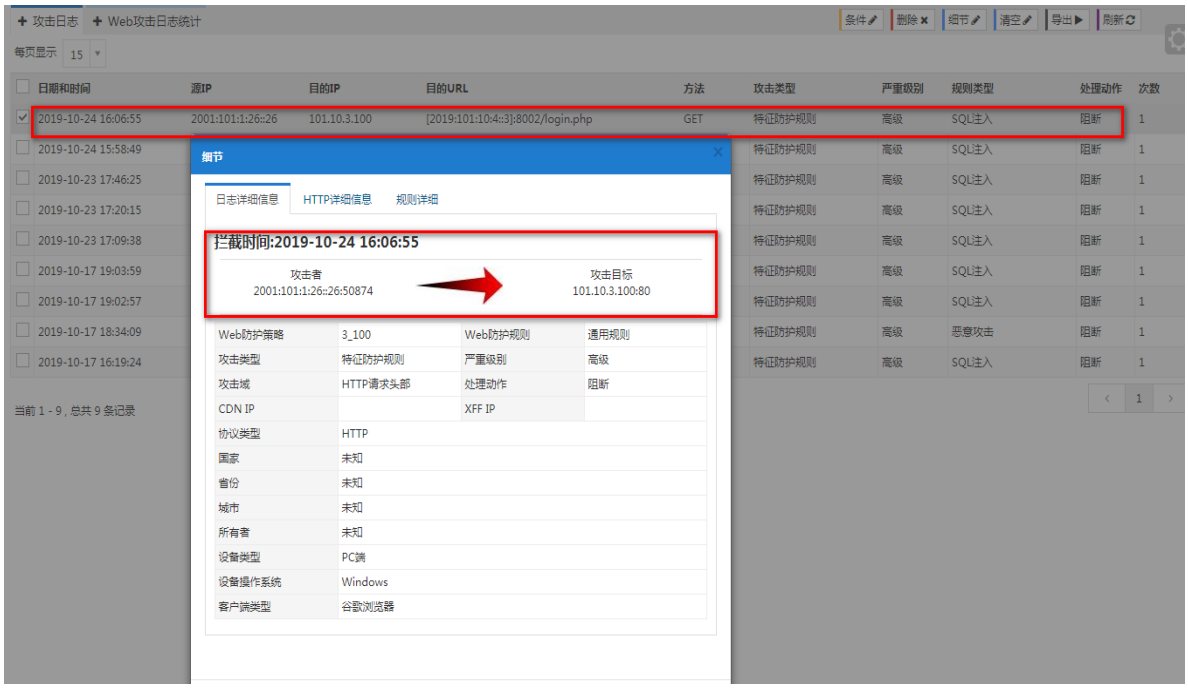
13.9 IPV6反代IPV4的验证配置

(1) 客户端访问 IPV6 的反代 IP 地址和端口，URL 为 http://[2019:101:10:4::3]:8002，可以正常访问。



(2) 加上攻击参数再次访问网站，URL 为 http://[2019:101:10:4::3]:8002/login.php?id=1 and 1=1，网站不能访问。

(3) 选择"日志系统>攻击日志"，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，且后端服务器为 IPV4 地址。



14 WEB 应用防火墙通过 PBR 策略路由实现物理旁路逻辑透明单机配置举例

14.1 简介

本文档介绍了 Web 应用防火墙通过 PBR 策略路由实现物理旁路逻辑透明部署配置举例。WAF 虽旁路部署在交换机侧，但通过流量牵引后，其模式仍为透明流模式。

支持功能：扫描防护、HTTP 协议校验、特征防护、爬虫防护、防盗链、防跨站请求伪造、文件上传、文件下载、敏感信息检测、弱密码检测、虚拟补丁、访问顺序、敏感词防护、DDoS 防护、威胁情报。

支持协议：HTTP。

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。

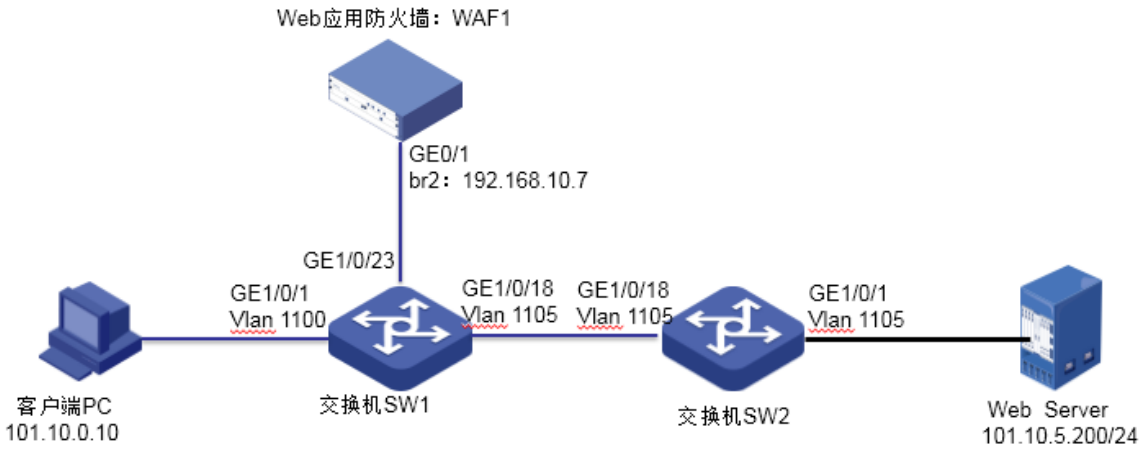
14.4 适用产品和版本

本次测试使用产品型号为 UNIS W2000-G50

软件版本号为 UNIS Uniware software, Version 1.10, E6713

14.5 组网需求

单台 WAF 旁路部署在交换机侧，通过策略路由将客户端访问服务端的流量牵引至 WAF，WAF 回包给服务器，服务器响应包进入 sw1 时，通过策略路由将流量牵引至 WAF，WAF 再回给客户端，从而实现物理上旁路，逻辑上透明组网。



14.6 配置步骤

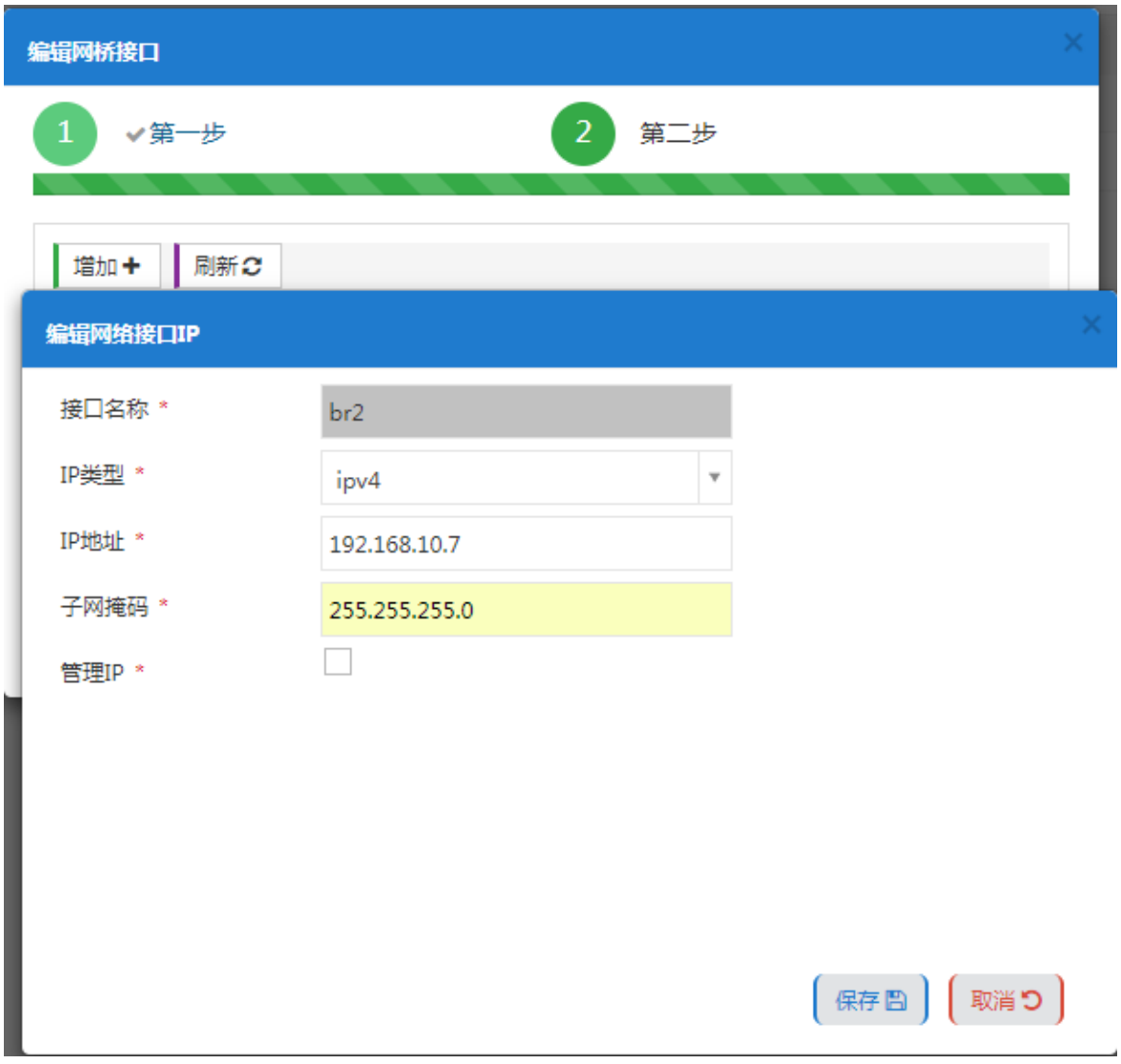
14.6.1 WAF 的接口及路由配置

登录 Web 应用防火墙：启动 IE/CHROME 浏览器，在地址栏内输入“https://192.168.0.1”即可进入 Web 网管登录页面。输入用户名“admin”、密码“admin”，点击<登录>按钮即可进入 Web 网管页面并进行相关操作。

登录应用防火墙后点击左侧菜单：网络管理-网络接口。与交换机直连接口 GE0/1 默认在网桥 br2 中。

双击网桥接口 br2，在弹出界面中，点击下一步，点击增加，增加桥 br2 接口 IP：192.168.10.7，界面如下图。


编辑网桥接口
1
第一步
2
第二步
网桥号 *
2
MTU *
1500
模式 *
普通模式
状态 *
启用
STP
下一步


编辑网桥接口
1
第一步
2
第二步
增加
刷新
编辑网络接口IP
接口名称 *
br2
IP类型 *
ipv4
IP地址 *
192.168.10.7
子网掩码 *
255.255.255.0
管理IP *
保存
取消

点击“网络管理-路由配置”，点击增加，增加 WAF 到交换机 sw1 的路由。

14.6.2 服务器配置

说明：服务器配置即配置后端的保护站点，本例中后端保护站点 IP 地址为：101.10.5.200。

点击左侧菜单“服务器管理-普通服务器管理-HTTP 服务器”，点击增加。

服务器名称：S1

IP 地址：后端保护站点的 IP 地址。

端口：后端保护站点的端口。

部署模式：串联

防护模式：流模式。

14.6.3 安全策略配置

说明：安全策略配置的目的是对后端保护站点添加相应的防护规则，如特征防护规则、扫描防护规则等，选择哪种规则根据实际需求配置。

进入“应用安全防护-Web 防护策略”，点击增加，新增 WEB 防护策略，该例选择默认的通用规则。如下图。

14.6.4 交换机配置

如组网图所示，交换机 sw1 作为三层交换机，客户端、服务端、WAF 的网关均指向 sw1。sw2 作为二层设备，不做路由配置，仅做报文转发。

进入交换机 sw1：

配置客户端、服务端、WAF 的网关地址。

[SW]interface Vlan-interface 168

[SW -Vlan-interface168]dis this

interface Vlan-interface168

ip address 192.168.10.1 255.255.255.0

[SW]interface Vlan-interface 1100

[SW -Vlan-interface1100]dis this

interface Vlan-interface1100

ip address 101.10.0.1 255.255.255.0

[SW]interface Vlan-interface 1105

[SW -Vlan-interface1105]dis this

interface Vlan-interface1105

ip address 101.10.5.1 255.255.255.0

新建两条 ACL 规则，允许目的网段为 101.10.5.200/32 和 101.10.0.0/24 报文通过。

[SW]acl number 3010

[SW -acl-adv-3010]rule 0 permit ip destination 101.10.5.200 0

[SW]acl number 3020

[SW -acl-adv-3020]rule 0 permit ip destination 101.10.0.0 0.0.0.255

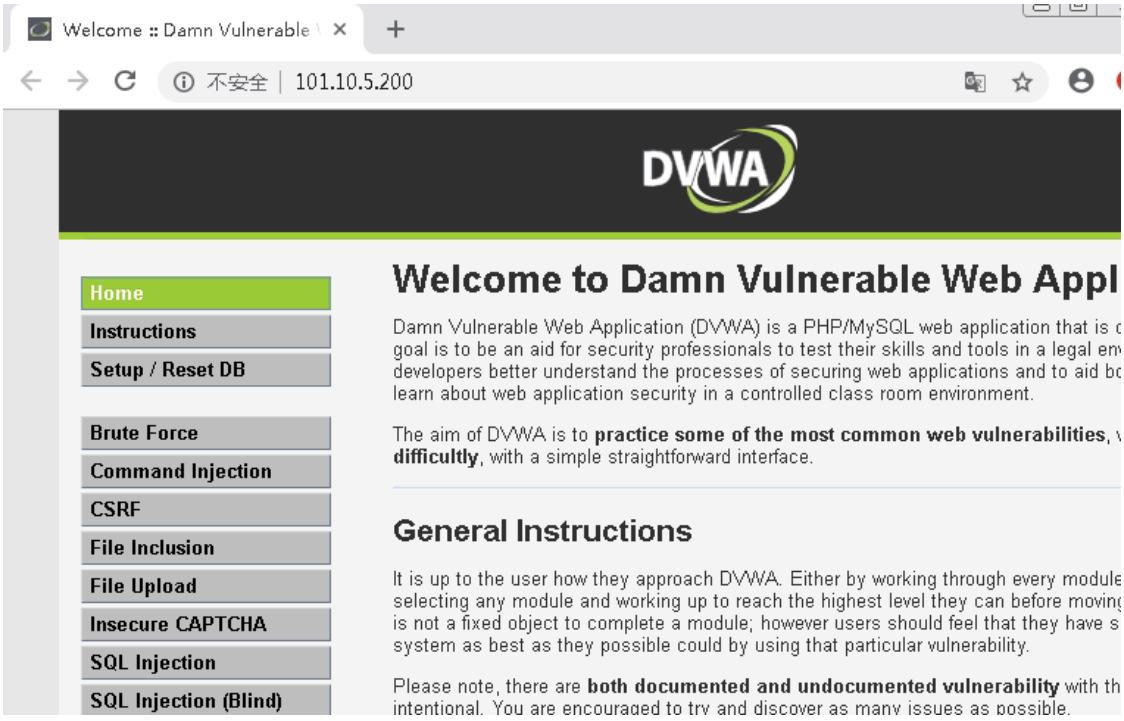
新建两条 PBR 策略路由 aaa 和 bbb，匹配相应的 ACL 规则，下一跳为 WAF 的接口地址。
[SW]policy-based-route aaa permit node 5
[SW -pbr-aaa-5]if-match acl 3010
[SW -pbr-aaa-5]apply next-hop 192.168.10.7
[SW -pbr-aaa-5]quit
[SW]policy-based-route bbb permit node 5
[SW -pbr-aaa-5]if-match acl 3020
[SW -pbr-aaa-5]apply next-hop 192.168.10.7
[SW -pbr-aaa-5]quit

分别进入客户端和服务端 vlan 子接口，客户端引用规则 aaa，服务端引用规则 bbb。
[SW]int vlan1100
[SW -Vlan-interface1100] ip policy-based-route aaa
[SW]int vlan1105
[SW -Vlan-interface1100] ip policy-based-route bbb

进入交换机 sw2，将接口划入 vlan1105。
[SW]vlan 1105
[SW -vlan1105]port GigabitEthernet 1/0/18
[SW -vlan1105]port GigabitEthernet 1/0/1

14.7 验证配置

- 客户端 PC 访问保护站点：http://101.10.5.200，可以正常访问 Web 页面。



- 在”日志系统—访问日志”中，能看到正常访问时的访问日志。

- 对服务器进行 SQL 注入，如客户端 URL 输入 http://101.10.5.200/vulnerabilities/sqli/?id=1 and 1=1，WEB 页面被阻断。

进入”日志系统—攻击日志“，可以看到规则类型为“SQL 注入”的攻击日志。

15 WEB 应用防火墙通过 PBR 策略路由实现物理旁路逻辑透明双机主备配置举例

15.1 简介

本文档介绍了 Web 应用防火墙通过 PBR 策略路由实现物理旁路逻辑透明部署配置举例。WAF 虽旁路部署在交换机侧，但通过流量牵引后，其模式仍为透明流模式。

支持功能：扫描防护、HTTP 协议校验、特征防护、爬虫防护、防盗链、防跨站请求伪造、文件上传、文件下载、敏感信息检测、弱密码检测、虚拟补丁、访问顺序、敏感词防护、DDoS 防护、威胁情报。

支持协议：HTTP。

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。

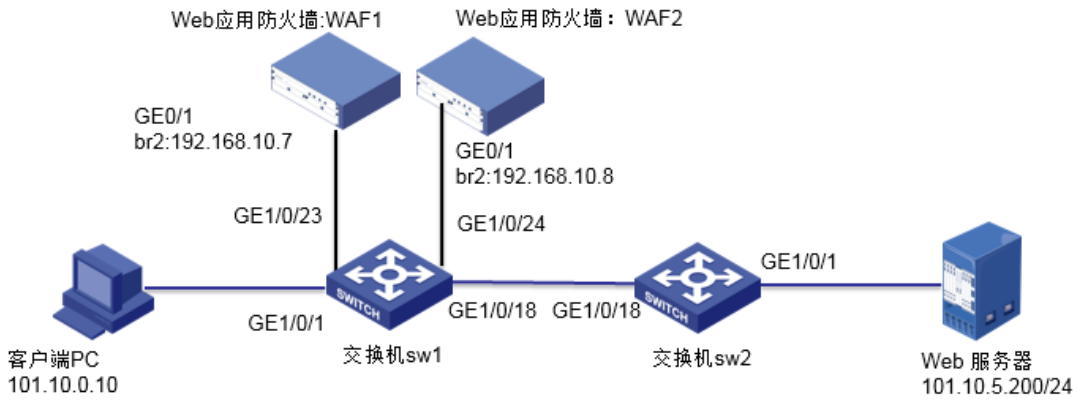
15.4 适用产品和版本

本次测试使用产品型号为 UNIS W2000-G50

软件版本号为 UNIS Uniware software, Version 1.10, E6713 组网需求

两台 WAF 旁路部署在交换机侧，配置 VRRP 主备关系，通过策略路由将客户端访问服务端的流量牵引至 WAF，WAF 回包给服务器，服务器响应包进入 sw1 时，通过策略路由将流量牵引至 WAF，WAF 再回给客户端，从而实现物理上旁路，逻辑上透明组网。

图 4-1 Web 应用防火墙配置举例组网图



15.5 配置步骤

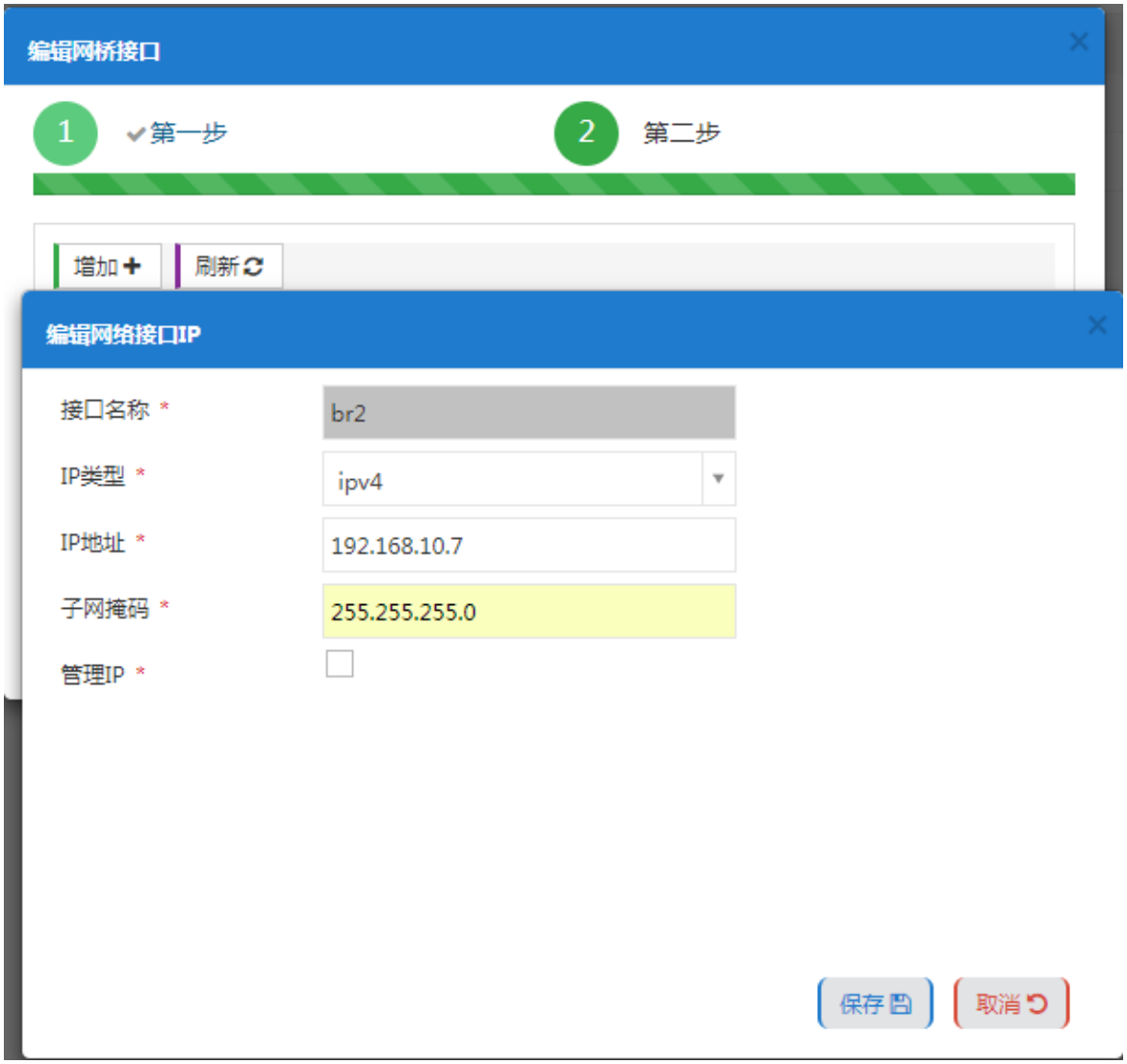
15.5.1 WAF 的接口及路由配置

登录 Web 应用防火墙：启动 IE/CHROME 浏览器，在地址栏内输入“https://192.168.0.1”即可进入 Web 网管登录页面。输入用户名“admin”、密码“admin”，点击<登录>按钮即可进入 Web 网管页面并进行相关操作。

注：以下配置以 WAF1 为例，WAF2 配置与 WAF1 类似，不同处下文标记。

登录应用防火墙后点击左侧菜单：网络管理-网络接口。

双击网桥接口 br2，在弹出界面中，点击下一步，点击增加，增加桥 br2 接口 IP：192.168.10.7，界面如下图（WAF2 配置 IP：192.168.10.8）。



点击“网络管理-路由配置”，点击增加，增加 WAF 到交换机 sw1 的路由。

15.5.2 服务器配置

说明：服务器配置即配置后端的保护站点，本例中后端保护站点 IP 地址为：101.10.5.200。

进入“服务器管理-普通服务器管理-HTTP 服务器”，点击增加。

服务器名称：S1

IP 地址：后端服务器的 IP 地址。

端口：后端服务器端口。

部署模式：串联

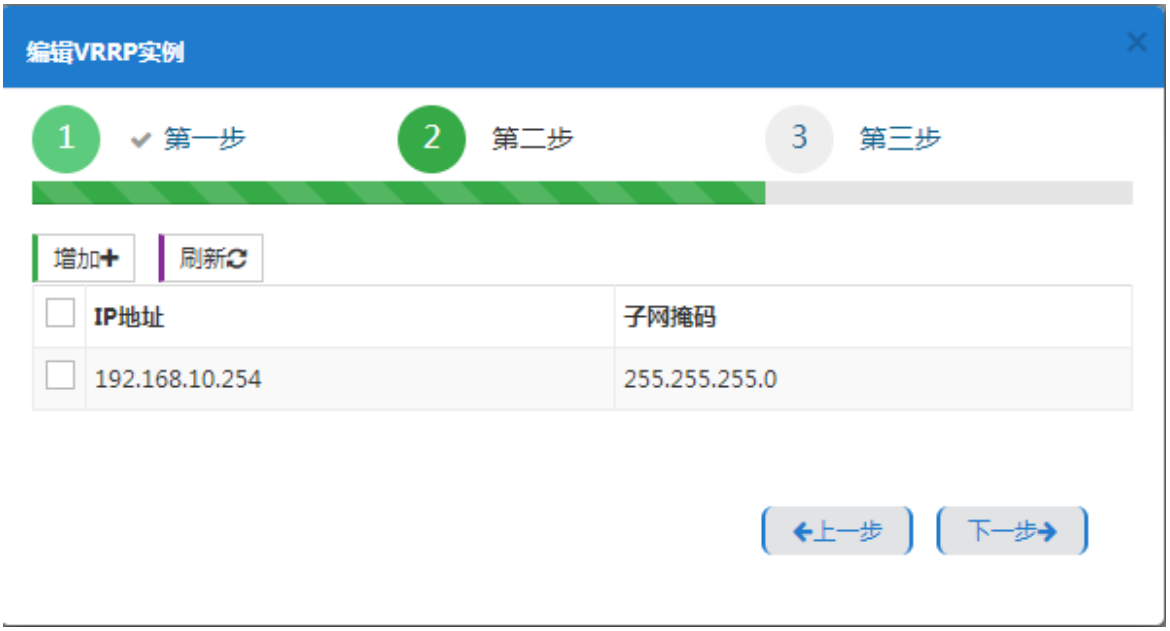
防护模式：流模式。

15.5.3 VRRP 配置

说明：VRRP 配置即配置两台 WAF 主备关系，根据状态及优先级来选择主备关系。

进入 “HA 管理-VRRP 配置-VRRP 实例”，点击增加。（WAF2 此处优先级选择 99，状态选择：备）

点击下一步，增加 VRRP 虚拟 IP 地址：192.168.10.254（WAF2 配置地址相同）：



点击下一步，选择 br2 对应的物理接口 GE0/1。

进入 VRRP 组，点击增加，将左侧的 VRRP 实例列表点击至右侧，点击保存。

注：以上在两台 WAF 上 VRRP 配置完成后，需点击右上角应用才能生效。

15.5.4 安全策略配置

说明：安全策略配置的目的是对后端保护站点添加相应的防护规则，如特征防护规则、扫描防护规则等，选择哪种规则根据实际需求配置。

进入“应用安全防护-Web 防护策略”，点击增加，新增 WEB 防护策略，选择默认的通用规则。如下图。

15.5.5 交换机配置

如组网图所示，交换机 sw1 作为三层交换机，客户端、服务端、WAF 的网关均指向 sw1。sw2 作为二层设备，不做路由配置，仅做报文转发。

进入交换机 sw1：

配置客户端、服务端、WAF 的网关地址。

[SW]interface Vlan-interface 168

[SW -Vlan-interface168]dis this

interface Vlan-interface168

ip address 192.168.10.1 255.255.255.0

[SW]interface Vlan-interface 1100

[SW -Vlan-interface1100]dis this

interface Vlan-interface1100

ip address 101.10.0.1 255.255.255.0

[SW]interface Vlan-interface 1105

[SW -Vlan-interface1105]dis this

interface Vlan-interface1105

ip address 101.10.5.1 255.255.255.0

新建两条 ACL 规则，允许目的网段为 101.10.5.200/32 和 101.10.0.0/24 报文通过。

[SW]acl number 3010

[SW -acl-adv-3010]rule 0 permit ip destination 101.10.5.200 0

[SW]acl number 3020

[SW -acl-adv-3020]rule 0 permit ip destination 101.10.0.0 0.0.0.255

新建两条 PBR 策略路由 aaa 和 bbb，匹配相应的 ACL 规则，下一跳为 WAF 的 VRRP 虚拟地址。

[SW]policy-based-route aaa permit node 5

[SW -pbr-aaa-5]if-match acl 3010

[SW -pbr-aaa-5]apply next-hop 192.168.10.254

[SW -pbr-aaa-5]quit

[SW]policy-based-route bbb permit node 5

[SW -pbr-aaa-5]if-match acl 3020

[SW -pbr-aaa-5]apply next-hop 192.168.10.254

[SW -pbr-aaa-5]quit

分别进入客户端和服务端 vlan 子接口，客户端引用规则 aaa，服务端引用规则 bbb。

[SW]int vlan1100

[SW -Vlan-interface1100] ip policy-based-route aaa

[SW]int vlan1105

[SW -Vlan-interface1100] ip policy-based-route bbb

进入交换机 sw2，将接口划入 vlan1105。

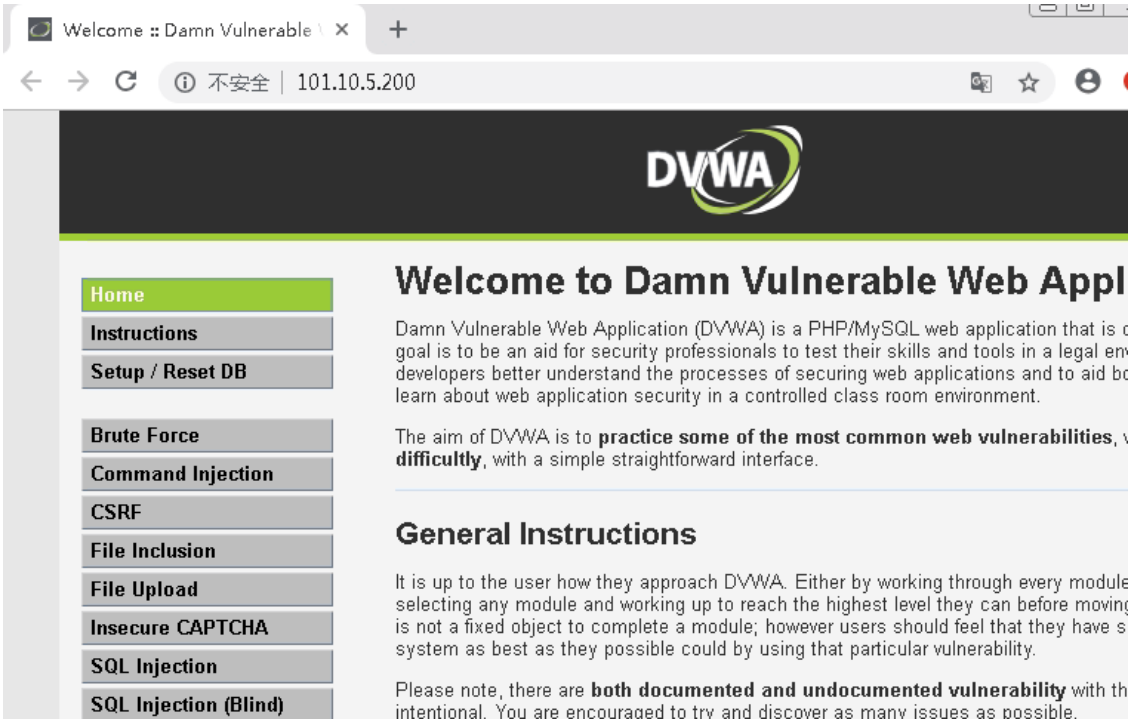
[SW]vlan 1105

[SW -vlan1105]port GigabitEthernet 1/0/18

[SW -vlan1105]port GigabitEthernet 1/0/1

15.6 验证配置

- 客户端 PC 访问保护站点：http://101.10.5.200，可以正常访问 Web 页面。



- 点击”日志系统—访问日志”，能看到正常访问时的访问日志。

- 对服务器进行 SQL 注入，如客户端 URL 输入 http://101.10.5.200/vulnerabilities/sqli/?id=1 and 1=1，WEB 页面被阻断。

- 进入”日志系统—攻击日志“，可以看到命中规则类型为“SQL 注入”的攻击日志。

- 断开主设备接口或给主设备断电，客户端再次对服务器进行 SQL 注入攻击，此时页面被阻断。

- 进入备设备，在“日志系统-攻击日志”中，可以看到命中规则类型为“SQL 注入”的攻击日志。