UNIS W2000-G 系列 Web 应用防火墙

典型配置举例

北京紫光恒越网络科技有限公司
http://www.unishy.com

资料版本：5W100-20180412

前 言

本配置举例主要介绍 UNIS W2000-G 系列 Web 应用防火墙的典型部署方式。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... } *	表示从多个选项中至少选取一个。
[x | y | ...] *	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

技术支持

用户支持邮箱：zgsm_service@thunis.com

技术支持热线电话：400-910-9998（手机、固话均可拨打）

网址：http://www.unishy.com

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：zgsm_info@thunis.com

感谢您的反馈，让我们做得更好！

反向代理模式部署配置举例

目 录

1 简介

本文档介绍了 Web 应用防火墙反向代理模式部署的配置举例。

Web 应用防火墙的反向代理部署模式可以更好的实现对 Web 服务器的安全防护。可以隐藏 Web 服务器的真实 IP 地址，也可以加强 Web 服务器操作系统及业务本身的漏洞防护，在攻击爆发时减低服务器流量压力，提高业务可用性。

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。

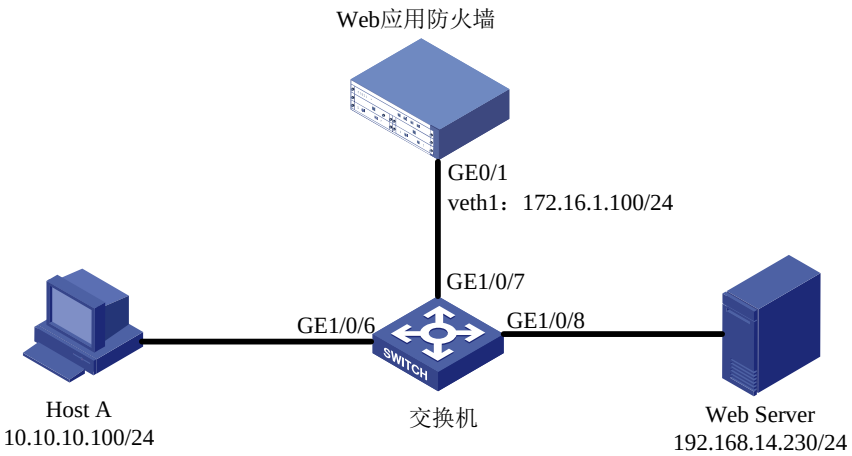
3 WEB应用防火墙反向代理部署配置举例

3.1 组网需求

设备在出厂时，默认所有接口都是属于 vlan1 的 access 口，用户可以按实际需求修改接口的类型。

如图所示，交换机分别建立 3 个 Vlan，分别是 10.10.10.0/24；172.16.1.0/24；192.168.14.0/24，三个 Vlan 的网关均在交换机上。Host A 可以访问到 Web 应用防火墙的业务地址，Web 应用防火墙可以访问到 Web Server 服务器。现在要求 Host A 通过访问 Web 应用防火墙的代理地址实现对 Web 服务器的应用访问。

图3-1 Web 应用防火墙反向代理部署配置举例组网图



3.2 使用版本

本举例是在系统版本：ESS6712 上进行配置和验证的。

3.3 配置步骤

3.3.1 部署模式配置

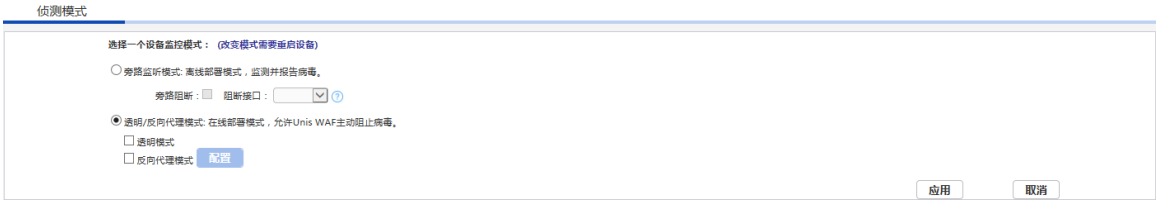
登录 Web 应用防火墙：启动 IE/FIREFOX 浏览器，在地址栏内输入“https://192.168.0.1”即可进入 Web 网管登录页面。输入用户名“admin”、密码“admin”，点击<登录>按钮即可进入 Web 网管页面并进行相关操作。

注意

推荐使用 IE10+及 Firefox56+及其以上版本的浏览器。

登录应用防火墙后点击左侧菜单：系统配置-侦测模式。

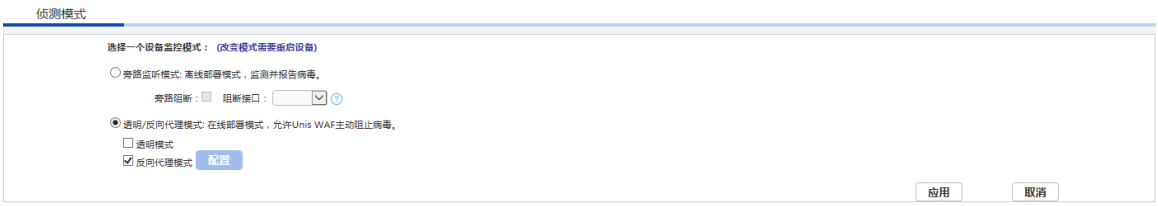
图3-2 侦测模式配置图-监控模式选择



在侦测模式配置页中，设备默认工作模式为透明模式，修改设备工作模式为反向代理模式，首先勾选反向代理模式前面的选择框，然后点击应用，并在页面右上角点击保存配置。之后需要重启设备以便使模式生效。

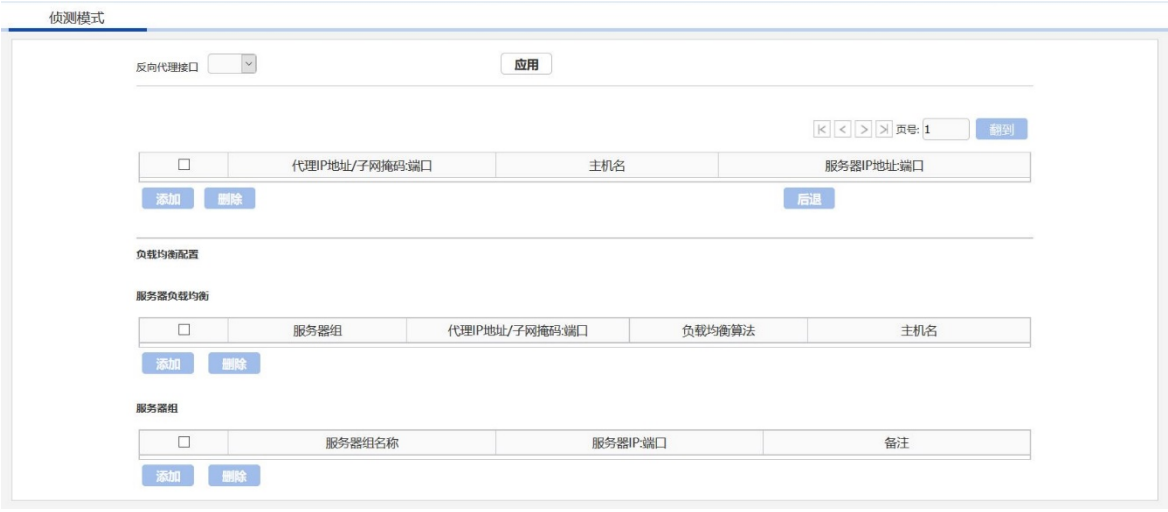
设备重启重新回到这个配置页面，此时反向代理模式前面的选择框是有勾选状态。

图3-3 侦测模式配置图-反向代理选择



此时点击反向代理模式后面的配置按钮进入反向代理配置界面。

图3-4 反向代理配置界面



在配置界面中首先需要配置的是反向代理的业务接口，可以在页面左上方反向代理接口处选择业务接口，以组网图 3-1 为例，本次案例使用 GE0/1 作为业务接口，选择后点击应用。

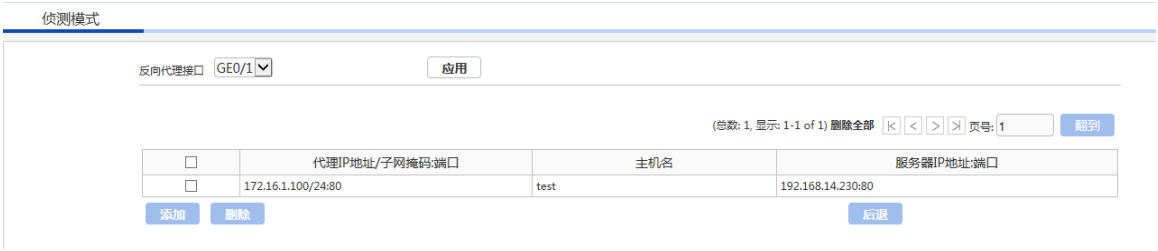
图3-5 反向代理接口配置图

接口选择完继续添加需要代理的 Web 服务器，在接口下方的服务器设置项点击添加按钮。

图3-6 反向代理服务器配置界面

在服务器添加配置页中，我们要设置用于代理的 IP 地址、子网掩码和代理端口，服务器 IP 地址端口为真实 Web 服务器地址和端口，填写完成后点击应用按钮完成代理服务器添加。添加完成后如图：此时 172.16.1.100 为代理地址，192.168.14.230 为真实 Web 服务器。

图3-7 反向代理服务器配置完成图



3.3.2 交换机配置

以组网图 3-1 为例，在交换机上建立 3 个 Vlan，分别是 10.10.10.0/24、172.16.1.0/24、192.168.14.0/24，并配置三个 Vlan 的网关。以下交换机配置命令均以 UNIS 交换机为例。

图3-8 创建 vlan 10 并配置网关

```
[SW]
[SW]vlan 10
[SW-vlan10]po                                    创建vlan10，并将GE1/0/6端口加入
[SW-vlan10]port g
[SW-vlan10]port GigabitEthernet 1/0/6
[SW-vlan10]quit
[SW]int
[SW]interface v
[SW]interface Vlan-interface 10
[SW-Vlan-interface10]ip ad
[SW-Vlan-interface10]ip address 10.10.10.1 255.255.255.0    配置vlan 10的网关
[SW-Vlan-interface10]
[SW-Vlan-interface10]
[SW-Vlan-interface10]quit
[SW]
[SW]
[SW]
```

图3-9 创建 vlan 172 并配置网关

```
[SW]
[SW]
[SW]vlan 172
[SW-vlan172]port g
[SW-vlan172]port GigabitEthernet 1/0/7    创建vlan 172，并将GE1/0/7端口加入
[SW-vlan172]quit
[SW]
[SW]int
[SW]interface v
[SW]interface Vlan-interface 172
[SW-Vlan-interface172]ip ad
[SW-Vlan-interface172]ip address 172.16.1.1 255.255.255.0    配置vlan 172的网关
[SW-Vlan-interface172]
[SW-Vlan-interface172]quit
[SW]
[SW]
[SW]
```

图3-10 创建 vlan 192 并配置网关

```
[SW]
[SW]
[SW]vlan 192
[SW-vlan192]port g                                          创建vlan 192，并将GE1/0/9端口加入
[SW-vlan192]port GigabitEthernet 1/0/8
[SW-vlan192]
[SW-vlan192]quit
[SW]int
[SW]interface v
[SW]interface vlan-interface 192
[SW-vlan-interface192]ip ad
[SW-vlan-interface192]ip address 192.168.14.1 255.255.255.0    配置vlan 192的网关
[SW-vlan-interface192]
[SW-vlan-interface192]quit
[SW]
[SW]
```

3.3.3 网络配置

代理配置完成后可以到网络配置-网络接口页观察配置情况。

图3-11 网络接口界面

注意

名称为 veth1 的接口，是 WAF 本身的一个虚接口，反向代理模式下，配置的代理 IP 都会关联到该虚接口上。

此时可以观察到，veth1 接口被配置了代理接口地址，工作模式为路由模式，此时代表反向代理模式配置成功。

注意

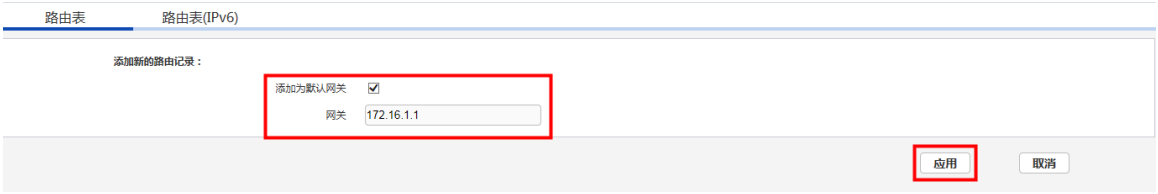
- 配置的其他接口地址和管理地址不能与业务代理地址在相同网段。否则会导致反向代理模式下监控策略失效。
- 若配置完反向代理接口地址后，ping 不通该地址，可以在“网络接口”页面点击 veth1 接口，查看其管理访问中的 ping 方式是否开启，若没有开启，勾选该方式并点击应用，之后再尝试是否能够 ping 通。

3.3.4 路由配置

由于系统仅有直连路由和添加的静态路由，因此需要在路由表中添加一条默认路由，使 WAF 上的业务流量都从反代业务口进出。

以组网图 3-1 为例，反代模式的代理 IP 为 172.16.1.100，反代业务口所连的交换机的网关为 172.16.1.1，因此添加一条路由，勾选“添加为默认网关”，网关为 172.16.1.1。

图3-12 WAF 路由配置



3.3.5 安全策略配置

点击左侧安全策略-Web 安全策略，根据需要添加调整 Web 应用防护策略。

图3-13 WAF 策略界面

点击添加按钮可以添加新 WAF 策略，点击策略右侧操作按键可以调整策略配置，可根据客户安全需求调整策略内容和动作等信息。调整完毕后点击确定。

图3-14 WAF 策略配置界面

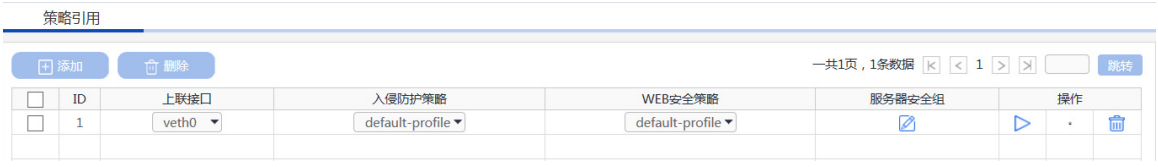
点击左侧安全策略-策略引用，将添加的 Web 应用策略与 Web 服务器进行关联。

点击左侧添加按钮，添加新的引用策略，上联接口一定要选择 veth0 接口，其他配置根据需要和配置选择入侵检测策略和 WEB 防护策略（上一步添加的 WAF 策略），点击服务器安全组按钮添加被保护服务器。

注意

反代模式下上联接口选择 veth0 接口的原因：由于反代模式下，配置的代理 IP 被关联到虚接口 veth1 上，而 veth0 和 veth1 是 WAF 本身的一对虚接口对，流量上代理时，是从 veth0 虚接口流入的，所以需要将 veth0 设为上联接口，才会对流量进行规则检测。

图3-15 策略引用界面

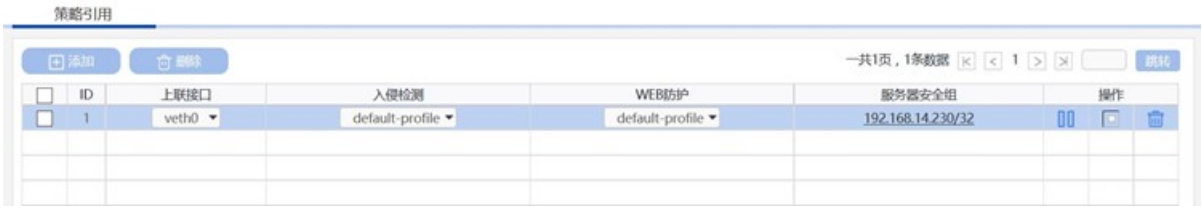


添加被保护服务器（此时被保护服务器为真实服务器地址）：在服务器列表里添加服务器地址和掩码，协议端口可根据业务情况进行填写和选择，填写完成后点击右侧的添加按钮即可添加到服务器列表中，可以添加多条服务器信息。添加完成后点击应用并返回上一级界面。

图3-16 服务器添加界面

策略引用配置完成后，默认情况下新添加的策略并不会立即启用，需点击界面的启用按键启用策略，策略启用后设备既可以实现对 WEB 服务器的安全防护功能。

图3-17 策略引用配置完成



3.4 验证配置

- Host A 访问 Web Server 可以正常打开 Web 的页面。
- 进行攻击测试。

攻击测试方法：

可以在目标服务器上安装测试靶机环境，靶机软件 DVWA 服务器端。

在客户端用浏览器登录靶机 DVWA 测试页面。

图3-18 SQL 注入

选择 SQL 注入选项，并点击测试方法项

图3-19 SQL 注入

- 进行攻击测试后，可以在 Web 安全策略中观察到策略命中数。
- 在左侧日志报表项-日志-WEB 安全日志中可以查看具体告警信息。

反向代理双机主备模式部署配置举例

目 录

1 简介

本文档介绍了 Web 应用防火墙反向代理模式双机主备部署的配置举例。

Web 应用防火墙的高可用性可以解决因 Web 应用防火墙出现的单点故障问题，可以在一台设备出现故障时，另一台设备接管完全的访问流量，保证业务始终处于正常运行，极大的减少设备故障时业务中断时间。

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 WEB应用防火墙反向代理模式双机主备部署配置举例

3.1 组网需求

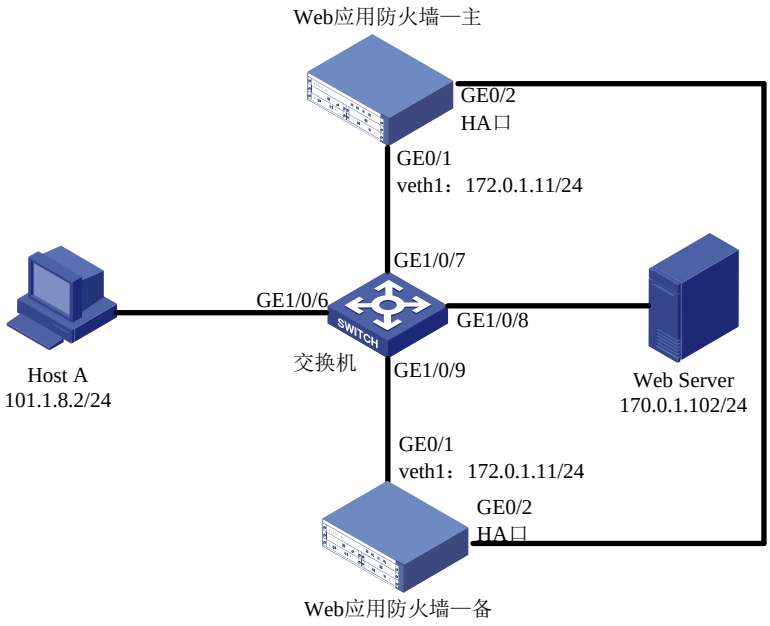
设备在出厂时，默认所有接口都是属于 vlan1 的 access 口，用户可以按实际需求修改接口的类型。

如图所示，Host A 可以访问到 Web 应用防火墙的业务地址，Web 应用防火墙可以访问到 Web Server 服务器。现在要求 Host A 通过访问 Web 应用防火墙的代理地址实现对 Web 服务器的应用访问，并在主应用防火墙出现故障时可以切换到备设备上。

注意

双机冗余模式要求 2 台 Web 应用防火墙的设备型号和软件版本完全相同。

图3-1 Web 应用防火墙反向代理模式双机主备部署配置举例组网图



3.2 使用版本

本举例是在系统版本：ESS6712 上进行配置和验证的。

3.3 配置步骤

3.3.1 部署模式配置

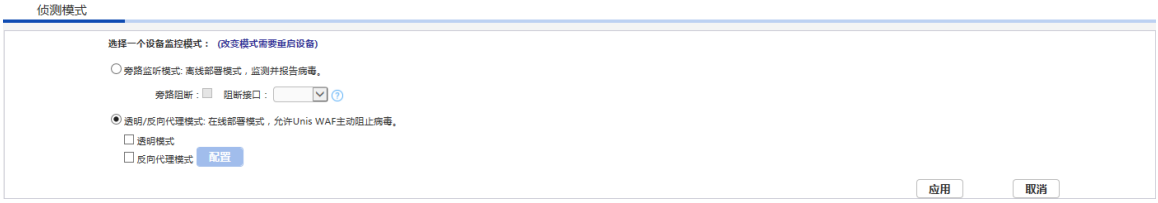
登录主 Web 应用防火墙：启动 IE/FIREFOX 浏览器，在地址栏内输入“https://192.168.0.1”即可进入 Web 网管登录页面。输入用户名“admin”、密码“admin”，点击<登录>按钮即可进入 Web 网管页面并进行相关操作。

注意

推荐使用 IE10+及 Firefox56+及其以上版本的浏览器。

登录主应用防火墙后点击左侧菜单：系统配置-侦测模式。

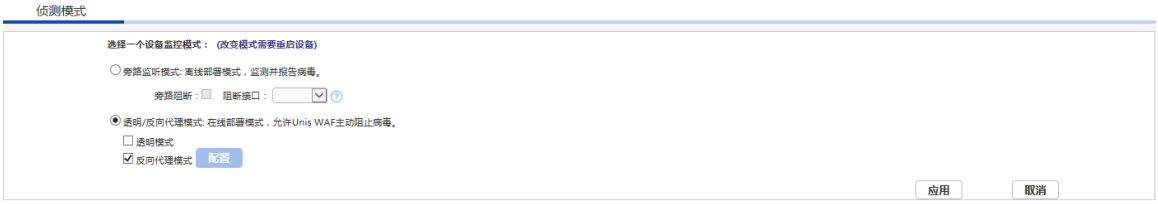
图3-2 侦测模式配置图-监控模式选择



在侦测模式配置页面中，设备默认工作模式为透明模式，修改设备工作模式为反向代理模式，首先勾选反向代理模式前面的选择框，然后点击应用，并在页面右上角点击保存配置。之后需要重启设备以便使模式生效。

设备重启后回到这个配置页面，此时反向代理模式前面的选择框是有勾选状态。

图3-3 侦测模式配置图-反向代理选择



此时点击反向代理模式后面的配置按钮进入反向代理配置界面。

图3-4 反向代理配置界面

在配置界面中首先需要配置的是反向代理的业务接口，可以在页面上部反向代理接口处选择指定的接口，以组网图 3-1 为例，我们在这里选择的是 GE0/1 接口，选择后点击应用。

图3-5 反向代理接口配置图

接口选择完继续添加需要代理的 Web 服务器，在接口下方的服务器设置项点击添加按钮。

图3-6 反向代理服务器配置界面

在服务器添加配置页中，我们要设置用于代理的 IP 地址、子网掩码和代理端口，服务器 IP 地址端口为真实 Web 服务器地址和端口，填写完成后点击应用按钮完成代理服务器添加。添加完成后如图：此时 172.0.1.11 为代理地址，170.0.1.102 为真实 Web 服务器。

图3-7 反向代理服务器配置完成图

备应用防火墙部署模式的配置，同样参考上述步骤。

3.3.2 交换机配置

以组网图 3-1 为例，在交换机上建立 3 个 Vlan，分别是 101.1.8.0/24、172.0.1.0/24、170.0.1.0/24，并配置三个 Vlan 的网关。以下交换机配置命令均以 UNIS 交换机为例。

图3-8 创建 vlan 101 并配置网关

```
[SW]
[SW]
[SW]vlan 101
[SW-vlan101]port g                                    创建vlan 101，并将GE1/0/6端口加入
[SW-vlan101]port GigabitEthernet 1/0/6
[SW-vlan101]
[SW-vlan101]quit
[SW]
[SW]int
[SW]interface v
[SW]interface vlan-interface 101
[SW-vlan-interface101]ip ad
[SW-vlan-interface101]ip address 101.1.8.1 255.255.255.0   配置vlan 101的网关
[SW-vlan-interface101]quit
[SW]
[SW]
[SW]
```

图3-9 创建 vlan 172 并配置网关

```
[SW]
[SW]
[SW]vlan 172
[SW-vlan172]port g
[SW-vlan172]port GigabitEthernet 1/0/7
[SW-vlan172]port GigabitEthernet 1/0/9
[SW-vlan172]quit
[SW]
[SW]int
[SW]interface v
[SW]interface vlan-interface 172
[SW-vlan-interface172]ip ad
[SW-vlan-interface172]ip address 172.0.1.1 255.255.255.0
[SW-vlan-interface172]quit
[SW]
[SW]
[SW]
```

创建vlan 172，并将GE1/0/7和GE1/0/9端口加入

配置vlan 172的网关

图3-10 创建 vlan 170 并配置网关

```
[SW]
[SW]
[SW]vlan 170
[SW-vlan170]port g
[SW-vlan170]port GigabitEthernet 1/0/8
[SW-vlan170]quit
[SW]
[SW]int
[SW]interface v
[SW]interface vlan-interface 170
[SW-vlan-interface170]ip ad
[SW-vlan-interface170]ip address 170.0.1.1 255.255.255.0
[SW-vlan-interface170]quit
[SW]
[SW]
[SW]
```

创建vlan 170，并将GE1/0/8端口加入

配置vlan 170的网关

3.3.3 网络配置

在主应用防火墙上，点击左侧菜单：网络配置-网络接口。

图3-11 网络接口界面

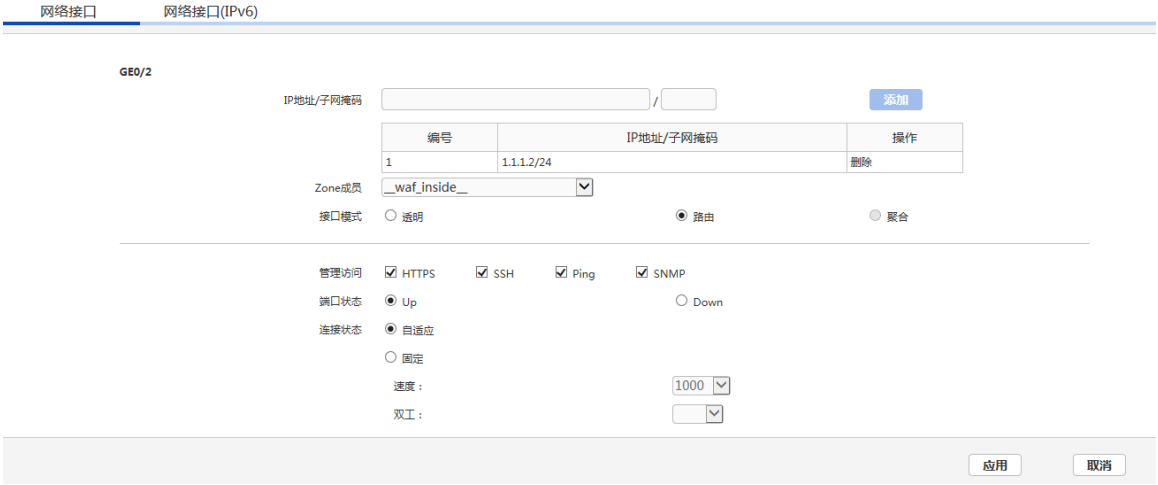
注意

名称为 veth1 的接口，是 WAF 本身的一个虚接口，反向代理模式下，配置的代理 IP 都会关联到该虚接口上。

此时可以观察到，veth1 接口被配置了代理接口地址，工作模式为路由模式，此时代表反向代理模式配置成功。

此时需要确定 HA 接口，本例我们选择 GE0/2 接口，点击编辑 GE0/2 接口，我们将 GE0/2 接口改为路由模式，并配置设备互联地址：1.1.1.2/24，点击应用。

图3-12 网络接口配置页面



备应用防火墙的网络配置，同样参考上述步骤。但不同的一点是，备应用防火墙 HA 口的 IP，需要设置为和主应用防火墙 HA 口 IP 在同一网段，本例中，我们可设置为 1.1.1.3/24。

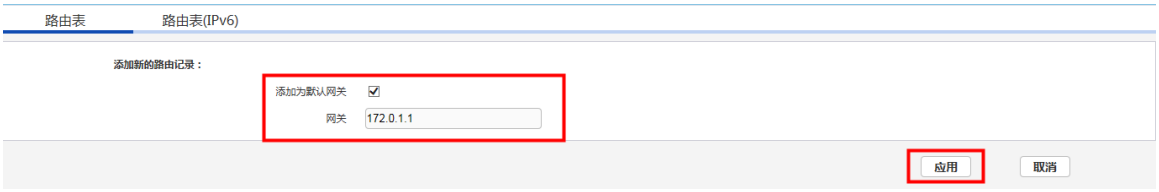
3.3.4 路由配置

在主应用防火墙上，进行路由配置。

由于系统仅有直连路由和添加的静态路由，因此需要在路由表中添加一条默认路由，使 WAF 上的业务流量都从反代业务口进出。

以组网图 3-1 为例，反代模式的代理 IP 为 172.0.1.11，反代业务口所连的交换机的网关为 172.0.1.1，因此添加一条路由，勾选“添加为默认网关”，网关为 172.0.1.1。

图3-13 WAF 路由配置



备应用防火墙的路由配置，同样参考上述步骤。

注意

- 以上部署模式、网络和路由配置，需在主、备应用防火墙上提前配置完成。并需要注意配置的其他接口和管理地址不能与业务代理地址在相同网段。
- 若配置完反向代理接口地址后，ping 不通该地址，可以在“网络接口”页面点击 veth1 接口，查看其管理访问中的 ping 方式是否开启，若没有开启，勾选该方式并点击应用，之后再尝试是否能够 ping 通。

3.3.5 双机配置

1. 配置主Web应用防火墙

开始配置主 Web 防火墙：点击左侧网络配置-高可用性，进入高可用性选项后，在顶部选择高可用性标签进入高可用性配置页；

分别配置：

(1) 选定启用 HA 选项；

(2) 设置 HA 模式，我们这里选择主备项；

(3) HA 接口配置 GE0/2；

(4) HA 优先级根据主备情况配置，现在配置主机，优先级设置为 200，数值低的为备机，数值高的为主机；

(5) 配置对等 IP（即 HA 对端设备 IP），我们这里配置 1.1.1.3；

(6) 监控接口，选择正常的业务接口，一旦被监控接口出现故障，就触发设备切换操作。

注意

由于主、备设备不同步“监控接口”部分的配置，建议部署时，主、备设备此处配置一致。

以上配置完成后点击应用。

图3-14 HA 高可用性配置界面

图3-15 HA 高可用性配置界面

2. 配置备Web防火墙

开始配置备 Web 防火墙，点击左侧网络配置-高可用性，进入高可用性选项后，在顶部选择高可用性标签进入高可用性配置页；

分别配置：

(1) 选定启用 HA 选项；

(2) 设置 HA 模式，我们这里选择主备项；

(3) HA 接口配置 GE0/2；

(4) HA 优先级根据主备情况配置，现在配置备机，优先级设置为 100，数值低的为备机，数值高的为主机；

(5) 配置对等 IP（即 HA 对端设备 IP），我们这里配置 1.1.1.2；

(6) 监控接口，选择正常的业务接口，一旦被监控接口出现故障，就触发设备切换操作。

注意

由于主、备设备不同步“监控接口”部分的配置，建议部署时，主、备设备此处配置一致。

以上配置完成后点击应用。

图3-16 HA 高可用性配置界面

图3-17 HA 高可用性配置界面

以上配置完成后即可完成 HA 的配置，此时 2 台设备已经工作在主备模式状况下。

表3-1 HA 配置参数说明

功能	说明
启用HA	启用双机
HA模式	主备模式
HA状态	Master/Backup，主机点击同步即可将配置同步到备机

功能	说明
Failover状态	故障切换状态，主机点击设置Failover即可切换为备机
HA接口	选择两个设备之间互连的心跳线接口
HA优先级	HA优先级根据主备情况配置，若两台机器均可正常工作，初始化后则数值低的为备机，数值高的为主机
组ID	两台设备需配置相同的组ID
保持间隔	两台设备之间发送VRRP报文的时间间隔
对等IP	对方设备的HA地址
跟踪超时	假设设置为3秒，意义为若跟踪主机在3秒内都无法连通，系统计算链路的权重值低于设定值时，VRRP才认为主设备的链路出现故障，由从设备来接替主设备的工作
设备切换频率临界值	与跟踪超时、跟踪主机配合使用
跟踪主机IP地址	可设置三个跟踪主机，且可分别设置加权系数
监控接口	系统监控接口的连接状态，主机监控接口Down掉导致接口的权重值低于备机时，VRRP才认为主设备的接口出现故障，由从设备来接替主设备的工作
启用先占模式	若不启用先占模式，主机故障会切换到备机，主机即使恢复也不会切换回来；若启用先占模式，设定先占延时时间，主机恢复正常时间超过先占延时时间，流量则会被切换回来

注意

HA 切换条件如下：

- HA 接口：设定心跳间隔，如果从设备在超过 3 个心跳间隔后依然没有收到主设备的 VRRP 报文，则认为主设备已经无法正常工作，从设备会自动切换为主设备。
- 手动切换：主机点击“设置 Failover”即可切换为备机，再点击“取消 Failover”则可恢复为主机（主设备启用了先占模式，且 HA 优先级较高）。
- 跟踪主机：设定监控主机来监控主设备连接的各个链路是否畅通，设定监控主机并为其设定不同的加权系数、权重值。当某链路故障，且该链接权重大于临界值时，主备机会比较当前存活主机个数，若主设备存活主机个数小于备机，此时认为主设备的链路出现故障，由从设备来接替主设备的工作。
- 监控接口：设定监控接口来监控主设备各个接口的工作状态，设定监控接口并为其设定不同的加权系数、权重值。当监控接口 Down 掉导致接口的权重值降低超过一定的限值时，VRRP 才认为主设备的接口出现故障，由从设备来接替主设备的工作。

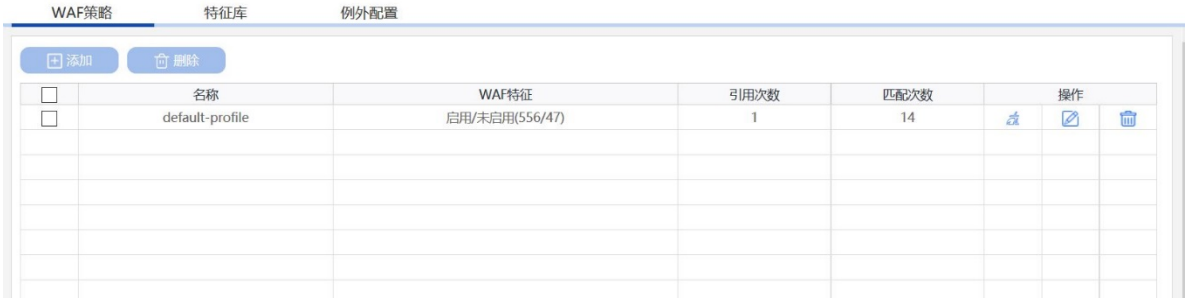
优先级：failover>跟踪主机>监控接口

3.3.6 安全策略配置

在主应用防火墙上，进行安全策略配置。

点击左侧安全策略-Web 安全策略，根据需要添加调整 Web 应用防护策略。

图3-18 WAF 策略界面



点击添加按钮可以添加新 WAF 策略，点击策略右侧操作按键可以调整策略配置，可根据客户安全需求调整策略内容和动作等信息。调整完毕后点击确定。

图3-19 WAF 策略配置界面

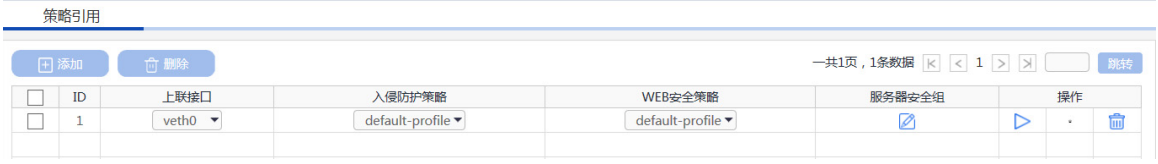
点击左侧安全策略-策略引用，将添加的 Web 应用策略与 Web 服务器进行关联。

点击左侧添加按钮，添加新的引用策略，上联接口一定要选择 veth0 接口，其他配置根据需要和配置选择入侵检测策略和 WEB 防护策略（上一步添加的 WAF 策略），点击服务器安全组按钮添加被保护服务器。

注意

反代模式下上联接口选择 veth0 接口的原因：由于反代模式下，配置的代理 IP 被关联到虚接口 veth1 上，而 veth0 和 veth1 是 WAF 本身的一对虚接口对，流量上代理时，是从 veth0 虚接口流入的，所以需要将 veth0 设为上联接口，才会对流量进行规则检测。

图3-20 策略引用界面



添加被保护服务器（此时被保护服务器为真实服务器地址）：在服务器列表里添加服务器地址和掩码，协议端口可根据业务情况进行填写和选择，填写完成后点击右侧的添加按钮即可添加到服务器列表中，可以添加多条服务器信息。添加完成后点击应用并返回上一级界面。

图3-21 服务器添加界面

添加策略引用后界面，默认情况下策略添加完成后并不会启用，需点击操作界面的启用按键启用策略，策略启用后设备既可以实现对 WEB 服务器的安全防护功能。

图3-22 策略引用配置完成

3.3.7 策略同步

策略配置可通过高可用性配置页的同步按键将主墙配置同步到备墙上：网络配置-高可用性；高可用性配置页下的 HA 状态后面的同步按钮。

图3-23 HA 高可用性配置界面

3.4 验证配置

- Host A 访问 Web Server 可以正常打开 Web 的页面，此时流量应该经过主应用防火墙；观察主备设备的 HA 工作模式。

图3-24 主设备截图：

图3-25 备设备截图：

- 断开主应用防火墙的业务接口，观察设备切换情况，并测试业务是否可以正常打开。
- 主备设备模式切换：备机成为主墙。

图3-26 HA 高可用性配置页面模式变化

- 至此 Web 应用防火墙完成主备切换，可进行业务攻击测试以验证备应用防火墙的防护策略是否生效。

- 进行攻击测试

攻击测试方法：

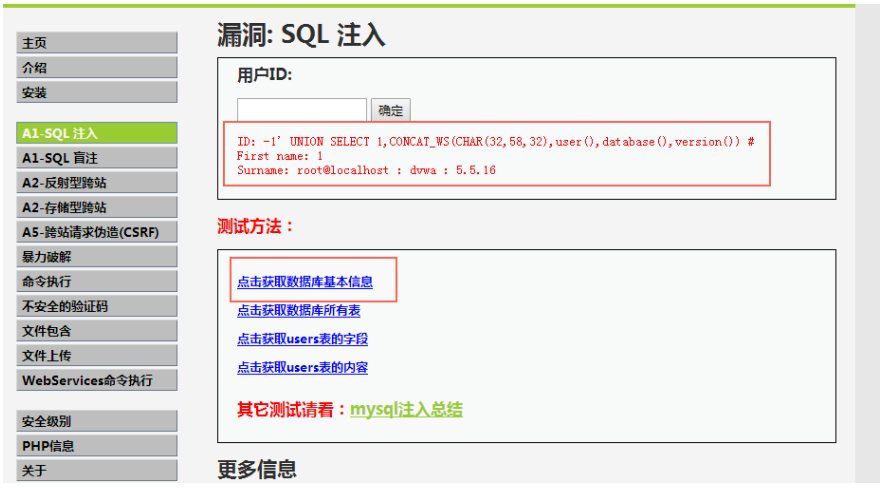
可以在目标服务器上安装测试靶机环境，靶机软件 DVWA 服务器端。

在客户端用浏览器登录靶机 DVWA 测试页面。

图3-27 SQL 注入

选择 SQL 注入选项，并点击测试方法项。

图3-28 SQL 注入



- 进行攻击测试后，可以在 Web 安全策略中观察到策略命中数。
- 在左侧日志报表项-日志-WEB 安全日志中可以查看具体告警信息。

旁路模式部署配置举例

目 录

1 简介

本文档介绍了 Web 应用防火墙旁路模式部署的配置举例。

Web 应用防火墙的旁路部署模式可以快速的实现部署，配置简单，不改变原有网络拓扑结构，可以快速实现对 Web 应用服务器访问流量的监视和告警。旁路部署模式可避免绝大多数的部署兼容性问题，降低因新设备部署带来的业务中断风险。

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 WEB应用防火墙旁路监听部署配置举例

3.1 组网需求

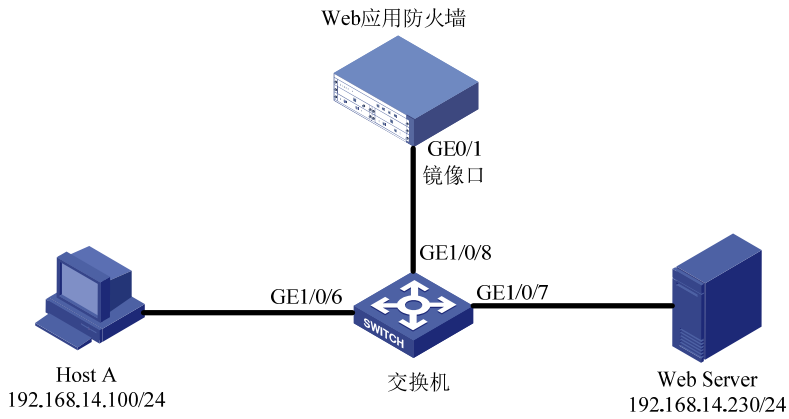
设备在出厂时，默认所有接口都是属于 vlan1 的 access 口，用户可以按实际需求修改接口的类型。

如图所示，现在要求 Web 应用防火墙通过交换机镜像接口 GE1/0/8 侦听交换机业务接口 GE1/0/6 和 GE1/0/7 的双向流量。通过分析镜像数据包，实现监视访问 Web 应用服务器的流量，并在出现攻击行为时实时报警。

注意

镜像接口必须镜像业务口的双向流量，以保证 Web 应用防火墙可以获取业务访问的全部往来流量。

图3-1 Web 应用防火墙旁路监听部署配置举例组网图



3.2 使用版本

本举例是在系统版本：ESS6712 上进行配置和验证的。

3.3 配置步骤

3.3.1 部署模式配置

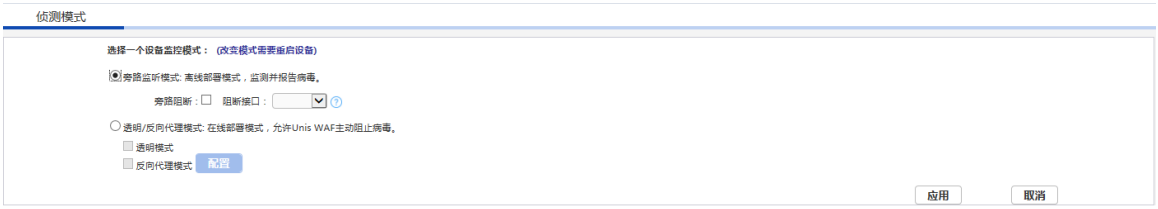
登录 Web 应用防火墙：启动 IE/CHROME 浏览器，在地址栏内输入“https://192.168.0.1”即可进入 Web 网管登录页面。输入用户名“admin”、密码“admin”，点击<登录>按钮即可进入 Web 网管页面并进行相关操作。

注意

推荐使用 IE10+及 Firefox56+及其以上版本的浏览器。

登录应用防火墙后点击左侧菜单：系统配置-侦测模式。

图3-2 侦测模式配置图-侦测模式选择



在配置模式中，默认情况下采用的是透明模式，此时我们需要选择旁路监听模式，点击旁路监听模式前面的选择框，然后点击应用，并在页面右上角点击保存配置。之后需要重启设备以便使模式生效。

旁路监听模式配置成功后，设备上的空闲透明模式配置的接口均可实现镜像流量监听。

3.3.2 交换机配置

以组网图 3-1 为例，在交换机上创建镜像组，并配置镜像口和监听口。以下交换机配置命令均以 UNIS 交换机为例。

图3-3 在交换机上创建镜像组

```
[SW]
[SW]
[SW]mirr
[SW]mirroring-group 1 lo                    创建镜像组1
[SW]mirroring-group 1 local
[SW]
[SW]mirroring-group 1 mirroring-port GigabitEthernet 1/0/6 both    配置GE1/0/6和GE1/0/7端口为镜像口
[SW]mirroring-group 1 mirroring-port GigabitEthernet 1/0/7 both
[SW]
[SW]mir
[SW]mirroring-group 1 moni
[SW]mirroring-group 1 monitor-p
[SW]mirroring-group 1 monitor-port g
[SW]mirroring-group 1 monitor-port GigabitEthernet 1/0/8    配置GE1/0/8端口为监听口
[SW]
[SW]
[SW]
```

3.3.3 安全策略配置

点击左侧安全策略-Web 安全策略，根据需要添加调整 Web 应用防护策略。

图3-4 WAF 策略界面

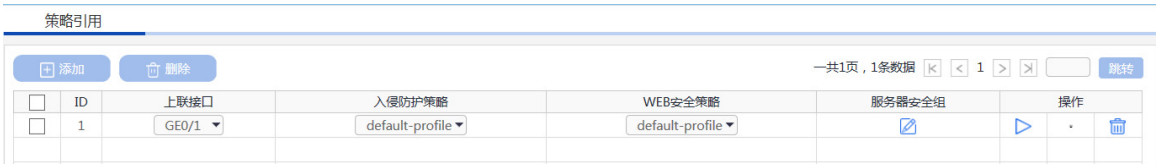
点击添加按钮可以添加新 WAF 策略，点击策略右侧操作按键可以调整策略配置，可根据客户安全需求调整策略内容和动作等信息。调整完毕后点击确定。

图3-5 WAF 策略配置界面

点击左侧安全策略-策略引用，将添加的 Web 应用策略与 Web 服务器进行关联。

点击左侧添加按钮，添加新的引用策略，上联接口选择作为镜像口的接口，以组网图 3-1 为例，我们这里选择的是 GE0/1 接口，如在后续使用中更换了镜像接口，我们也要在这里更改为相应的接口。其他配置根据需要和配置选择入侵检测策略和 WEB 防护策略（上一步添加的 WAF 策略），点击服务器安全组按钮添加被保护服务器。

图3-6 策略引用界面

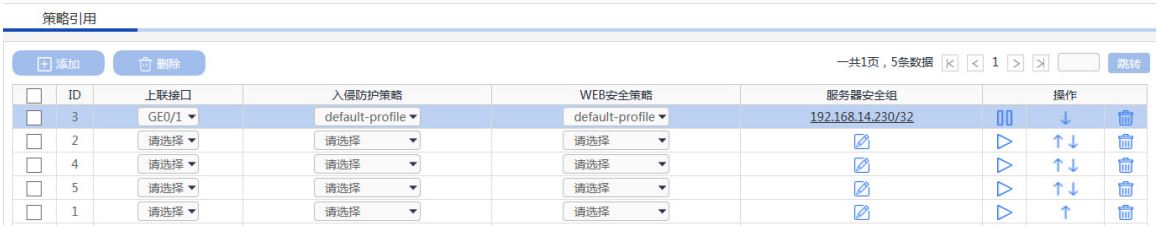


添加被保护服务器（此时被保护服务器为真实服务器地址）：在服务器列表里添加服务器地址和掩码，协议端口可根据业务情况进行填写和选择，填写完成后点击右侧的添加按钮即可添加到服务器列表中，可以添加多条服务器信息。添加完成后点击应用并返回上一级界面。

图3-7 服务器添加界面

策略引用配置完成后，默认情况下新添加的策略并不会立即启用，需点击操作界面的启用按键启用策略，策略启用后设备即可以实现对 WEB 服务器的安全防护功能。

图3-8 策略引用配置完成



点击左侧状态监控-系统状态，进入系统状态显示页面，在打开的页面上方点击网络信息，可以在网络信息中查看镜像接口的流量信息，以便确认镜像接口正常接收到镜像流量。

图3-9 网络信息接口流量监控图

接口	IP	状态	工作模式	TX packet	Error packet	Rx packet	Error
GE0/0	183.1.5.22	up	route	307,502	0	873,672	0
GE0/1	0.0.0.0	up	transparent	8,958	0	41,255	0
GE0/2	1.1.1.2	up	route	55,433	0	567	0
GE0/3	0.0.0.0	down	route	0	0	0	0
GE0/4	0.0.0.0	down	route	0	0	0	0
GE0/5	0.0.0.0	down	route	0	0	0	0
veth1	172.0.1.11	up	route	9,038	0	41,258	0

3.4 验证配置

- Host A 访问 Web Server 可以正常打开 Web 的页面。
- 查看网络信息，观察镜像接口可以收到镜像流量。
- 进行攻击测试，可以在 Web 安全策略中观察到策略命中数。
- 在左侧日志报表项-日志-WEB 安全日志中可以查看具体告警信息。

4 WEB应用防火墙旁路阻断部署配置举例

4.1 组网需求

设备在出厂时，默认所有接口都是属于 vlan1 的 access 口，用户可以按实际需求修改接口的类型。

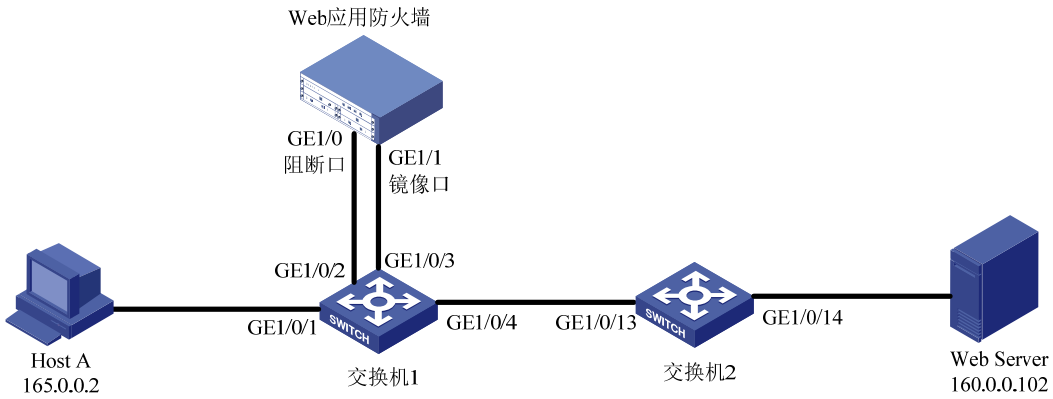
如图所示，现在要求 Web 应用防火墙通过交换机镜像接口 GE1/0/3 侦听交换机业务接口 GE1/0/1 和 GE1/0/4 的双向流量，通过分析镜像数据包，实现监视访问 Web 应用服务器的流量，并在出现攻击行为时实时报警。交换机的 GE1/0/2 接口连接 WAF 的阻断口 GE1/0，在出现攻击行为时通过 GE1/0 口发送阻断请求。

在旁路阻断模式下，WAF 通过交换机的镜像接口，可以侦测到与 WEB 服务器通信的流量，通过应用协议代理可以分析出是否有攻击发生。当攻击发生时，旁路阻断模块需通过收集的攻击的连接信息，伪造和发送 TCP RST 报文，来中断攻击的连接。

注意

- 镜像接口必须镜像业务口的双向流量，以保证 Web 应用防火墙可以获取业务访问的全部往来流量。
- 与 Web 应用防火墙阻断口相连的交换机接口，和与客户端相连的交换机接口，需要配置在同一 vlan 中。
- 组网时，建议 WAF 的阻断口和镜像口不要选择一对 Bypass 口；或者如果选择了一对 Bypass 口，建议将与这两个口相连的交换机接口（如组网图 4-1 中的 GE1/0/2 和 GE1/0/3）配置在不同的 vlan 中，以防 WAF 断电或重启时，导致环路。

图4-1 Web 应用防火墙旁路阻断部署配置举例组网图



4.2 使用版本

本举例是在系统版本：ESS6712 上进行配置和验证的。

4.3 配置步骤

4.3.1 部署模式配置

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。

注意

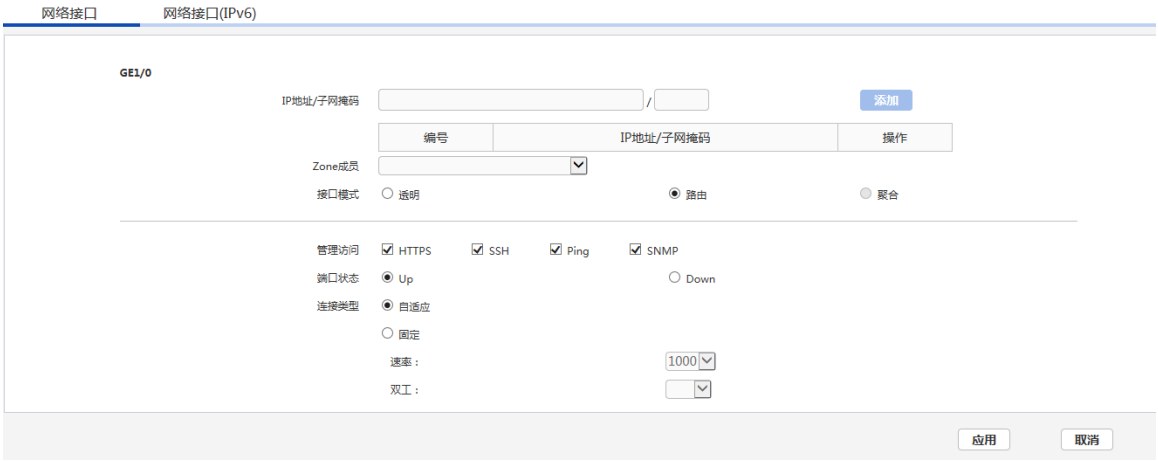
推荐使用 IE10+及 Firefox56+及其以上版本的浏览器。

登录应用防火墙后点击左侧菜单：网络配置-网络接口。

图4-2 网络接口界面

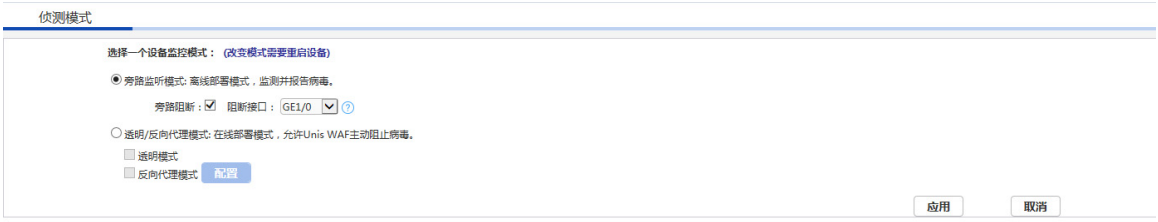
点击“编辑”，将阻断口 GE1/0 的模式改为“路由模式”。

图4-3 网络接口配置页面



点击左侧菜单：系统配置-侦测模式。

图4-4 侦测模式配置图-侦测模式选择



在配置模式中，默认情况下采用的是透明模式，此时我们需要选择旁路阻断模式，点击旁路阻断模式后面的选择框，并将阻断接口选择为组网图上配置的 GE1/0 口，然后点击应用，并在页面右上角点击保存配置。之后需要重启设备以便使模式生效。

4.3.2 交换机配置

以组网图 4-1 为例，在交换机 1 上创建镜像组，并配置镜像口和监听口。以下交换机配置命令均以 UNIS 交换机为例。

图4-5 在交换机 1 上创建镜像组

```
[NBH9SW3]
[NBH9SW3]
[NBH9SW3]mir
[NBH9SW3]mirroring-group 1 local      创建镜像组1
[NBH9SW3]
[NBH9SW3]mir
[NBH9SW3]mirroring-group 1 mir
[NBH9SW3]mirroring-group 1 mirroring-port GigabitEthernet 1/0/1 both   配置GE1/0/1和GE1/0/4端口为镜像口
[NBH9SW3]mirroring-group 1 mirroring-port GigabitEthernet 1/0/4 both
[NBH9SW3]
[NBH9SW3]mir
[NBH9SW3]mirroring-group 1 moni
[NBH9SW3]mirroring-group 1 monitor-port GigabitEthernet 1/0/3    配置GE1/0/3端口为监听口
[NBH9SW3]
[NBH9SW3]
[NBH9SW3]
```

参照组网图 4-1，在交换机 1 上，将与客户端相连的 GE1/0/1 端口和与 WAF 阻断口相连的 GE1/0/2 端口设置在同一 vlan 中，如设置在 vlan 2 中，并配置 vlan 2 的网关；并将与交换机 2 相连的 GE1/0/3 端口设置在另一个 vlan 中，如设置在 vlan 3 中，并配置 vlan 3 的网关。

图4-6 在交换机 1 上创建 vlan 2 并配置网关

```
[NBH9SW3]
[NBH9SW3]
[NBH9SW3]
[NBH9SW3]vlan 2
[NBH9SW3-vlan2]port g
[NBH9SW3-vlan2]port GigabitEthernet 1/0/1  创建vlan 2，并将GE1/0/1和GE1/0/2端口加入vlan 2
[NBH9SW3-vlan2]port GigabitEthernet 1/0/2
[NBH9SW3-vlan2]quit
[NBH9SW3]int
[NBH9SW3]interface vlan
[NBH9SW3]interface Vlan-interface 2
[NBH9SW3-Vlan-interface2]ip address 165.0.0.1 24    配置vlan 2的网关
[NBH9SW3-Vlan-interface2]quit
[NBH9SW3]
[NBH9SW3]
```

图4-7 在交换机 1 上创建 vlan 3 并配置网关

```
[NBH9SW3]
[NBH9SW3]
[NBH9SW3]vlan 3
[NBH9SW3-vlan3]port GigabitEthernet 1/0/4  创建vlan 3，并将GE1/0/4端口加入vlan 3
[NBH9SW3-vlan3]quit
[NBH9SW3]interface Vlan-interface 3
[NBH9SW3-Vlan-interface3]ip address 160.0.0.2 24    配置vlan 3的网关
This subnet overlaps with another interface!
[NBH9SW3-Vlan-interface3]quit
[NBH9SW3]
[NBH9SW3]
```

参照组网图 4-1，在交换机 2 上，将 GE1/0/13 口和 GE1/0/14 口设置在同一 vlan 3 中。

图4-8 在交换机 2 上创建 vlan 3

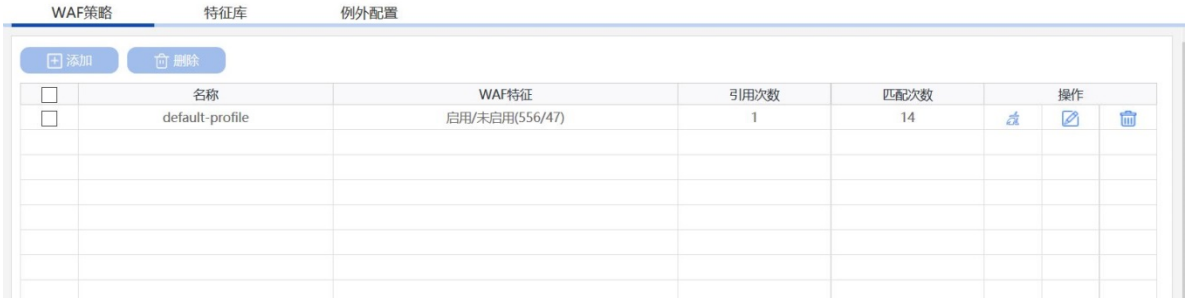
```
[SW]
[SW]
[SW]vlan 3
[SW-vlan3]port g
[SW-vlan3]port GigabitEthernet 1/0/13
[SW-vlan3]port GigabitEthernet 1/0/14
[SW-vlan3]
[SW-vlan3]
```

创建vlan 3，并将GE1/0/13和GE1/0/14端口加入vlan 3

4.3.3 安全策略配置

点击左侧安全策略-Web 安全策略，根据需要添加调整 Web 应用防护策略。

图4-9 WAF 策略界面



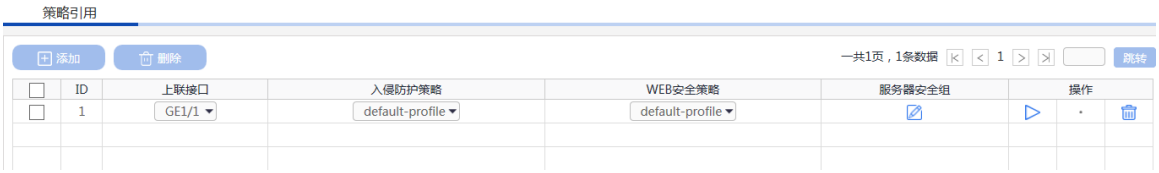
点击添加按钮可以添加新 WAF 策略，点击策略右侧操作按键可以调整策略配置，可根据客户安全需求调整策略内容和动作等信息。调整完毕后点击确定。

图4-10 WAF 策略配置界面

点击左侧安全策略-策略引用，将添加的 Web 应用策略与 Web 服务器进行关联。

点击左侧添加按钮，添加新的引用策略，上联接口选择作为镜像口的接口，以组网图 4-1 为例，我们这里选择的是 GE1/1 接口，如在后续使用中更换了镜像接口，我们也要在这里更改为相应的接口。其他配置根据需要和配置选择入侵检测策略和 WEB 防护策略（上一步添加的 WAF 策略），点击服务器安全组按钮添加被保护服务器。

图4-11 策略引用界面

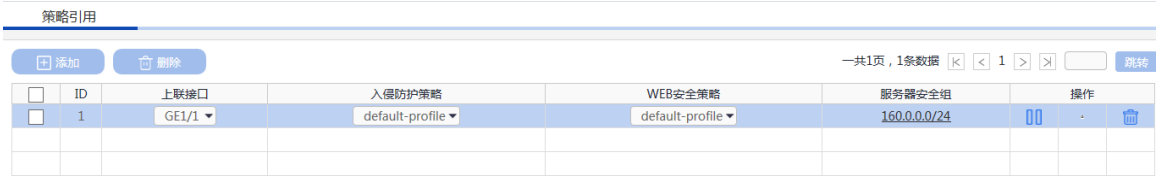


添加被保护服务器（此时被保护服务器为真实服务器地址）：在服务器列表里添加服务器地址和掩码，协议端口可根据业务情况进行填写和选择，填写完成后点击右侧的添加按钮即可添加到服务器列表中，可以添加多条服务器信息。添加完成后点击应用并返回上一级界面。

图4-12 服务器添加界面

策略引用配置完成后，默认情况下新添加的策略并不会立即启用，需点击操作界面的启用按键启用策略，策略启用后设备既可以实现对 WEB 服务器的安全防护功能。

图4-13 策略引用配置完成



点击左侧状态监控-系统状态，进入系统状态显示页面，在打开的页面上方点击网络信息，可以在网络信息中查看镜像接口的流量信息，以便确认镜像接口正常接收到镜像流量。

图4-14 网络信息接口流量监控图

接口	IP	状态	工作模式	Tx Pkts	Tx Errors	Rx Pkts	Rx Errors
GE0/0	183.1.5.44	up	route	160,051	0	849,849	0
GE0/1	0.0.0.0	down	transparent	0	0	0	0
GE1/0	0.0.0.0	up	route	275	0	263,794,654	0
GE1/1	0.0.0.0	up	transparent	0	0	509,871,869	0
GE1/2	0.0.0.0	down	transparent	0	0	0	0
GE1/3	0.0.0.0	down	transparent	0	0	0	0
GE1/4	0.0.0.0	down	transparent	0	0	0	0
GE1/5	0.0.0.0	down	transparent	0	0	0	0
GE1/6	0.0.0.0	down	transparent	0	0	0	0
GE1/7	0.0.0.0	down	transparent	0	0	0	0
veth1	0.0.0.0	up	route	4	0	0	0

4.4 验证配置

- Host A 访问 Web Server 可以正常打开 Web 的页面。
- 查看网络信息，观察镜像接收口可以收到镜像流量。
- 进行攻击测试，可以在 Web 安全策略中观察到策略命中数。
- 在左侧日志报表项-日志-WEB 安全日志中可以查看到具体告警信息。
- 在客户端抓包，可以抓到 WAF 阻断口发送出的 TCP RST 报文。

注意

- 以下功能支持旁路阻断：URL 访问控制、cookie 溢出检查、禁止直接访问、防盗链、参数防护、暴力破解攻击/扫号攻击检查、溢出检查、CSRF 检查、HTTP 协议检查、IIS 短文件、文件夹防泄漏、HTTP 请求方法控制、网络爬虫防护、扫描防护、启用动态攻击黑名单和 SQL 注入。
- 根据组网环境，服务器返回的响应包可能比 WAF 发送的 TCP RST 包优先到达客户端，这种情况下，从客户端访问页面观察不到明显的阻断现象。

透明模式部署配置举例

目 录

1 简介

本文档介绍了 Web 应用防火墙透明模式部署的配置举例。

Web 应用防火墙的透明部署模式可以在不改变现有网络拓扑结构的情况下实现对 Web 服务器进行安全防护的目的。可以低成本、高效的将 Web 防火墙快速部署到现有网络中，减少因网络改造而对业务产生的影响。

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 WEB应用防火墙透明部署配置举例

3.1 组网需求

设备在出厂时，默认所有接口都是属于 vlan1 的 access 口，用户可以按实际需求修改接口的类型。

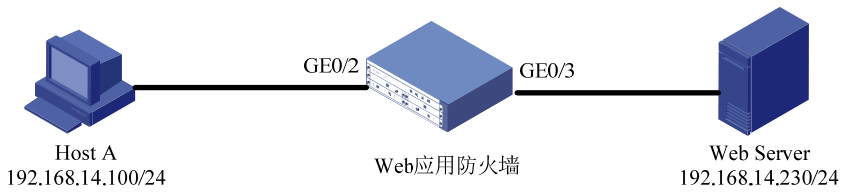
如图所示，Host A 和 Web Server 服务器属于同一网段，可以实现直接互联访问，现要求在 Host A 和 Web Server 服务器中间透明部署 Web 应用防火墙实现对 Host A 访问 Web 服务器流量的监控。

本案例我们选择 Web 应用防火墙的 GE0/2 和 GE0/3 接口作为业务接口。正式部署可根据用户环境选择相应接口作为业务接口。

注意

- 透明部署时，如需要 Bypass 功能，WAF 的进、出口需要选择一对 Bypass 口。
- 各型号设备包含的 Bypass 口以及各型号插卡包含的 Bypass 口，可参照产品的规格说明。

图3-1 Web 应用防火墙透明部署配置举例组网图



3.2 使用版本

本举例是在系统版本：ESS6712 上进行配置和验证的。

3.3 配置步骤

3.3.1 网络配置

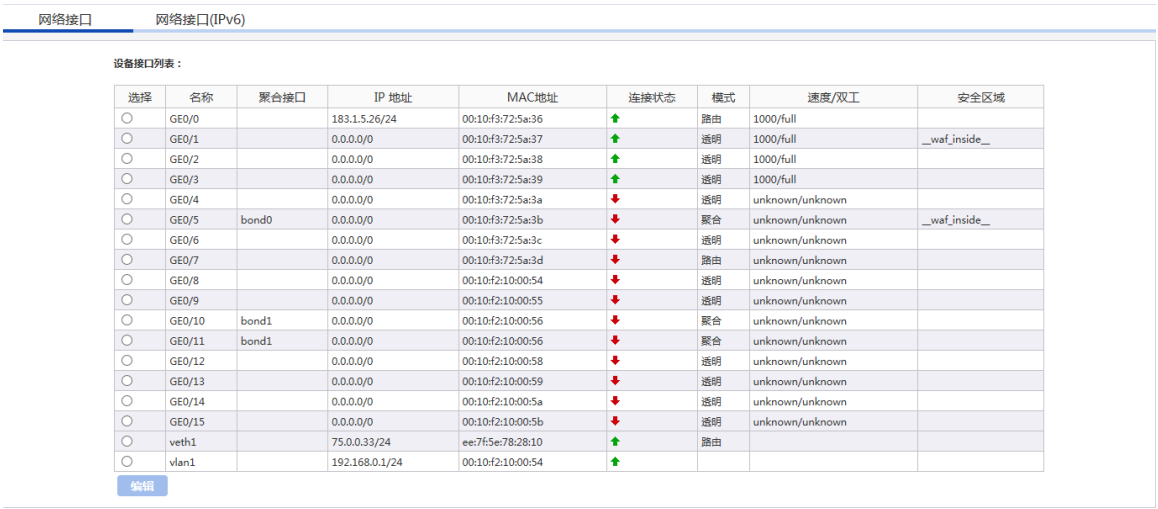
登录 Web 应用防火墙：启动 IE/FIREFOX 浏览器，在地址栏内输入“https://192.168.0.1”即可进入 Web 网管登录页面。输入用户名“admin”、密码“admin”，点击<登录>按钮即可进入 Web 网管页面并进行相关操作。

注意

推荐使用 IE10+及 Firefox56+及其以上版本的浏览器。

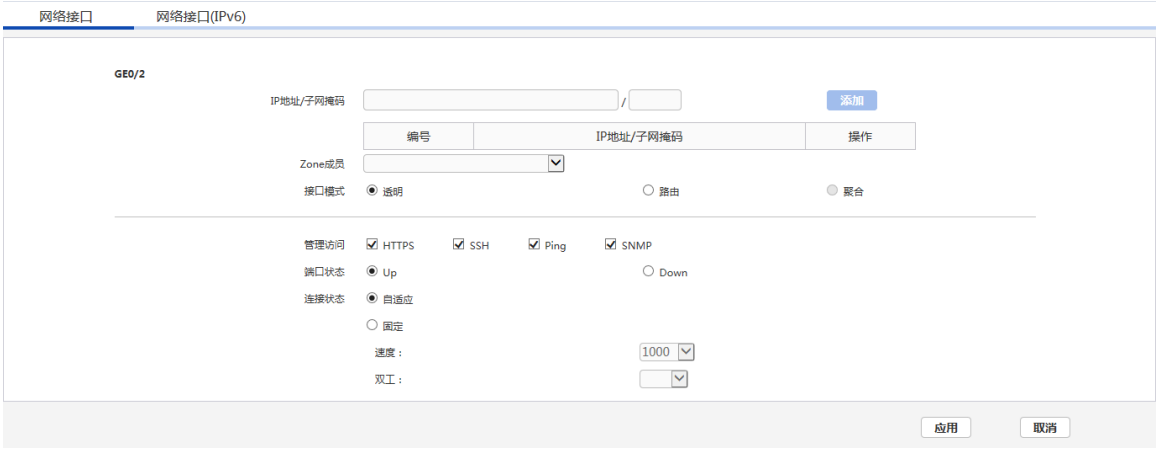
登录应用防火墙后点击左侧菜单：网络配置-网络接口。

图3-2 网络接口界面



点击 GE0/2 前的选择框并点击编辑：配置接口模式为透明模式；端口状态为 Up。GE0/3 接口配置相同。

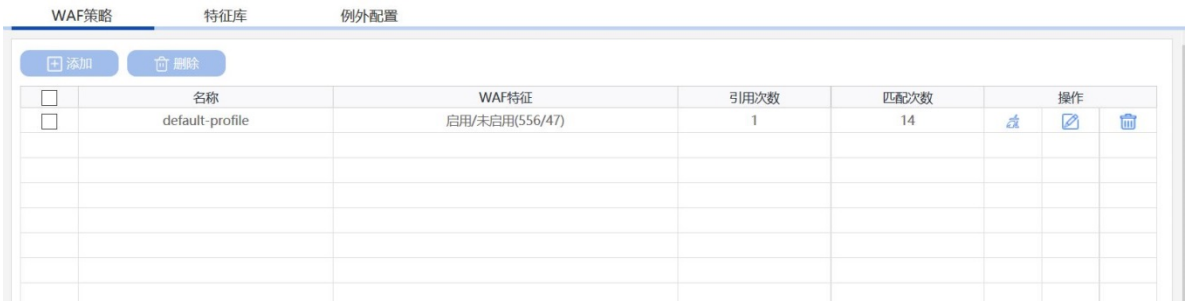
图3-3 网络接口配置页面



3.3.2 安全策略配置

点击左侧安全策略-Web 安全策略，根据需要添加调整 Web 应用防护策略。

图3-4 WAF 策略界面

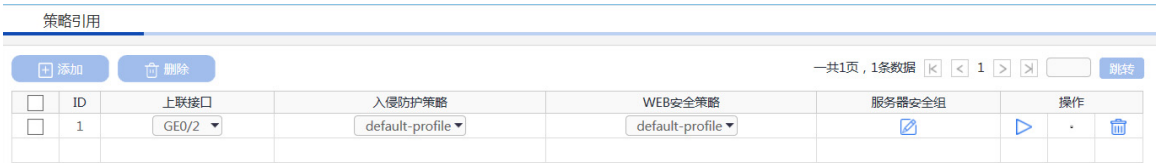


点击添加按钮可以添加新 WAF 策略，点击策略右侧操作按键可以调整策略配置，可根据客户安全需求调整策略内容和动作等信息。调整完毕后点击确定。

图3-5 WAF 策略配置界面

点击左侧菜单栏安全策略-策略引用，将入侵检测策略及 Web 防护策略与 Web 服务器进行关联。点击左上方添加按钮，添加新的策略，上联接口选择流量入接口（以组网图 3-1 为例，即 GE0/2 接口），根据业务情况选择入侵检测策略和 WEB 防护策略，点击服务器安全组按钮添加被保护服务器。

图3-6 策略引用界面

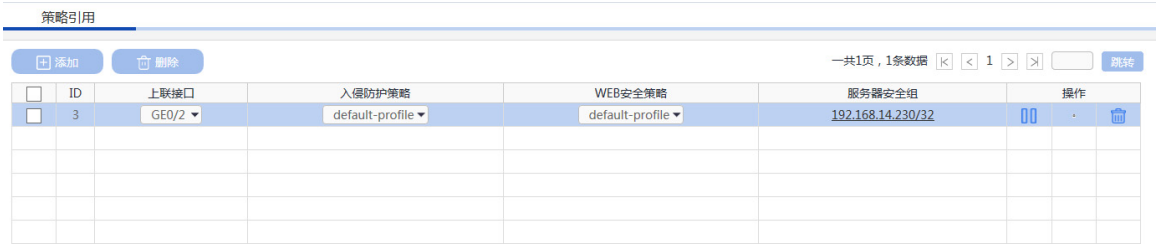


添加被保护服务器：在服务器列表里添加服务器地址和掩码，协议端口可根据业务情况进行填写和选择，填写完成后点击右侧的添加按钮即可添加到服务器列表中，可以添加多条服务器信息。添加完成后点击应用并返回上一级界面。

图3-7 服务器添加界面

添加策略引用后界面，默认情况下策略添加完成后并不会启用，需点击操作界面的启用按键启用策略，策略启用后对 Web 服务器进行安全防护。

图3-8 策略引用配置完成



3.4 验证配置

- Host A 访问 Web Server 可以正常打开 Web 的页面。
- 进行攻击测试。

攻击测试方法：

可以在目标服务器上安装测试靶机环境，靶机软件 DVWA 服务器端。

在客户端用浏览器登录靶机 DVWA 测试页面。

图3-9 SQL 注入

选择 SQL 注入选项，并点击测试方法项

图3-10 SQL 注入

- 进行攻击测试后，可以在 Web 安全策略中观察到策略命中数。
- 在左侧日志报表项-日志-WEB 安全日志中可以查看具体告警信息。

透明双机主备模式部署配置举例

目 录

1 简介

本文档介绍了 Web 应用防火墙透明双机主备模式部署的配置举例。

Web 应用防火墙的高可用性可以解决因 Web 应用防火墙出现的单点故障问题，可以在一台设备出现故障时，另一台设备接管完全的访问流量，保证业务始终处于正常运行，极大的减少设备故障时业务中断时间。

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 WEB应用防火墙透明双机主备模式部署配置举例

3.1 组网需求

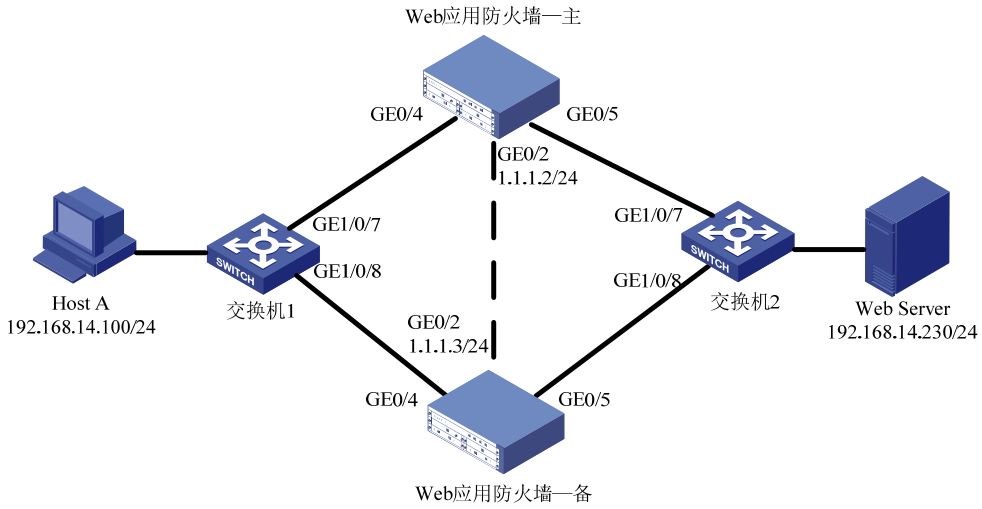
设备在出厂时，默认所有接口都是属于 vlan1 的 access 口，用户可以按实际需求修改接口的类型。

如图所示，Host A 和 Web Server 服务器属于同一网段，可以实现直接互联访问，现要求在 Host A 和 Web Server 服务器中间透明部署 2 台 Web 应用防火墙，2 台 Web 应用防火墙之间开启主备冗余模式，保证在一台 Web 应用防火墙出现故障时，Host A 正常访问 Web 服务器。

注意

- 双机冗余模式要求 2 台 Web 应用防火墙的设备型号和软件版本完全相同。
- 若实际使用透明双机主备组网时，不需要使用 bypass 功能，建议组网过程中不要使用一对 bypass 口，以免设备故障之后，流量直接通过 bypass 转发而不检测。

图3-1 Web 应用防火墙 HA 主备模式部署配置举例组网图



3.2 使用版本

本举例是在系统版本：ESS6712 上进行配置和验证的。

3.3 配置步骤

登录 Web 应用防火墙：启动 IE/FIREFOX 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。

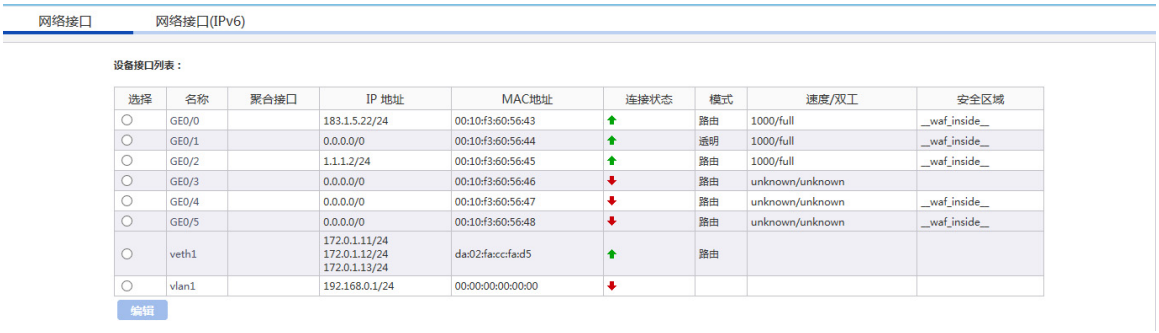
注意

推荐使用 IE10+及 Firefox56+及其以上版本的浏览器。

3.3.1 网络配置

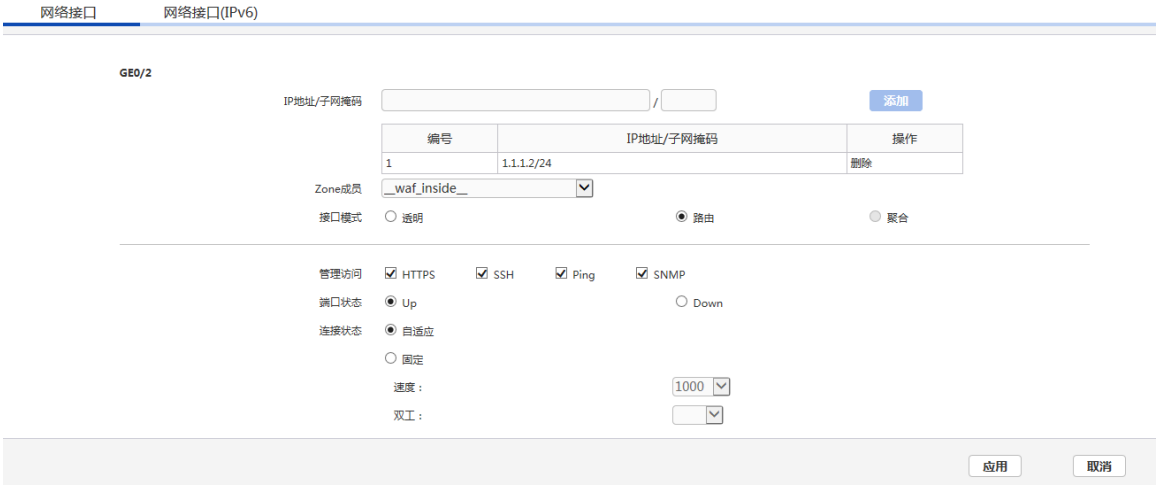
首先配置主应用防火墙的网络配置；点击左侧菜单：网络配置-网络接口。

图3-2 主设备网络接口界面



先确定 HA 接口，本例我们选择 GE0/2 接口，点击编辑 GE0/2 接口，我们将 GE0/2 接口改为路由模式，并配置设备互联地址：1.1.1.2/24，点击应用。

图3-3 主设备网络接口配置页面

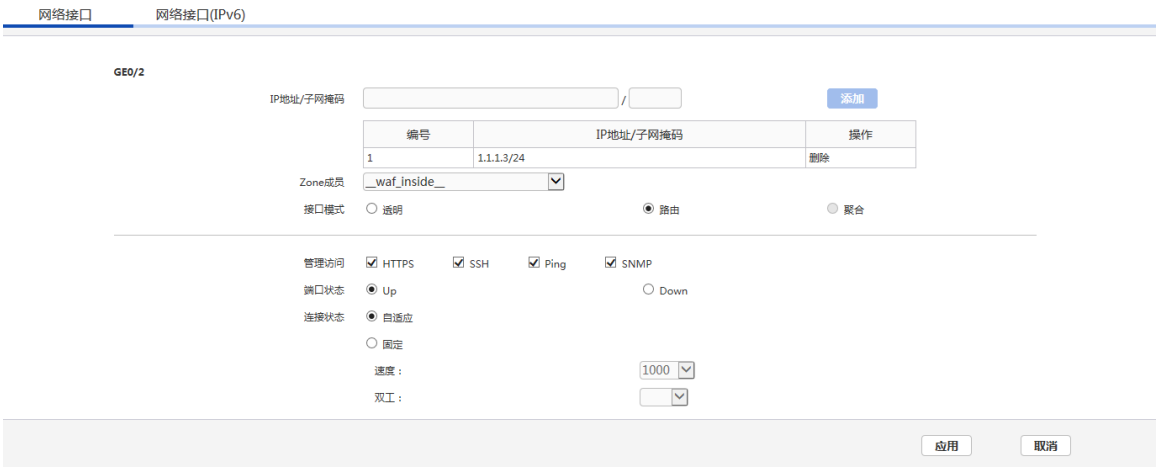


开始配置备防火墙：点击左侧菜单：网络配置-网络接口。

图3-4 备设备网络接口界面

确定 HA 接口，本例我们选择 GE0/2 接口，点击编辑 GE0/2 接口，我们将 GE0/2 接口改为路由模式，并配置设备互联地址：1.1.1.3/24，点击应用。

图3-5 备设备网络接口配置页面



3.3.2 双机配置

1. 配置主Web应用防火墙

开始配置主 Web 应用防火墙 HA：点击左侧网络配置-高可用性，进入高可用性选项后，在顶部选择高可用性标签进入高可用性配置页。

分别配置：

(1) 选定启用 HA 选项；

(2) 设置 HA 模式，我们这里选择主备项；

(3) HA 接口配置 GE0/2；

(4) HA 优先级根据主备情况配置，现在配置主机，优先级设置为 200，数值低的为备机，数值高的为主机；

(5) 配置对等 IP（即 HA 对端设备 IP），我们这里配置 1.1.1.3；

(6) 监控接口，选择正常的业务接口，一旦被监控接口出现故障，就触发设备切换操作。

注意

由于主、备设备不同步“监控接口”部分的配置，建议部署时，主、备设备此处配置一致。

以上配置完成后点击应用。

图3-6 主设备 HA 高可用性配置界面

图3-7 主设备 HA 高可用性配置界面（续）

2. 配置备Web应用防火墙

开始配置备 Web 应用防火墙 HA：点击左侧网络配置-高可用性，进入高可用性选项后，在顶部选择高可用性标签进入高可用性配置页。

分别配置：

(1) 选定启用 HA 选项；

(2) 设置 HA 模式，我们这里选择主备项；

(3) HA 接口配置 GE0/2；

(4) HA 优先级根据主备情况配置，现在配置备机，优先级设置为 100，数值低的为备机，数值高的为主机；

(5) 配置对等 IP（即 HA 对端设备 IP），我们这里配置 1.1.1.2；

(6) 监控接口，选择正常的业务接口，一旦被监控接口出现故障，就触发设备切换操作。

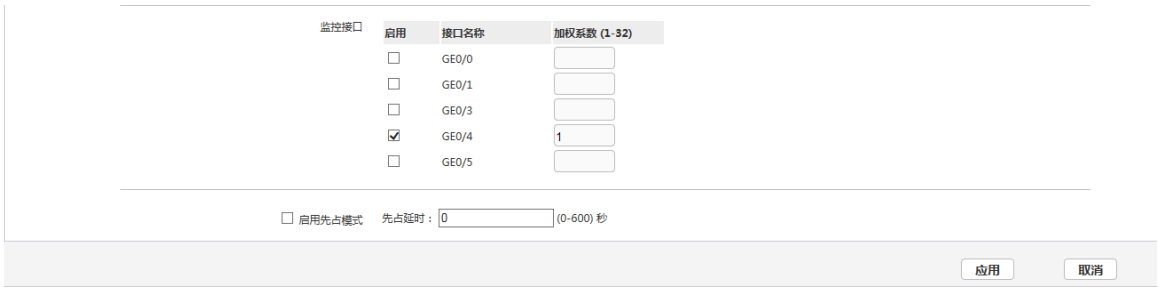
注意

由于主、备设备不同步“监控接口”部分的配置，建议部署时，主、备设备此处配置一致。

以上配置完成后点击应用。

图3-8 备设备 HA 高可用性配置界面

图3-9 备设备 HA 高可用性配置界面（续）



以上配置完成后即可完成 HA 的配置，此时 2 台设备已经工作在主备模式状况下。

表3-1 HA 配置参数说明

功能	说明
启用HA	启用双机
HA模式	主备模式/主主模式
HA状态	Master/Backup，主机点击同步即可将配置同步到备机
Failover状态	故障切换状态，主机点击设置Failover即可切换为备机

功能	说明
HA接口	选择两个设备之间互连的心跳线接口
HA优先级	HA优先级根据主备情况配置，若两台机器均可正常工作，初始化后则数值低的为备机，数值高的为主机
组ID	两台设备需配置相同的组ID
保持间隔	两台设备之间发送VRRP报文的时间间隔
对等IP	对方设备的HA地址
跟踪超时	假设设置为3秒，意义为若跟踪主机在3秒内都无法连通，系统计算链路的权重值低于设定值时，VRRP才认为主设备的链路出现故障，由从设备来接替主设备的工作
设备切换频率临界值	与跟踪超时、跟踪主机配合使用
跟踪主机IP地址	可设置三个跟踪主机，且可分别设置加权系数
监控接口	系统监控接口的连接状态，主机监控接口Down掉导致接口的权重值低于备机时，VRRP才认为主设备的接口出现故障，由从设备来接替主设备的工作
启用先占模式	若不启用先占模式，主机故障会切换到备机，主机即使恢复也不会切换回来；若启用先占模式，设定先占延时时间，主机恢复正常时间超过先占延时时间，流量则会被切换回来

注意

HA 切换条件如下：

- HA 接口：设定心跳间隔，如果从设备在超过 3 个心跳间隔后依然没有收到主设备的 VRRP 报文，则认为主设备已经无法正常工作，从设备会自动切换为主设备。
- 手动切换：主机点击“设置 Failover”即可切换为备机，再点击“取消 Failover”则可恢复为主机（主设备启用了先占模式，且 HA 优先级较高）。
- 跟踪主机：设定监控主机来监控主设备连接的各个链路是否畅通，设定监控主机并为其设定不同的加权系数、权重值。当某链路故障，且该链接权重大于临界值时，主备机会比较当前存活主机个数，若主设备存活主机个数小于备机，此时认为主设备的链路出现故障，由从设备来接替主设备的工作。
- 监控接口：设定监控接口来监控主设备各个接口的工作状态，设定监控接口并为其设定不同的加权系数、权重值。当监控接口 Down 掉导致接口的权重值降低超过一定的限值时，VRRP 才认为主设备的接口出现故障，由从设备来接替主设备的工作。

优先级：failover>跟踪主机>监控接口

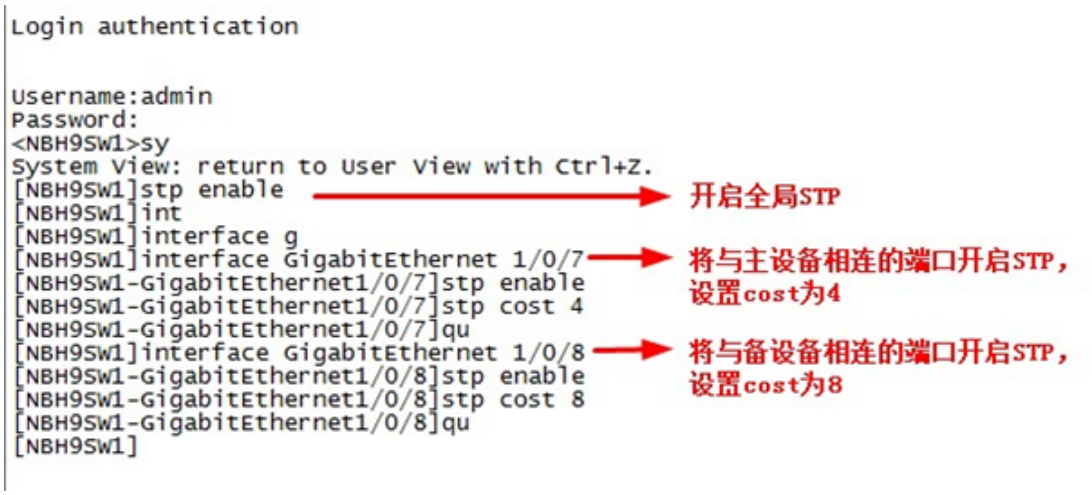
3.3.3 交换机配置

透明双机主备模式下，主备机间需要连接 HA 线，是通过 vrrp 来决定流量走哪条链路的。但是，特殊情况下，如果 HA 线故障，两台设备都会变为主设备，可能会导致业务流量异常，建议透明双机主备模式下也对交换机进行 STP 配置。

以组网图 3-1 为例，需要开启交换机 1、交换机 2 上全局的 STP 功能，并将和两台 WAF 相连的交换机端口的 STP 功能开启。此外，在透明双机主备正常工作的情况下，为了保证交换机 STP 所选择的链路与当前工作主机的链路保持一致，还需要将与主设备相连端口的 cost 值设置为较低的数值。以下交换机配置命令均以 UNIS 交换机为例。

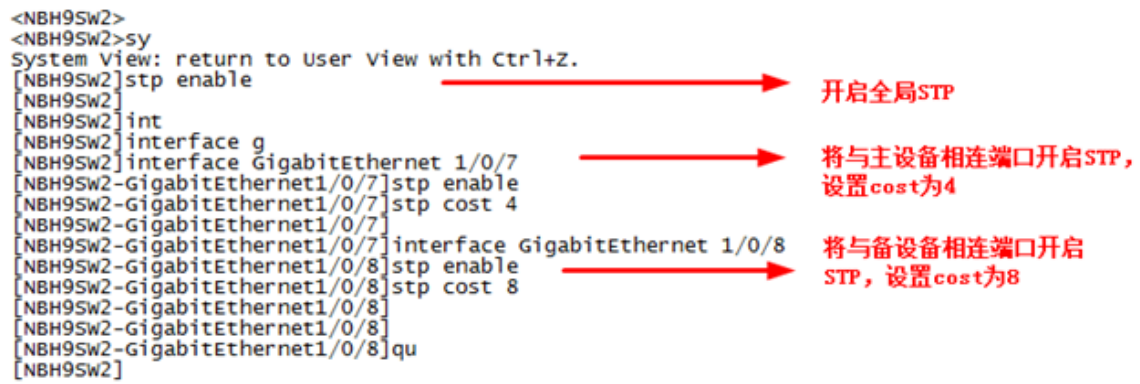
首先，登录交换机 1，开启全局 STP，开启与 WAF 相连的端口 GE1/0/7、GE1/0/8 的 STP，如图 3-10 所示。

图3-10 开启交换机 1 的全局 STP 以及端口的 STP



与上类似，登录交换机 2，开启全局 STP，开启与 WAF 相连的端口 GE1/0/7、GE1/0/8 的 STP，如图 3-11 所示。

图3-11 开启交换机 2 的全局 STP 以及端口的 STP



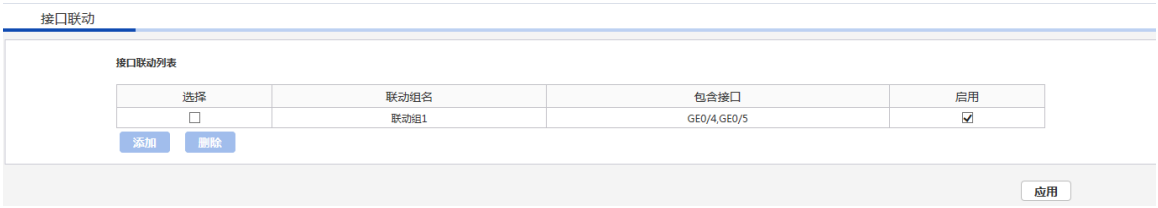
3.3.4 接口联动配置

可根据具体的业务情况和实际环境增加联动接口配置。

点击左侧网络配置-接口联动。

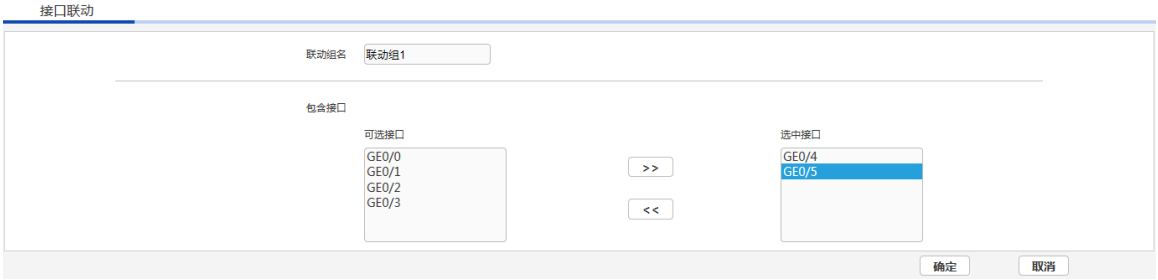
在接口联动配置页点击添加按钮打开接口联动配置页。

图3-12 接口联动界面



在接口联动配置页，从左侧可选接口框根据需要选择到右侧选中接口框内完成联动接口配置。完成点击确定。

图3-13 接口联动配置界面



配置完成后需要启用接口联动选项，点击相应的联动配置右侧的启用选择框，并保存配置完成接口联动配置。

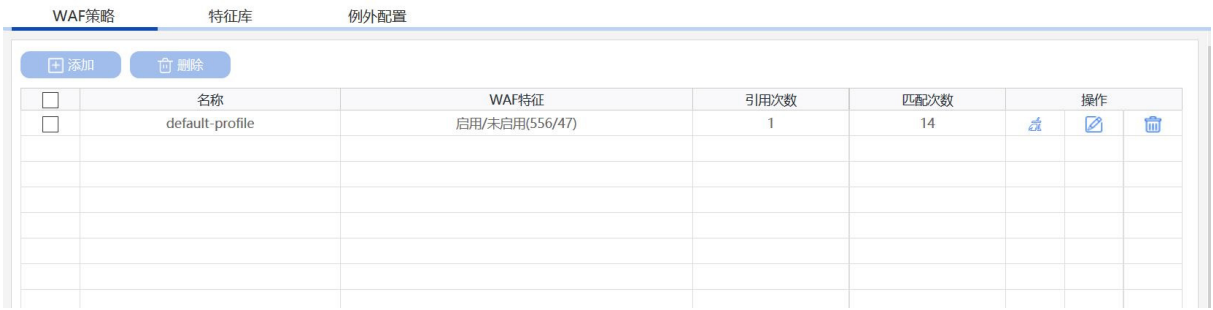
注意

接口联动配置也需要在主备两台设备上分别进行配置。

3.3.5 安全策略配置

点击左侧安全策略-Web 安全策略，根据需要添加调整 Web 应用防护策略。

图3-14 WAF 策略界面



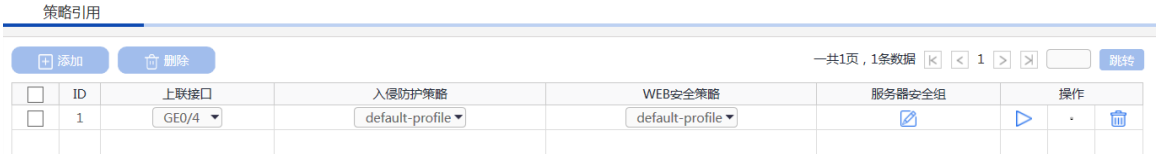
点击添加按钮可以添加新 WAF 策略，点击策略右侧操作按键可以调整策略配置，可根据客户安全需求调整策略内容和动作等信息。调整完毕后点击确定。

图3-15 WAF 策略配置界面

点击左侧安全策略-策略引用，将添加的 Web 应用策略与 Web 服务器进行关联。

点击左侧添加按钮，添加新的引用策略，上联接口选择流量进入接口（以组网图 3-1 为例，即 GE0/4 接口），根据需要和配置选择入侵检测策略和 WEB 防护策略（上一步添加的 WAF 策略），点击服务器安全组按钮添加被保护服务器。

图3-16 策略引用界面

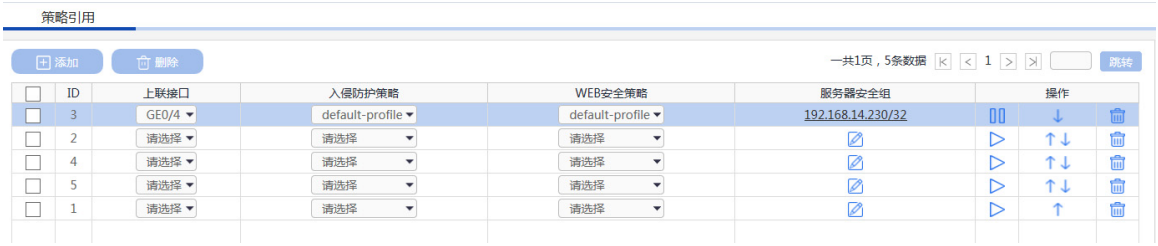


添加被保护服务器：在服务器列表里添加服务器地址和掩码，协议端口可根据业务情况进行填写和选择，填写完成后点击右侧的添加按钮即可添加到服务器列表中，可以添加多条服务器信息。添加完成后点击应用并返回上一级界面。

图3-17 服务器添加界面

添加策略引用后界面，默认情况下策略添加完成后并不会启用，需点击操作界面的启用按键启用策略，策略启用后设备既可以实现对 WEB 服务器的安全防护功能。

图3-18 策略引用配置完成



3.3.6 策略同步

策略配置可通过高可用性配置页的同步按键将主墙配置同步到备墙上：网络配置-高可用性；高可用性配置页下的 HA 状态后面的同步按钮。

图3-19 HA 高可用性配置界面

3.4 验证配置

- Host A 访问 Web Server 可以正常打开 Web 的页面，此时流量应该经过主应用防火墙；观察主备设备的 HA 工作模式。

图3-20 主设备截图

图3-21 备设备截图

- 断开主应用防火墙的业务接口，观察设备切换情况，并测试业务是否可以正常打开。
- 主备设备模式切换：备机成为主墙。

图3-22 HA 高可用性配置页面模式变化

- 至此 Web 应用防火墙完成主备切换，可进行业务攻击测试已验证备应用防火墙的防护策略是否生效。

- 进行攻击测试。

攻击测试方法：

可以在目标服务器上安装测试靶机环境，靶机软件 DVWA 服务器端。

在客户端用浏览器登录靶机 DVWA 测试页面。

图3-23 DVWA 测试页面

选择 SQL 注入选项，并点击测试方法项

图3-24 DVWA 测试页面测试结果

- 进行攻击测试后，可以在 Web 安全策略中观察到策略命中数。
- 在左侧日志报表项-日志-WEB 安全日志中可以查看具体告警信息。

透明双机主主模式部署配置举例

目 录

1 简介

本文档介绍了 Web 应用防火墙透明双机主主模式部署的配置举例。

Web 应用防火墙的高可用性可以解决因 Web 应用防火墙出现的单点故障问题，可以在一台设备出现故障时，另一台设备接管完全的访问流量，保证业务始终处于正常运行，极大的减少设备故障时业务中断时间。

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 WEB应用防火墙透明双机主主模式部署配置举例

3.1 组网需求

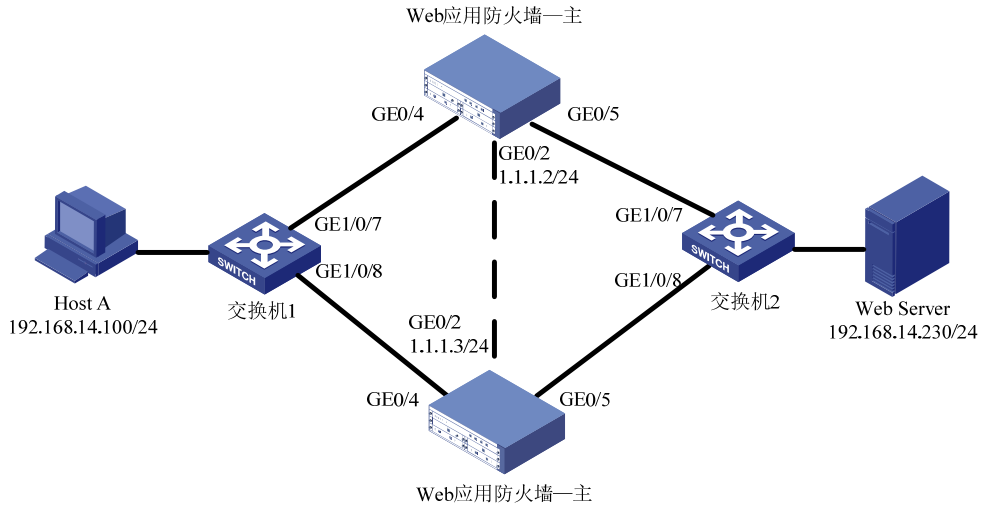
设备在出厂时，默认所有接口都是属于 vlan1 的 access 口，用户可以按实际需求修改接口的类型。

如图所示，Host A 和 Host B 可以实现对 Web Server 服务器的互联访问，现要求在两台交换机中间透明部署 2 台 Web 应用防火墙，2 台 Web 应用防火墙之间开启主主冗余模式，保证在一台 Web 应用防火墙出现故障时，Host A 依然可以正常访问 Web 服务器。

注意

- 双机冗余模式要求 2 台 Web 应用防火墙的设备型号和软件版本完全相同。
- 若实际使用透明双机主主组网时，不需要使用 bypass 功能，建议组网过程中不要使用一对 bypass 口，以免设备故障之后，流量直接通过 bypass 转发而不检测

图3-1 Web 应用防火墙 HA 主主模式部署配置举例组网图



3.2 使用版本

本举例是在系统版本：ESS6712 上进行配置和验证的。

3.3 配置步骤

3.3.1 网络配置

登录 Web 应用防火墙：启动 IE/FIREFOX 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。

注意

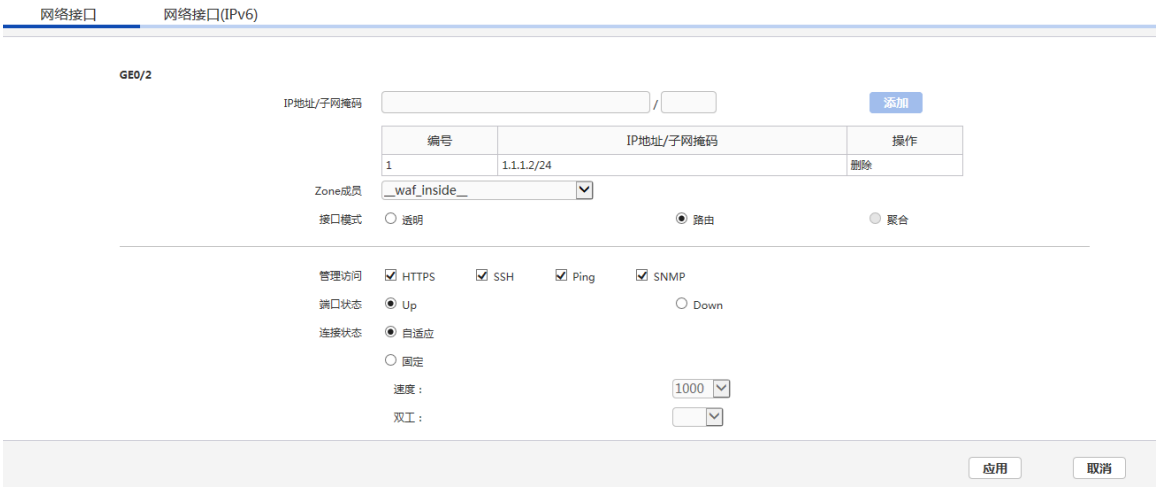
推荐使用 IE10+及 Firefox56+及其以上版本的浏览器。

首先配置第一台应用防火墙；点击左侧菜单：网络配置-网络接口。

图3-2 主设备网络接口界面

先确定 HA 接口，本例我们选择 GE0/2 接口，点击编辑 GE0/2 接口，我们将 GE0/2 接口改为路由模式，并配置设备互联地址：1.1.1.2/24，点击应用。

图3-3 第一台设备网络接口配置页面

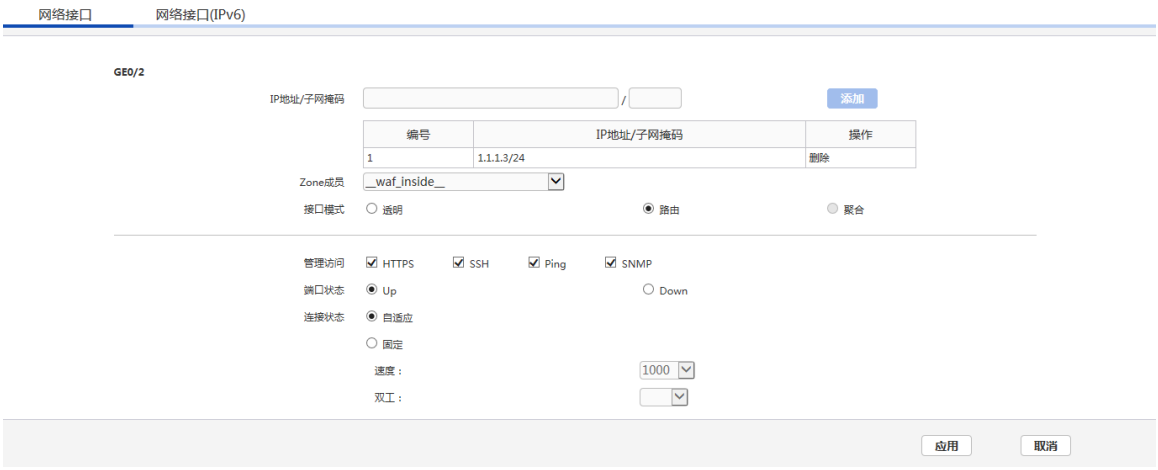


开始配置第二台应用防火墙：点击左侧菜单：网络配置-网络接口。

图3-4 备设备网络接口界面

确定 HA 接口，本例我们选择 GE0/2 接口，点击编辑 GE0/2 接口，我们将 GE0/2 接口改为路由模式，并配置设备互联地址：1.1.1.3/24，点击应用。

图3-5 第二台设备网络接口配置页面



3.3.2 双机配置

1. 配置第一台Web应用防火墙

开始配置第一台 Web 应用防火墙 HA：点击左侧网络配置-高可用性，进入高可用性选项后，在顶部选择高可用性标签进入高可用性配置页。

分别配置：

(1) 选定启用 HA 选项；

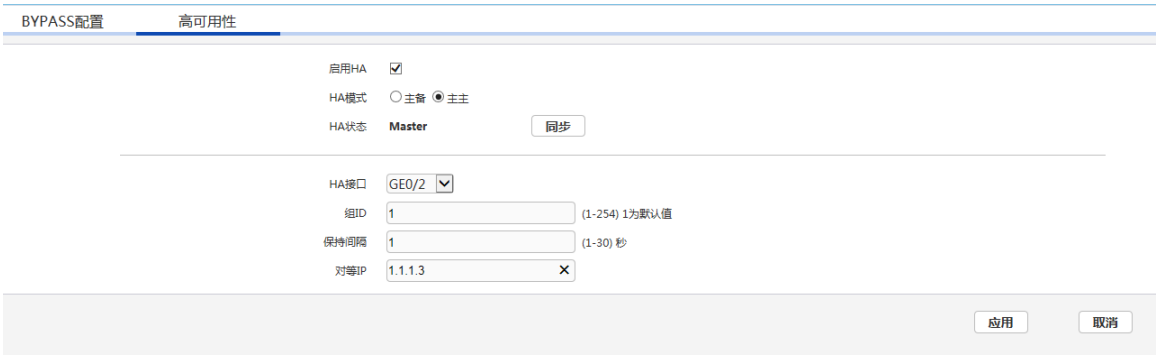
(2) 设置 HA 模式，我们这里选择主主项；

(3) HA 接口配置 GE0/2；

(4) 配置对等 IP（即 HA 对端设备 IP），我们这里配置 1.1.1.3。

以上配置完成后点击应用。

图3-6 第一台 WAF 的 HA 高可用性配置界面



2. 配置第二台Web应用防火墙

开始配置第二台 Web 应用防火墙 HA：点击左侧网络配置-高可用性，进入高可用性选项后，在顶部选择高可用性标签进入高可用性配置页。

分别配置：

(1) 选定启用 HA 选项；

(2) 设置 HA 模式，我们这里选择主主项；

(3) HA 接口配置 GE0/2；

(4) 配置对等 IP（即 HA 对端设备 IP），我们这里配置 1.1.1.2。

以上配置完成后点击应用。

图3-7 第二台 WAF 的 HA 高可用性配置界面

以上配置完成后即可完成 HA 的配置，此时 2 台设备均工作在主模式状况下。

表3-1 HA 配置参数说明

功能	说明
启用HA	启用双机
HA模式	主备模式/主主模式
HA状态	Master/Backup，主机点击同步即可将配置同步到备机
HA接口	选择两个设备之间互连的心跳线接口
组ID	两台设备需配置相同的组ID
保持间隔	两台设备之间发送VRRP报文的时间间隔
对等IP	对方设备的HA地址

3.3.3 交换机配置

透明双机主主模式下，需要在交换机上开启 STP，通过交换机来决定流量走哪条链路。

以组网图 3-1 为例，需要开启交换机 1、交换机 2 上全局的 STP 功能，并将和两台 WAF 相连的交换机端口的 STP 功能开启。以下交换机配置命令均以 UNIS 交换机为例。

首先，登录交换机 1，开启全局 STP，开启与 WAF 相连的端口 GE1/0/7、GE1/0/8 的 STP，如图 3-8 所示。

图3-8 开启交换机 1 的全局 STP 以及端口的 STP

```
[NBH9SW1]
[NBH9SW1]stp en
[NBH9SW1]stp enable          开启全局STP
[NBH9SW1]
[NBH9SW1]
[NBH9SW1]int
[NBH9SW1]interface g
[NBH9SW1]interface GigabitEthernet 1/0/7   开启端口GE1/0/7的STP
[NBH9SW1-GigabitEthernet1/0/7]stp enable
[NBH9SW1-GigabitEthernet1/0/7]quit
[NBH9SW1]
[NBH9SW1]
[NBH9SW1]int
[NBH9SW1]interface g
[NBH9SW1]interface GigabitEthernet 1/0/8   开启端口GE1/0/8的STP
[NBH9SW1-GigabitEthernet1/0/8]stp enable
[NBH9SW1-GigabitEthernet1/0/8]quit
[NBH9SW1]
[NBH9SW1]
```

与上类似，登录交换机 2，开启全局 STP，开启与 WAF 相连的端口 GE1/0/7、GE1/0/8 的 STP，如图 3-9 所示。

图3-9 开启交换机 2 的全局 STP 以及端口的 STP

```
[NBH9SW2]
[NBH9SW2]
[NBH9SW2]stp en
[NBH9SW2]stp enable          开启全局STP
[NBH9SW2]
[NBH9SW2]
[NBH9SW2]int
[NBH9SW2]interface g
[NBH9SW2]interface GigabitEthernet 1/0/7
[NBH9SW2-GigabitEthernet1/0/7]stp ena      开启端口GE1/0/7的STP
[NBH9SW2-GigabitEthernet1/0/7]stp enable
[NBH9SW2-GigabitEthernet1/0/7]quit
[NBH9SW2]
[NBH9SW2]
[NBH9SW2]int
[NBH9SW2]interface g
[NBH9SW2]interface GigabitEthernet 1/0/8
[NBH9SW2-GigabitEthernet1/0/8]stp en       开启端口GE1/0/8的STP
[NBH9SW2-GigabitEthernet1/0/8]stp enable
[NBH9SW2-GigabitEthernet1/0/8]quit
[NBH9SW2]
[NBH9SW2]
```

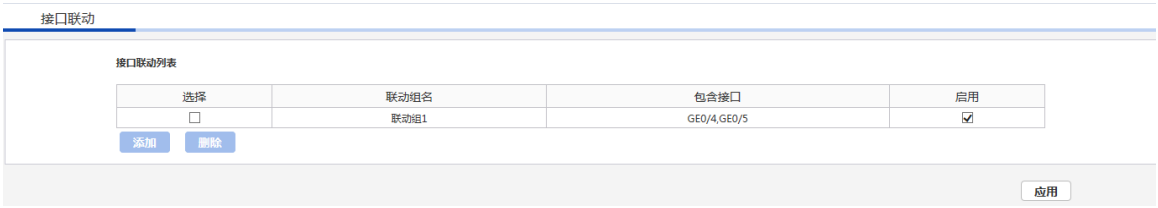
3.3.4 接口联动配置

可根据具体的业务情况和实际环境增加联动接口配置。

点击左侧网络配置-接口联动。

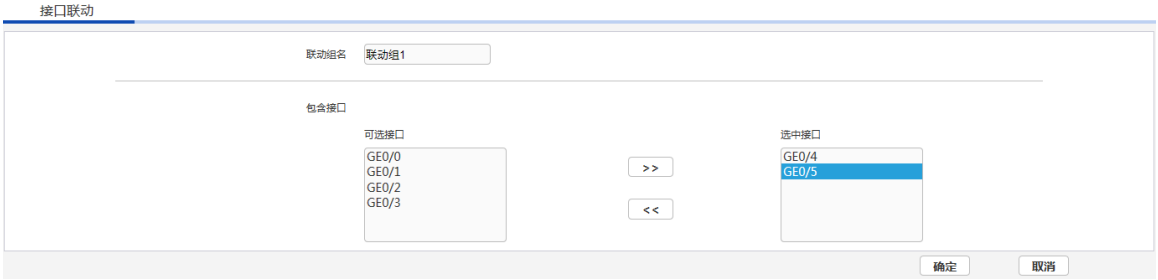
在接口联动配置页点击添加按钮打开接口联动配置页。

图3-10 接口联动界面



在接口联动配置页，从左侧可选接口框根据需要选择到右侧选中接口框内完成联动接口配置。完成点击确定。

图3-11 接口联动配置界面



配置完成后需要启用接口联动选项，点击相应的联动配置右侧的启用选择框，并保存配置完成接口联动配置。

注意

接口联动配置也需要在两台设备上分别进行配置。

3.3.5 安全策略配置

点击左侧安全策略-Web 安全策略，根据需要添加调整 Web 应用防护策略。

图3-12 WAF 策略界面

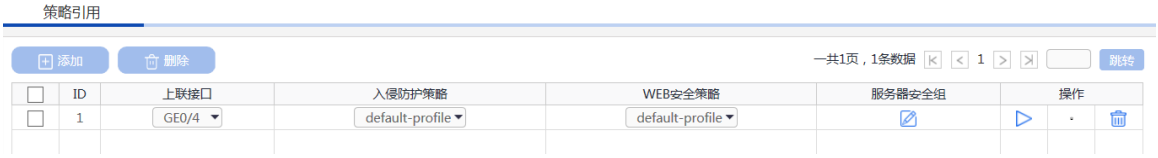
点击添加按钮可以添加新 WAF 策略，点击策略右侧操作按键可以调整策略配置，可根据客户安全需求调整策略内容和动作等信息。调整完毕后点击确定。

图3-13 WAF 策略配置界面

点击左侧安全策略-策略引用，将添加的 Web 应用策略与 Web 服务器进行关联。

点击左侧添加按钮，添加新的引用策略，上联接口选择流量入接口（以组网图 3-1 为例，即 GE0/4 接口），根据需要和配置选择入侵检测策略和 WEB 防护策略（上一步添加的 WAF 策略），点击服务器安全组按钮添加被保护服务器。

图3-14 策略引用界面

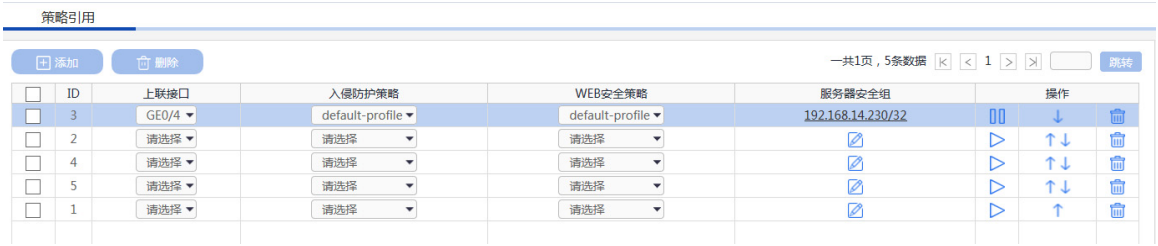


添加被保护服务器：在服务器列表里添加服务器地址和掩码，协议端口可根据业务情况进行填写和选择，填写完成后点击右侧的添加按钮即可添加到服务器列表中，可以添加多条服务器信息。添加完成后点击应用并返回上一级界面。

图3-15 服务器添加界面

添加策略引用后界面，默认情况下策略添加完成后并不会启用，需点击操作界面的启用按键启用策略，策略启用后设备既可以实现对 WEB 服务器的安全防护功能。

图3-16 策略引用配置完成



3.3.6 策略同步

策略配置可通过高可用性配置页的同步按键将配置同步到另一台 Web 应用防火墙上：网络配置-高可用性；高可用性配置页下的 HA 状态后面的同步按钮。

图3-17 HA 高可用性配置界面

3.4 验证配置

- Host A 访问 Web Server 可以正常打开 Web 的页面，此时流量会经过其中一台 Web 应用防火墙，具体过哪个设备由交换机决定。

图3-18 第一台设备截图：

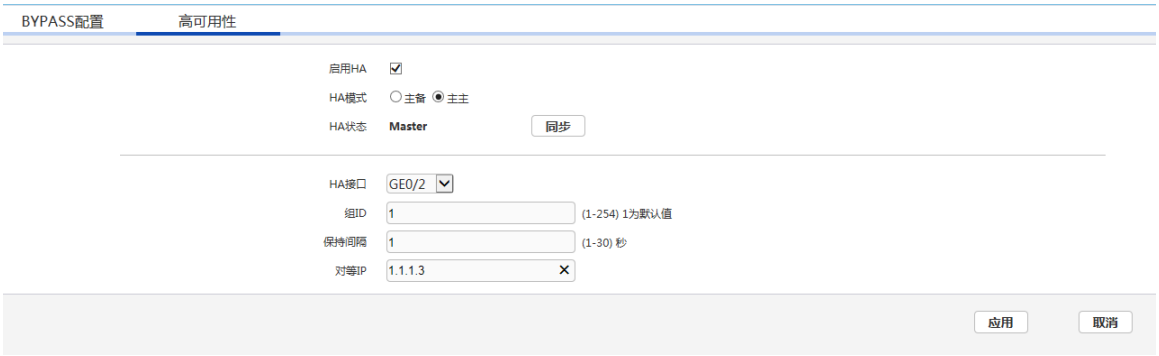


图3-19 第二台设备截图

此时两台设备均为主设备，HA 状态均为 Master。

- 断开当前工作的那台应用防火墙的业务接口，观察设备切换情况，并测试业务是否可以正常打开。
- 测试告警信息是否已经出现在新 Web 应用防火墙上。
- 如果测试攻击事件出现在新设备上，代表设备切换正常，至此 Web 应用防火墙完成主主切换，所有策略可正常运行和告警。
- 进行攻击测试。

攻击测试方法：

可以在目标服务器上安装测试靶机环境，靶机软件 DVWA 服务器端。

在客户端用浏览器登录靶机 DVWA 测试页面。

图3-20 DVWA 测试页面

选择 SQL 注入选项，并点击测试方法项。

图3-21 DVWA 测试界面

- 进行攻击测试后，可以在 Web 安全策略中观察到策略命中数。
- 在左侧日志报表项-日志-WEB 安全日志中可以查看具体告警信息。