### UNIS W2000-G 系列 Web 应用防火墙 典型配置举例

Copyright © 2020 紫光恒越技术有限公司及其许可者版权所有,保留一切权利。 非经本公司书面许可,任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部, 并不得以任何形式传播。本文档中的信息可能变动,恕不另行通知。

1 透明流模式部署配置举例1
1.1 简介1
1.2 配置前提1
1.3 使用限制1
1.4 适用产品和版本1
1.5 组网需求1
1.6 配置思路2
1.7 配置步骤2
1.8 验证配置4
2透明代理模式部署配置举例6
2.1 简介6
2.2 配置前提6
2.3 使用限制6
2.4 适用产品和版本6
2.5 组网需求6
2.6 配置思路7
2.7 配置步骤7
2.8 验证配置9
3 透明反向代理模式部署配置举例11
3.1 简介11
3.2 配置前提11
3.3 使用限制11
3.4 适用产品和版本11
3.5 组网需求11
3.6 配置思路12
3.7 配置步骤12
3.8 验证配置14
4 反向代理模式部署配置举例16
4.1 简介16
4.2 配置前提16
4.3 使用限制16
4.4 适用产品和版本

	45组网需求	
	46 配置思路	
	47 配置步骤	
	48 验证配置	
5 15	7. 后代理模式 HTTPS 服冬哭部睾配罟举例	
	5.1 周升	
	5.2 配置前提	
	5.4 适用产品和版本	
	5.5 组网需求	
	5.5 组内而示	
	5.0 配直心明	
	5.7 配直步骤 5.8 哈证配置	
د <del>ع</del>	5.5 巡 业 印 直	20
6		
	6.1 间介·····	
	6.2	
	<b>6.3</b> 使用限制	
	6.4 适用产品和版本······	
	6.5 组网需求	
	6.6 配直忠路	
	6.7 配直步骤	
	6.8 验证配置	
7 旁	等路镜像检测&阻断模式部署配置举例	
	7.1 简介	
	7.2 配置前提	
	7.3 使用限制	
	7.4 适用产品和版本	
	7.5 组网需求	
	7.6 配置思路	
	7.7 配置步骤	
	7.8 验证配置	
8 透	透明代理双机模式部署配置举例	41
	8.1 简介	41
	8.2 配置前提	41
	8.3 使用限制	41
	8.4 适用产品和版本	

	8.5 组网需求	41
	8.6 配置思路	42
	8.7 配置步骤	42
	8.8 验证配置	51
9反	向代理双机模式部署配置举例	53
	9.1 简介	53
	9.2 配置前提	53
	9.3 使用限制	54
	9.4 适用产品和版本	54
	9.5 组网需求	54
	9.6 配置思路	54
	9.7 配置步骤	54
	9.8 验证配置	60
10 🕯	链路聚合部署配置举例	61
	10.1 简介	61
	10.2 配置前提	61
	10.3 使用限制	62
	10.4 适用产品和版本	62
	10.5 组网需求	62
	10.6 配置思路	62
	10.7 配置步骤	62
	10.8 验证配置	65
11 7	Frunk 部署配置举例	65
	11.1 简介	65
	11.2 配置前提	65
	11.3 使用限制	65
	11.4 适用产品和版本	65
	11.5 组网需求	65
	11.6 配置思路	66
	11.7 配置步骤	66
12	网页防篡改配置举例	69
	12.1 简介	69
	12.2 配置前提	69
	12.3 使用限制	69
	12.4 适用产品和版本	69
	12.5 组网需求	69

12.6 配置思路	
12.7 配置步骤	70
12.8 验证配置	73
13 IPV6 反向代理配置举例	73
13.1 简介	73
13.2 配置前提	74
13.3 使用限制	74
13.4 适用产品和版本	74
13.5 组网需求	74
13.6 配置思路	74
13.7 配置步骤	75
13.8 IPV4 反代 IPV6 的验证配置	
13.9 IPV6 反代 IPV4 的验证配置	81
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	83
14.1 简介	
14.2 配置前提	
14.3 使用限制	
<b>14.4</b> 适用产品和版本	
14.5 组网需求	
14.6 配置步骤	
14.6.1 WAF 的接口及路由配置	
14.6.2 服务器配置	
14.6.3 安全策略配置	87
14.6.4 交换机配置	
14.7 验证配置	
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	90
15.1 简介	90
15.2 配置前提	91
15.3 使用限制	91
15.4 适用产品和版本	91
15.5 配置步骤	91
15.5.1 WAF 的接口及路由配置	91
15.5.2 服务器配置	94
15.5.3 VRRP 配置	94
15.5.4 安全策略配置	97
15.5.5 交换机配置	97

# 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。



#### 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

增加网桥接口			
1 第一步		2 第二步	
网桥号 *	10		
MTU *	1500		
模式 *	普通模式	Ŧ	
状态 *	启用	Ŧ	
STP			
			世一才

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

增加网桥接口				>
1 √第─步		2 第二步		
增加╋●刷新2				
IP地址	子网掩码	版本号	管理IP	
没有检索到数据				
			▲ ├――――――――――――――――――――――――――――――――――――	h
				J

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

编辑Port接口			×
接口名称 *	GE0/2		
备注			
Channel接口 *	空	*	
网桥接口 *	br10	٣	
启用状态 *	启用	۳	
链路状态	启用	٣	
			保存 🖺 🔵 取消 🕽

#### 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

编辑HTTP服务器		~
HTTP服务器		
服务器名称 *	test	
IP地址* 🛛	172.16.101.74	
端口 *	80	
部署模式 *	串联 ▼	
防护模式 *	流模式  ▼	
启用*	$\checkmark$	
		(保存 🖺 )(取消 🕽 )

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

+ 増加Web防护策略										
Web防护策路基本信息配置										
策略名称 *	test1				错误页面标题 🕜				11	
Web主机 🕢	请输入或选择		v		错误页面内容 🕜				11	
服务籍	test		Ŧ	配置 〇	■定向URL Ø					
灏IP	空		Ŧ					li.		
访问日志	关闭		٣		Cookie加圖					
优先级 * 🛛 😮	0				Cookie加密					
启用	¥									
Web防护规则配置										
扫描防护规则	空	v	增加 +		文件上传规则	空	v	增加 🕇		
HTTP协议校验规则	通用规则	Ψ	增加 +	编辑 🖌	文件下戴规则	空	w.	增加 +		
HTTP访问控制规则	垒	Ψ	增加+		數感信息检測规则	空	Ŧ	增加 +		
特征防护规则	通用规则	Ψ	增加+	编辑 🖌	關密码检测规则	空	Ŧ	增加 +		
爬虫防护规则	垒	Ŧ	增加 +		虚拟补丁规则	空	Ŧ	增加 🕇		
防盗性规则	垒	Ŧ	增加 +		访问顺序规则	空	Ŧ	增加 🕇		
防算站请求伪造规则	Ŷ	Ŧ	増加 +		敏感词防护规则	÷	×	增加 +		
									(保存日)(取	<b>満つ</b> )

#### 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。

O 社区动力 DISCUZ!		用户名 🔽 密码	admin	<ul> <li>□ 自动登录 找回密码</li> <li>登录 立即注册</li> </ul>
门户 论坛 群组 家园 排行榜				快捷导航 -
〇、 请输入搜索内容	帖子 <b>· 搜索</b>	<b>热搜:</b> 活动 交友	discuz	
♠ 〉论坛				
勐 今日:0│昨日:0│帖子:0│会员:1				查看新帖
Discuz!				-
型 新认版块			0/0 从未	
在线会员 - 2 人在线 - 0 会员(0 隐身), 2 位游客 - 最高记录是 4 于 2019-6-27.				-
💶 管理员 📃 超级版主 💽 版主 🔽 会员				
当前只有游客或隐身会员在线				
<b>官方论坛</b> Diseuz.net 提供最新 Discuz! 产品新闻、软件下载与技术交流				
Comsenz 漫游平台 Yeswan 我的领地				
Powered by <b>Discuz!</b> X2 © 2001-2011 Comsenz Inc.		GMT+8, 2	019-6-27 17:07 , Processed in	Archiver   Comsenz Inc. 0.029540 second(s), 11 queries .

(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。

- -> C 📀 172.16.101.74/forum.php?id=1%20and%201=1

无法访问此网站	
注 安 C 単 直。 请试试以下 わ法: • 检查 网络连接 • 检查代理服务 器和防火墙 • 运行 Windows 网络诊断	
ERR_CONNECTION_RESET	
重新加载	详细信息

(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。

+ 攻击日志 + Web攻击日志统计						条件 / 清	空∕ 导出▶ 月	创新℃
每页显示 15 🔻								
日期和时间	源IP	目的IP	目的URL	方法	攻击类型	规则类型	处理动作	次数
2019-06-28 01:21:36	192,168,7,138	172,16,101,74	172.16.101.74/forum.php	GET	特征防护规则	SOL注λ	阴断	8

# 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。



#### 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

增加网桥接口				
1 第一步		2 第二步		
网桥号 *	10			
MTU *	1500			
模式 *	普通模式	٣		
状态 *	启用	v		
STP				
			(下-	-步 → )

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

增加网桥接口				
1 →第一步		2 第二步		
增加┿刷新₽				
IP地址	子网掩码	版本号	管理IP	
没有检索到数据				
			← 上──步 保存 [	8)

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

编辑Port接口			×
接口名称 *	GE0/2		
备注			
Channel接口 *	空	Ŧ	
网桥接口 *	br10	٣	
启用状态 *	启用	٣	
链路状态	启用	٣	
			(保存 🖺 ) (取消 つ)

#### 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

编辑HTTP服务器			~
HTTP服务器	数据压缩 高速缓存		
服务器名称 *	test		
IP地址* 🕜	172.16.101.74		
端口 *	80		
部署模式 *	串联	<b>v</b>	
防护模式 *	代理模式	<b>v</b>	
接口 *	br10	<b>v</b>	
客户端IP还原	● 是 ○ 否		
启用 *	$\checkmark$		
		(保存問)	(取消り)

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

+ 増加Web防护策略										ð
Web防护策路基本信息配置										101
策略名称*	test1				错误页面标题 📀				11	
Web主机 🛛	请输入或选择		v		措決页面内容				11	
服务器	test			配置 〇	重定向URL 😧					
源IP	空							li.		
访问日志	关闭				Cookie加阔					
优先级 * 🕑	0				Cookie加密					
启用	$\checkmark$									
Web防护规则配置										
扫描防护规则	窒	٣	增加 +		文件上传规则	室	Ŧ	增加 +		
HTTP协议校验规则	通用规则	٣	增加 +	编辑 🖌	文件下截规则	空	٣	增加 +		
HTTP访问控制规则	空	٣	增加 +		敏感信息检测规则	奈	٣	增加 +		
特征防护规则	通用规则	٣	增加 +	编辑 🖌	認密码检测规则	幸	٣	增加 +		
爬虫防护规则	호	Ŧ	增加 +		虚拟补丁规则	空	٣	增加 +		
防盗链规则	空	٣	增加+		访问顺序规则	幸	٣	增加 +		
防肺站请求伪造规则	空	٣	增加+		敏感词防护规则	蓥	٣	增加 +		
									保存 四	取満り

#### 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。

O 社区动力 DISCUZ!		用户名 ✓ ad 密码 ►•	min	] 自动登录 技回密码 登录 立即注册
门户 论坛 群组 家园 排行榜				快捷导航 🗸
○ 请输入捜索内容	帖子 <b>· 搜索</b>	<b>热搜:</b> 活动 交友 disc	uz	
♠ 〉论坛				
础 今日:0│昨日:0│帖子:0│会员:1				查看新帖
Discuz!				-
型 默认版块		(	0/0 从未	
在线会员 - 2 人在线 - 0 会员(0 隐身), 2 位游客 - 最高记录是 4 于 2019-6-27.				-
📃 管理员 📃 超級版主 📃 版主 🔽 会员				
当前只有游客或隐身会员在线				
<b>官方论坛</b> Disouz.net 提供最新 Discuz! 产品新闻、软件下载与技术交流				
Comsenz 漫游平台 Yeswan 我的领地				
Powered by <b>Discuz!</b> X2 © 2001-2011 Comsenz Inc.		GMT+8, 2019-	Ar 6-27 17:07 , Processed in 0.02	rchiver   Comsenz Inc. 29540 second(s), 11 queries .

(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

- → C ③ 172.16.101.74/forum.php?id=1%20and%201=1

#### 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。

+ 攻击日志 + Web攻击日志	场计					会件』	控∕导出▶□月	制新ご
每页显示 15 🔻								
日期和时间	源IP	目的IP	目的URL	方法	政击类型	规则类型	处理动作	次数

# 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。



#### 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

增加网桥接口			
1 第一步		2 第二步	
网桥号 *	10		
MTU *	1500		
模式 *	普通模式	Ŧ	
状态 *	启用	v	
STP			
			(下步 🔸 )

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

扁蜡网桥接口				
1 ▼第一步		2 第二步		
增加+ 刷新 3				
IP地址	子网掩码	版本号	管理IP	
172.16.101.100	255.255.255.0	ipv4	否	
				_

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。

【 ← 上─步 】 【 保存 🖺 】

#### 图3-4 port 口划分到新网桥

编辑Port接口			×
接口名称 *	GE0/2		
备注			
Channel接口 *	空	Ŧ	
网桥接口 *	br10	v	
启用状态 *	启用	v	
链路状态	启用	v	
			保存 🖺 🔵 取消 🧿

#### 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。

编辑HTTP服务器			~
HTTP服务器	数据压缩 高速缓存		
服务器名称 *	test		
IP地址* 🕜	172.16.101.74		
端口*	80		
部署模式 *	串联	v	
防护模式 *	代理模式	v	
接口 *	br10	v	
客户端IP还原	○是 ⑧ 否		
启用*	$\checkmark$		
			(保存 🖺 ) (取消 🔊 )

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

╋ 増加Web防护策略										8
Web防护策路基本信息配置										
策略名称 *	test1				错误页面标题 🕜				11	
Web主机 🕑	请输入或选择		٧		错误页面内容 🕜				11	
服务器	test			- 配置 ♥	重定向URL 😧					
源IP	空			٣				li		
访问日志	关闭			Ŧ	Cookie <u>7</u> ]]#					
优先级 * 🛛	0				Cookie加密					
启用	~									
Web防护规则配置										
扫描防护规则	空	Ŧ	增加 🕇		文件上传规则	空	×	增加 🕇		
HTTP协议校验规则	通用规则	Ψ.	增加 🕇	编辑 🖌	文件下數規则	空	¥	增加 <b>+</b>		
HTTP访问控制规则	空	Ŧ	增加 +		數感信息检测规则	空	×	增加 🕇		
特征防护规则	通用规则	Ŧ	增加 🕇	编辑 🖌	調密码检测规则	空	Ŧ	增加 +		
爬虫防护规则	호	Ŧ	增加 +		虚拟补丁规则	空	٣	增加+		
防盗链规则	호	Ŧ	増加 +		访问顺序规则	空	Ŧ	增加+		
防算站请求伪造规则	空	Ŧ	增加+		敏感词防护规则	空	٣	增加 +		
									保存習	取満り

#### 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。

O 社区动力 DISCUZ!		用户名 ▼ adm 密码 ▶•••	in 自动登 •• 登录	<ul> <li>禄 找回密码</li> <li>立即注册</li> </ul>
门户 论坛 群组 家园 排行榜				快捷导航 🗸
Q、 请输入搜索内容	帖子 ▼ 搜索	<b>热搜:</b> 活动 交友 discu:	z	
★ 〉论坛				
.₁₁ 今日:0   昨日:0   帖子:0   会员:1				查看新帖
Discuz!				-
		0 /	/ 0 从未	
在线会员 - 2 人在线 - 0 会员(0 隐身), 2 位游客 - 最高记录是 4 于 2019-6-2	7.			-
💶 管理员 📃 超级版主 📃 版主 🔲 会员				
当前只有游客或隐身会员在线				
<b>官方论坛</b> Discuz.net 提供最新 Discuz! 产品新闻、软件下载与技术交流				
Comsenz 漫游平台 Yeswan 我的领地				
Powered by <b>Discuz!</b> X2 © 2001-2011 Comsenz Inc.		GMT+8, 2019-6-	Archiver 27 17:07 , Processed in 0.029540 sec	Comsenz Inc.

(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。

- -> C (3 172.16.101.74/forum.php?id=1%20and%201=1

#### 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。

+ 攻击日志 + Web攻击日志统计						条件》	清空✔ 号出▶ 風	新 <b>C</b>
每页显示 15 *								
日期和时间	源IP	目的IP	目的URL	方法	政击类型	规则类型	处理动作	次数
2019-06-28 01:43:40	192.168.7.138	172.16.101.74	172.16.101.74/forum.php	GET	特征防护规则	SQL注入	阻断	1

# 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。



#### 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

曾加网桥接口			
1 第一步		2 第二步	
网桥号 *	10		
MTU *	1500		
模式 *	普通模式	•	
状态 *	启用	v	
STP			
			下一步 🔸

如下图所示,在网桥 br10 中增加业务 IP 地址。

# 图4-3 増加业务 IP 地址 毎日の新住口 ● 第一步 2 第二步 「塩加+」 刷新ご □ IP地址 子网掩码 版本号 管理IP □ 192.168.7.15 255.255.255.0 ipv4 星

( 🗲 上一步 🗍	(保存 🖺
-----------	-------

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

增加路由			
IP地址 *	0.0.0.0		
子网掩码 *	0.0.0.0		
下一跳 *	192.168.7.1	×	
Metric			
	保存 🗅		図消 つ )

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

编辑Port接口			×
接口名称 *	GE0/2		
备注			
Channel接口 *	空	Ŧ	
网桥接口 *	br10	٣	
启用状态 *	启用	Ŧ	
链路状态	启用	٣	
			保存 🖺 🔵 取消 🔊

#### 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。

編HTTP服务器			
HTTP服务器	数据压缩 高速缓存		
服务器名称 *	test		
IP地址* 🕜	172.16.101.74	4	
端口 *	80		
部署模式 *	串联		Ŧ
防护模式 *	代理模式		Ŧ
接口 *	br10		Ŧ
客户端IP还原	○ 是 (	• 否	
启用 *	<b>~</b>		
			保存 🖪 🔵 取消 🔊

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

增加HTTP代理服务器			×
HTTP代理服务器	数据压缩 高速缓存		
服务器名称 *	test1		
IP地址 * 😮	192.168.7.15		
端口 * 🕜	80		
后端服务器 * 💡	test	•	
接口 *	br10	•	
启用 *	$\checkmark$		
		保存日	(取消つ)

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

Loss I and a second second second second									
Web防护策略量本信息配置 策略名称*	test1				错误页面标题 👔				
Web 丰和 <b>Q</b>	遗输入或洗择								
R68	tert			· FE 0	错误贝国内容 🗸				li
DATE NO.	test				重定向URL 📀				
源IP	空			Ŧ	0 1: 407				
访问日志	关闭			Ψ.	Cookiejjujiki				
优先级 * 🕢	0				Cookie加密				
启用	×								
Web防护规则配置									
扫描防护规则	空	Ŧ	增加 🕇		文件上传规则	空	¥	增加 🕇	
扫描防护规则 HTTP协议校验规则	空通用规则	Ψ Ψ	增加 + 増加 +	编辑 🖌	文件上传规则 文件下载规则	호 호	Т	增加 + 增加 +	
扫描的护机风则 HTTP协议校验规规则 HTTP协问控制规规则	空 通用规则 空	Ψ Ψ	增加 + 增加 + 增加 +	编辑 /	文件上传规则 文件下载规则 敏感信息绘测规则	호 호 호	* *	增加 + 增加 + 增加 +	
1日編約分4規則 HTTP1か以均益規則 HTTP1か1日200 特(正約分4規則)	空 通用规则 空 通用规则	Y           Y           Y           Y           Y           Y	增加 + 増加 + 増加 + 増加 +	编辑 / 编辑 /	文件上传规则 文件下戰規則 戰壓信譽检與规则 顕電码检測规则	호 호 호		增加 + 增加 + 增加 + 增加 +	
扫描成554000 HTTP:协议校验规则 HTTP:协同检制规则 特征35549000 和由35549000	空 適用規則 空 適用規則 空	Ψ           Ψ           Ψ           Ψ           Ψ           Ψ           Ψ           Ψ           Ψ           Ψ           Ψ           Ψ	增加 + 增加 + 増加 + 増加 + 増加 +	通道 / 調道 /	文件上传规则 文件下数规则 载客信息检测规则 顾客符检规规则 虚拟补丁规则	* * * * *	V           V           V           V           V           V           V           V           V           V           V	增加 + 增加 + 增加 + 增加 + 增加 +	
お目摘がならい現内 HTTPけなどなななか現内 HTTPけなりでは全分的原因 特征正かなかり用り 原生生かなかり用り 取り法律権利用り	空 通用规则 空 通用规则 空 空	V           V           V           V           V           V           V           V           V           V           V           V	增加 + 增加 + 增加 + 增加 + 增加 + 增加 + 增加 +	编辑 / 编辑 /	文件上特规则 文件下转规则 敏感信息检测规则 限高词检测规则 虚拟计了规则 论问题序规则	2 2 2 2 2 2 2 2 2 2 2	* * * *	増加 + 増加 + 増加 + 増加 + 増加 + 増加 +	

#### 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。

○ 社区动力		用户名 🔽	admin	□ 自动登录 找回密码
DISCUZ!		密码		登录立即注册
门户 论坛 群组 家园 排行榜				快捷导航 🗸
Q、 请输入搜索内容	帖子 ▼ <b>搜索</b>	<b>热搜:</b> 活动 交友	discuz	
♠ 〉论坛				
今日:0│昨日:0│帖子:0│会员:1				查看新帖
Discuz!				-
默认版块			0/0 从未	
在线会员 - 2 人在线 - 0 会员(0 隐身), 2 位游客 - 最高记录是 4 于 2019-6-27.				-
💶 管理员 🗾 超级版主 📃 版主 🔲 会员				
当前只有游客或隐身会员在线				
<b>官方论坛</b> Discuz.met 提供最新 Discuz! 产品新闻、软件下载与技术交流				
Comsenz 漫游平台 Yeswan 我的领地				
Powered by Discuz! X2				Archiver   Comsenz Inc.
© 2001-2011 Comsenz Inc.		GMT+8,	2019-6-27 17:07 , Processed in	0.029540 second(s), 11 queries .

(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。

+ 攻击日志 + Web攻击日志统计						条件』 清空』	导出▶	fi C
每页显示 15 *								
日期和时间	源IP	目的IP	目的URL	方法	攻击类型	規则类型	处理动作	次数
2019-06-28 03:03:33	192.168.7.138	172.16.101.74	192.168.7.15/forum.php	GET	特征防护规则	SQL注入	阻断	1

(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。

#### 400 Bad Request

### 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。



#### 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

增加网桥接口		
1 第一步		2 第二步
网桥号 *	10	
MTU *	1500	
模式 *	普通模式	Ŧ
状态 *	启用	v
STP		

如下图所示,在网桥 br10 中增加业务 IP 地址。

# 图5-3 増加业务 IP 地址 编辑网桥接口 1 →第一步 2 第二步 「增加+ 刷新ご □ IP地址 子网掩码 版本号 管理IP 1 192.168.7.15 255.255.255.0 ipv4 是

( ← ⊥—∌ )	(保存 🖺 )
-----------	---------

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

增加路由			
IP地址 *	0.0.0.0		
子网掩码 *	0.0.0.0		
下一跳 *	192.168.7.1	×	
Metric			
	保存圖	(取消り)	

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

编辑Port接口			×
接口名称 *	GE0/2		
备注			
Channel接囗 *	空	٣	
网桥接口 *	br10	٣	
启用状态 *	启用	٣	
链路状态	启用	*	
			保存 🖺 🔵 取消 🔊

#### 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

编HTTPS服务器		
HTTPS服务器 数	居压缩 高速缓存	
服务器名称 *	test	
IP地址 * 🕜	172.16.101.74	
端口 *	443	
部署模式 *	串联   ▼	
防护模式 *	代理模式	
客户端IP还原	◎ 是 ⑧ 否	
接口 *	br10 *	,
ssl站点密钥 * (.key)	xbtest.key ►选择	
ssl站点证书 * (.crt)	xbtest.crt ►选择	
协议类型 *	SSLv2 SSLv3 TLSv1	
启用 *	$\checkmark$	
		(保存 🖺 ) 🌘 取消 🔊 )

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

編出TTPS代理服务器				
HTTPS代理服务器	数据压缩 高速缓存			
服务器名称 *	test1			
IP地址* 🛛	192.168.7.15			
端口* 🕢	443			
后端服务器 * 🕜	test:	Ŧ		
接口 *	br10	v		
ssl站点密钥 * (.key)	xbtest.key	选择		
ssl站点证书 * (.crt)	xbtest.crt	选择		
协议类型 *	✓ SSLv2 ✓ SSLv3 ✓ ✓ TLSv1.1 ✓ TLSv1.2	TLSv1		
启用 *	$\checkmark$			
			保存日	取消り

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。

100

# + 增加Web防护策略

#### 图5-8 配置安全防护策略

Web防护策略基本值息配置									
策略名称 *	test1				错决页面标题 €				11
Web主机 💿	请输入或选择		v		惜決页面内容 €				11
服务器	test			配置の	重定向URL 😧				
源IP	斑							li.	
访问日志	关闭			r	Cookie加漏				
优先级* 🕤	0				CookiežD8				
启用	V								
Web防护规则配置									
扫描防护规则	空	Ŧ	増加 +		文件上傳規則	堂	¥	增加 +	
HTTP协议校验规则	通用规则	Ŧ	増加 +	编辑 /	文件下數規則	堂	¥	増加 +	
HTTP访问控制规则	空	Ŧ	増加 +		敏感信息检测规则	堂	٧	増加 +	
特征防护规则	週用规则	Ŧ	増加 +	编辑 /	調密研检測規則	堂	٧	増加 +	
爬虫防护规则	훞	Ŧ	増加 +		虚拟补丁规则	堂	٣	増加 +	
防盗链规则	훞	Ŧ	増加 +		访问顺序规则	室	٣	増加 +	
防持站请求伪造规则	至	Ŧ	増加 +		敏感词防护规则	2	٣	增加 +	
									(保存習)(取消つ)

#### 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。

O 社区动力 DISCUZ!		用户名 🔽 密码	admin	<ul> <li>□ 自动登录 找回密</li> <li>登录 立即3</li> </ul>	码 È册
门户 论坛 群组 家园 排行榜				快捷导航	-
○ 请输入搜索内容	帖子 <b>· 搜索</b>	<b>热搜:</b> 活动 交友	discuz		
〉论坛					
→ 今日:0 昨日:0 帖子:0 会员:1				查看新	府站
Discuz!				-	-
默认版块			0/0 从未		
在线会员 - 2 人在线 - 0 会员(0 隐身), 2 位游客 - 最高记录是 4 于 2019-6-27.				-	-
💶 管理员 📃 超级版主 📃 版主 🗾 会员					
当前只有游客或隐身会员在线					
<b>官方论坛</b> Disouz.net 提供最新 Discuz! 产品新闻、软件下载与技术交流					
Comsenz 漫游平台 Yeswan 我的领地					
Powered by <b>Discuz!</b> X2 © 2001-2011 Comsenz Inc.		GMT+8, 2	019-6-27 17:07 , Processed ir	Archiver   Comsenz Ii	nc.

(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。

```
→ C S 192.168.7.15/forum.php?id=1%20and%201=1
```

#### 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。

+ 攻击日志 + Web攻击日志统计						条件 <b>/</b> 清空/	母出▶ 開	ff C
每页显示 15 🔻								
日期和时间	源IP	目的IP	目的URL	方法	攻击类型	规则类型	处理动作	次数
2019-06-28 03:03:33	192.168.7.138	172.16.101.74	192.168.7.15/forum.php	GET	特征防护规则	SQL注入	阻断	1

# 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₽

创建vlan101,将GE1/0/6口划入该vlan [SWUP\_For\_AVG\_NewWAF-vlan101]port GigabitEthernet 1/0/6-/

[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]jp address 192.168.7.1 244/

[SWUP\_For\_AVG\_NewWAF-Vlan-interface101]int vlan 1024 为vlan配置IP地址,作为客户端

[SWUP\_For\_AVG\_NewWAF-VIan-interface102]jp address 172.16.101.1 24~ 和服务器网关地址。

[SWUP\_For\_AVG\_NewWAF-Vlan-interface102]guit

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+/ 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。

图6-4 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 br10

增加网桥接口				
1 第一步		2 第二步		
网桥号 *	10			
MTU *	1500			
模式 *	普通模式	Ŧ		
状态 *	启用	v		
STP				
			(	下步

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。

31

## 图6-5 port 口划分到新网桥

编辑Port接口			×
接口名称 *	GE0/2		
备注			
Channel接口 *	空	٣	
网桥接口 *	br10	٣	
启用状态 *	启用	۳	
链路状态	启用	*	
			(保存 🖺 ) (取消 🕽 )

## 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

增加HTTP服务器							
HTTP服务器	数据压约	宿 高速缓存					
服务器名称 *		test					
IP地址* 😯		172.16.101.74					
* 口識		80					
部署模式 *		旁路	٣	none	٣	(阻断接口)	
防护模式 *		流模式	٣				
启用 *		*					
					保存	🖹 🔵 🕻 取消 🅽	)

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

Web防护策路基本信息配置				_						
策略名称 *	test1				错误页面标题 📀				/i	
Web主机 🕑	请输入或选择		v		错误页面内容 🕜				li	
服务器	test			* 配置 0	重定向URL 📀					
源IP	空			Ŧ						
访问日志	关闭			×	Cooke別山画					
优先级 * 😝	0				Cookie加密					
启用	$\checkmark$									
Web防护规则配置										
扫描防护规则	空	Ŧ	增加 🕇		文件上传规则	空	×	增加 🕇		
HTTP协议校验规则	通用规则	Ŧ	增加 +	编辑 🖌	文件下戴规则	空	¥	增加 +		
HTTP访问控制规则	空	v	增加 🕇		敏感信息检测规则	空	×	增加 🕇		
特征防护规则	通用规则	Ŧ	增加 +	编辑 🖌	關密码检测规则	空	¥	增加 +		
爬虫防护规则	空	٣	增加+		虚拟补丁规则	空	Ŧ	增加 +		
防盗性规则	蓥	٣	增加 +		访问顺序规则	空	¥	增加 +		
					飲成に同時は白銀月					

# 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。

		用户名 🔽 密码	admin	<ul> <li>□ 自动登录 找回密码</li> <li>登录 立即注册</li> </ul>
				快捷导航 -
○ 请输入搜索内容	帖子 ▼ 搜索	热搜:活动交友	discuz	
今日:0│昨日:0│帖子:0│会员:1				查看新帖
Discuz!				-
默认版块			0/0 从未	
在线会员 - 2 人在线 - 0 会员(0 隐身), 2 位游客 - 最高记录是 4 于 2019-6-27.				-
📃 管理员 📃 超级版主 📃 版主 📃 会员				
当前只有游客或隐身会员在线				
<b>官方论坛</b> Discuz net 提供最新 Discuz! 产品新闻、软件下载与技术交流				
Comsenz 漫游平台 Yeswan 我的领地				
Powered by Discuz! X2				Archiver   Comsenz Inc.
© 2001-2011 Comsenz Inc.		GMT+8,	2019-6-27 17:07 , Processed in (	0.029540 second(s), 11 queries .

(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。

O 社区动力 DISCUZ!		用户名 🔽 密码	admin	自动登录     找回密码       登录     立即注册
门户 论坛 群组 家园 排行榜				快捷导航 🗸
〇、「请输入捜索内容	帖子 ▼ 搜索	<b>热搜:</b> 活动 交友	discuz	
★ 〉论坛				
┛ 今日:0│昨日:0│帖子:0│会员:1				查看新帖
Discuz!				-
默认版块			0/0 从未	
在线会员 - 2 人在线 - 0 会员(0 隐身), 2 位游客 - 最高记录是 4 于 2019-6-27.				-
💶 管理员 📃 超级版主 💽 版主 🗾 会员				
当前只有游客或隐身会员在线				
<b>官方论坛</b> Disouz.net 提供最新 Discuz! 产品新闻、软件下载与技术交流				
Comsenz 漫游平台 Yeswan 我的预地				
Powered by Discuz! X2				Archiver   Comsenz Inc.
© 2001-2011 Comsenz Inc.		GMT+8,	2019-6-27 17:07 , Processed	in 0.029540 second(s), 11 queries .

(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。

◆ 攻击日志 ◆ Web攻击日志统计						条件/ 清空/	导出▶ 刷	₩C
每页显示 15 🔻								
日期和时间	源IP	目的IP	目的URL	方法	攻击类型	规则类型	处理动作	次数
2019-06-28 01:21:36	192,168,7,138	172.16.101.74	172.16.101.74/forum.php	GET	特征防护规则	SOLIŦλ	阴新	8

# 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₽ 创建vlan101,将GE1/0/6口划入该vlan [SWUP\_For\_AVG\_NewWAF-vlan101]port GigabitEthernet 1/0/6+/ [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+/ 为vlan配置IP地址,作为客户端 [SWUP\_For\_AVG\_NewWAF-Vlan-interface101]int vlan 1024 [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]guite/ 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 2:4 Type: Local4

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 vian 1024

## 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

增加网桥接口				
1 第一步		2 第二步		
网桥号 *	10			
MTU *	1500			
模式 *	普通模式	v		
状态 *	启用	Ŧ		
STP				
			(下步 🔸 )	

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

增加网桥接口			×
1 第一步		2 第二步	
网桥号 *	11		
MTU *	1500		
模式 *	普通模式	Ψ.	
状态 *	启用	Ψ	
STP			
			(下步 🔶 )

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

编辑Port接口			×
接口名称 *	GE0/2		
备注			
Channel接口 *	空	v	
网桥接口 *	br10	Ψ	
启用状态 *	启用	Ŧ	
链路状态	启用	Ŧ	
ı			(保存 🖺 ) (取消 🅽 )
编辑Port接口			×
接口名称 *	GE0/3		
备注			
Channel接口 *	空	Ŧ	
网桥接口 *	br11	•	
启用状态 *	启用	•	
链路状态	启用	٣	

## 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

编辑HTTP服务器		×
HTTP服务器	数据压缩 高速缓存	
服务器名称 *	test	
IP地址* 💡	172.16.101.74	
端口 *	80	
部署模式 *	旁路	▼ GE0/3 ▼ (阻断接口)
防护模式 *	流模式	v
启用 *	$\checkmark$	
		保存 🖺 🛛 取消 🕽

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

╋ 増加Web防护策略										
Web防护策路基本信息配置										
策略名称 *	test1				错误页面标题 📀				11	
Web主机 📀	请输入或选择		٧		错误页面内容 📀				11	
服务器	test			- 配置 €	■定向URL Ø					
源IP	空			*						
访问日志	关闭			Ŧ	Cookie加圖					
优先级 * 😡	0				Cookie加密					
启用	~									
Web防护规则配置										
扫描防护规则	空	v	増加 🕇		文件上传规则	空	Ψ.	增加 🕇		
HTTP协议校验规则	通用规则	٣	增加 +	编辑 🖌	文件下戰規則	空	×	增加 +		
HTTP访问控制规则	空	Ŧ	增加 🕇		散感信息检测规则	空	×	增加 🕇		
特征防护规则	通用规则	v	增加+	编辑 🖌	關密码检测规则	空	×	增加 +		
爬虫防护规则	空	Ψ.	增加 +		虚拟补丁规则	空	¥	增加 +		
防盗链规则	호	Ψ.	增加 +		访问顺序规则	空	¥	增加 +		
防脾站请求伪造规则	호	٣	增加+		敏感词防护规则	空	×	增加 +		
									保存 🖺 💧	取満り

# 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。

O 社区动力 DISCUZ!		用户名 🔽 密码	admin  •••••	<ul> <li>□ 自动登录 扰回密码</li> <li>登录 立即注册</li> </ul>
门户 论坛 群组 家园 排行榜				快捷导航 -
○ 请输入搜索内容	帖子 <b>· 搜索</b>	<b>热搜:</b> 活动 交友	discuz	
〉论坛				
┛ 今日:0│昨日:0│帖子:0│会员:1				查看新帖
Discuz!				-
默认版块			0/0 从未	
在线会员 - 2 人在线 - 0 会员(0 隐身), 2 位游客 - 最高记录是 4 于 2019-6-27.				-
💶 管理员 📃 超级版主 📃 版主 🔽 会员				
当前只有游客或隐身会员在线				
<b>官方论坛</b> Disouz.net 提供最新 Discuz! 产品新闻、软件下载与技术交流				
Comsenz 漫游平台 Yeswan 我的领地				
Powered by Discuz! X2				Archiver   Comsenz Inc.
© 2001-2011 Comsenz Inc.		GMT+8,	2019-6-27 17:07 , Processed	in 0.029540 second(s), 11 queries .

(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。

_	$\rightarrow$	C	0	172.16.101.	74/forum	.php?id=1%20and%201=1
---	---------------	---	---	-------------	----------	-----------------------

无法访问此网站	
请试试以下办法:	
ERR_CONNECTION_RESET	
重新力力电影	详细信息

(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。

+ 攻击日志 + Web攻击日志统计						条件』 清空』	导出▶  周	¥Ω
每页显示 15 *								
日期和时间	源IP	目的IP	目的URL	方法	攻击类型	规则类型	处理动作	次数
2019-06-28 01:21:36	192.168.7.138	172.16.101.74	172.16.101.74/forum.php	GET	特征防护规则	SQL注入	阻断	8

# 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。



## 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

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

编辑网桥接口		
1 第一步		2 第二步
网桥号 *	100	
MTU *	1500	
模式 *	普通模式	Ŧ
状态 *	启用	٣
STP		

如下图所示,在桥 br100 上添加业务 IP。

## 图8-3 添加业务 IP-br100

编辑网桥接口				
1 √第一步		2 第二步		
增加 <b>+</b> 刷新 <b>2</b>				
IP地址	子阿掩码	版本号	管理IP	
172.16.0.3	255.255.255.0	ipv4	否	

( 🗲 上一步 🌖 🤇 保存 🖺 🌖

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

编辑网桥接口		
1 第一步		2 第二步
网桥号 *	200	
MTU *	1500	
模式 *	普通模式	٣
状态 *	启用	v
STP		

如下图所示,在桥 br200 上添加业务 IP。

## 图8-5 添加业务 IP-br200

编辑网桥接口				
1 →第一步		2 第二步		
增加┿刷新₽				
IP地址	子网掩码	版本号	管理IP	
172.16.101.15	255.255.255.0	ipv4	否	
		(	◆ 上─步 ) ( 保存 🖺 )	

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

编辑Port接口			×
接口名称 *	GE0/2		
备注			
Channel接口 *	空	٣	
网桥接口 *	br100	٣	
启用状态 *	启用	٣	
链路状态	启用	٣	
			(保存 🖺 ) 🛛 取消 🕽 )
编辑Port接口			×
接口名称 *	GE0/3		
备注			
Channel接口 *	空	٣	
网桥接口 *	br200	Ŧ	
启用状态 *	启用	٣	
链路状态	启用	٣	
			保存 🖺 🔵 取消 🕽 🔵

## 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

增加VRRP实例		×
1 第一步	2 第二步	3 第三步
冗余ID *	1	
绑定接口 *	br100	v
优先级 *	100	
状态 *	主	¥
通告时长 *	1	(秒)
延迟时长 *	10	(秒)
启用 *	启用	¥
		(下一步→ )

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。

增加VRRP实例			×
1 ✔ 第一步	2 第二步	3 第三步	
增加 <b>+</b> 刷新 <b>℃</b>			
IP配置			×
冗余ID	1		
IP地址 *	172.16.0.254		
子网掩码 *	255.255.255.0	]	
保存習			

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

增加VRRP实例		>	<
1 ▼第-步	2 ✔ 第二步	3 第三步	
增加 <b>+</b> 刷新 <b>2</b> 物理链路接口			
物理链路绑定			K
冗余ID *	1		
接口 *	GE0/2	Ŧ	
(保存巴)			
		(《上一步)(元陇)	

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

增加VRRP实例		×
1 第一步	2 第二步	3 第三步
冗余ID *	2	
绑定接口 *	br200	v
优先级 *	100	
状态 *	主	•
通告时长 *	1	(秒)
延迟时长 *	10	(私)
启用*	启用	<b>v</b>
		( 下──歩→ )

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

增加VRRP实例			×
1 🗸 第一步	2 第二步	3 第三步	
增加+ 刷新℃			
IP配置			
冗余ID	2		
IP地址 *	172.16.101.1		
子网掩码 *	255.255.255.0		
(保存四)			

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

增加VRRP实例		×
1 √第─步	2 → 第二步 3 第三步	
增加 + 刷新 2 物理链路接口		
物理链路绑定		×
冗余ID *	2	
接口 *	GE0/3	
保存巴		

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

增加VRRP组			×
VRRP组名称 *	test		
启用 *	启用		T
VRRP实例列表 *			1
			2
		$\Leftrightarrow$	
			保存四
如下图所示,应用?	忝加完成的"test"VF	RP组。	٥
图8-14 应用 VRRF	)		

+ VRRP实例 + VRRP组		编辑 / 删除 × 增加 + 刷新 2 应用 ▶
✓ VRRP组名称	VRRP实例列表	启用
✓ test	1,2	启用

## 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

增加HTTP服务器					×
HTTP服务器	数据压缩 高	ā速缓存			
服务器名称 *	test				
IP地址* 🔞	172.16	5.101.74			
端口 *	80				
部署模式 *	串联		Ŧ		
防护模式 *	代理核	試	Ŧ		
接口 *	br100	)	Ŧ		
客户端IP还原	◎ 是	• 否			
启用*	$\checkmark$				
				保存日	取消り)

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。

Web防护策路基本信息配置									
策略名称 *	test1			]	错误页面标题 😮				h
Web主机 🛛	请输入或选择		v		错误页面内容 🔞				1
服务器	test		¥	配置 〇	重定向URL 😧				
源IP	2		¥					11	
访问日志	关闭		¥		Cookie加固				
优先级 * 🛛 🛛	0				Cookie加密				
启用	$\checkmark$								
Web防护规则配置									
扫描防护规则	Ŕ	Ŧ	增加 +		文件上传规则	Ŷ	٣	增加 +	
扫描防护规则 HTTP协议校验规则	空通用规则	v v	增加 + 增加 +	编辑 /	文件上传规则 文件下戰规则	9	v v	增加 + 增加 +	
扫描防护规则 HTTP协议校验规则 HTTP访问控制规则	空 適用规则 空	* *	增加 + 增加 + 增加 +	编辑 /	文件上传规则 文件下數规则 敏密值最检测规则	64 64		增加 + 增加 + 增加 +	
扫描防护规则 HTTP协议校验规则 HTTP访问控制规则 特征防护规则	空 適用規則 空 適用規則	* * *	增加 + 增加 + 增加 + 增加 +	966 / 966 /	文件上侍规则 文件下戰规则 敏感信息检测规则 弱能积检测规则	84 84 84	* * *	增加 + 增加 + 增加 + 增加 +	
扫描的护规则 HTTP协议检验规则 HTTP访问控制规则 特征的护规则 爬虫防护规则	空 適用規则 空 適用規则 空	* * * *	增加 + 增加 + 增加 + 增加 + 增加 + 增加 +	### ♪ ### ♪	交件上传规则 交件下戰规则 截至信誉检测规则 時需得检测规则 通知补丁规则	포 포 포 포 포	* * *	增加 + 增加 + 增加 + 增加 + 增加 +	
扫描的护规则 HTTP协议依疑规则 HTTP访问控制规则 HTTP访问控制规则 施证的护规则 施证的护规则	空 通用規則 空 通用規則 空 空	* * * *	道加 + 道加 + 道加 + 道加 + 道加 + 道加 + 道加 +	病语 / 病徒 /	文件上件规则 文件下假规则 敏感信息检测规则 器或得检测规则 虚拟补丁规则 论问顺序规则	8 8 8 8 8 8 8 8 8 8	* * *	增加 + 增加 + 增加 + 增加 + 增加 + 增加 + 增加 +	

## 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。

O 社区动力 DISCUZ!		用户名 🔽 密码	admin	<ul> <li>□ 自动登录 找回?</li> <li>登录 立即?</li> </ul>	₹码 主册
门户 论坛 群组 家园 排行榜				快捷导航	•
Q、 请输入搜索内容	帖子 ▼ 搜索	<b>热搜:</b> 活动 交友	discuz		
✿ 〉论坛					
勐 今日:0│昨日:0│帖子:0│会员:1				查看新	肺枯
Discuz!					-
型 默认版块			0/0 从未		
在线会员 - 2 人在线 - 0 会员(0 隐身), 2 位游客 - 最高记录是 4 于 2019-6-27.					-
🔽 管理员 📃 超级版主 📃 版主 🔽 会员					
当前只有游客或隐身会员在线					
<b>官方论坛</b> Discuz.net 提供最新 Discuz! 产品新闻、软件下载与技术交流					
Comsenz 漫游平台 Yeswan 我的预地					
Powered by <b>Discuz!</b> X2 © 2001-2011 Comsenz Inc.		GMT+8,	2019-6-27 17:07 , Processed ii	Archiver   Comsenz ] n 0.029540 second(s), 11 que	nc.

(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。

- -> C (3) 172.16.101.74/forum.php?id=1%20and%201=1

# 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。

+ 攻击日志 + Web攻	击日志统计					条件》	腔∕₿出▶┃₽	創新ご
每页显示 15 🔻								
日期和时间	源IP	目的IP	目的URL	方法	政击类型	规则类型	处理动作	次数
2010-06-28 01-21-26	102 168 7 128	172 16 101 74	172 16 101 74/forum php	GET	44-27月53日2月1日	5013± X	88 W.C	2

(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。

# 400 Bad Request

(5) 在备机上查看有攻击日志,证明流量已切换至备机。

+ 攻击日志 + Web攻击日志统计						条件》 清	空∕ 导出▶ 月	)新C
每页显示 15 🔻								
日期和时间	源IP	目的IP	目的URL	方法	攻击类型	规则类型	处理动作	次数
2019-06-28 01:21:36	192.168.7.138	172.16.101.74	172.16.101.74/forum.php	GET	特征防护规则	SQL注入	阻断	8

# 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

增加网桥接口			ľ
1 第一步		2 第二	步
网桥号 *	10		
MTU *	1500		
模式 *	普通模式		٣
状态 *	启用		٣
STP			

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

编辑网桥接口			
1 √第─步		2 第二步	
增加+ 刷新 3			
□ IP地址	子网掩码	版本号	管理IP
172.16.101.15	255.255.255.0	ipv4	否
		( <b>←</b> 上-	-步 🔵 🤇 保存 🖺 🌖

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

编辑Port接口				×
接口名称 *	GE0/2			
备注				
Channel接口 *	空	Ŧ		
网桥接口 *	br10	Ŧ		
启用状态 *	启用	Ŧ		
链路状态	启用	v		
			(保存 🖺 )	〔取消つ〕

#### 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:

增加VRRP实例				
1 第一步	2 第二步		3 第三步	
冗余ID *	1			
绑定接口 *	br10	٣		
优先级 *	100			
状态 *	主	٣		
通告时长 *	1		(秒)	
延迟时长 *	10		(秒)	
启用 *	启用	٣		
			(下一步+)	

## 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

增加VRRP实例			×
1 ▼ 第一步	2 第二步	3 第三步	
增加 <b>+</b> 刷新 <b>ご</b>	7	网掩码	
IP配置			×
冗余ID	1		
IP地址 *	172.16.101.100		
子网掩码 *	255.255.255.0		
保存四)			

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

编辑VRRP实例			
1 → 第一步	2 ✔ 第二步	3 第三步	
增加+ 删除× ✓ 物理链路接口	刷新€		
「 物理链路绑定			×
冗余ID *	1		
接口 *	GE0/2	v	
保存图			
		( ←上一步 ) 〔 完成 〕	

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

增加VRRP组				×
VRRP组名称 *	test			
启用 *	启用		v	
VRRP实例列表 *		⇔	1	
				RFB)
如下图所示,应用添加 图9-9 应用 VRRP	口完成的"test"VRRP	组。		

+ VRRP实例 + VRRP组		编辑》 删除× 增加+ 刷新2 应用>
✓ VRRP组名称	VRRP实例列表	启用
✓ test	1	启用

## 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

增加HTTP服务器			×
HTTP服务器 数	刘据压缩 高速缓存		
服务器名称 *	test		
IP地址 * 😮	172.16.101.74		
端口 *	80		
部署模式 *	串联	Ŧ	
防护模式 *	代理模式	Ŧ	
接口 *	br10	Ŧ	
客户端IP还原	○ 是 ● 否		
启用 *	$\checkmark$		
		保有	(取消り)

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

增加HTTP代理服务器			×
HTTP代理服务器	数据压缩 高速缓存		
服务器名称 *	test1		
IP地址 * 😮	172.16.101.100		
端口 * 😧	80		
后端服务器 * 💡	test	v	
接口 *	br10	v	
启用 *	$\checkmark$		
		保存 🖺 🔵	取消り

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

14-12-22-22-22-22-22-22-22-22-22-22-22-22-									
₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩	test1				错误页面标题 📀				h
Web主机 📀	请输入或选择		v		错误页面内容 🕢				11
服务器	test			▼ 配置 €	聖定向URL Ø				
源IP	空			Ŧ				- lê	
访问日志	关闭			*	Cookie加圖				
优先级 * 📀	0				CookietDite				
启用	~								
Web防护规则配置									
扫描防护规则	幸	٣	增加 +		文件上传规则	幸	٣	增加 🕇	
HTTP协议校验规则	通用规则	v	增加 +	編載 🖌	文件下戰規則	蓥	¥	增加 🕇	
HTTP访问控制规则	空	Ŧ	增加 +		數感信息检测规则	空	×	增加 +	
特征防护规则	通用规则	Ŧ	增加 +	编辑 🧨	調密码检测规则	空	٣	增加 +	
爬虫防护规则	空	٣	增加 +		虚拟补丁规则	空	٣	增加+	
防盗继规则	空	٣	増加 +		访问顺序规则	空	٣	增加 +	
防跨站请求伪造规则	空	v	增加+		敏感词防护规则	空	Ψ.	增加 +	
									(保存日)(取消つ)

# 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。

O 社区动力 DISCUZ!		用户名 🔽 密码	admin	<ul> <li>□ 自动登录 找回密码</li> <li>登录 立即注册</li> </ul>
门户 论坛 群组 家园 排行榜				快捷导航 🗸
Q、 请输入搜索内容	帖子 ▼ <b>搜索</b>	<b>热搜:</b> 活动 交友	discuz	
♠ > 论坛				
」今日:0   昨日:0   帖子:0   会员:1				查看新帖
Discuz!				-
型 新认版块			0/0 从未	
在线会员 - 2 人在线 - 0 会员(0 隐身), 2 位游客 - 最高记录是 4 于 2019-6-27.				-
💶 管理员 📃 超级版主 📃 版主 🗾 会员				
当前只有游客或隐身会员在线				
<b>官方论坛</b> Discuz.net 提供最新 Discuz! 产品新闻、软件下载与技术交流				
Comsenz 漫游平台 Yeswan 我的领地				
Powered by <b>Discuz!</b> X2 © 2001-2011 Comsenz Inc.		GMT+8,	2019-6-27 17:07 , Processed in	Archiver   Comsenz Inc. 0.029540 second(s), 11 queries .

(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。

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。

+ 攻击日志 + Web攻击日志统计	ŀ				\$	《件 / 清空 / 导出)	▶    刷新2	
每页显示 15 🔻								<b>Q</b>
日期和时间	源IP	目的IP	目的URL	方法	攻击类型	规则类型	处理动作	次数
2019-06-28 07:00:33	192.168.7.1	172.16.101.74	172.16.101.100/forum.php	GET	特征防护规则	SQL注入	阻断	1

(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。

$\leftarrow$ $\rightarrow$ C $rac{1}{2}$	Q 172.16.101.100/forum.php?id=1 and 1=1	
	400 Bad Request	

(5) 在备机上查看攻击日志,证明流量已切换至备机。

+ 攻击日志 + Web攻击日志统计	t				4	条件 / 清空 / 导出	▶ 刷新2	
每页显示 15 🔻								0
日期和时间	源IP	目的IP	目的URL	方法	攻击类型	规则类型	处理动作	次数
2019-06-28 07:00:33	192.168.7.1	172.16.101.74	172.16.101.100/forum.php	GET	特征防护规则	SQL注入	阻断	1

# 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_AUG_NewWAF]interface Bridge-Aggregatio [SWUP_For_AUG_NewWAF-Bridge-Aggregation2]quit	on 2 创建聚合组2	
[SWUP_For_AUG_NewWAF]interface GigabitEthernet 1 [SWUP_For_AUG_NewWAF-GigabitEthernet1/0/3]port 1 [SWUP_For_AUG_NewWAF]interface GigabitEthernet 1	L/0/3 Link-aggregation group 2 L/0/4	将接口GE1/0/3加入到聚合组2
[SWUP_For_AVG_NewWAF-GigabitEthernet1/0/4]port ]	link-aggregation group 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

增加网桥接口			×
1 第一步		2 第二步	
网桥号 *	10		
MTU *	1500		
模式 *	普通模式	*	
状态 *	启用	•	
STP			
			(下步 🔸 )

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10-5 增加业务 IP 地址

接口名称 * IP类型 * IP地址 * 子网掩码 * 管理IP *	br10 ipv4 172.16.101.15 255.255.255.0	•			
IP类型 * IP地址 * 子网掩码 * 管理IP *	ipv4 172.16.101.15 255.255.255.0	•			
IP地址 * 子网掩码 * 管理IP *	172.16.101.15 255.255.255.0				
子网掩码 * 管理IP *	255.255.255.0				
管理IP *					
	$\checkmark$				
			(保存	取消り)	

## 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

编辑Channel接口		
接口名称 *	1	
备注		
网桥接口 *	空	Ŧ
状态 *	启用	٣

## 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
-------	---------------

编辑Port接口			×
接口名称 *	GE0/0		
备注			
Channel接口 *	1	٣	
网桥接口 *	空	٣	
启用状态 *	启用	٣	
链路状态	启用	٣	
			保存・日 取消 つ

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

编辑Channel接口		
接口名称 *	1	
备注		
网桥接口*	br10	Ŧ
状态 *	启用	Ŧ

编辑Channel接口			~
接口名称 *	2		
备注			
网桥接口*	br10	Ŧ	
状态 *	启用	Ŧ	
			(保存 🖺 ) 🌘 取消 🕽 )

# 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

增加网桥接口		
1 第一步		2 第二步
网桥号 *	10	
MTU *	1500	
模式 *	普通模式	Ŧ
状态 *	启用	v
STP		

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

1 ▼第一步		2 第二步	
增加+ 刷新			
IP地址	子网掩码	版本号	管理IP
没有检索到数据			

#### 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

编辑Port接口				×
接口名称 *	GE0/0			
备注				
Channel接口 *	空	٣		
网桥接口 *	br10	٣		
启用状态 *	启用	v		
链路状态	禁用	٣		
			保存 🖺 🔵 🛛 取消 🤊 🔵	

#### 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

增加Trunk接口		
1 第一步		2 第二步
接口 *	br10	Ψ
备注		
VLAN标签 *	2	
模式 *	Port-Mode	v
状态 *	启用	Ŧ

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

加Trunk接口		
1 ✔ 第一步	2 第二步	
増加+ 刷新ご		
□ IP地址 ◆ 子网掩码	版本号管理IP	
没有检索到数据		
	( 🗲 上一步 ) ( 保存 🖺 )	

## 12 网页防篡改配置举例

记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。

✤ 防护客户端下载		74
<b>下載Windows客户端</b> 通过下面的按钮下载Windows阿页肋氯改客户端 高击 』 来保存 Windows 2003 32位 Windows 2003 32位 Windows 2012 64位	<b>F载CentOS/Redhat/Debian/Ubuntun客户端</b> 通过下面的按钮下载Debian/Ubuntun/CentOS/Redhat网页防幕改客户端 点由 및 米保存32位 点由 및 米保存64位	

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。

<b>k</b>	wkas 1.0	X
-管理中心-		确定
域名或IP	183. 1. 15. 7	取消
-发布中心 -		]
域名或IP	127. 0. 0. 1	
-发布配置-		
线程	1	
空闲发布时	j间(秒) 300	
正点发布时	1间(以分号隔开)	
0;1;2;3;4	:5;6;7;8;9;10;11;12;13;14;15;16;17;	

#### 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

+ 防护服务器探测			生成配置+ 刷新ご
主机名	IP地址	操作系统类型	版本号
c-171	183.1.8.171	Windows	1.0

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

+ 防护服务器探测						生成配置+ 刷新ご
主机名	防护服务器配置				版本号	
>171	1 第一步	2 第二步	3 第三步		1.0	
	Web名称 *	win2012_8_171				
	主机名 *	c-171				
	IP地址 *	183.1.8.171				
	工作模式	防护模式 *				
	启用	启用 ▼ 下一步 ○ )				

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

防护服务器配置		×
1 ▼第一步	2 第二步 3	第三步
操作系统类型	Windows *	
Web根目录* 🕜	c:\test	
例外目录/文件 🕜		
例外文件类型 🕜		
例外进程 🛛		
(	⊕上─步 ) ( 下─步 ○ )	

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。

防护服务器配置					$\times$
1 ▼第一步	2	✔第二步	3	第三步	
发布服务器	<del>ç</del>		•		
	( ⊛⊥—∌	) ( 完成 ⊙	)		

## 12.8 验证配置

(1) 在防护目录中新增文件。

	目	标文件夹访问被	<b>披拒绝</b>	X	
4	你需要权限来执行此操	作			
_		test 创建日期: 2019/	110/28 17:31 重试(R)	取消	
(2) 査	看防篡改日志。				
+ 防篡改日志     +       毎页显示     15	▶ 网页防籯改日志统计			条件 🥒 制度	â× 细节◢ 清空◢ 尋出▶ 刷新C
日期和时间	Web名称	设备名称	进程名	文件名	攻击类型
2019-10-28 17	v:31:07 win2012_8_171	c-171	explorer	C:\test	修改

## **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

增加网桥接口		
1 第一步		2 第二步
网桥 <del>号</del> *	10	
MTU *	1500	
模式 *	普通模式	٣
状态 *	启用	Ŧ
STP		

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

<b>揖网桥接口</b>				
1 ▼第一步		2 第二步		
增加+ 刷新 €				
IP地址	子网掩码	版本号	管理IP	•
101.10.4.3	255.255.255.0	ipv4	否	

( 🗲 上一步 🔵	) 🤇 保存 🖺	
-----------	----------	--

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

增加路由			×
IP类型 *	ipv4		v
IP地址 *	0.0.0.0		
子网掩码*	0.0.0		
下一跳 *	101.10.4.1		
Metric			
		(保存 🖺 )	(取消っ)

#### 图13-4 增加 IPV6 路由

增加路由		×
IP类型 *	ірvб	v
IP地址 *	::	
子网掩码 *	0	
下一跳 *	2019:101:10:4::1	
Metric		
	(保存 🖺 )	(取消り)

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

编辑Port接口		
接口名称*	GE0/0	
备注		
Channel接囗 *	室	Ŧ
网桥接口 *	br10	Ŧ
启用状态 *	启用	Ŧ
链路状态	启用	Ŧ

#### 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

编辑HTTP服务器					×
HTTP服务器	数据压缩	高速缓存			
服务器名称 *	:	101_10_3_100			
IP地址 * 😮	:	101.10.3.100			
端口 *	:	80			
部署模式 *		串联		*	
防护模式 *		代理模式		٣	
接口 *		br10		٣	
客户端IP还原		是 🖲	否		
启用*	•	<b>~</b>			
					保存 🖺 🔵 取消 🕽 🔵

#### 图13-7 创建 IPV6 HTTP 服务器

编辑HTTP服务器					×
HTTP服务器	数据压缩	音 高速缓存			
服务器名称 *		ipv6_3_100			
IP地址* 🛛		2019:101:10:3::100			
端口 *		80			
部署模式 *		串联	Ŧ		
防护模式 *		代理模式	٣		
接口 *		br10	٣		
客户端IP还原		◎ 是 ⑧ 否			
启用*		$\checkmark$			
				(保存 🖺 ) 🔵 取消 🕽	

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

编辑HTTP代理服务器			×
HTTP代理服务器	数据压缩 高速缓存		
服务器名称 *	ірv4_ірvб		
IP地址 * 🕜	101.10.4.3		
端口 * 🕑	8003		
后端服务器 * 🛛 🕢	ipv6_3_100	<b>v</b>	
接口 *	br10	<b>v</b>	
启用 *	$\checkmark$		
		(保存日)	) (取消り)

#### 图13-9 增加 IPV6 反代 IPV4 的代理服务器

编辑HTTP代理服务器		
HTTP代理服务器	数据压缩 高速缓存	
服务器名称 *	ipv6_ipv4	
IP地址 * 🕜	2019:101:10:4::3	
端口* 🛛	8002	
后端服务器 🎽 🖓	101_10_3_100	Ŧ
接口 *	br10	Ψ.
启用 *	$\checkmark$	

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

									12 II
Web防护策略基本信息配置									
策略名称*	3_100				错误页面标题 🕜				11
Web主机 🕜	请输入或选择		Ŧ		错误页面内容 🕑				11
服务器	101_10_3_100			● 配置 ●	重定向URL 😧				
源IP	窒			r					11
访问日志	开启			7	Cookie加画	_			
优先级 * 🕜	1				Cookie加密				
启用	~								
Web防护规则配置									
扫描防护规则	空	Ŧ	增加 🕇		文件上传规则	空	٣	增加 🕇	
HTTP协议校验规则	通用规则	٣	增加 🕇	编辑 🖉	文件下载规则	空	٣	增加 🕇	
HTTP访问控制规则	空	Ŧ	增加 🕇		敏感信息检测规则	空	٣	增加 🕇	
特征防护规则	通用规则	Ψ	增加 +	编辑 🖋	歸密码检测规则	空	٣	增加 🕇	
爬虫防护规则	空	Ŧ	增加 🕇		虚拟补丁规则	空	٣	增加 🕇	
防盗链规则	空	Ŧ	增加 +		访问顺序规则	空	٣	增加 🕇	
防跨站请求伪造规则	호	v	增加 🕇		敏感词防护规则	空	٣	增加 🕇	
									保存 🖺 🔵 🛛 取消 🕽 🔵

#### 图13-11 配置 IPV6 服务器安全防护策略

Web防护策略基本信息配置								
策略名称*	ipv6_3_100			错误页面标题 🕜				1
Web主机 🛿	请输入或选择		Ŧ	错误页面内容 🕜				li.
服务器	ipv6_3_100		▼ 配置 ⊙	重定向URL 🕜				
源IP	空		¥					
访问日志	开启		Ŧ	Cookie加幽				
优先级 * 🕜	4			Cookie加密				
启用	×							
Web防护规则配置								
扫描防护规则	空 *	增加 🕇		文件上传规则	空	Ŧ	增加 🕇	
HTTP协议校验规则	通用规则	增加 🕇	编辑 🖉	文件下戰規则	空	Ŧ	增加 🕇	
HTTP访问控制规则	空 *	增加 🕇		敏感信息检测规则	空	Ŧ	增加 🕇	
特征防护规则	通用规则 🔻	增加 🕇	编辑 🖋	弱密码检测规则	空	Ŧ	增加 🕇	
爬虫防护规则	空 *	增加 🕇		虚拟补丁规则	空	Ŧ	增加 🕇	
防盗链规则	空 *	增加 🕇		访问顺序规则	窒	Ŧ	增加 🕇	
防跨站请求伪造规则	空 *	增加 🕇		敏感词防护规则	空	Ŧ	增加 🕇	
								(保存 🖺 ) 🌘 取満 🔈 🌖

## 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。

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WAF已经 正常防护,且后端服务器为 IPV6 地址。

+ 攻击日志 + Web攻击日志	统计						条件 🖋 🚽 删除 🗙	细节』清空』	▶   导出▶   刷新:	2
每页显示 15 *										
日期和时间	源IP	目的IP	目的URL		方法	攻击类型	严重级别	规则类型	处理动作	次数
2019-10-24 15:58:49	101.1.26.26	2019:101:10:3::100	101.10.4.3:8003/login.php		GET	特征防护规则	高级	SQL注入	阻断	1
2019-10-23 17:46:25	细节					特征防护规则	高级	SQL注入	阻断	1
2019-10-23 17:20:15						特征防护规则	高级	SQL注入	阻断	1
2019-10-23 17:09:38	日志详细信息	HTTP详细信息 规则	リ洋蚶			特征防护规则	高级	SQL注入	阻断	1
2019-10-17 19:03:59	拦截时间:201	19-10-24 15:58:4	9			特征防护规则	高级	SQL注入	阻断	1
2019-10-17 19:02:57	Į.	欠击者		攻击目标		特征防护规则	高级	SQL注入	阻断	1
2019-10-17 18:34:09	101.1.2	26.26:65460		2019:101:10:3::100:80		特征防护规则	高级	恶意攻击	阻断	1
2019-10-17 16:19:24	Web防护策略	ipv6_3_100	Web防护规则	通用规则	_	特征防护规则	高级	SQL注入	阻断	1
	攻击类型	特征防护规则	严重级别	高级						1 \
当前1-8, 总共8条记录	攻击域	HTTP请求头部	处理动作	阻断						1 /
	CDN IP		XFF IP							
	协议类型	HTTP								
	国家	中国								
	省份	香港								
	城市									
	所有者									
	设备类型	PC端								
	设备操作系统	Windows								
	客户端类型	谷歌浏览器								
	_									

## 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。

#### ← → C ① 不安全 | [2019:101:10:4::3]:8002/index.php

← → C ① 不安全   [2019:101:10:4::3]:8002/index.php		07 (	2	9 :
	DYWA			
Home Instructions Setup / Reset DB Brute Force Command Injection CSRF File Inclusion File Upload Insecure CAPTCHA SQL Injection SQL Injection SQL Injection SQL Injection SQL Injection (Blind) Weak Session IDs XSS (Reflected) XSS (Reflected) XSS (Reflected) XSS (Stored) CSP Bypass JavaScript DVWA Security PHP Info About	<section-header><section-header><section-header><text><text><section-header><text><text><text><text><text><text></text></text></text></text></text></text></section-header></text></text></section-header></section-header></section-header>			
	measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person's who uploaded and installed it.			

(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。

$\leftrightarrow$ $\rightarrow$	С	⑥ 不安全   [2019:101:10:4:3}8002/login.php?id=1%20and%201=1	☆	Θ	:
		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 WAF 已经 正常防护,且后端服务器为IPV4地址。

+ 攻击日志 + Web攻击日志 每页显示 15 ×	5统计					27	:件♪ 删除 ×	细节』清空』		0 (
日期和时间	源IP	目的IP	目的URL		方法	攻击类型	严重级别	规则类型	处理动作	次数
2019-10-24 16:06:55	2001:101:1:26::26	101.10.3.100	[2019:101:10:4::3]:8002/log	gin.php	GET	特征防护规则	高级	SQL注入	阻断	1
2019-10-24 15:58:49	细节				×	特征防护规则	高级	SQL注入	阻断	1
2019-10-23 17:46:25						特征防护规则	高级	SQL注入	阻断	1
2019-10-23 17:20:15	日志详细信息	HTTP详细信息  规则说	師			特征防护规则	高级	SQL注入	阻断	1
2019-10-23 17:09:38	拦截时间:201	9-10-24 16:06:55				特征防护规则	高级	SQL注入	阻断	1
2019-10-17 19:03:59		(击者)		-1	特征防护规则	高级	SQL注入	阻断	1	
2019-10-17 19:02:57	2001:101	:1:26::26:50874		101.10.3.100:80		特征防护规则	高级	SQL注入	阻断	1
2019-10-17 18:34:09	Web防护策略	3_100	Web防护规则	通用规则		特征防护规则	高级	恶意攻击	阻断	1
2019-10-17 16:19:24	攻击类型	特征防护规则	严重级别	高级		特征防护规则	高级	SQL注入	阻断	1
	攻击域	HTTP请求头部	处理动作	阻断						4
当前1-9,总共9条记录	CDN IP		XFF IP							1 ,
	协议类型	HTTP								
	国家	未知								
	省份	未知								
	城市	未知								
	所有者	未知								
	设备类型	PC端								
	设备操作系统	Windows								
	客户端类型	谷歌浏览器								

# 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。

+ Port接□	+ Channel接口 + 网桥接口	] 🕇 Trunk接口	╋ 端口联动				刷新
接口名称		备注		Channel接口	网桥接口	启用状态	链路状态
GE0/0				空	MngtBridge	启用	启用
GE0/1				空	br2	禁用	禁用

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。

輯网桥接口			
1 第一步		2 第二步	
网桥号 *	2		
MTU *	1500		
模式 *	普通模式	v	
状态 *	启用	Ŧ	
STP			
			(下步 🔺 )

编辑网桥接口				×
1 ▼第一步	2	第二步		
增加+ 刷新2				
编辑网络接口IP				
接口名称 *	br2			
IP类型 *	ipv4	v		
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	l sw1	的路由。
----------------	-------	-------------	-------	------

増加路由	×
IP类型 *	ipv4 *
IP地址 *	0.0.0.0
子网掩码 *	0.0.0.0
下一跳*	192.168.10.1
Metric	
	保存 🖺 🔵 取消 🕽 🔵

## 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。

+ HTTP服务器     + HTTPS服务器       増加+								
每页显示 15 *	( <del>Q</del>							
服务器名称	IP地址	端口	部署模式	防护模式	接口	启用		
□ s_±	101.10.5.200	80	串联	代理模式	br100	启用		
当前 1 - 1 , 总共 1 条记录	当前 1 - 1 , 总共 1 祭记录							

增加HTTP服务器		×
HTTP服务器		
服务器名称 *	sl	
IP地址* 😮	101.10.5.200	
端口 *	80	
部署模式 *	串联	
防护模式 *	流模式	
启用 *	$\checkmark$	
		(保存 🖺 ) 🌘 取消 🕽 🌖

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。

╋ Web防护策略								增加 +	刷新℃
每页显示 15 🔻									E.
名称	服务器	Web主机	源IP	访问日志	启用	优先级	是否自动生成	Cookie加固	Cookie加密
🗌 fh	s_主	호	空	开启	启用	0	否	禁用	禁用
当前1-1,总共1条记录									$\langle$ 1 $\rangle$

╋ 编辑Web防护策略									8
Web防护策略基本信息配置									
策略名称 *	fh1				错误页面标题 🕜				11
Web主机 🛿	请输入或选择-	-		,	错误页面内容 🕜				11
服务器	s1		,	▼ 配置 €	重定向URL 😧				
源IP	空			Y					11
访问日志	开启			Y	Cookie加固				
优先级 * 🕜	0				Cookie加密				
启用	$\checkmark$								
Web防护规则配置									
扫描防护规则	空	٣	増加		文件上传规则	空	٣	增加 🕇	
HTTP协议校验规则	通用规则	٣	増加 🕇	编辑 🖋	文件下载规则	空	٣	増加 🕇	
HTTP访问控制规则	空	٣	增加 🕇		敏感信息检测规则	空	٣	增加 🕇	
特征防护规则	通用规则	٣	増加	编辑 🖌	弱密码检测规则	Ŷ	Ŧ	増加 🕇	
爬虫防护规则	空	٣	増加		虚拟补丁规则	室	Ŧ	增加 🕇	
防盗链规则	空	Ŧ	增加 🕇		访问顺序规则	空	Ŧ	增加 🕇	
防跨站请求伪造规则	窒	Ŧ	增加 🕇		敏感词防护规则	空	Ŧ	增加 🕇	
									保存 🖺 🔵 🛛 取消 🕽 🔵

#### 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



• 在"日志系统—访问日志"中,能看到正常访问时的访问日志。

+ 访问日志 + Web访问日志	统计					条件》 清空》 导	出▶ 刷新2
毎页显示 15 ▼							
日期和时间	源IP	源端口	目的IP	站点域名/IP	目的URL	方法	次数
2019-09-19 08:56:11	101.10.0.10	52512	101.10.5.200	101.10.5.200	101.10.5.200/	GET	1
2019-09-19 08:56:11	101.10.0.10	52512	101.10.5.200	101.10.5.200	101.10.5.200/	GET	1

 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。

+ 攻击日志 + Web攻击日	日志统计					条件。	/ 清空/ 导出▶	刷新€	
每页显示 15 🔻									- E
日期和时间	源IP	目的IP	目的URL	方法	攻击类型	严重级别	规则类型	处理动作	次数
2019-09-19 09:00:27	101.10.0.10	101.10.5.200	101.10.5.200/vulnerabilities/sqli/	GET	特征防护规则	高级	SQL注入	阻断	1

# 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。

╋ Port接口	+ Channel接口 + 网桥接口	] + Trunk接口 + 端口联	动			刷新
接口名称		备注	Channel接口	网桥接口	启用状态	链路状态
GE0/0			空	MngtBridge	启用	启用
GE0/1			空	br2	禁用	禁用

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)。

编辑网桥接口					
1 第一步		2 第二	二步		
网桥号 *	2				
MTU *	1500				
模式 *	普通模式		•		
状态 *	启用		Ŧ		
STP					
				(下步 🔸 )	

编辑网桥接口			×
1 ▼第一步	2	第二步	
增加+ 刷新2			
编辑网络接口IP			
接口名称 *	br2		
IP类型 *	ipv4	Y	
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。

增加路由			×
IP类型 *	ipv4		v
IP地址 *	0.0.0.0		
子网掩码 *	0.0.0.0		
下—跳*	192.168.10.1		
Metric			
		(保存 🖺 )	(取消り)

#### 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。

+ HTTP服务器 + HTTP	PS服务器					增加+ 刷新2
每页显示 15 *						Ŷ
服务器名称	IP地址	端口	部署模式	防护模式	接口	启用
□ s_±	101.10.5.200	80	串联	代理模式	br100	启用
当前 1 - 1 , 总共 1 条记录						< 1 >
增加HTTP服	务器					×
HTTP服务	물문					
服务器名和	家 *	s1				
IP地址 *	0	101.10.5.200				
端口 *		80				
部署模式	*	串联		-		
防护模式	*	流模式		•		
启用*		$\checkmark$				
					(保存習	(取消り)

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)

增加VRRP实例				×
1 第一步	2 第二步		3 第三步	
冗余ID *	1			
绑定接口 *	br2	٣		
优先级 *	100			
状态 *	±	٣		
通告时长 *	1		(秒)	
延迟时长 *	10		(秒)	
启用 *	启用	٣		
			(下一步→ )	

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

编辑VRRP实例	
1 → 第一步 2 第二步	3 第三步
增加 <b>+</b> 刷新 <b>2</b>	
IP地址	子网掩码
192.168.10.254	255.255.255.0
	<b>(←上──歩</b> )(下──歩→ )

点击下一步,选择 br2 对应的物理接口 GE0/1。

编辑VRRP实例		
1 ✔ 第一步	2 ✔ 第二步	3 第三步
増加まし刷新な		
物理链路接口		
GE0/1		

(	完成)
---	-----

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。

编辑VRRP组				×
VRRP组名称 *	test			
启用 *	禁用		v	
VRRP实例列表 *			1	
		$\Rightarrow$		
				(保存四)

## 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。

+ VRRP实例 + VRRP组	★ VRRP组					
VRRP组名称	VRRP实例列表	肩用				
test	1	启用				

#### 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。

										t	増加+ 刷新 2
页显示 15 ▼											
名称	服务器	Web主机	源IP		访问日志	启用	优先级	是否自动的	E成	Cookie加固	Cookie加速
fh	s_主	空	空		开启	启用	0	否			
前1-1,总共1条记	<b>录</b>										< 1
辑Web防护策略 Web防护策略基本	信息配置										
策略名称 *	fh1					错误页面标题	0				11
Web主机 🕜	请	输入或选择 ▼		v		错误页面内容	错误页面内容 🕜				11
服务器	-1			_	*J						
	51			*		軍定向URL 🔮					
源IP	51 空			v		重定向URL 🧃	•				h
源IP 访问日志	51 空 开fi	白		Y Y Y		重定向URL 《 Cookie加固	•				11
源IP 访问日志 优先级* <b>②</b>	51 空 开fi 0	ЯП П		Y Y		重定向URL Cookie加国 Cookie加函	)				1
源IP 访问日志 优先级 * 🕜 启用	SI 空 开A 0	10		<b>v</b>		重定向URL 《 Cookie加固 Cookie加密					l
源IP 访问日志 优先级 <sup>*</sup> <b>♀</b> 启用   Web防护规则配置	SI 空 开fi 0 ✓	2		V           V           V		重定向URL 《 Cookie加国 Cookie加密	•				i.
<ul> <li></li></ul>	51 空 开fi 0 ✓	â	▼	* * *	助王 V	重定向URL 《 Cookie加函 Cookie加密 文件上传规则			¥	增加 <b>十</b>	<i>I</i>
源IP 访问日志 优先级 <sup>*</sup> <b>④</b> 启用 <b>  Web防护规则配置</b> 扫描防护规则 HTTP协议校验规则	SI 空 开析 の マ い の 、 ブ 日 日 日 日 二 二 二 二 二 二 二 二 二 二 二 日 日 日 日	自	▼ <sup>培加 +</sup>	<ul> <li>▼</li> <li>▼</li> <li>▼</li> <li>+</li> <li>#</li> </ul>	咸重 ♥	重定向URL Cookie加国 Cookie加密 文件上传规则 文件下载规则	•	· · · · ·	v	增加 <b>+</b> 墙加 <b>+</b>	1
濵IP 访问日志 优先级 * 倉用 Web防护规则配置 扫描防护规则 HTTP协议校验规则 HTTP访问控制规则	51 空 开が マ マ 通 調 型	自	<ul> <li>&gt; 増加</li> <li>× 増加 *</li> <li>× 増加 *</li> </ul>	+ + +	扁搔 /	重定向URL Cookie加函 Cookie加密 文件上传规则 文件下载规则 敏感信息检测规则		· · · · · · · · · · · · · · · · · · ·	<b>v</b> <b>v</b>	增加 + 增加 + 增加 +	<i>i</i> ,
源IP 访问日志 优先级 <sup>*</sup>	SI 空 开fi の マ 、 通 り 空 電 、 通 り 空 電	<ul> <li>         日本         日初回り         日初回り         日初回り         日初回り     </li> </ul>	<ul> <li>&gt; 増加 +</li> <li>&gt; 増加 +</li> <li>&gt; 増加 ・</li> <li>× 増加 ・</li> </ul>	• • • •	殿王 ●	重定向URL 《 Cookie加国 Cookie加密 文件上传规则 文件下载规则 敏感信息检测规则 弱密码检测规则			V V V	增加 + 增加 + 增加 + 增加 +	1
源IP 访问日志 优先级 * 倉用 Web防护规则配置 扫描防护规则 HTTP访问控制规则 HTTP访问控制规则 特征防护规则 爬虫防护规则	SI 空 开A ○ ✓ 通 週 章 空 通 『 空 』	<b>吉</b> 	<ul> <li>× 増加・</li> <li>増加・</li> <li>増加・</li> <li>× 増加・</li> <li>× 増加・</li> <li>× 増加・</li> </ul>	• • • • •	■王 ●	重定向URL 《 Cookie加函 Cookie加密 文件上传规则 文件下载规则 敏感信息检测规则 弱密码检测规则 虚拟补丁规则		· · · · · · · · · · · · · · · · · · ·	V V V V	增加 + 增加 + 增加 + 增加 + 增加 +	<i>i</i>
源IP 访问日志 优先级" ● 启用 】 <b>Web防护规则配置</b> 扫描防护规则 HTTP协议校验规则 HTTP协问控制规则 特征防护规则 施生防护规则 防盗链规则	51 空 开fi 0 マ 2 通 道 定 空 通 定 空 で の マ マ の マ マ の マ マ の マ の の マ の の マ の	<b>吉</b> 	<ul> <li>× 増加 *</li> <li>増加 *</li> <li>増加 *</li> <li>増加 *</li> <li>増加 *</li> <li>増加 *</li> <li>増加 *</li> </ul>	• • • • • •	■ ■ ●	重定向URL Cookie加面 Cookie加密 文件上传规则 文件下戰规则 敏密信息检测规则 感密码检测规则 處拟补丁规则 访问顺序规则		· 호 호 호 · · · · · · · ·	V V V V	增加 + 增加 + 增加 + 增加 + 增加 + 增加 +	<i>i</i> ,

## 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]apply next-hop 192.168.10.254

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。

🖉 Welcome :: Damn Vulnerable 🗆 🗙	+
← → C ③ 不安全   101.1	0.5.200 🔤 🛧 😝 (
	DYWA
Home	Welcome to Damn Vulnerable Web Appl
Instructions Setup / Reset DB	Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is c goal is to be an aid for security professionals to test their skills and tools in a legal em developers better understand the processes of securing web applications and to aid bc learn about web application security in a controlled class room environment.
Brute Force Command Injection	The aim of DVWA is to <b>practice some of the most common web vulnerabilities</b> , v <b>difficultly</b> , with a simple straightforward interface.
CSRF File Inclusion	General Instructions
File Upload Insecure CAPTCHA	It is up to the user how they approach DVWA. Either by working through every module selecting any module and working up to reach the highest level they can before moving is not a fixed object to complete a module; however users should feel that they have s
SQL Injection SQL Injection (Blind)	system as best as they possible could by using that particular vulnerability. Please note, there are <b>both documented and undocumented vulnerability</b> with th intentional. You are encouraged to try and discover as many issues as possible.
占击"日志系统——访问F	1末"。能看到正堂访问时的访问日末。

+ 访问日志 + Web访问日志纲	充计					条件∥ 清空∥ 导	出▶ 刷新2
每页显示 15 💌							
日期和时间	源IP	源端口	目的IP	站点域名/IP	目的URL	方法	次数
2019-09-19 08:56:11	101.10.0.10	52512	101.10.5.200	101.10.5.200	101.10.5.200/	GET	1
2019-09-19 08:56:11	101.10.0.10	52512	101.10.5.200	101.10.5.200	101.10.5.200/	GET	1

• 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。



• 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。

+ 攻击日志 + Web攻击日志统计 タ州 → 第空 / 号出 > 開設									
每页显示 15 *									- E
日期和时间	源IP	目的IP	目的URL	方法	攻击类型	严重级别	规则类型	处理动作	次数
2019-09-19 09:00:27	101.10.0.10	101.10.5.200	101.10.5.200/vulnerabilities/sqli/	GET	特征防护规则	高级	SQL注入	阻断	1