应用安全使用手册

目录

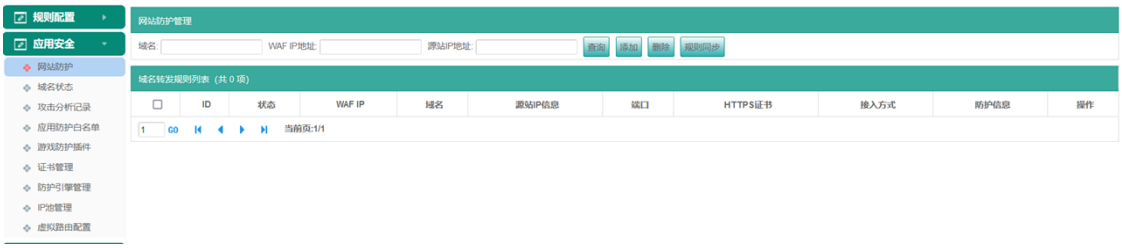
一、 概述

应用安全是用于网站业务的防护与管理，当前网站的接入方式支持透明转发与反向代理，该系统在网络环境中不需要物理上与网络环境有连接，只需要逻辑上互通。该系统在网络环境中的连接方式有 二层模式与三层模式。

二、 功能介绍

2、 应用安全菜单说明

功能介绍：应用安全配置菜单入口，位于防火墙 WEB 管理页面【首页】-【规则配置】与【牵引配置】之间。其下含有 9 个子菜单分别是【网站防护】、【域名状态】、【攻击分析】、【应用域名白名单】、【游戏防护插件】、【证书管理】、【防护引擎管理】、【IP 池管理】、【虚拟路由配置】。



功能	功能描述
网站防护	此功能可以查看站已接入网站的源站信息、接入方式、HTTPS 证书、以及 WAF IP，也可以手动添加防护规则操作。
域名状态	可以通过域名状态查看已接入的防护域名的实时流量、每个防护域名的请求方法的统计、域名响应状态的计数信息、访问域名的协议统计和访问域名的系统分析并进行统计，以提供客户查看。为了方便对异常域名的防护，次功能处可以直接对异常域名进行添加防护和被防护域名的攻击分析。
攻击分析	针对已经记录的域名攻击进行分析，支持导出，导出格式为 xls 表格。

应用防护白名单	对加白的客户端地址进行添加和删除的操作，可以按照客户端地址删除和按照 WAF IP 的方式进行删除。该白名单中的客户端地址是通过被防护域名添加的防护规则触发添加的。
游戏防护插件	智能游戏防护插件，对游戏业务类型的攻击提供防护。
证书管理	网站证书管理，接入网站防护时需要上传证书。
防护引擎管理	用于防护规则中的 web 应用攻击防护规则，防护引擎中包含攻击防护与告警功能。
IP 池管理	IP 地址池中的 IP 地址主要存在两种角色：转发地址和回源地址。主要用于网站防护，对接入网站配置防护 IP，转发地址：代理转发接入时，防护域名对外的 WAF IP 地址。代理 IP：代理转发接入模式，用于回源源站地址时使用的 IP 地址。
虚拟路由配置	用于设置应用安全模块的部署，支持三层模式部署和二层模式部署。

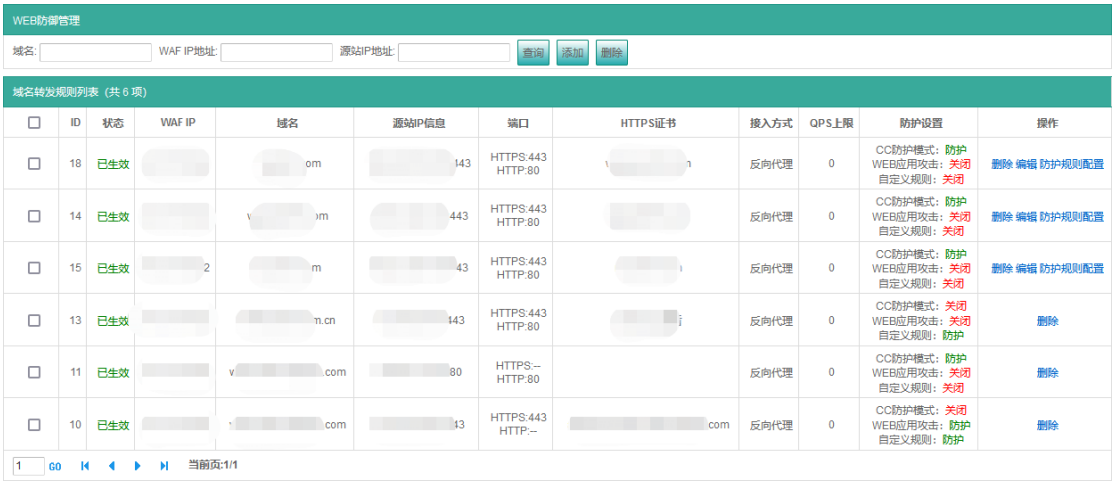
2.1、 网站防护

首页-应用安全-网站防护

功能介绍：网站防护可以针对当前业务下的网站进行防护，可以针对域名、WAF IP 地址、源站 IP 地址进行网站的防护查询，查询结果会列出所查信息的 ID、状态、WAF IP 、域名、源站 IP 信息、端口、https 证书、接入方式、防护信息、操作等显示出来，如状态会显示当前域名转发规则的防护状态。

接入方式处可以显示该域名的接入方式，包括反向代理和透明代理。

操作模块可以针对当前网站防护状态进行删除编辑防护规则配置等操作。

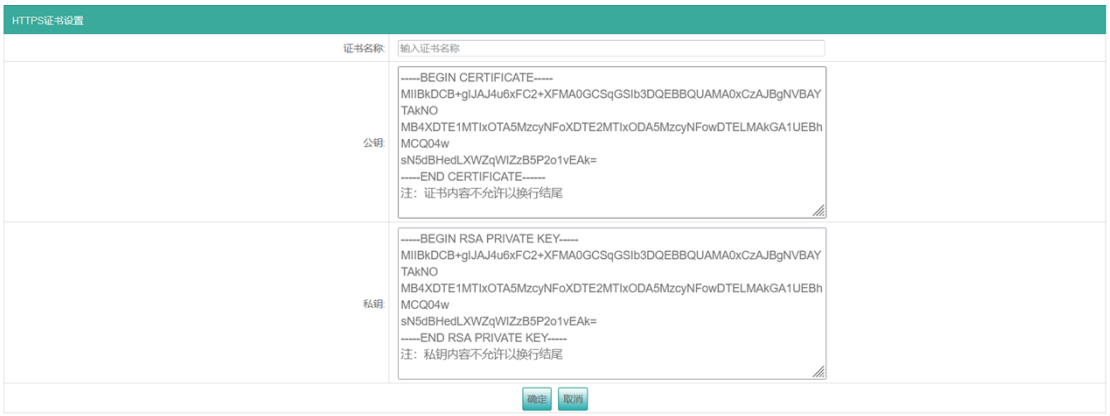


编号	名称	定义
1	查询	根据输入的IP地址、WAF IP地址和源站地址进行指定域名转发规则的查询；
2	添加	添加域名转发规则；
3	删除	对域名转发规则列表中选的域名转发规则进行删除操作；
4	规则同步	对于现有的域名转发规则进行同步下发；
5	编辑	编辑已经创建的域名转发规则；
6	防护规则配置	手动添加网站防护规则；
7	状态	显示当前域名转发规则的状态，存在“待下发”，“已生效”两种状态；
8	WAF IP	开启web防御后，为域名分配的转发地址；
9	域名	域名转发规则防护的域名；
10	源站IP信息	源站IP；
11	端口	网站访问端口；
12	HTTPS证书	域名转发规则应用的https证书；
13	接入方式	网站接入方式是反向代理还是透明转发；
14	防护信息	域名转发规则应该的防护规则名称；
15	操作	包括对当前域名转发规则的删除、编辑和防护规则配置；

1.1 新增网站接入

添加域名转发规则前需要先添加网站证书，之后再进行域名转发规则的添加
在【应用安全】栏选择【证书管理】点击页面中的【添加】

添加证书页面，上方公钥，下方私钥。



打开【应用安全】栏中的【网站防护】，在页面点击【添加】

图 1-1 新增接入网站

编号	名称	定义
1	防护域名	需要保护的域名；
2	接入方式	网站接入方式，可选透明转发和反向代理；
3	协议	网站所使用的协议，HTTP、HTTPS、还是WebSocke，同时HTTP支持强制调转HTTPSt；
4	HTTPS强制跳转	当网站用的协议为HTTPS时，可勾选HTTPS强制跳转，使防护域名强制使用HTTPS进行访问；
5	回源方式	防火墙对接入的域名转发规则回源方式，当前支持HTTP、HTTPS；
6	源站IP与端口	防护域名的源站及源站端口；

例如：给网站添加反向代理怎么操作？

首先添加网站的证书，然后查看地址池是否还有可用资源，在【应用安全】的【IP 池管理】中进行查看。

IP 资源不足可以自行添加。

检查有可用资源再进行添加转发规则，

点击【网站防护】，点击【添加】，信息填写完成之后点击确定。返回页面等待 1 分钟转发规则就可以生效。

出现以下状态标准转发规则已生效

2.2、 域名状态

首页-应用安全-域名状态

功能介绍：域名状态中会记录已接入网站的实时状态，根据实时流量状态、请求方法的类型、响应状态、客户请求中的协议进行协议分析记录、以及客户请求中的客户端类型进行分析记录并统计。

编号	名称	定义
1	实时流量状态	记录网站实时的流量信息以及网站的当前连接数和新建连接数；

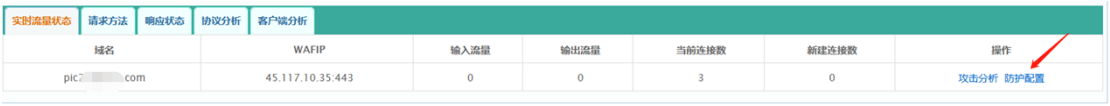
		当接入的网站为透明转发时，WAF IP不会记录任何信息。
2	请求方法	分析请求中的请求方法并进行统计记录。
3	响应状态	记录当前网站的响应状态码。
4	协议分析	对客户端访问完网站的请求中的协议进行记录。
5	客户端分析	根据访问网站的客户端类型进行分析记录，包括windows、linux、MAC、android、IOS和other。

2.1 查看某个防护网站的实时流量状态

打开【应用安全】点击【域名状态】，在域名状态搜索框中输入某一个防护的域名进行搜索查看指定的网站信息。也可以通过 WAF IP 进行指定内容的搜索

2.3 针对域名数据异常添加防护

在【域名状态】中查看到域名的流量数据或异常连接数据，可以直接添加防护，点击【防护配置】根据对业务异常数据的分析可以添加对应的防护。



CC 攻击防护

参数说明

编号	名称	定义
1	状态	cc防护功能开关
2	模式一	JS验证
3	模式二	Cookie验证
4	代理屏蔽	通过代理访问的连接将会被屏蔽
5	爬虫豁免	会检测请求报文中是否有爬虫特征，存在会进行访问频率限制
6	协议检测	检测客户端发送请求中的协议是否属于规范请求。

WEB 应用攻击防护

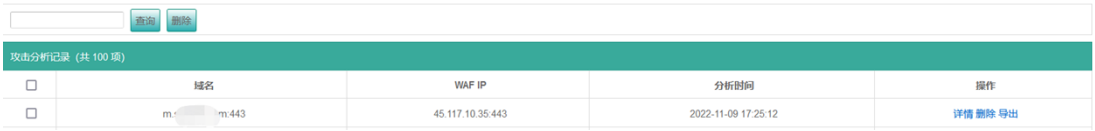
参数说明

编号	名称	定义
1	状态	WEB应用攻击防护功能开关。
2	模式	防护：针对域名攻击进行防护。 告警：针对域名的攻击只进行告警不进行防护拦截。
3	WEB应用规则策略	中等规则：

2.3、 攻击分析

首页-应用安全-攻击分析

功能介绍：通过对防护网站的实时抓包进行攻击分析，攻击记录是在【域名状态】中查看攻击分析产生并记录。



编号	名称	定义
1	查询	查看指定网站的攻击分析记录。
2	删除	删除选中的网站攻击分析记录。

3	详情	查看防护网站的攻击详细信息。
4	删除	删除当前攻击分析录。
5	导出	导出网站的攻击分析记录并已xls表格的格式进行记录。

Comment [A1]: 描述---已修改

3.1 攻击分析查看

当网站被攻击时，攻击分析会对攻击时刻内进行抓包，抓包时间可选。

编号	名称	定义
1	重新分析	将攻击结果进行重新分析，重新分析结果获取时间与设置的统计周期相关；
2	统计周期	在设置的周期内对当前域名统计重新进行统计；
3	导出	与攻击分析记录页面的导出功能一致；
4	URL分析	统计当前周期内请求URL的总数，并以请求次数进行排名，排名只会记录前20名；
7	URL	显示域名请求中的URL链接
8	次数	显示URL出现次数
9	操作	对当前URL请求进行防护；

HTTP 响应分析

编号	名称	定义
1	HTTP响应分析	统计当前周期内HTTP响应次数，并以响应次数进行排名，排名只会记录前20名；
2	CODE-TYPE	HTTP响应代码；
3	次数	HTTP响应代码在请求中出现的次数；
4	操作	对当前请求内容进行防护；

HTTP 请求分析

编号	名称	定义
1	HTTP请求分析	统计当前周期内请求方法种类的总数，并以请求次数进行排名，排名只会记录前20名。统计结果会以GET、POST等请求方法的请求次数进行统计；
2	方法	记录HTTP请求方法；
3	次数	记录HTTP请求中某种请求方法出现的次数；

User-Agent 分析

编号	名称	定义
1	User-Agent分析	统计当前收起内User-Agent种类的总数，并对User-Agent的种类进行排名统计，排名只会记录前20名；
2	User-Agent	显示当前攻击记录内User-Agent内容。

REFERER 分析

编号	名称	定义
1	REFERER分析	统计当前收起内HTTP携带Referer连接的次数，并对所携带的链接出现次数进行排名统计，排名只会记录前20名；
2	REFERER	显示当前攻击记录内，HTTP请求携带REFERER的链接；

客户端流量分析

编号	名称	定义
1	客户端流量分析	统计当前周期内访问的客户端地址总数，并对每个客户端访问的流量大小由高到低进行排名统计，针对异常客户端 IP 可以进行加黑操作
2	批量加黑	根据客户端流量分析结果，针对设置流量数值大于的客户端进行加黑；

客户端连接分析

编号	名称	定义
1	客户端连接分析	统计当前周期内客户端访问当前域名的次数，并对客户端访问域名的次数进行排名统计，针对请求次数异常的客户端 IP 进行加黑，被加黑的客户端 IP 会加到动态黑名单中，默认加黑时间为 9999 秒；
2	批量重置	根据客户端连接数分析，设置连接数大小，对于连接数大于指定数值的进行连接重置；

其他分析

编号	名称	定义
1	其他分析	显示当前攻击记录内的请求协议名称和版本；

攻击分析-防护配置

攻击分析会对 URL、HTTP 响应和请求等进行分析记录，并且每一个记录模块都有一个防护功能。点击【防护】会跳转到对应的模块防护功能面板，可以对异常数据进行防护，决定对当前数据进行加黑还是放行加白。

注：应用安全模块的加黑会自动加到【全局状态】中的【静态黑名单】中。而加白则是加入到【应用安全】模块的【应用防御白名单】

Comment [□□□2]: 透明转发模式如何添加白名单

2.4、 应用防御白名单

首页-应用安全-应用防护白名单

功能介绍：应用防御白名单是通过给客户端地址加白的方式允许客户端对网站进行方案，白名单中客户端 IP 是由防护规则触发执行放行并加白行为添加的，同时支持手动添加白名单

参数说明

编号	名称	定义
1	按客户端地址删除	根据选中的客户端地址删除不同WAF IP下的客户端地址白名单。
2	按WAF IP删除	将白名单中选中的WAF IP下的客户端地址白名单删除。
3	全部释放	释放全部已经加白的客户端地址。
4	导入	将文本中客户端地址加入到应用防御白名单中，格式为：{“wafip”:”x.x.x.x”,”cip”:”x.x.x.x”}。
5	导出	将应用安全防护白名单中的白名单列表以文本txt的格式记录下载。
6	添加	手动给客户端地址进行加白。

2.5、 游戏防护插件

首页-应用安全-游戏防护插件

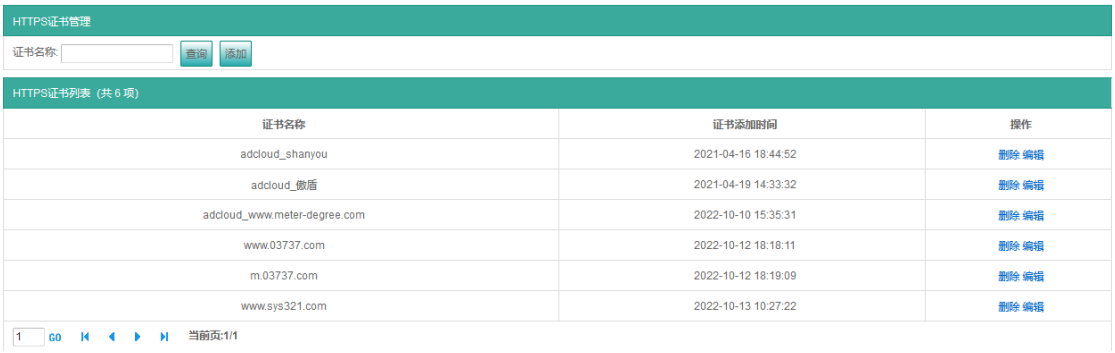
功能介绍：游戏防御插件管理，防火墙系统新游戏插件管理入口，可导入、升级、删除游

戏插件。

2.6、 证书管理

首页-应用安全-证书管理

功能介绍：网站 SSL 证书管理配置页面。HTTPS 业务接入时需上传 SSL 证书，所在上传的 SSL 在本处统一管理。



编号	名称	定义
1	查询	输入指定的证书名称进行管理查看
2	添加	添加网站证书

点击添加

编号	名称	定义
1	**证书名称**	输入对应域名即可
2	**公钥**	证书公钥
3	**私钥**	证书私钥

注意：证书以及私钥的内容不允许以换行结尾。

2.7、 防护引擎管理

首页-应用安全-防护引擎管理

功能介绍：显示、配置、升级当前设备防护引擎

编号	名称	定义
1	查询	通过引擎名称对其进行管理
2	添加	添加防护引擎
3	引擎	引擎名称
4	版本	当前使用的引擎版本
	更新日期	最后一次更新引擎或添加引擎的时间
	操作	对当前使用的防护引擎进行升级

2.8、 Ip 池管理

首页-应用安全-IP 池管理

功能介绍：应用防护 IP 配置，定义网站防护时用到的转发 IP、代理 IP。

编号	名称	定义
1	**转发地址**	代理转发接入模式时，防护域名对对外的 WAF IP 地址。
2	**回源地址**	代理转发接入模式时，用于回源源站地址时使用的 IP 地址（透明模式不需要）

2.9、 虚拟路由配置

首页-应用安全-虚拟路由配置

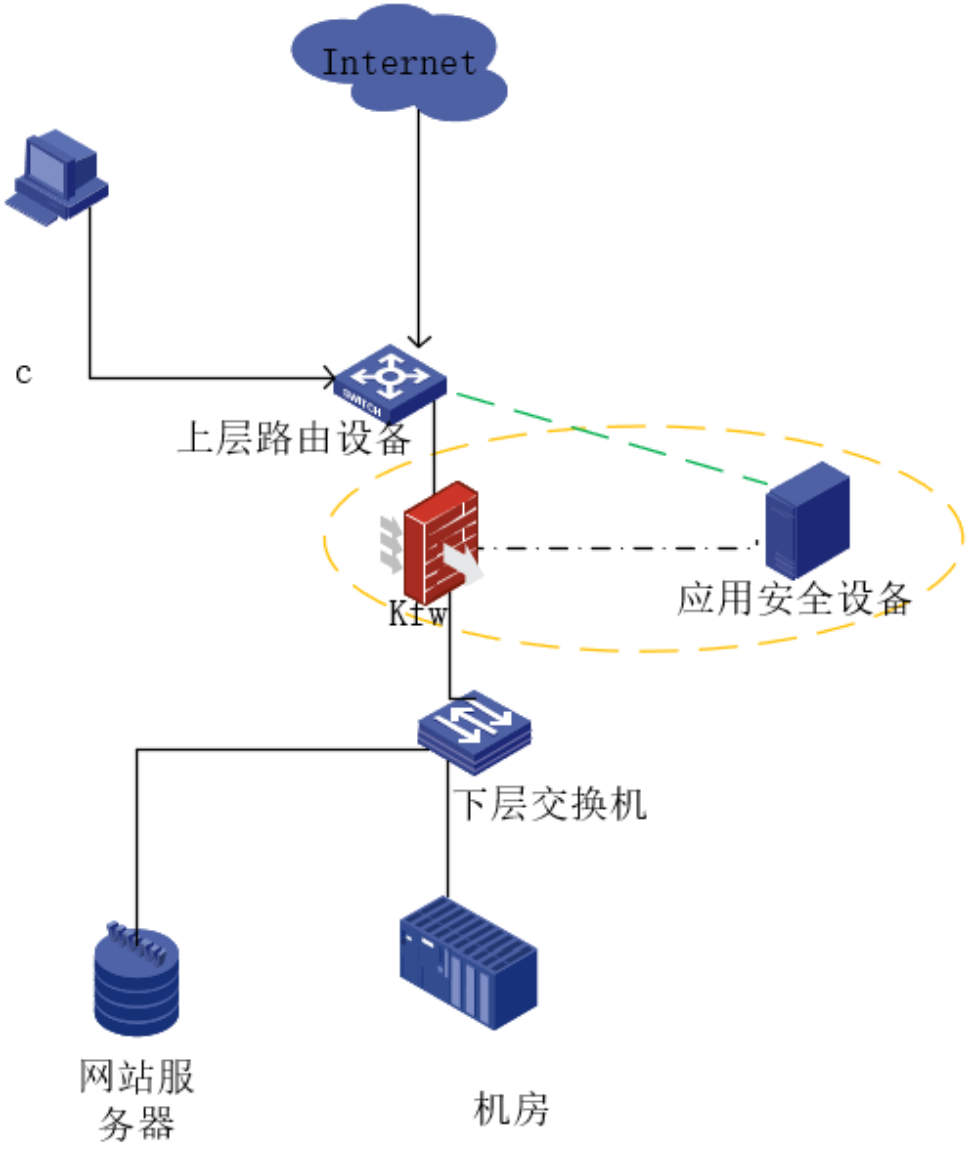
功能介绍：用于应用安全部署到网络环境，当前部署模式支持二层模式和三层模式。

三、 部署要求

3.1应用安全串联环境部署配置

当前应用安全部署模式有两种二层和三层模式

3.1.1 二层模式部署



配置说明：

当使用二层模式在串联环境中部署应用安全设备时，只需要在虚拟路由中填写与防火墙设备上层接口相连的对侧交换机接口 mac 地址。

操作配置：

首页-应用安全-虚拟路由配置

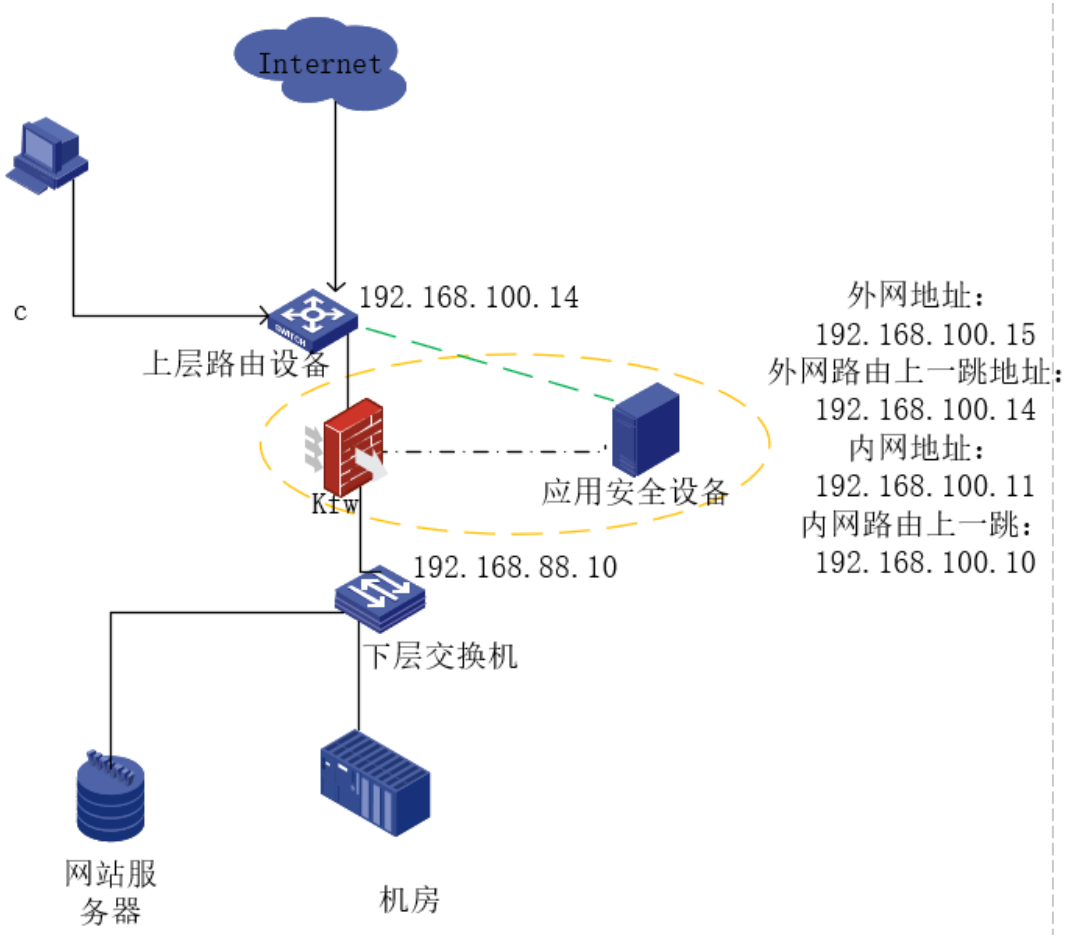
网络模式修改为【二层模式】

【外部网络接口的对等 MAC 地址】填写为防火墙设备与上层路由设备相连的路由器侧的接口 MAC 地址。

3.1.2 三层模式部署

配置说明：

使用三层模式部署时，需要在防火墙的内网网口配置一个虚拟 IP 地址，以及与防火墙相连的上下层接口都需要配置一个虚拟 IP 地址。



配置前提：

首先给上层路由设备与防火墙相连的接口配置上虚拟 IP，然后再给下层交换机与防火墙连线的接口配置上虚拟 IP。

配置说明：

在串联环境中使用三层模式部署时，需要在防火墙的上下层设备接口配置虚拟 IP 地址，然后在应用安全模块的虚拟路由配置中设置与防火墙相连的上下层设备同网段的内外网口虚拟 IP 地址

操作配置：

首页-应用安全-虚拟路由配置

第一步，网络配置改为三层模式，

第二步，设置一个与防火墙设备的上下层设备互联接口同段 IP 给外网地址和内网地址

参考配置如下图所示：

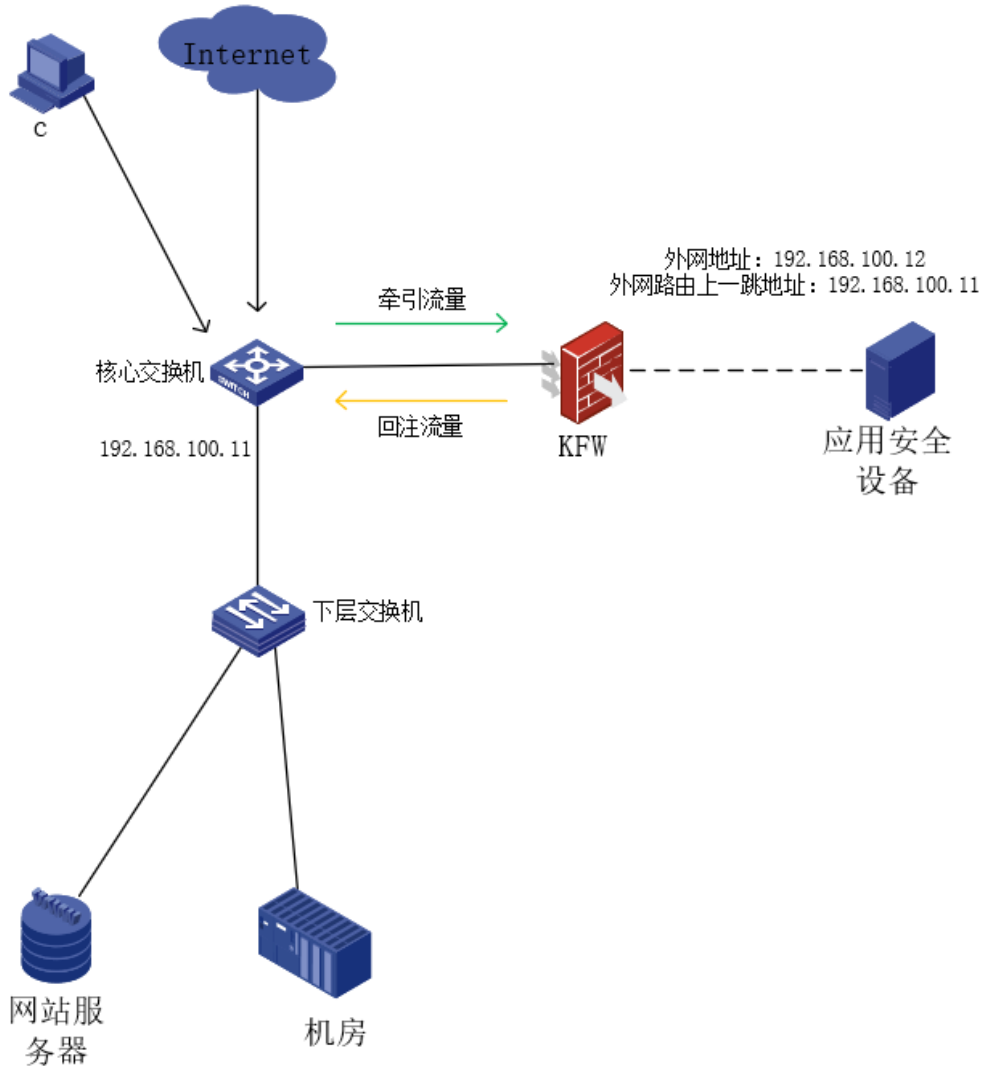
第三步，点击保存，下发配置。

3.2 应用安全旁路环境部署配置

3.2.1 二层部署模式

配置说明：
在旁路环境中使用二层模式部署时，只需要获取与防火墙设备相连的路由设备接口的 MAC 地址。
操作配置：
第一步，获取与防火墙设备相连的路由设备接口 MAC 地址，
第二步，将获取到的 MAC 地址填写在**首页-应用安全-虚拟路由配置**中的外部网络接口的对等 MAC 地址中。

3.2.2　三层部署模式



配置说明：

在旁路环境中使用三层模式部署时，只需要给核心交换机与防火墙互联接口配置一个虚拟 IP，然后再**首页-应用安全-虚拟路由配置**上配置一个外网地址，该外网地址需要与核心交换机的虚拟 IP 地址在同一地址段内。

操作说明：

首页-应用安全-虚拟路由配置

第一步，网络配置改为三层模式

第二步，将分配好的外网地址与掩码填写在【外网地址】内，将核心交换机侧的虚拟 IP 地址填写到【外网路由上一跳地址】。

第三步，保存，下发配置

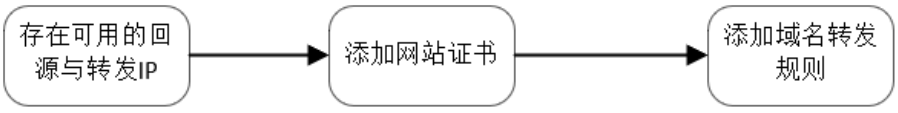
四、 攻击防护配置举例

4、 反向代理转发接入配置举例

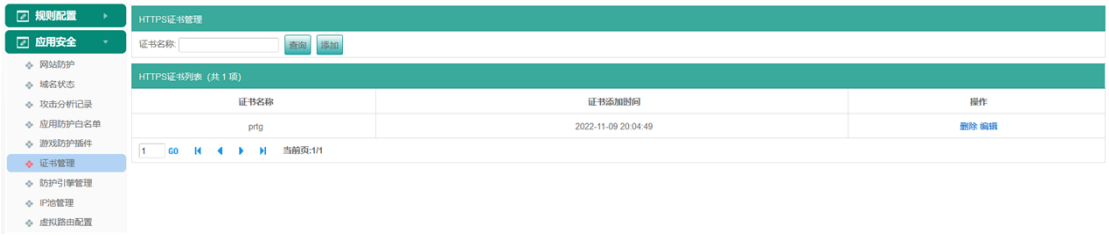
4.1 业务需求

域名：www.text.com
协议：https
源站地址地址：1.1.1.1
源站端口：4431
需求：转发地址只可以通过 https 的方式进行方案，端口 443。

4.2 业务配置



第一步，查看 IP 池是否存在可用的回源地址和转发地址
第二步，添加网站的证书，点击【应用安全】选择【证书管理】添加测试网站的证书



第三步，添加域名转发规则

4.3 业务验证与接入

将域名解析到 WAF　IP 上，打开测试网站进行测试查看是否可以打开，使用 ping 命令测试域名解析地址是否为 WAF IP 地址。

1. 透明转发代接入配置举例

4.1 业务需求

域名：www.text.com
协议：https
源站地址地址：1.1.1.1
源站端口：4431
需求：转发地址可以通过 https 和 http 的方式进行方案，端口 443 和 80。

4.2 业务配置

第一步添加网站证书
第二步添加域名转发规则，选择透明转发

4.3 业务验证与接入

通过网页直接访问网站查看是否能成功访问到，使用 ping 命令查看网站解析地址是否为源站地址。

2. WEB CC 攻击防护配置兴例

自动防御

5.1Javascripts 防护

启用 Javascripts 防护，点击【应用安全】选择【网站防护】，点击【防护规则配置】跳转到【cc 攻击防护】页。

状态开启，模式选择【模式一】，点击确定，Javascripts 防护启用成功。

5.2Set-cookie 防护

启用 set-cookie 防护。点击【应用安全】选择【网站防护】，点击【防护规则配置】跳转到【cc 攻击防护】页。

开启防护点击【状态】表示开启防护，set-cookie 防护选择【模式二】。点击确定，跳转回【网站防护】页可以看到成功开启防护。

5.3web 应用攻击防护

如何开启 web 应用攻击防护？
点击【应用安全】-【网站防护】-【防护规则配置】选择到 web 应用攻击防护页，点击状态开启防护，防护模式可选择【防护】与【告警】

5.4HTTP 关键字段限制

自定义防御

例：拦截 get 请求
点击【应用安全】选择【网站防护】，再点击【防护规则配置】，会跳转到防护页，选择上方菜单栏【自定义防护】具体设置如下：