奇墨科技(ITQM) WAF应用防火墙 产品使用手册

创建时间: 2024年3月14日

修改时间: 2024年4月22日

文件修订记录

版本号	变化状态	简要说明	变更人	变更日期	备注
V0. 1	С	创建文档		2024/3/14	
V1.0	А	补充功能说明		2024/3/22	

变化状态: C-创建, A-增加, M-修改, D-删除

目录

1	L WAF 接入操作	5
	1.1 接入步骤概览:	5
	1.2 步骤 1: 整理接入信息	5
	1.3 步骤 2: 域名添加	6
	1.4 步骤 3:本地测试	9
	1.5 步骤 4: 修改 DNS 解析	
	1.6 步骤 5: 设置安全组	
	1.7 步骤 6:验证测试	
	1.8 步骤 7:业务测试	
2	2 WAF 维护操作	
	2.1 安全概览	17
	2.2 攻击总览	
	全部域名	
	单个域名	
	2.3 黑白名单配置	20
	添加 IP 黑名单	
	编辑 IP 黑名单	
	删除 IP 黑名单	
	添加 IP 白名单	
	编辑 IP 白名单	
	删除 IP 白名单	
	2.4 规则白名单	27
	2.5 攻击日志	29
	<i>背景信息</i>	
	检索攻击日志	
	分析攻击日志	
	攻击处置	
3	3 功能说明	
	3.1 WAF 支持端口列表	
	3.2 日志详情字段说明	
4	1 配置案例	
	4.1 接入网站架构	
	4.2 登录 ITQM 平台	
	4.3 选择 SECOM 安全中心	

4.4	选择应用防护(WAF)
4.5	添加域名40
4.6	关联证书和录入证书(HTTPS)40
4.7	添加域名字段说明
4.8	本地测试44
4.8.1	修改本地 HOSTS44
4.8.2	访问验证45
4.9	修改 DNS
4.9.1	添加 CNAME 记录
4.9.2	记录值获取
4.10	访问测试47
4.11	安全组开放

- 1 WAF 接入操作
- 1.1 接入步骤概览:
- 步骤 1: 整理接入信息
- 步骤 1: 域名添加
- 步骤 2: 本地测试
- 步骤 3: 修改 DNS 解析
- 步骤 4: 设置安全组
- 步骤 5: 验证测试
- 步骤 6: 业务测试

1.2 步骤 1: 整理接入信息

- 1. 确认接入域名使用的协议(http、https、websocket)、端口、证书等信息;
 - a) 若使用 https, 请准备证书;
 - b) 若使用了 websocket, 请在 WAF 域名接入高级配置中启用 websocket 支持;
 - c) 若使用非 http 非标准端口号,请查阅《WAF 支持端口列表》确认端口在支持范围内。
- 2. 确认 WAF 接入后的流量路径,是否有高防、CDN 等设备在 WAF 前端。



- a) 若配有 CDN 或 DDoS 高防,请在 WAF 域名接入中启用代理;
- b) 若配有 CDN 或 DDoS 高防,请按上图把对应设备的配置的回源地址指向下一节点的 cname 或 IP, FW 为透明设备;
- c) 若配有 DDoS 高防,请把 DDoS 高防 IP 配置到 WAF 白名单。

1.3 步骤 2: 域名添加

使用 Web 应用防火墙(WAF)防护您的 Web 业务前,需要先将防护的网站接入到 Web 应用防火墙。未完成接入前,您的 Web 应用防火墙防护将无法生效。本文档将指导您如何在 WAF 中接入域名。

1. 登录 Web 应用防火墙控制台,在左侧导航栏中,选择资产中心 > 接入管理,进入域 名接入页面。

2. 在域名接入页面,单击添加域名,进入添加域名页面。

3. 在添加域名页面, 配置相关基础参数。

新增域名		
* 域名	请输入	
	支持填写一级域名(例如:abc.com)或二级域名(例如:www.abc.com)	
*服务器配置 ⑦	✓ http 80 × 8080 ×	~
	✓ https 443 ×	~
	证书配置: 关联证书	
	高级设置 ~ 洗择HTTPS时,证书配置不能为空	
*代理情况 🕜	● 否 ○ 是	
* 源站地址 ②	 ● IP地址 ○ 域名地址 	
	请输入IP地址	
	请输入源站IPv4或v6地址,用回车分隔多个IP,最多支持输入50个	_1
* 负载均衡策略	● 轮询 ○ IP hash	

字段说明

域名:在域名输入框中添加需要防护的域名 yyyyy. xxxxxx. cn。

服务器配置:协议和端口可按实际情况选择。更多端口添加请参见 接入相关端口。

选择 HTTP 协议, 输入端口。

选择 HTTPS 协议,输入端口后需要配置关联证书、HTTPS 强制跳转和 HTTPS 回源方式。 关联证书:单击关联证书,根据需求选择/导入证书。

HTTPS 强制跳转:如需开启 HTTPS 强跳,需同时勾选 HTTP 和 HTTPS 访问协议。

HTTPS 回源方式: HTTP 或 HTTPS。

说明:

选择 HTTP 协议时可以指定配置回源端口;选择 HTTPS 暂不支持指定配置回源端口,端口和对外开放端口一致。

选择 HTTPS 协议时支持开启回源 SNI 开关,并选择保持源请求 host、修正为源站 host 或自定义 host。

代理情况:根据实际情况选择是否已使用了高防、CDN、云加速等代理。

选择否:表示 WAF 收到的业务请求来自发起请求的客户端。WAF 直接获取与 WAF 建立连接的 IP 地址作为客户端 IP。

选择是: 表示 WAF 收到的业务请求来自其他七层代理服务转发,而非直接来自发起请求 的客户端。为了保证 WAF 可以获取真实的客户端 IP,进行安全分析和防护,您需要进一步设 置客户端 IP 判断方法。

读取请求 Header 字段 X-Forwarded-For (XFF) 中的第一个 IP 地址作为客户端 IP。

获取网络层的 remote_ip 作为客户端的源 IP,防止 XFF 伪造。

获取指定 header 字段的 IP 地址。

说明:

推荐您在业务使用自定义 Header 存放客户端 IP, 并在 WAF 中配置对应 Header 字段。 该方式可以避免攻击者伪造 XFF 字段, 屏蔽 WAF 的防护规则, 有效提高业务的安全性。

源站地址:根据实际需求选择 IP 或域名。

IP: 请输入源站 IPv4 或 IPv6 地址, 用回车分隔多个 IP, 最多支持输入 50 个。

域名:请输入源站域名,注意:源站域名不能和防护域名相同。

加权回源: 当源站地址设置多 IP 回源时。可以选择加权回源方式,并设置不同的权重。 **负载均衡策略:** 默认为轮询方式,可根据实际需求选择轮询、 IP Hash 或加权轮询方式。

4. 配置完基础参数后,可根据需求配置高级参数,单击确定保存。

高级设置 ^	
回源连接方式	○ 短连接 • ● 长连接
	默认使用长连接回源,请确认源站是否支持长连接,若不支持,即使设置长连接,也会使用短连接
写超时时长	- 300 + 秒,范围1~600秒
读超时时长	- 300 + 秒,范围1~600秒
开启HTTP2.0 ⑦	• 否 〇 是
	请确保您的的源站支持并开启了HTTP2.0,否则,即使配置开启2.0也将降级1.1
开启WebSocket	● 否 ○ 是
	如果您的网站使用了Websocket,建议您选择是
开启健康检查	● 否 ○ 是
TLS版本	请选择
加密套件模版	● 通用型模版 ○ 安全型模版 ○ 自定义模版
开启XFF重置	• 否 〇 是
	清空X_Forwarded_For字段值,请确认WAF前无7层代理服务后开启

字段说明

回源连接方式:默认使用长连接回源,请确认源站是否支持长连接,若不支持,即使设置 长连接,也会使用短连接。

开启 HTTP2.0: 请确保您的源站支持并开启了 HTTP2.0, 否则, 即使配置开启 2.0 也将降 级为 1.1。

开启 Websocket: 如果您的网站使用了 Websocket, 建议您选择是。

开启健康检查:企业版以及以上版本,支持开启基于回源 IP 的四层健康检查机制。

开启 XFF 重置: 支持清空 X-Forwarded-For 字段值,请确认 WAF 前无七层代理服务后 开启。

5. 完成配置后,可在域名接入页面看到新添加的域名。当前界面显示未配置 CNAME 记录, 需要 本地验证测试 后,再 修改 DNS 解析。

说明:

Web 应用防火墙将会为每个添加到 Web 应用防火墙的域名(不区分一级域名和二级域名) 分配一个唯一的 CNAME。



1.4 步骤 3:本地测试

本文档将指导您如何在修改 DNS 解析前进行本地测试,防止直接接入时导致生产业务中断。

本地机器访问网站需要做 DNS 解析,在这之前会优先从本地 hosts 文件中获取目标域名 对应的 IP 地址。所以可以用修改 hosts 文件的方式把本地的访问流量导向 Web 应用防火墙, 从而测试经过 Web 应用防火墙访问 Web 站点的线路连通性,避免直接修改 DNS 解析记录, 影响到公网用户对站点的访问。

1. 登录 Web 应用防火墙控制台,在左侧导航栏中,选择资产中心 > 接入管理,在域名 列表中查看接入域名的 CNAME 地址。

saas.itqm.com DNS解析正常 ⊙	-q cloudcjgj.com 🗍	规则:拦截模式 Al引擎:关闭模式	111.230.122.0/24 129.204.26.0/24 查看更多 〉	编辑 删除 防护设置

如需要获取对应域名的 VIP 地址, 可通过 ping 该 CNAME 地址获取。

1.1 在 Windows 操作系统中, 打开 cmd 命令行工具。

1.2 执行以下命令: ping <已复制的 WAF CNAME 地址>。

Microsoft Windows (c) 2019 Microsoft	[Version 10.0.18363.1316] Corporation。保留所有权利。	
C:\Use	ping	dzygj.com
Pingin		with 32 bytes of data:
Reply Trom III	204. Dytes=32 time=0m5 []	- در-با
Reply from 111	254: bytes=32 time=6ms TT	L=53
Reply from 111	254: bytes=32 time=7ms TT	L=53
Reply from 111	254: bytes=32 time=7ms TT	L=53
Ping ⁻ c	r 111 :	₽/]\
Fuckets, sent	= 4, necessary $- 4$, LOST $= 0$ (0)	% IOSS),
Approximate round Minimum = 6ms,	Maximum = 7ms, Average = 6ms	

1.3 在 ping 命令的返回结果中,记录域名对应的 WAF IP 地址,即为后续操作需要的 VIP 地址。

2. 修改 hosts 文件。

在 Windows 下修改 C:\Windows\System32\drivers\etc\hosts, 增加条目。 格式: <WAF VIP 地址> + 空格 + <接入 WAF 中被防护域名>

在 Linux 下 修改 /etc/hosts, 增加条目。 格式: <WAF VIP 地址> + 空格 + <接入 WAF 中被防护域名>

[root@cent	os73 ~]# cat /etc/hosts		
127.0.0.1	localhost localhost.lo	caldomain localhost4	localhost4.localdomain4
::1	localhost localhost.lo	caldomain localhost6	localhost6.localdomain6
	190 waf.qcloudwaf.com		
[root@cent	os73 ~]# 📕		

在 MAC 下修改 /etc/hosts, 打开访达, 单击前往 > 前往文件夹, 修改 /etc/hosts, 在弹框中输入 /etc, 进入 /ect 目录且修改下面的 hosts 文件。

格式: <WAF VIP 地址> + 空格 + <接入 WAF 中被防护域名>



3. 访问测试。 在本地电脑上访问 Web 站点,若站点能够正常打开,说明 Web 应用防火 墙访问 Web 源站的线路连通性正常。

3.1 在浏览器中输入下面的网址并访问。

http://接入域名/?test=alert(123)

3.2 浏览器返回阻断页面,说明 Web 应用防火墙防护功能正常。

说明

该拦截页面,可以通过访问: Web应用防火墙(WAF)默认提示页面获取。



很抱歉,您提交的请求可能对网站造成威胁,请求已被管理员设置的策略阻断

本页面为腾讯T-Sec Web应用防火墙(WAF)默认提示页面,如有疑问请联系网站管理员并提供UUID信息 您的请求UUID为

1.5 步骤 4: 修改 DNS 解析

本文档将指导您如何修改 DNS 的解析记录, 使公网用户访问网站的流量经过 Web 应用防 火墙的防护。 为了使公网用户访问网站的流量经过 Web 应用防火墙的防护,需要修改 DNS 的解析记录。 下面以在腾讯云 DNS 解析 DNSPod 上修改测试站点 waf.qcloudwaf.com 的 DNS 解析为例, 说明配置步骤。

1. 登录 DNS 解析 DNSPod 控制台,在左侧导航栏中,单击我的域名,找到需要接入 Web 应用防火墙的域名 technical support.cn,单击解析进入解析配置界面。

添加域名	购买解析套餐批量操作▼				
	域名	解析状态 ()	解析套餐	最后操作时间	操作
	technicalsupport.cn	正常解析	免费版	2021-11-22 11:36:46	解析 升级套餐 D 更多 ▼

2. 单击添加记录。

勪	記录	快速添加网站/邮箱解析 暫停	开启一删除	分配至项目				青榆入您要搜索的记
	主机记录	记录类型 ▼	线路类型	记录值	MX优先级	TTL (秒)	最后操作时间	操作
			默认	ALC: NO. 171-10.	-	-	2019-07-24 15:25:19	修改 暂停 删除

3. 在当前配置页面中填写相应信息。

3.1 主机记录填写对应网站的主机记录,本例中需要防护的是 saas.technicalsupport.cn, 即填写 saas。

saas	CNAME	1949Y	物如下提示造填		600	-	保存 取消		
主机记录	记录类型 ▼	线路类型	记录值	MX优先级	TTL (#)	番后操作时间	操作		
3.2 记录类	关型选择	CNAME.							
主机记录	记录类型 ▼	线路类型	记录值	MX优先级	TTL(秒)	最后操作时间	操作		
按如下提示	CNAME	默认	按如下提示	-	600	-	保存取消		
提示 将城名指向云服务器 将城名指向另一个城 建立邮箱请选择「M2	提示								
A	用来指定域名的IP	/4地址(如:8.8.8.8)) , 如果需要将域名指向-	一个IP地址,就需要注	泰加A记录。				
CNAME	如果需要将域名指	向另一个域名,再由另	引一个域名提供ip地址,就	就需要添加CNAME记	录。				
МХ	如果需要设置邮箱	,让邮箱能收到邮件,	就需要添加MX记录。						

3.3 记录值填写 Web 应用防火墙分配的 CNAME 域名,分配的 CNAME 域名样式为: xxxx.qcloudcjgj.com。

主机记录	记录类型 ▼	线路类型	记录值	MX优先级	TTL (秒)	最后操作时间	操作
saas	CNAME	默认	xxxx.qcloudcjgj.com	-	600	÷	保存取消
揭示 填写一个域名,如: cloud tence	ent.com						

说明:

CNAME 域名可以前往 接入管理 > 域名接入页面,选择目标域名,在接入信息列获取。

	saas.itqm.com DNS解析正常 📀	cloudcjgj.c	.q	规则:拦截模式 Ai引擎:关闭模式	111.230.122.0/24 129.204.26.0/24 查看更多 〉	编辑	删除防	护设置
3.	4 填写完毕	≦后,	单击保存。					

修改完成之后,待 DNS 记录生效,Web 应用防火墙即可对访问网站的流量进行防护了。
 同时,Web 应用防火墙检测到被防护域名解析正常之后,Web 应用防火墙控制台 上将提示"正常防护"。

2021-12-10 16:39:03

说明:

saas

DNS 记录生效需要 10 分钟左右时间。

saas.technicalsupport.cn 后 正常防护 规则: 拦截模式 $\overline{}$

1.6 步骤 5: 设置安全组

本文档将指导您如何设置安全组, SAAS-WAF 中需要用户在各产品安全组(如: CLB、防火 墙等安全设备)中放通 WAF 回源 IP, 仅允许来自 Web 应用防火墙的流量访问网站。

安全组是腾讯云提供的实例级别防火墙,可对任意云服务器进行入或出流量控制。在安全 组中设置仅允许来自 Web 应用防火墙的流量访问网站,可避免攻击者绕过 Web 应用防火墙直 接攻击网站源站。 下面以在安全组中放行 Web 应用防火墙的回源 IP 111.230.27.90 为例, 说明配置过程。

注意

回源 IP 可在 Web 应用防火墙控制台的 域名列表 中查看。

1. 登录 云服务器控制台, 在左侧目录中, 单击安全组。

2. 进入安全组页面,单击新建,根据要求填写信息,模板选择自定义,输入安全组的名称(例如 my-security-group),填写相关备注,填写完成后,单击确定。

新建安全组

模板	自定义	¥
名称	请输入安全组名称	
所属项目	默认项目	*
备注		
高级选项 🕨		
显示模板规	则	
	确定	取消

- 3. 在安全组列表中,找到新建的安全组,单击其 ID 进入详情页。
- 4. 在入站规则页面中,单击添加规则。

全组规则	关联实例				
入站规则	出站规则				
添加规则	导入规则	排序	删除	一键放通	教我设置已
来源 ()	8				协议端口①

5. 在弹出框中填写相关信息,类型选择 "HTTP(80)",来源中填写需要放行的回源 IP, 根据需求填写端口及策略,填写完毕后,单击完成。

添加入站规则

类型		来源 🛈	协议端口 ①	策略	备注	
自定义	•	回源ip	TCP:443,80	允许 ▼		
自定义	•	0.0.0.0/0	TCP:443,80	拒绝 🔻		٥
			+新增一行			

6. 单击选项卡中的关联实例,在云服务器页面下,单击新增关联。

安全组规则	关联实例		
云主机(1)	弹性网卡(0) ③	云数据库Mysql(0)	负载均衡(0)
新增关联	批量移出		

7. 在弹出框中选择需要绑定的云服务器,单击确定即可。

封译	安全组:	1000	"要绑定的实例			已选择(1/100)			
輸	入名称/ID/IP (化	又显示未关联该家	安全组的实例)	Q		实例ID/名称	所属网络	主 IP 地址	
	实例ID/名称	所属网络	主 IP 地址	Â					×
2		Concession in the	(1), (6, 1), (7), (6), (6, 1), (7), (7), (6), (6), (7), (7), (6), (7), (7), (7), (7), (7), (7), (7), (7			respire.	Sec.e.m.	100,000,000	
	the second se	Sec. Pri			\leftrightarrow				
		Sec. 10	$\begin{array}{c} (1) & (1, 1) & (1, 1) \\ (1) & (1, 1) & (1, 1) \\ (2) & (1, 1) & (2) \end{array}$						
	Ruffer.	(martin)		•					

>

或者您还可以进入 云服务器列表页,查看或修改某云服务器已绑定的安全组,在列表页 选择需要调整安全组的云服务器 ID,在右侧操作栏,选择更多 > 安全组 > 配置安全组,选 择安全组进行绑定。



1.7 步骤 6: 验证测试

本文档将指导您如何验证 SaaS 型 WAF 是否生效。

1. WAF 通过域名和源站进行绑定,对流量进行防护。验证 SaaS 型 WAF 是否生效,请先确保本地电脑可以正常访问在 SaaS 不同实例下添加的域名。

2. 在浏览器中输入网址 http:// saas.technicalsupport.cn/?test=alert(123)并访问, 浏览器返回阻断页面,说明 Web 应用防火墙防护功能正常。

注意

saas.technicalsupport.cn 为本案例中域名,此处需要将域名替换为实际添加的域名。



很抱歉,您提交的请求可能对网站造成威胁,请求已被管理员设置的策略阻断

本页面为腾讯T-Sec Web应用防火墙(WAF)默认提示页面,	如有疑问请联系网站管理员并提供UUID信息
您的请求UUID为	

1.8 步骤 7: 业务测试

本文档将指导您如何验证 SaaS 型 WAF 接入后确保业务访问不被拦截。 对接入的业务系统的关键业务流程进行验证,确保攻击日志中不存在拦截的记录。

2 WAF 维护操作

2.1 安全概览

- 1. 登录 Web 应用防火墙控制台,在左侧导航栏中,选择概览,进入概览页面。
- 2. 在概览页面, 左上角选择对应实例或域名, 即可查看该实例或域名的概览信息。

± movie == M 2/20 ↑ 添加暖名	2/2 [^]	
用启防护域名数 2 ↑ Martin mpi	未开启防护域名数 0 ↑ 11.05719	

2.2 攻击总览

全部域名

1. 当安全概览为全部域名时,攻击总览统计数据为全局攻击数,统计周期可以通过筛选显示。

域名 全部域	名 ~	统计时间	2024-04-21 00:00:00 至 202	4-04-21 23:59:55	今天 昨天 近7	Ŧ		
攻击 总览								
全部请求 3.57	万次		Web攻击 0 次			ссът 0 ж		
基础安全分	析							
1								
0.8								
0.6								
0.4								
0.2								
0 2024-04-21	2024-04-27 0	2024-04-21 04:5	2024-04-21 07:15:00	2024-04-21;	2024-04-21 14: 2:05:00	2024-04-21 16:55:00	2024-04-21 19:20:00	2024-04-21 21:45:00
			— We	b攻击 — CC攻击 — 访	问控制			

2. 同时,在页面下方可以查看域名 Web 攻击次数 TOP5(次)、攻击来源 IP TOP5(次)、 域名 CC 攻击次数 TOP5(次)、攻击类型占比等信息。



字段说明:

域名 Web 攻击次数 TOP5(次):展示全部实例中受到攻击最多的5个域名。 攻击来源 IP TOP5(次):展示全部实例中受到攻击最多的5个 IP。 域名 CC 攻击次数 TOP5(次):展示全部实例中受到攻击最多的5个域名。 攻击类型占比:展示全部实例中攻击类型的分布。

单个域名

1. 当安全概览为单个域名时,攻击总览统计数据为单个域名受到攻击数,统计周期可以通过筛选显示。

域名	saas.itqm.com	~	统计时间	⑤ 2024-04-21 00:00:00 至 2024-04-21 23:59:59	今天	昨天	近7天
	(



2. 同时,在页面下方可以查看攻击来源 IP TOP5(次)、攻击类型占比等信息。

」 攻击来源 <mark>10₽3</mark>	攻击类型占比
重无数据	暫无数据

字段说明:

攻击来源 IP TOP5(次):展示全部实例中受到攻击最多的5个 IP。

攻击类型占比:展示全部实例中攻击类型的分布。

2.3 黑白名单配置

Web 应用防火墙的黑白名单功能,指的是对经过 Web 应用防火墙防护域名的访问源 IP 进行黑白名单设置,以及对多个 HTTP 特征进行精准白名单设置,主要功能包括: IP 黑白名单设置和精准白名单设置。

IP 黑白名单设置,支持设置基于域名或全局的 IP 黑白名单规则,支持网段设置。

精准白名单设置,支持从 HTTP 报文的请求路径、GET 参数、 POST 参数、 Referer 和 User-Agent 等多个特征进行组合,通过特征匹配来对特定公网用户的访问进行加白。

同时,可以添加基于域名的黑白名单或基于全局的黑白名单,生效优先级说明如下所示: 黑白名单的优先级仅低于 Web 应用防火墙精准白名单策略,高于其他检测逻辑。

黑白名单优先级从高到低顺序:精准白名单策略 > 全局白名单 > 域名白名单 > 域名 名单 > 全局黑名单 > WAF 其他模块。

添加 IP 黑名单

1. 登录 Web 应用防火墙控制台,在左侧导航栏中,选择配置中心 > 黑白名单。

2. 在黑白名单页面, 左上角选择需要防护的域名, 单击 IP 黑名单。

SecOM安全中心	Ē	SecOM安全中心 / 应用防护(WAF) /	黑白名单						
受 安全洞察	\sim	域名 saas.itqm.com	~						
国 响应与分析	\sim								
◎ 安全加固	\sim	IP白名单 I P黑名单 规则白	名单						
🗋 合规与测评	~								
📋 应用防护(WAF)	^	+ 添加地址							
概览		IP地址	来源	截止时间	更新时间				
攻击日志									
接入管理									
安全防护				¢					
黑白名单					暂无数据				

3. 在 IP 黑名单页面,单击添加地址,进入添加黑名单页面。

4. 在添加黑名单页面,配置相关参数,单击确定。

新增黑名单	<u> </u>
* 域名	saas.itqm.com
* 地址	请输入
*截止时间	● 长期生效 ○ 限定日期
备注	请输入备注,最多支持50字 0/50
	取消 确定

字段说明:

IP 地址: 支持任意 IP 地址,例如 10.0.0.10 或 FF05::B5; 支持 CIDR 格式地址,例如 10.0.0.0/16 或 FF05:B5::/60,使用换行符进行分隔,一次最多添加 20 个。

说明:

选择域名为全局时,添加的 IP 地址或 IP 段为全局的黑白名单。

各个版本每个域名规格限制分别为:1000条/域名、5000条/域名,每个 IP 地址或者 IP 段占用一条额度。

截止时间:永久生效或限定日期。

备注: 自定义, 50个字符以内。

编辑 IP 黑名单

1. 在 黑白名单页面, 左上角选择需要防护的域名, 单击 IP 黑名单。

2. 在 IP 黑名单页面,选择所需 IP 地址,单击操作列的编辑,修改截止时间和备注, 单击确定保存。

IP地址	来源 🔻	截止时间	更新时间 \$	备注	操作
	自定义	永久生效	2021-12-14 11:13:15	测试	编辑删除
	自定义	生效中,截止时间:2021-12-24 10:55:58	2021-12-14 10:56:09	测试	编辑删除

删除 IP 黑名单

1. 在 黑白名单页面, 左上角选择需要防护的域名, 单击 IP 黑名单。

2. 在 IP 黑名单页面, 支持删除单个、部分、全部地址, 具体操作如下:

单个:选择单个 IP 地址,单击删除地址或操作列的删除,弹出"确认删除"弹窗。

说明:

删除后将无法恢复,重新添加才能生效。

濍	別地址 全部删除	导入数据 导出全部筛选结果				多个关键字用器线 T 分隔,多个过速标签用固车键分隔 Q 🗘
	IP地址	来源 ▼	截止时间	更新时间 \$	备注	操作
		自定义	永久生效	2021-12-14 11:13:15	测试	编辑图》
		自定义	生效中,截止时间:2021-12-24 10:55:58	2021-12-14 10:56:09	测试	编辑 動除

部分:选择多个 IP 地址,单击删除地址,弹出"确认删除"弹窗。

说明:

删除后将无法恢复,重新添加才能生效。

添加地址 副除地址 全部翻	除导入数据导出全部游选结果				多个关键字用显线 17 分隔,多个过诸顷签用回车键分隔	Q
V IP地址	来源 〒	截止时间	更新时间 \$	备注	部件	
	自定义	永久生效	2021-12-14 11:13:15	剡试	編載 删除	
	自定义	生效中,截止时间:2021-12-24 10:55:58	2021-12-14 10:56:09	测试	编辑删除	

全部:单击全部删除,弹出"确认删除"弹窗。

注意

此操作将清除当前域名下所有的 IP 黑白名单信息,请谨慎操作!删除后将无法恢复,重 新添加才能生效。

3. 在"确认删除"弹窗中,单击确定,即可删除地址。

添加 IP 白名单

1. 登录 Web 应用防火墙控制台,在左侧导航栏中,单击配置中心 > 黑白名单,进入黑白名单页面。

2. 在黑白名单页面, 左上角选择需要防护的域名, 单击 IP 白名单, 进入 IP 白名单页面。

SecOM安全中心	Ē	SecOM安全中心 / 应用防护(WAF)	/ 黑白名单		
④ 安全洞察	\sim	域名 saas.itgm.com	\sim		
⑤ 响应与分析	\sim				
◎ 安全加固	\sim	IP白名单 IP黑名单 规则	旧名单		
🗋 合规与测评	\sim				
🗐 应用防护(WAF)	^	+ 添加地址			
概览		IP地址	来源	截止时间	更新时间
攻击日志					
接入管理					
安全防护				<	?
黑白名单					暂无数据

3. 在 IP 白名单页面,单击添加地址,进入添加白名单页面。

4. 在添加白名单页面,配置相关参数,单击确定。

新增白名皇	É.	<
* 域名	saas.itqm.com	
* 地址	请输入	
	∠ 支持任意IP地址,例如10.0.0.10或FF05::B5;支持CIDR格式地址,例如 10.0.0.0/16或 FF05:B5.:/60,使用换行符进行分隔,一次最多添加20个	
* 截止时间	● 长期生效 ○ 限定日期	
备注	请输入备注,最多支持50字 0/50	
	取消 确定	

参数说明

IP 地址: 支持任意 IP 地址,例如 10.0.0.10 或 FF05::B5; 支持 CIDR 格式地址,例如 10.0.0.0/16 或 FF05:B5::/60,使用换行符进行分隔,一次最多添加 20 个。

说明

选择域名为全局时,添加的 IP 地址或 IP 段为全局的白名单。

各个版本每个域名规格限制分别为:1000条/域名、5000条/域名,每个 IP 地址或者 IP 段占用一条额度。

截止时间:长期生效或限定日期。

备注: 自定义, 50个字符以内。

编辑 IP 白名单

1. 在 黑白名单页面, 左上角选择需要防护的域名, 单击 IP 白名单, 进入 IP 白名单页面。

2. 在 IP 白名单页面,选择所需 IP 地址,单击操作列的编辑,修改截止时间和备注, 单击确定保存。

添加地址 翻除地址 全部删除	导入数据导出全部描述结果				多个关键字用篮线 11分码,多个过滤标签用回车键分码	Q	φ
IP地址	来源 ▼	裁止时间	更新的问 \$	香注	操作		
	自定义	永久生效	2021-12-14 11:38:59	测试	编辑		
	自定义	永久生效	2021-12-14 11:38:46	测试	编辑制绘		

删除 IP 白名单

1. 在 黑白名单页面, 左上角选择需要防护的域名, 单击 IP 白名单, 进入 IP 白名单页面。

2. 在 IP 白名单页面, 支持删除单个、部分、全部地址, 具体操作如下:

单个:选择单个 IP 地址,单击删除地址或操作列的删除,弹出"确认删除"弹窗。

说明

删除后将无法恢复,重新添加才能生效。

添加地址	全部删除 导入数据 导出全部	财物还结果		多个关键	字用篮线 17 分隔,多个过速标签用回车键分隔
IP地址	来源 ▼	截止时间	更新时间 \$	备注	操作
	自定义	永久生效	2021-12-14 11:38:59	测试	编辑》
	自定义	永久生效	2021-12-14 11:38:46	测试	編輯 散除

部分:选择多个 IP 地址,单击删除地址,弹出"确认删除"弹窗。

说明

删除后将无法恢复,重新添加才能生效。

添加地址 金部潮除	导入数据 导出全部筛选结果				多个关键学用整线 T 分隔,多个过端标签用回车键分隔 Q 🗘
✓ IP地址	来源 🍸	截止时间	更新时间 \$	备注	操作
	自定义	永久生效	2021-12-14 11:38:59	測试	编辑题论
	自定义	永久生效	2021-12-14 11:38:46	測试	编辑 删除

全部:单击全部删除,弹出"确认删除"弹窗。

注意

此操作将清除当前域名下所有的 IP 黑白名单信息,请谨慎操作!删除后将无法恢复,重新添加才能生效。

3. 在"确认删除"弹窗中,单击确定,即可删除地址。

2.4 规则白名单

在生产环境中如出现正常访问流量被 WAF 规则引擎拦截时,可以通过黑白名单中的规则 白名单进行加白相应规则,加白该规则后就不会被拦截。

1. 登录 Web 应用防火墙控制台,在左侧导航栏中,单击配置中心 > 黑白名单。

2. 在黑白名单页面, 左上角选择需要防护的域名, 单击规则白名单。

ა.	仕方	死则日名	囬, 平击添加;	观则,评 出邓	加日名半坪面	0	
Sec	OM安全中	P心 / 应用防护(WAF) / 黑白名单					
-	域名 s	saas.itqm.com					
	IP白名单	IP黑名单 规则白名单					
1	+ 添加	血规则					请输入加白规则ID
		加白规则ID	匹配方式	匹配路径	规则开关	修改时间	操作
		50080031	前缀匹配			2024–04–07 14:58:45	编辑 删除
		50080033	前缀匹配			2024–04–07 14:52:39	编辑删除
		50250003	前缀匹配			2024–04–01 18:19:42	编辑 删除

3. 在规则白名单页面,单击添加规则,弹出添加白名单弹窗。

4. 在添加规则弹窗中, 配置相关参数, 单击确定。

新增白名单规则	×	
* 白名单规则ID	请选择	
匹配方式	完全匹配	
* URL路径	请输入以/开头的路径,128个字符以内,不要包含域名	
白名单开关		
	取消 确定	

字段说明:

白名单规则 ID: 填写需要加白的规则 ID, 一条策略可添加最多 10 个规则 ID。获取方法 如下所示:

在安全防护页面,选择所需规则 ID,复制。

SecOM安全中心	ē	SecOM安全中心	/ 应用防护(WAF) /	安全防护							
攻击日志		域名 saas	.itqm.com	~							
接入管理											
安全防护		WEB安全(262	20) 🔵 访问控	割(0) () Ci	C防护(0) 💽						
黑白名单		×									
主机安全	^	规则引擎	AI引擎 (即将上线)								
概览		防护模式:	观察模式 💿	拦截模式	防护等级: 正常	~	恶意文件检测: 💿 否 🔾	是			
安全事件		68 批量启	用 認 批量禁/	用 查看攻击日 [Б					请输入CVE编号	
日志分析		- #		市主米刑	相同社会	○√に信号	修改时间	察听+钟 尼士(61)	π×	场 <i>中</i>	
授权管理			Clinity	以田英里	260,001 m. AL	UVE编号	1912(13[0]	M[10]	77	DRTF	
四 平台管理	^	5	0270083	一般攻击	本规则用于检测数据库 文件敏感信息访问行 为,本规则匹配的目标	-	2024–04–18 15: 29:54	2024–04–17 21:0 1:28		加白名单 查看	自名单
云账号管理					是URL						
接入网关			0340082	已知器占	本规则用于检测Restful api 敏感信息访问行	_	2024-04-18 15:	2024-04-17 21:0		加白名的 奋骤	白之田
告警中心	~		004002	D7#99777	为,本规则匹配的目标 是URL		29:54	1:28		MDD# 24	

在日志页面,选择所需数据,复制该数据的 rule_id。

日志详情		×
method	GET	
pan	saas.itqm.com	
risk_level	高危	
rule_id	10000063	
rule_name		
scene_id		
2 scene_module		
z sec_chain		
.2		
status	拦截	
uri	/alert(xsss)	
user_agent		
1		
2		ļ

匹配方式: 加白 URL 路径的匹配方式,支持完全匹配(默认)、前缀匹配和后缀匹配。 URL 路径: 需要加白的 URL 路径,同一个域名下 URL 不可重复添加。

白名单开关: 白名单策略生效开关, 默认为开启。

2.5 攻击日志

本文为您介绍如何使用攻击日志进行攻击日志索引、快速分析和查询。

背景信息

Web 应用防火墙默认提供攻击日志功能,详细记录攻击产生的时间、攻击源 IP、攻击类型及攻击详情等信息。攻击日志仅支持查询或导出最近 30 天日志。攻击日志支持全文检索、 模糊搜索和组合条件搜索等检索方式,同时支持根据检索条件下载日志,支持百万级日志下载。

检索攻击日志

1. 登录 Web 应用防火墙控制台,在左侧导航栏中,选择攻击日志。

 在日志服务页面,您可以根据需要,选择域名、攻击类型、执行动作、风险等级及时 间维度等信息,筛选查看攻击日志。

SecOM安全中心 / 应用防护	'(WAF) / 攻击日志							
攻击日志				全	部域名 🗸 🗸	© 2024-04-01	1 00:00:00 至 202	4-04-21 23:59:59
攻击类型 请选择			~ 执行	亍动作 请选择			~	
风险等级 请选择			~					搜索重置
日志时间	攻击IP	执行动作	攻击IP所属国家	攻击IP所属省份	攻击IP所属城市	攻击类型	风险等级	操作
2024-04-19 14:53:1	11	拦截	中国	广东	广州	XSS攻击	高危	查看详情 源IP封禁
2024–04–19 09:40:	52	拦截	中国	广东	广东	已知弱点	中危	查看详情 源IP封禁
2024–04–18 19:31:1	2	拦截	中国	广东	广州	XSS攻击	高危	查看详情 源IP封禁

字段名称	字段说明
域名	支持多选, 默认显示全部域名。
攻击类型	支持多选,默认为全部攻击类型,攻击类型包括各个安全模块产生 的观察和拦截日志。
执行动作	单选,默认为全部执行动作,包括观察、重定向、人机识别、拦截 四种类型。
风险等级	单选, 默认为全部风险等级, 包括高危、中危和低危三种类型。
时间范围	默认为近一小时,支持筛选最近时间及相对时间。
3. 设置	置完成检索条件,单击检索,即可查看检索结果。

日志时间	攻击IP	执行动作	攻击IP所属国家	攻击IP所属省份	攻击IP所属城市	攻击类型	风险等级	操作
2024–04–19 14:53:11		拦截	中国	广东	广州	XSS攻击	高危	查看详情 源IP封禁
2024-04-19 09:40:52		拦截	中国	广东	广东	已知弱点	中危	查看详情 源IP封禁
2024–04–18 19:31:12		拦截	中国	广东	广州	XSS攻击	高危	查看详情 源IP封禁
2024–04–18 18:56:35		拦截	中国	湖南	长沙	一般攻击	高危	查看详情 源IP封禁
2024-04-18 18:55:50		拦截	中国	湖南	长沙	一般攻击	高危	查看详情 源IP封禁
2024–04–18 18:55:14		拦截	中国	广东	广州	XSS攻击	高危	查看详情 源IP封禁

分析攻击日志

1. 在攻击日志数据列表右方,单击查看详情,即可查看日志详情。

ά

日志详情	×	٦
action	र्जा श्रेष्ट	24
action	观示	攻
appid	1319853108	
args_name	URL	
attack_category	-	
attack_content	{"field":"N\/A","sid":"050270034","action":3,"mc":"一般攻	
	击","match":"\/H7mQXNOr.php3","target":"URL","data":"\/	
	H7mQXNOr.php3","type":1,"offset":0,"level":3,"sc":"敏感文	e
	件读取"}	
attack_ip	119.34.177.116	
attack_place	URL	
attack_time	2024-04-21T01:06:05+08:00	_
attack_type	一般攻击	

攻击处置

1. 在攻击日志数据列表中,支持单击操作列中的源 IP 封禁,快速添加处置规则。

攻击日志				全部域名	~ @	2024–04–21 00	:00:00 至 2024-	-04-21 23:59:59
日志时间	攻击IP	执行动作	攻击IP所	攻击IP所…	攻击IP所…	攻击类型	风险等级	操作
2024–04–21 01:06:05		观察	中国	广东	广州	一般攻击	中危	查看详情源IP封禁
2024–04–21 01:06:02		观察	中国	广东	广州	一般攻击	中危	查看详情 源IP封禁
2024–04–21 01:06:02		观察	中国	广东	广州	一般攻击	低危	查看详情 源IP封禁

源 IP 封禁: 支持一键添加 IP 黑名单, 拦截对应 IP 的访问, 完成修改后, 单击确定。

" 現石	saas.itqm.com V
* 地址	请输入
	之 支持任意IP地址,例如10.0.0.10或FF05:: B5;支持CIDR格式地址,例如 10.0.0.0/16或 FF05: B5.: /60,使用换行符进行分隔,一次最多添加20个
* 截止时间	● 长期生效 ○ 限定日期

3 功能说明

3.1 WAF 支持端口列表

WAF 套餐端口支持情况,可以在控制台进行查看并配置。

1. 登录 Web 应用防火墙控制台,在左侧导航中,选择 Web 安全防护 > 防护设置,进入防护设置页面。

2. 在防护设置页面,单击添加域名,进入添加域名页面。

 在添加域名页面的"服务器配置"中,选择对应的协议查看并配置端口,一个域名最 多可配置5个端口。

WAF 高级版默认支持 HTTP (80/8080) 和 HTTPS (443/8443) 标准端口防护,不支持非标端口。

WAF 企业版和旗舰版套餐中除了默认支持 HTTP(80/8080)和 HTTPS(443/8443)标准端口防护外,还支持非标端口。 企业版和旗舰版支持的所有端口详情如下:

协议名称 端口

HTTP 协议	80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 97, 800, 805, 808, 1000, 1090, 2020, 3333, 3501, 3601, 5000, 5222, 6001, 6666, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7007, 7008, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7040, 7070, 7081, 7082, 7083, 7088, 7097, 7510, 7621, 7777, 7800, 8000, 8002, 8003, 8004, 8005, 8006, 8007, 8008, 8009, 8010, 8011, 8012, 8020, 8021, 8022, 8060, 8025, 8026, 8060, 8077, 8078, 8080, 8081, 8082, 8083, 8086, 8087, 8088, 8089, 8090, 8106, 8181, 8182,
HTTP 协议	8004、8005、8006、8007、8008、8009、8010、8011、8012、8020、 8021、8022、8060、8025、8026、8060、8077、8078、8080、8081、 8082、8083、8086、8087、8088、8089、8090、8106、8181、8182、 8184、8210、8215、8334、8336、8445、8686、8800、8888、8889、 8999、9000、9001、9002、9003、9021、9023、9027、9037、9080、 9081、9082、9180、9182、9200、9201、9205、9207、9208、9209、 9210、9211、9212、9213、9898、9908、9916、9918、9919、9928、 9929、9939、10000、10001、10080、10083、12601、20080、20083、 25060、28080、28080、33702、48800、52301
HTTPS 协议	443、4443、5100、5200、5443、6443、7443、8084、8085、8091、 8442、8443、8553、8663、9443、9550、9553、9663、10803、18980

3.2 日志详情字段说明

字段名称	字段说明
host	客户端访问的域名信息。
uri	请求 URI : 用于标识请求资源的字符串。
attack_ip	攻击源 IP: 客户端攻击的源 IP。
attack_type	攻击类型:攻击具体命中的攻击类型。
rule_id	规则 ID: 触发防护策略的规则 ID, 其中 AI 引擎检出的攻击 详情的规则 ID 为 O。

字段名称	字段说明
scene_id	场景 ID: 触发防护策略的场景 ID。
scene_module	场景模块: 触发防护策略的场景模块, 包括前端对抗 (jsinject)、自定义规则(ucb)、智能分析(autoanalyze)。
method	请求方法:客户端攻击请求方法。
user_agent	User-Agent: 攻击源 IP 向服务器表明的浏览器类型和操作系 统标识等信息。
risk_level	风险等级:客户端攻击触发的风险等级,包括高危(1)、中危(2)、低危(3)三种风险等级。
status	执行状态:攻击请求的处置结果,包括观察(0)、拦截(1)、 人机识别(2)、重定向(3)四种处理结果。
count	聚合攻击次数,相同攻击源 IP 和攻击类型,汇总每10秒产 生的攻击次数。
domain	客户端攻击的域名信息。
pan	接入域名或 CLB 对象信息。
prote_domain	接入域名或 CLB 对象信息。
domain_name	客户端访问的域名信息。
attack_time	攻击时间, 客户端攻击触发的时间。
attack_place	攻击位置,攻击方式在 HTTP 请求中的位置。

字段名称	字段说明
action	执行动作,客户端攻击触发的处置动作,包括观察(0)、拦截(1)、人机识别(2)、重定向(3)四种处理结果。
ipinfo_nation	攻击 IP 所属国家名称。
ipinfo_province	攻击 IP 所属省份信息。
ipinfo_city	攻击 IP 所属城市。
ipinfo_state	攻击 IP 所属国家信息,国家英文缩写。
ipinfo_dimensiona lity	攻击 IP 所属纬度信息。
instance	域名接入的 Web 应用防火墙实例名称。
attack_category	攻击一级分类,暂未提供。
edition	域名接入的 Web 应用防火墙实例类型: 分为 sparta-waf (SaaS 型 WAF)和 clb-waf(负载均衡型 WAF)。
uuid	日志唯一标识。
attack_content	攻击内容:客户端触发攻击的内容。
http_log	记录 HTTP 请求和响应信息的日志文件: 包含此次 http 请求 的所有 http 信息。
headers	协议头部信息:包括自定义头部信息。
rule_name	规则名称,暂未提供。

字段名称	字段说明
args_name	参数名称: HTTP 请求中的参数名
ipinfo_isp	攻击 IP 运营信息。
appid	用户腾讯云账号的 APPID。
ipinfo_longitude	攻击 IP 的经度信息。
is_white	是否为情报白名单地址。
sec_chain	请求经过的安全模块及对应执行动作。

4 配置案例

4.1 接入网站架构



4.2 登录 ITQM 平台

访问此域名 https://saas.itqm.com, 登录 ITQM 进行域名配置。

			简体中文 ~
ITQM 欢迎您!			
真正享用可控、安全、高效的云上服务,专注业务增长。	密	昭码登录 验证码登录	
	± test		
	I5q7y	N 150744	
	☑ 自动登录	免费注册 📗 忘记密码	
		登录	
	粵ICP备11033900号广州青莲网络科技有限公司版权所有		

4.3 选择 SecOM 安全中心

ITOM		Qi	前令人内容	🛇 🖸 🥵 û 🕜 💠 A 🆓 奇麗科語
企业数字资产的日 基于客观现实,为企业提供低成本	ERP 高品质的数字化能力保障,全	力提升社会数字化应用价值。		" De land
工具	了解更多 >	应用		产品
3	-	e	۹ ایک	2
堡垒机 跨云备份	备份一体机 应用拨测	QM质量管理 ACM全云管理	Finops智慧财务 ITSC服务中心	质柳云
۵.	2	2	0	
APK检测 等保自测	合规源检	BIM业务洞察 DBM备份中心	SecOM安全中心 DEM数字化效能	
我的权益	您当前业务系统评级QM支持	奇墨活动 关注 [奇墨][6	QM】公众号,获取平台最新动态	奇墨质算云
主机安全-旗舰版	使用记录	ITOM BEING	连锁企业数字化转型沙龙	奇墨以先进的算力资源与ITQM的质量引擎结合,提供质算资源, 力于让每一次计算的价值最大化,帮助企业在激烈的市场竞争中 结婚生地位
有效期: 2024-03-06 至 2024-04-06	昭 28月: 0	進級企业数字化转型 沙龙分享会	カチェ 活动时间: 2023年02月24日	14.661.0-1017*
🥥 云账号使用权益	购买 使用记录	活动时间:2月24日周至1600-1730	圳市-南山区	
有效期: 2023-08-09 至 2025-02-27	MERE: 1008	····	杭州第19届亚运会	
🤳 拨测任务使用权益	购买 使用记录	11运完	活动时间: 2023年9月23日 至	

4.4 选择应用防护(WAF)



4.5 添加域名

ITQM			C) 请输入内容	🕐 🛇 E	ш 🤔 ф	⑦ III A 🍓 奇麗科技。
SecOM安全中心	IJ	SecOM安全中心 / 应用防护(V	VAF) / 接入管理				
④ 安全洞察	^						
资产洞察		<u></u>	即域名数		主域名数		
漏洞管理		3	/30 🕆		3/3	个	
基线管理							
账号安全		ла ты	自防护域名数		······ 未开启防护	中域名数	
🛛 响应与分析	~	3	· 个		≥ 0 🖈		
◎ 安全加固	~		/				
合規与測評	~						
🗋 应用防护(WAF)	^	+ 添加域名 🐵 i	MRG.				
概览		域名/接入状态	CNAME 信息	使用模式	回源地址	WAF 开关	操作
安全防护		www.test.bilib	ili.com	规则:拦截模式	111.230.122.0		
攻击日志		未配置 CNAM C	记录 25d3ccba95405e30796e8e7970 3a443.qcloudzygj.com ①	AI引擎:关闭模 式	129.204.26.0/24 查看更多 >		编辑 删除 防护设置
黑白名单		lanhuapp.com	710cc89371b2c40bc9ed262aa4	2	111.230.122.0	_	
接入管理		未配置 CNAMI O	记录 844e3.qcloudwzgj.com 🗍	- 规则:拦截模式	129.204.26.0/24 查看更多 >		编辑 删除 防护设置

填写域名,不需要加https://,选择【服务配置】根据现有的业务进行选择,如使用https则需要关联证书。

		新增域名	×
SecOM安全中心 프 ① 安全洞察 ^	28₩88 3/30 ↑	* 域名 finops.itqm.com 支持编写一级编名(例如:abc.com) 成二级通名(例如:www.abc.com)	
资产洞察		* 服务器配置 ① 2 http 80× 8080×	
漏洞管理	开启防护域名数	https 443 ×	
基线管理	3 🗸	证书起闢 羅斯夫职	
账号安全		证书状态: 有效 #************************************	
四 响应与分析 ~		- テムの内内: 2024-00-13 25:39:39 高級设置 へ	
窗安全加固 ~	+ 添加城名 @ 删除	нттръзданцияе 💿 🛛 💭	
合规与测评 ~	试名/接入状态 CNAME 信	нттрударод нттр • нттру	
☐ 应用防护(WAF) へ 概覧	www.test.billibili.com 25d3cc6a5 未配置 CNAME 记录 3a443.qcfc Q	ElighNi升来 ● ● 否 ● 是	
安全防护 攻击日志	Ianhuapp.com 710cc8937 未配置 CNAME 记录 844e3.qcle	* 源弘地址 ① ● IP地址 「境名地址 47.113.231.89	
黑白名单	gpt.91chat-ai.cn b80e2f183	请输入源站Pv46%结地,用国车分隔多个PP,最多支持输入50个	
接入管理	e 62bf.qclou	*	
日 主机安全 ~		1053	肖 确定

4.6 关联证书和录入证书 (https)

手动录入证书,或者可选择已经导入的证书。

		新增域名			×
SecOM安全中心 国 ③ 安全調察 ^	Alimetation (1997)	*城名	https://fi 支持填写一级	nops.itqm.com/ 崎谷 (例知: abc.com) 成二現場谷 (例初: www.abc.com)	
资产调察		*服务器配置 ①	http	80 × 8080 ×	
漏洞管理	开启防护域名数		https	443 ×	
基线管理	3			· 征书配置: 关联证书	
账号安全	证书配置			×	
图 响应与分析 ~	* 证书来源 🌑	选择已有证书	手动录入		
◎ 安全加固 ~	+ 添加域名 會 團隊	全部 ~	itqm.com	~	
日 合規与測評 · ·	域名/接入状态	_		能入50个	4
II 应用防护(WAF) 个	www.test.bilibili.c			取消 确定	
概然	未配置 CNAME 记录 3a443.qc で	clo 高级设置 ~			
安全防护	lanhuapp.com 710cc89	37			
攻击日志	C 844e3.qc	clo			
黑白名单	gpt.91chat-ai.cn 未配置 CNAME 记录	83!			
接入管理	e 62bf.qcl	out			
二 主机安全 ~					NVSIH ANDE

手动录入证书,证书两个文件.pem的需要使用记事本打开将其复制进入【证书】.key 也需要使用记事本打开复制进入【私钥】当中,确认即可。使用 https 的需要关联证书,选择手动录入证书

	新婚姻名	×
SecOM安全中心 III III III III III III III III III I	全部域名数 2/20	
① 安全洞察 へ	UTT	
资产消除 漏洞管理	*证书来源 透辉已有证书 • 手动泉入 开启的 *证书 (证书规则所干代内所干注意: 定即例会证书语	
基线管理 账号安全	3 这里输入证书.pem 后缀的内容	
四 响应与分析 ~		
◎ 安全加固 ~		
日 合規与測評 · ·	- AAU3 ##10368394LT260397959) - 城名/接入状态	
□ 应用助护(WAF) へ 概念 安全防护	这里输入证书.key 后缀的内容 www.test.bilibil.c 示 未配置 CNAME 记 C	
攻击日志	ianhuap.com ティング CNAME 旧 CO	
黑白名单	gpt91chat-sicn	h
接入管理	⊙ 62bfqcloui * 份额均衡荷额 ▲ aota iP hach	
日 主机安全 · ·		取消 柳定

				新增域名			×
SecOM安全中心 ① 安全洞察	•	全部域名数 3/30	Ŷ	* 域名	finops.it 支持填写一级	m.com 総否 (例如: abc.com) 成二型原色: (例如: www.abc.com)	
资产洞察				*服务器配置 ②	🗹 http	80 × 8080 ×	Ŷ
漏洞管理		开启防护域名数			https	443 ×	~
基线管理		3 🔍				证书配置: 重新关联	
账号安全						证书状态:有效	
圆 响应与分析						年378世月時: 2024-08-13-23:59:59 高級役置 ヘ	
受全加固	~ +	添加域名 會 翻譯				HTTPS强制的转 ③	
合规与测评	* I To	城名/接入状态	CNAME 信			HTTPS圆源方式 HTTP O HTTPS	
□ 应用防护(WAF) 概%		www.test.bilibili.com 未配置 CNAME 记录	25d3cc6a9 3a443.gclo			园源SNI开关	
100.00		e	surrangeno	*代理情况 ②	否	○ 是	
女王的外		lanhuapp.com 未配置 CNAME 记录	710cc8937	*源站地址 ②	 IP地地 	○ 域名地址	
攻击日志		e	844e3.qcio		请输入IP	地址	4
黑白名单		gpt.91chat-ai.cn 主配署 CNAME 记录	b80e2f183		请输入游站IP	4或v6地址,用回车分隔多个IP,最多支持输入50个	
接入管理		e	62bf.qclout	* 伯载均衡策略	 46461 	ID hach	
□ 主机安全	~						取消 确定

4.7 添加域名字段说明

	新增域名	×
SecOM安全中心 3 SecOM安全中心 / 应用防护(WAF) / 接入管理 ① 安全詞除 ^	* 域名	
资产制度 全部域名数	* 影务函配置 ② 【2 http 80 × 8080 × V	
Montester 3/30 个 Met管理	https 编码程	
繁号安全		
图 响成与分析 ~ 开启防护域名数	* 源站地址 ② • IP地址 域名地址	
@ gênna ~ 3 ∧	游船入JPIR3社 病他入游社P-R46-6拍社,用回车346多个P,最多支持他入50个 *	
□ 合規与選評 ∨	●负载均衡策略 ● 轮询 IP hash	
◎ 成用防护(WAF) ^ 株施	高级设置~	
安全防护 运名/接入状态 CNAME (
攻击日志 finops.itqm.com 38a0004fi 正常初炉 ひ 105b.qdg 更日名単	d. U	
接入管理 www.test.bilbili.com 25d3cc6a 未配置 CNAME 记录 3add3 ad		
□ 主机安全 · · · · · · · · · · · · · · · · · · ·	取功消	确定

域名:在域名输入框中添加需要防护的域名 yyyyy. xxxxxx. cn。

服务器配置:协议和端口可按实际情况选择。

选择 HTTP 协议, 输入端口。

选择 HTTPS 协议,输入端口后需要配置关联证书、HTTPS 强制跳转和 HTTPS 回源方式。 关联证书:单击关联证书,根据需求选择或导入证书。

HTTPS 强制跳转:如需开启 HTTPS 强跳,需同时勾选 HTTP 和 HTTPS 访问协议。

HTTPS 回源方式: HTTP 或 HTTPS。

源站地址:根据实际需求选择 IP 或域名。

IP: 请输入源站 IPv4 或 IPv6 地址, 用回车分隔多个 IP, 最多支持输入 50 个。

域名:请输入源站域名,注意:源站域名不能和防护域名相同。

加权回源: 当源站地址设置多 IP 回源时。可以选择加权回源方式,并设置不同的权重

负载均衡策略:默认为轮询方式,可根据实际需求选择轮询、 IP Hash 或加权轮询方式。 配置完基础参数后,可根据需求配置高级参数,单击确认保存。

WebSocket 检查,通过开发者模式检查是否有; ws:// 或 wss:// 开头的地址,通常这个网站是 WebSocket 会有 ws:// 或 wss:// 开头的地址。



			新增域名	×
SecOM安全中心	19	SecOM安全中心 / 应用防护(WAF) / 接入管理		请输入1892日24455688年,用国车分隔多个中,最多支持输入50个
⑦ 安全洞察 资产洞察 漏洞管理 基线管理		شیند 3/30 ش	* 负载均衡策略 高级设置 へ 回源连接方式	 轮询 IP hash 超连接 长连接 K连接 如从使用长连细题牌,随等电源站是否支持长连续,若不支持,图映设置长连接,也会使用短连接
账号安全			写超时时长	- 300 + 秒,范围1~600秒
圆 响应与分析		开启防护域名数	读超时时长	- 300 + 秒范围1~600秒
· 安全加固		→ 3 ↔	开启HTTP2.0 ⑦	· 否 0 是
□ 合规与测评				请确保您的游战支持并开启了HTTP2.0,否则。即使配置开启2.0也将律级1.1
日 应用防护(WAF)		+ 滿加峡名 會 翻論	开启WebSocket	● 否 □ 是 SURFERSINGAGERT/Websocket, 建区的影响器
安全防护		域名/接入状态 CNAME 借	开启健康检查	● 否 ○ 是
攻击日志		finops.itgm.com 38a0004fd 正常防护 O 105b.gclou	开启XFF重置	● 否 ○ 是 请全X-Forwarded-For学段绩,请确认WAF确无7国代理服务后开启
(集日名単 接入管理 目 主机安全		www.test.bilibili.com 25d3cc6at 末記國 CNAME 记录 3a443.qclo		102)H 40 02

字段说明:

回源连接方式:默认使用长连接回源,请确认源站是否支持长连接,若不支持,即使设置 长连接,也会使用短连接。

开启 HTTP2.0: 请确保您的源站支持并开启了 HTTP2.0, 否则, 即使配置开启 2.0 也将降 级为 1.1。

开启 Websocket: 如果您的网站使用了 Websocket, 建议您选择是。

开启健康检查:企业版以及以上版本,支持开启基于回源 IP 的四层健康检查机制。

开启 XFF 重置: 支持清空 X-Forwarded-For 字段值,请确认 WAF 前无七层代理服务后 开启。

注: Web 应用防火墙将会为每个添加到 Web 应用防火墙的域名(不区分一级域名和二级 域名)分配一个唯一的 CNAME。

5. 完成配置后,可在域名接入页面看到新添加的域名。当前界面显示未配置 CNAME 记录, 需要 本地验证测试 后,再 修改 DNS 解析。

≡ itom				Q initial	认内容	🕐 🛇 🗉	ш 🤗 ф	⑦ III A 奶 奇麗科技~ 1
SecOM安全中心	Iŭ		全部域名数			主域名数		
④ 安全洞察	^		3/30	^		3/3	\uparrow	
资产洞察								
漏洞管理			开启防护域名数			未开启防护	词成名数	
基线管理			3 🔶			💙 O 🖈		
账号安全								
回 响应与分析	~	1.4						
⑧ 安全加固	~	+ 添加域名	© 1983					
□ 合规与测评	~	域名	3/接入状态	CNAME 信息	使用模式	回源地址	WAF 开关	操作
🗐 应用防护(WAF)	^	fin	ops.itam.com			111.230.122.0	-	
概览		E9	前防护 〇		规则: 拦截模式	129.204.26.0/24 查看更多 >		编辑 删除 防护设置
安全防护		ww.	w.test.bilibili.com	25d3cc6a95405e30796e8e7970a	規则: 拦截模式	111.230.122.0		ACTIVE INTER PERSONNER
攻击日志		e v	ELL CIVAIVE IESK	3a443.qcloudzygj.com 🗇	AISI單: 天闭模 式	查看更多 >		5月1日 7月1月4日 873-07-122 MA
黑白名单		lan ‡ë	huapp.com 記書 CNAME 记录	710cc89371b2c40bc9ed262aa42	抱創・持動模式	111.230.122.0		编辑 删除 防护设备
接入管理		0		844e3.qcloudwzgj.com 🗍	00000 3-B0(9030	查看更多 >	-	more entroy 1723 EX.am.
🗒 主机安全	\sim							

4.8 本地测试

4.8.1 修改本地 hosts

修改本地 hosts 文件进行测试, Windows10 举例以管理员的身份打开 C:\Windows\System32\drivers\etc\hosts 在末尾添加通过 ping CNAME 值得到的 IP 地址进行 验证

[C:\~]\$ pipg 3850004fde75f7/c00f12/2fc6d0105b gc]oudzygi com		
[C:\~]\$ ping 38a000410275174C99112421C6031050.qC toud2yg].com 正在 Ping 1c1b3beb1a6eb7f2-cl2.qcloudwzgj.com [106.55.113.168] 具有 32 字节的数据: 来自 106.55.113.168 的回复: 字节=32 时间=24ms TTL=52 来自 106.55.113.168 的回复: 字节=32 时间=24ms TTL=52 来自 106.55.113.168 的回复: 字节=32 时间=24ms TTL=52		
106.55.113.168 的 Ping 统计信息: 数据包: 己发送 = 3, 己接收 = 3, 丢失 = 0 (0% 丢失), 往返行程的估计时间(以毫秒为单位): 最短 = 22ms, 最长 = 24ms, 平均 = 23ms AC		
Contraction 2700+		
■ 10515 10344 ○ 20476 報告(1) 表示(1) 表示(1) 表示(1) 表示(1)		~
		^
# Additionally, comments (such as these) may be inserted on individual # lines or following the machine name denoted by a '#' symbol. # # For example: #		
# 102.54.94.97 rhino.acme.com # source server # 38.25.63.10 x.acme.com # x client host		
# localhost name resolution is handled within DNS itself. # 127.0.0.1 localhost # ::1 localhost		
64.233.189.191 translate.googleapis.com		
64.233.189.191 translate.google.com 127.0.0.1 activate.navicat.com		
		~
第30行,第31列 100% Windows (CR	LF) UTF-8	

添加完成保存退出,验证<u>https://finops.itqm.com/(变更为实际受保域名)</u>站点是否 正常。

4.8.2 访问验证

在本地电脑上访问 Web 站点,若站点能够正常打开,说明 Web 应用防火墙访问 Web 源站的线路连通性正常。



在浏览器中输入下面的网址并访问(此为例子,实际域名变更为"受保护域名")。

https://finops.itqm.com/?test=alert(123)

浏览器返回阻断页面,说明 Web 应用防火墙防护功能正常。



4.9 修改 DNS

4.9.1 添加 CNAME 记录

为了使公网用户访问网站的流量经过 Web 应用防火墙的防护。需要登录 DNS 解析控制台 添加 CNAME 记录

CNAME-将域名指向另外一个域名	~	
主机记录 ❷		
finops	.itqm.com	?
析请求来源		
指域名访问者所在的地区和使用的运营商网络。		?
默认 - 必填!未匹配到智能解析线路时,返回【默认】线路设置结果	\vee	
<mark>级至企业版DNS</mark> ,支持按更精细线路(省份、国家)请求来源返回不同记录值。		
记录值 🛛		
38a0004fde75f74c99f1242fc6d9105b.qcloudzygj.com		
10 分钟	\sim	

主机记录 ⑦ ⇔	记录类型 ③ 🍦	解析请求来源(isp) ⑦ 💲	记录值⑦	TTL 🕜	状态② 💲
finops	CNAME	默认	38a0004fde75f74c99f1242fc6d9105b.qc loudzygj.com	10 分钟	启用

4.9.2 记录值获取

CNAME 记录值获取, 登录 IQTM > [应用防护 WAF] > [CNAME 信息] 中获取

≡	ITQM				Q谐频	俞入内容	🍨 🛇 🖻) 111 A 崎 奇麗科技~	
Se	cOM安全中心	H	1	全部域名数			主域名数			
٢	安全洞察	~		3/30	\uparrow		> 3/3	\uparrow		
E.	响应与分析	~								
۲	安全加固	\sim	(开启防护域名数			未开启防!	户域名数		
	合规与测评	~		3 🔒			≥ 0 🖈			
	应用防护(WAF)	^								
	概览				+					
	安全防护		十 添加	14名 亩 删除						
	攻击日志			域名/接入状态	CNAME 信息	使用模式	回源地址	WAF 开关	操作	
	黑白名单			finans itam com	28-000464-75674-99612426-649	规则: 拦截模式	111.230.122.0	1.000		
	接入管理			正常防护 📀	105b.qcloudzygj.com	AI引擎:关闭模 式	129.204.26.0/24 查看更多 >		编辑 删除 防护设置	
	主机安全	~		www.test.bilibili.com	25d3cc6a95405e30796e8e7970a	规则:拦截模式	111.230.122.0		47400 PMIRA 044441000	
~	平台管理	~		木配置 CNAME 记家 ·	3a443.qcloudzygj.com 🗇	AI51寧: 天闭模 式	129.204.26.0/24 查看更多 >		骗帽 制序 防护设置	
				lanhuapp.com 未配置 CNAME 记录 오	710cc89371b2c40bc9ed262aa42 844e3.qcloudwzgj.com 🗇	规则:拦截模式	111.230.122.0 129.204.26.0/24 查看更多 >		編編 删除 防护设置	

4.10 访问测试

正常访问,如下图显示成功



非法访问出现如下图,说明成功



4.11 安全组开放

如访问测试无法通过需开放安全组进行测试,以腾讯云为例:

添加一个安全组规则

安全组规则	关联实例					
入站规则	出站规则					
添加规则	导入规则	排序	删除	一键放通	教我设置已	
□ 来源 ()					协议端口①	

在弹出框中填写相关信息,类型选择 "HTTP(80)",来源中填写需要放行的回源 IP, 根据需求填写端口及策略,填写完毕后,单击完成。

原 (i) 协议端口 (i)	44.77		
	策語	备注	
到源ip TCP:443,80	允许 ▼		
.0.0.0/0 TCP:443,80	拒绝 🔻		0
	TCP:443,80 0.0.0/0 TCP:443,80	I願p TCP:443,80 允许 * 0.0.0/0 TCP:443,80 拒绝 *	I願p TCP:443,80 允许 *

单击选项卡中的关联实例,在云服务器页面下,单击新增关联

安全组规则	关联实例		
云主机(1)	弹性网卡(0) (j)	云数据库Mysql(0)	负载均衡(0)
新增关联	批量移出		

新增实例关联

选择	安全组:	100	"要绑定的实例			已选择(1/100)			
请输	入名称/ID/IP (1)	又显示未关联该实	安全组的实例)	Q		实例ID/名称	所属网络	主IP地址	
~	实例ID/名称 	所属网络	主 IP 地址			nogeth.			×
	nageth.				\leftrightarrow				
		Sec.e.m.							
	-								

以上就是安全组开放流程。

(完)