

WAF 虚拟化版本 Web API 接口

目录

- 目录..... 1
- 1 接口约定 5
- 接口设置 5
- 2 认证流程 5
- 3 接口说明 8
 - 3.1 获取系统信息 8
 - 3.2 管理员用户 9
 - 3.2.1 获取单个用户..... 9
 - 3.2.2 添加用户..... 10
 - 3.2.3 删除用户..... 11
 - 3.2.4 修改用户密码..... 12
 - 3.2.5 解锁用户..... 13
 - 3.3 业务口 IP 配置 14
 - 3.3.1 获取单个业务口..... 14
 - 3.3.2 修改单个业务口..... 15
 - 3.4 DNS 配置 16
 - 3.4.1 获取 DNS 配置..... 16
 - 3.4.2 修改 DNS 配置..... 17
 - 3.5 NTP 服务器配置..... 18
 - 3.5.1 获取 NTP 服务器配置..... 18
 - 3.5.2 修改 NTP 配置..... 19

3.6	授权	20
3.6.1	导入授权.....	20
3.6.2	激活授权.....	21
3.6.3	查看授权.....	22
3.7	防护策略配置	24
3.7.1	获取所有防护策略.....	24
3.7.2	获取单个防护策略.....	27
3.7.3	添加防护策略.....	29
3.7.4	修改防护策略.....	32
3.7.5	删除防护策略.....	34
3.7.6	启用/禁用防护策略.....	35
3.8	站点安全配置	35
3.8.1	新建站点安全.....	35
3.8.2	删除站点安全.....	36
3.8.3	查看站点安全.....	37
3.8.4	查看扫描防护.....	39
3.8.5	修改扫描防护.....	41
3.8.6	查看暴力破解.....	43
3.8.7	修改暴力破解.....	44
3.8.8	查看慢速攻击.....	46
3.8.9	修改慢速攻击.....	47
3.8.10	查看 SQL 注入防护.....	49
3.8.11	修改 SQL 注入防护.....	50
3.8.12	查看 XSS 攻击防护.....	52

3.8.13 修改 XSS 攻击防护	53
3.8.14 查看敏感信息防护	54
3.8.15 修改敏感信息防护	56
3.8.16 修改事件引擎	58
3.9 SSL 证书配置	59
3.9.1 查看证书	59
3.9.2 删除证书	62
3.9.3 导入证书	63
3.10 事件库升级	64
3.10.1 事件库立即升级	64
3.10.2 获取事件库升级日志	65
3.11 安全事件统计	66
3.11.1 获取安全事件统计	66
3.12 FLOOD 防护	67
3.12.1 查看智能 TCP FLOOD 防御配置	67
3.12.2 修改智能 TCP FLOOD 防御配置	68
3.13 软件 BYPASS	69
3.13.1 修改软件 Bypass	69
3.14 黑/白名单配置	70
3.14.1 获取所有黑/白名单	70
3.14.2 添加/修改黑/白名单	72
3.14.3 删除黑/白名单	74
3.14.4 开启/关闭黑/白名单	75
3.15 网关配置	76
3.15.1 获取所有网关	76
3.15.2 添加网关	77

3.15.3 删除网关	78
3.16 静态路由配置	79
3.16.1 获取所有静态路由.....	79
3.16.2 添加静态路由	80
3.16.3 修改路由	81
3.16.4 删除路由	82
3.17 设备参数	83
3.17.1 设备重启	83
3.17.2 保存配置	84

1 接口约定

1. 接口URI：供第三方服务调用，用来获取WAF信息的访问地址
2. 接口遵循restful风格，略有调整
3. 允许使用http、https访问，受限于WAF设备本身开放的权限：如协议（HTTP、HTTPS）访问限制、IP访问限制
4. 每个接口的默认前缀为**http://ip:port/v2/**
5. 允许port为多个，具体设置需请咨询技术人员
6. POST参数为json格式，编码为utf-8编码

接口设置

Restful—api默认端口82，如果需要修改端口，可以再web管理界面进行修改

系统配置--->基本配置--->修改接口



Restful端口配置	
原始端口	82
新端口	<input type="text" value=""/> (1-65535)
<input type="button" value="提交"/>	

2 认证流程

1. 用户名为系统用户，密码为账户对应的密码。
-

2. 请求api接口时，需要携带两个参数：ts，表示13位unix时间戳（毫秒）；

sign，表示签名（无需携带密码参数）

3. ts时间戳如果与服务器时间戳之差超过10分钟，则视为无效。

4. sign计算方式：sign = user + ':' + md5 (ts + api_uri + user + md5(pass))，其中ts表示时间戳，api_uri表示api的

uri，user表示用户名，pass表示密码

举例：请求/v2/sysinfo 这个接口：

api_uri = /v2/sysinfo,

ts = 1468395806542,

按照sign=user + ':' + md5 (ts + api_uri + user + md5(pass))计算，可得sign
值为：

user:64234aeb5392f125c811513e3b702ca7

所以最终的url为

**http://ip:port/v2/sysinfo?ts=1460362301129&sign=virtual.user:64234aeb
5392f125c811513e3b702ca7**

接口中的公共部分

返回 HTTP 200代表接口成功调用，否则说明接口调用有误，比如URL地址错误。

即使返回HTTP 200，也不能说明业务逻辑正常调用。

**每个接口的返回内容中，用json字符串说明返回结果。其中包括result字段，为数值
类型，0表示执行成功，非0表示出错。**

错误对照表

0	成功
1	失败, ts时间戳之差超过10分钟
2	失败, sign错误
3	其他失败原因, 详细参加错误描述errmsg
4	

返回错误数据对应内容

返回数据	数据
ts时间戳之差超过10分钟	<pre>{ "result" : 1, "errmsg" : "ts check error", "serv_time": 1460363462234 //表示服务器当前时间戳 }</pre>
sign错误	<pre>{ "result" : 2, "errmsg" : "sign error" }</pre>
其他错误	<pre>{ "result" : 3, "errmsg" : "here is error message" // 这里会返回相关错误信息 }</pre>

	}
--	---

3 接口说明

3.1 获取系统信息

请求接口	http://ip:port/v2/sysinfo?action=show
请求方式	GET
请求参数	需携带ts、sign两个参数，具体见认证流程。
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" , //参加错误码对照表 "sysinfo" : { "cpu_usage" : "2.25", //cpu 利用率百分比 "mem_usage" : "65", //内存利用率百分比 "conn_num" : "1000", //连接数 "disk_usage" : "51", //硬盘利用率百分比 "sys_uptime" : "10000", //系统运行时间(秒) } }</pre>

	<pre>"halfopen_conn_num" : "0"//半连接数 } }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>
--	---

3.2 管理员用户

3.2.1 获取单个用户

请求接口	http://ip:port/v2/adminuser?action=show&username=xxx
请求方式	GET
请求参数	需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。 这里的username必填
返回码	200
返回格式	application/json;charset=utf-8
返回数据	正确数据： { "result" :" 0" , //参见错误码对照表 "adminuser" :

	<pre>{ "usrname": "user", //用户名，字符串，6-20长度 "passwd": "abcdef", //密码，字符串，6-20长度 "type": "0" , //类型，0表示普通用户，1表示radius用户 "role": "2" , //角色，只能为2，表示配置管理员 "priv": "2" , //权限，1表示只读权限，2表示读写权限 "radius_server_name": "radiusServer", //radius服务器名 "email": "test@163.com", //邮箱名 "phone": 13311234312, //手机号 "desc": "描述" //描述信息 }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>
--	---

3.2.2 添加用户

请求接口	http://ip:port/v2/adminuser?action=add
请求方式	POST
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。只能单个添加</p> <p>POST的参数：</p> <pre>{</pre>

	<pre> "username": "user", //用户名，字符串，6-20长度 "passwd": "abcdef", //密码，字符串，6-20长度 "type": 0, //类型，0表示普通用户，1表示radius用户 "role": 2, //角色，只能为2，表示配置管理员 "priv": 2, //权限，1表示只读权限，2表示读写权限 "radius_server_name": "radiusServer", //radius服务器名 "email": "test@163.com", //邮箱名 "phone": "13910110111", //手机号或固定电话 "desc": "描述" //描述信息 } </pre>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" }</pre> //参见错误码对照表 <p>错误数据返回请参见返回错误数据对应内容</p>

3.2.3 删除用户

请求接口	http://ip:port/v2/adminuser?action=delete&username=xxx
请求方式	GET
请求参数	需携带ts、sign两个参数，具体见认证流程（这两个参数建

	议放到url里) 。 username不能为空
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.2.4 修改用户密码

请求接口	http://ip:port/v2/adminpassword?action=mod
请求方式	POST
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <p>POST的参数：</p> <pre>{ "username": "user", //用户名，字符串，6-20长度 "oldpasswd": "abcdef", //旧密码 "newpasswd": "ZaSef" //新密码 }</pre>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	正确数据：

	<pre>{ "result" : "0" }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>
--	--

3.2.5 解锁用户

请求接口	http://ip:port/v2/adminUnblock?action=mod
请求方式	POST
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <p>POST的参数：</p> <pre>{ "ipaddr": "192.12.32.12", //要解锁的IP, IPv4 }</pre>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.3 业务口 IP 配置

3.3.1 获取单个业务口

请求接口	http://ip:port/v2/interface?action=show&name=xxx
请求方式	GET
请求参数	需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。获取接口name必填，如gev0/1
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result": "0", "interface": { "type": 0, //类型必填，0 为静态 IP，1 为 DHCP "name": "GEV0/1", //接口名称 "desc": "描述", "hw_addr": "00-0c-29-42-61-36", //mac 地址 "ipaddr": "192.168.1.2", //ipv4 地址 "ipaddr_v6": "2001:da8:8000:d010::1", // ipv6 地址 "ping": 0, //是否允许 ping，0 不允许，1 允许 } }</pre>

	<pre>"mtu": 1500 //mtu }</pre> <p>}错误数据返回请参见返回错误数据对应内容</p>
--	---

3.3.2 修改单个业务口

请求接口	http://ip:port/v2/interfacesub?action=mod
请求方式	POST
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <p>POST的参数：</p> <pre>{ "type": "0" ,//类型必填，0为静态IP，1为DHCP "name": "GEV0/1", //接口名称必填 "desc": "描述", "ipaddr": "192.168.31.1/24",//ipv4地址/掩码 必填 "ipaddr_v6": "2001:da8:8000:d010::1/64", // ipv6地址 选填 "ping": 0, //是否允许ping，0不允许，1允许 "mtu": 1500 //mtu }</pre>

返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.4 DNS 配置

3.4.1 获取 DNS 配置

请求接口	http://ip:port/v2/dns?action=show
请求方式	GET
请求参数	需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" , "dns_ipv4" : {</pre>

	<pre>"first_dns": "114.114.114.114",//首选 "second_dns": "8.8.8.8" //备选 }, "dns_ipv6" : { "first_dns": "",//首选 "second_dns": "" //备选 } }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>
--	---

3.4.2 修改 DNS 配置

请求接口	http://ip:port/v2/dns?action=mod
请求方式	POST
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <pre>{ "dns_ipv4" : { "first_dns": "114.114.114.114",//首选 "second_dns": "8.8.8.8" //备选</pre>

	<pre> }, "dns_ipv6" : { "first_dns": "",//首选 "second_dns": "" //备选 } } </pre>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.5 NTP 服务器配置

3.5.1 获取 NTP 服务器配置

请求接口	http://ip:port/v2/ntp?action=show
请求方式	GET
请求参数	需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。
返回码	200
返回格式	application/json;charset=utf-8

返回数据	<p>正确数据:</p> <pre>{ "result" : "0" , "ntp" : { "ntp_server_ip": "pool.ntp.org",//服务器是网址或 ip "ntp_interval": "5" //ntp服务器同步时间间隔, 单位分钟 } }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>
------	--

3.5.2 修改 NTP 配置

请求接口	http://ip:port/v2/ntp?action=mod
请求方式	POST
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <p>POST参数</p> <pre>{ "ntp_server_ip": "pool.ntp.org",//服务器是网址或 ip "ntp_interval": "5" //ntp服务器同步时间间隔, 单位分钟 }</pre>

返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.6 授权

3.6.1 导入授权

请求接口	http://ip:port/v2/license?action=mod
请求方式	POST
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <p>POST参数</p> <pre>{ "license": "QvjfpVWt9NpxNUU", "generated_tmp_license": 1//表示是否产生过临时授权, 0 没有, 1 有 }</pre>
返回码	200
返回格式	application/json;charset=utf-8

返回数据	<p>正确数据：</p> <pre>{ "result" : "0" }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>
------	---

3.6.2 激活授权

请求接口	http://ip:port/v2/license?action=mod
请求方式	POST
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <p>分别有临时授权和激活授权，通过add_action区分</p> <p>POST参数</p> <pre>{ "add_action": 1, //1-临时授权, 2-激活 "generated_tmp_license": 1 //表示是否产生过临时授权, 0 没有, 1 有 }</pre>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.6.3 查看授权

请求接口	http://ip:port/v2/license?action=show
请求方式	GET
请求参数	需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" , "license" : { //以下功能项中 enable 的含义:0-未授权, 1-试用授权, 2-正式授权 "ips_license_enable": 2, //特征库授权状态 "ips_license_time": "188267379", //授权剩余有效期, 单位毫秒, 以下有效期单位一致 "ips_alert": 0, //授权提示, 授权时间小于30天时为1 "ssl_license_enable": 2, //HTTPS 应用防护授权状态 "ssl_license_time": "188267379", //授权剩余有效期 "ssl_alert": 0, //授权提示, 授权时间小于30天时为1</pre>

	<p>"accel_lincense_enable": 1, //缓存加速授权状态</p> <p>"accel_lincense_time": "188267379", //授权剩余有效期</p> <p>"accel_alert": 0, //授权提示, 授权时间小于 30 天时为 1</p> <p>"ipcheck_lincense_enable": 1, //源区域访问控制授权状态</p> <p>"ipcheck_lincense_time": "188267379", //授权剩余有效期</p> <p>" ipcheck_alert": 0, //授权提示, 授权时间小于 30 天时为 1</p> <p>"webtakeover_lincense_enable": 1, //网站锁授权状态</p> <p>"webtakeover_lincense_time": "188267379", //授权剩余有效期</p> <p>"webtakeover_alert": 0, //授权提示, 授权时间小于 30 天时为 1</p> <p>"portnum": 23, //授权端口总数</p> <p>"generated_tmp_license": 1, //是否产生过临时授权, 1-产生过, 0-没有</p> <p>"license": 0, //标志位, 始终为 0</p> <p>"if_list": [//当前授权的端口 {"ifname": "ge0/4"},</p>
--	--

	<pre>{ "ifname": "ge0/3", "ifname": "ge0/2", "ifname": "ge0/1", "ifname": "eth1" } }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.7 防护策略配置

3.7.1 获取所有防护策略

请求接口	http://ip:port/v2/protectedPolicy?action=show
请求方式	GET
请求参数	需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。
返回码	200
返回格式	application/json;charset=utf-8
返回数据	正确数据：

	<pre> { "result" : "0" , "protect_policy" : [{ "name": "default", //站点防护策略名称, 最大长度 64 字节 "mode": "0", //0-桥模式, 1-代理模式, 2-单臂模式, 3- 路由模式 "ip": "", //代理 ip (代理模式和单臂模式填充) , 最大长 度 64 字节 "protocal": "http", //应用类型 "port": "80", //代理端口 (代理模式和单臂模式填充) "ssl_enable": "0", //是否开启 ssl 配置, 0-不开启, 1-开 启 "local_cert": "", //本地证书, 长度 64 字节 "ssl_version": "SSL3.0", //SSL 版本, 10 字节 "cipher_suit": "", //算法套件, 1024 字节 "website_safe": "high_level", //站点安全名称 "doname": "" ,//域名, 字符串 "real_server" : [{ "type" : "0", //真实服务器类型, 0-主机, 1-子网, 2-范围, 10-ipv6 主机, 11-ipv6 子网, 12-ipv6 范围 </pre>
--	--

	<p>"host" : "192.168.53.12", //type 为主机, 64 字节, 格式如: 192.168.54.191</p> <p>"net" : "192.168.54.191/32", //type 为子网, 64 字节, 格式: 192.168.54.191/32</p> <p>"range1" : "", //type 范围, 64 字节, 起始 ip 地址</p> <p>"range2" : "", //type 范围, 64 字节, 结束 ip 地址</p> <p>"port": "80", //真实服务器端口</p> <p>"protocal": "http", //协议, 8 字节</p> <p>"ssl_enable": "0", //是否开启 ssl 配置, 0-不开启, 1-开启</p> <p>"ssl_version" : "SSL3.0" //SSL 版本, 10 字节</p> <p>}</p> <p>]</p> <p>}</p> <p>]</p> <p>}错误数据返回请参见返回错误数据对应内容</p>
--	--

3.7.2 获取单个防护策略

请求接口	http://ip:port/v2/protectedPolicy?action=show&name=xxx
请求方式	GET
请求参数	需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。名字如default
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" , "protect_policy " : [{ "name": "default", //站点防护策略名称，最大长度 64 字节 "mode": "0", //0-桥模式， 1-代理模式， 2-单臂模式， 3-路由模式 "ip": "", //代理 ip（代理模式和单臂模式填充），最大长度 64 字节 "protocol": "http", //应用类型 "port": "80", //代理端口（代理模式和单臂模式填充）</pre>

	<p>"ssl_enable": "0", //是否开启 ssl 配置, 0-不开启, 1-开启</p> <p>"local_cert": "", //本地证书, 长度 64 字节</p> <p>"ssl_version": "SSL3.0", //SSL 版本, 10 字节</p> <p>"cipher_suit": "", //算法套件, 1024 字节</p> <p>"real_server" : {</p> <p> "type" : "0", //真实服务器类型, 0-主机, 1-子网, 2-范围, 10-ipv6 主机, 11-ipv6 子网, 12-ipv6 范围</p> <p> "host" : "192.168.53.12", //type 为主机, 64 字节, 格式如: 192.168.54.191</p> <p> "net" : "192.168.54.191/32", //type 为子网, 64 字节, 格式: 192.168.54.191/32</p> <p> "range1" : "", //type 范围, 64 字节, 起始 ip 地址</p> <p> "range2" : "", //type 范围, 64 字节, 结束 ip 地址</p> <p> "port": "80", //真实服务器端口</p> <p> "protocal": "http", //协议, 8 字节</p> <p> "ssl_enable": "0", //是否开启 ssl 配置, 0-不开启, 1-开启</p>
--	---

	<div>"ssl_version" : "SSL3.0" //SSL 版本, 10 字节</div> <div>},</div> <div>"website_safe": "high_level", //站点安全名称</div> <div>"doname": "" //域名, 字符串</div> <div>}</div> <div>}</div> <div>错误数据返回请参见返回错误数据对应内容</div>
--	--

3.7.3 添加防护策略

请求接口	http://ip:port/v2/protectedPolicy?action=add
请求方式	POST
请求参数	<div>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</div> <div>此处以桥模式为例</div> <div>POST参数</div> <div>{</div>

	<p>"name": "default", //站点防护策略名称, 最大长度 64 字节</p> <p>"mode": 0, //0-桥模式, 1-代理模式, 2-单臂模式, 3-路由模式</p> <p>"ip": "", //代理 ip (代理模式和单臂模式填充) , 最大长度 64 字节</p> <p>"protocol": http, //应用类型</p> <p>"port": 80, //代理端口 (代理模式和单臂模式填充)</p> <p>"ssl_enable": 0, //是否开启 ssl 配置, 0-不开启, 1-开启</p> <p>"local_cert": "", //本地证书, 长度 64 字节</p> <p>"ssl_version": "SSL3.0", //SSL 版本, 10 字节</p> <p>"cipher_suit": "", //算法套件, 1024 字节</p> <p>"real_server" : {</p> <p> "type" : 0, //真实服务器类型, 0-主机, 1-子网, 2-范围, 10-ipv6 主机, 11-ipv6 子网, 12-ipv6 范围</p> <p> "host" : "192.168.53.12", //type 为主机, 64 字节, 格式如: 192.168.54.191</p> <p> "net" : "192.168.54.191/32", //type 为子网, 64 字节, 格式: 192.168.54.191/32</p>
--	--

	<pre> "range1": "", //type 范围, 64 字节, 起 始 ip 地址 "range2": "", //type 范围, 64 字节, 结 束 ip 地址 "port": 80, //真实服务器端口 "protocal": http, //协议, 8 字节 "ssl_enable": 0, //是否开启 ssl 配置, 0- 不开启, 1-开启 "ssl_version": "SSL3.0" //SSL 版本, 10 字节 }, "website_safe": "high_level", //站点安全名称 "doname": "" //域名, 字符串 } </pre>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据:</p> <pre>{"result" : 0}</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.7.4 修改防护策略

请求接口	http://ip:port/v2/protectedPolicy?action=mod
请求方式	POST
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <p>修改防护策略与添加防护策略结构体一致</p> <p>此处以桥模式为例</p> <p>POST参数</p> <pre>{ "name": "default", //站点防护策略名称，最大长度 64 字节 "mode": 0, //0-桥模式，1-代理模式，2-单臂模式，3-路由模式 "ip": "", //代理 ip（代理模式和单臂模式填充），最大长度 64 字节 "protocol": http, //应用类型 "port": 80, //代理端口（代理模式和单臂模式填充） "ssl_enable": 0, //是否开启 ssl 配置，0-不开启，1-开启 "local_cert": "", //本地证书，长度 64 字节</pre>

	<p>"ssl_version": "SSL3.0", //SSL 版本, 10 字节</p> <p>"cipher_suit": "", //算法套件, 1024 字节</p> <p>"real_server" : {</p> <p> "type" : 0, //真实服务器类型, 0-主机, 1-子网, 2-范围, 10-ipv6 主机, 11-ipv6 子网, 12-ipv6 范围</p> <p> "host" : "192.168.53.12", //type 为主机, 64 字节, 格式如: 192.168.54.191</p> <p> "net" : "192.168.54.191/32", //type 为子网, 64 字节, 格式: 192.168.54.191/32</p> <p> "range1" : "", //type 范围, 64 字节, 起始 ip 地址</p> <p> "range2" : "", //type 范围, 64 字节, 结束 ip 地址</p> <p> "port": 80, //真实服务器端口</p> <p> "protocal": http, //协议, 8 字节</p> <p> "ssl_enable": 0, //是否开启 ssl 配置, 0-不开启, 1-开启</p> <p> "ssl_version" : "SSL3.0" //SSL 版本, 10 字节</p> <p>},</p> <p>"website_safe": "high_level", //站点安全名称</p>
--	--

	<pre>"doname": "" //域名, 字符串 }</pre>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.7.5 删除防护策略

请求接口	http://ip:port/v2/protectedPolicy?action=del&name=x xx
请求方式	GET
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <p>name必须填写</p>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" }</pre>

	错误数据返回请参见 返回错误数据对应内容
--	--------------------------------------

3.7.6 启用/禁用防护策略

请求接口	http://ip:port/v2/protectedPolicyState?action=mod
请求方式	POST
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <p>POST参数</p> <pre>{ "name": "porxy", // 启用/禁用的防护策略名字 "disable": 1//1-不启用, 0-启用 }</pre>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.8 站点安全配置

3.8.1 新建站点安全

请求接口	http://ip:port/v2/siteSecurity?action=add
------	---

请求方式	POST
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <p>POST参数</p> <pre>{ "name": "123", // 站点名称 "domain": "", //站点域名 "file_path": ""//填写空 }</pre>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.8.2 删除站点安全

请求接口	http://ip:port/v2/siteSecurity?action=del&name=xxx
请求方式	GET
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <p>name为站点名称</p>

返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.8.3 查看站点安全

请求接口	http://ip:port/v2/siteSecurity?action=show&name=xxx
请求方式	GET
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <p>name为站点名称</p>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" , "site_security" : [{ "name": "default", // 站点名称 "domain": "", //站点域名 "req_param": "", //占位符，无意义 }] }</pre>

	<p>//以下功能项 0-不启用, 1-启用</p> <p>"site_taking": "0", //网站锁,</p> <p>"protect_param": "1", //HTTP 协议合规锁</p> <p>"slow_attack": "1", //慢攻击</p> <p>"anti_escape": "1", //防逃逸</p> <p>"cookie_protect": "0", //cookie 防护</p> <p>"appd_ppr": "0", //网页防篡改</p> <p>"cc_protect": "0", //HTTP Flood(cc)防护</p> <p>"csrf_protect": "1", //CSRF 防护</p> <p>"sql_inject_protect": "1", //SQL 注入防护</p> <p>"xss_protect": "1", //XSS 攻击防护</p> <p>"hot_link_protect": "1", //盗链防护</p> <p>"access_ctrl ": "0", //URL 访问控制</p> <p>"url_flow_limit": "0", //URL 流量控制</p> <p>"trojan_protect": "1", //网页挂马防护</p> <p>"violence_scan": "1", //暴力破解防护</p> <p>"spider_protect": "1", //WEB 恶意扫描防护</p> <p>"file_filter": "1", //文件上传/下载过滤</p> <p>"cashespeed": "1", //缓存加速</p> <p>"keywordfilter": "1", //WEB 表单关键字过滤</p> <p>"cid_check_url": "1", //客户端访问控制</p> <p>" ip_check ": "1", //源区域访问控制</p>
--	---

	<pre> "xml_dos": "1", //XML Dos 防护 "weak_pwd": "1", //弱口令防护 "apt_detect": "1", //恶意样本检测 "appd_psm ": "0", //敏感信息防护 "virtual_patch": "0", //虚拟补丁 "business_check": "0", //业务合规 "ref_flag": "1" //引用次数, 大于 0 不允许删 }] }错误数据返回请参见返回错误数据对应内容 </pre>
--	---

3.8.4 查看扫描防护

请求接口	http://ip:port/v2/scanProtect?action=show&profile=xx &module=0
请求方式	GET
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <p>暴力破解和扫描防护共用GET请求</p> <p>profile为对应的站点安全名</p> <p>module=0为扫描防护</p>
返回码	200

返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre> { "result" : "0" , "profile": "default", // 站点名称 "sub_mod": [{ "type": 1, //类型, 1-爬虫, 2-CGI 扫描, 3-漏洞扫描, 4-暴力破解 "action": "0", //执行动作, 0-通过, 1-阻断 "enable": "1", //开关, 0-关闭, 1-开启 //以下为默认值 "log_enable": "1", //日志开关, 0-关闭, 1-开启 "log_level": "6", //日志级别, 6-信息, 5-通知, 4-警示, 1-告警 "acl_block_time": "0", //阻断时间(分钟) "detect_level ": "0", //检测等级, 0-低, 1-中, 2-高, 3-最高。(只有扫描防护有此节点, 暴力破解不需要这个节点) "resp": "4224", //响应方式, 4224-邮件和短信, 4096-短信, 128-邮件, 0-无 "ipex_enable": "0", //IP 例外开关, 0-关闭, 1-开启 </pre>

	<p>"ipex_addr_obj_name": "any" //IP 例外对象名, 只有当 ipex_enable 开启时可配置(地址对象名)</p> <p>}}</p> <p>}</p> <p>错误数据返回请参见返回错误数据对应内容</p>
--	--

3.8.5 修改扫描防护

请求接口	http://ip:port/v2/scanProtect?action=mod
请求方式	POST
请求参数	<p>需携带ts、sign两个参数, 具体见认证流程 (这两个参数建议放到url里) 。</p> <p>暴力破解和扫描防护共用一个xml</p> <p>POST参数</p> <pre>{ "profile": "default", // 站点名称 "sub_mod": { "type": 1, //类型, 1-爬虫, 2-CGI 扫描, 3-漏洞扫描, 4-暴力破解 "action": 0, //执行动作, 0-通过, 1-阻断 "enable": 1, //开关, 0-关闭, 1-开启 } }</pre>

	<p>//以下为默认值</p> <p>"log_enable": 1, //日志开关, 0-关闭, 1-开启</p> <p>"log_level": 6, //日志级别, 6-信息, 5-通知, 4-警示, 1-告警</p> <p>"acl_block_time": 0, //阻断时间(分钟)</p> <p>"detect_level ": 1, //检测等级, 0-低, 1-中, 2-高, 3-最高。(只有扫描防护有此节点, 暴力破解不需要这个节点)</p> <p>"resp": 4224, //响应方式, 4224-邮件和短信, 4096-短信, 128-邮件, 0-无</p> <p>"ipex_enable": 0, //IP 例外开关, 0-关闭, 1-开启</p> <p>"ipex_addr_obj_name":"" //IP 例外对象名, 只有当 ipex_enable 开启时可配置(地址对象名)</p> <p>}</p> <p>}</p>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据:</p> <p>{ "result" : "0" }</p> <p>错误数据返回请参见返回错误数据对应内容</p>

3.8.6 查看暴力破解

请求接口	http://ip:port/v2/scanProtect?action=show&profile=xx &module=1
请求方式	GET
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <p>暴力破解和扫描防护共用GET请求</p> <p>profile为对应的站点安全名</p> <p>module=1为暴力破解， module=0为扫描防护</p>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" , "profile": "default", // 站点名称 "sub_mod": { "type": 1, //类型， 1-爬虫， 2-CGI 扫描， 3-漏洞扫描， 4-暴力破解 "action": 0, //执行动作， 0-通过， 1-阻断 "enable": 1, //开关， 0-关闭， 1-开启</pre>

	<p>//以下为默认值</p> <p>"log_enable": 1, //日志开关, 0-关闭, 1-开启</p> <p>"log_level": 6, //日志级别, 6-信息, 5-通知, 4-警示, 1-告警</p> <p>"acl_block_time": 0, //阻断时间(分钟)</p> <p>"detect_level ": 0, //检测等级, 0-低, 1-中, 2-高, 3-最高。(只有扫描防护有此节点, 暴力破解不需要这个节点)</p> <p>"resp": 4224, //响应方式, 4224-邮件和短信, 4096-短信, 128-邮件, 0-无</p> <p>"ipex_enable": 0, //IP 例外开关, 0-关闭, 1-开启</p> <p>"ipex_addr_obj_name": "any" , //IP 例外对象名, 只有当 ipex_enable 开启时可配置(地址对象名)</p> <p>},</p> <p>"protect_url": "" // 被保护的 url(暴力破解才有此节点)</p> <p>}</p> <p>错误数据返回请参见返回错误数据对应内容</p>
--	--

3.8.7 修改暴力破解

请求接口	http://ip:port/v2/scanProtect?action=mod
请求方式	POST

请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <p>暴力破解和扫描防护共用一个xml</p> <p>POST参数</p> <pre>{ "profile": "default", // 站点名称 "sub_mod": { "type": 1, //类型, 1-爬虫, 2-CGI 扫描, 3-漏洞扫描, 4-暴力破解 "action": 0, //执行动作, 0-通过, 1-阻断 "enable": 1, //开关, 0-关闭, 1-开启 //以下为默认值 "log_enable": 1, //日志开关, 0-关闭, 1-开启 "log_level": 6, //日志级别, 6-信息, 5-通知, 4-警示, 1-告警 "acl_block_time": 0, //阻断时间(分钟) "detect_level ": 1, //检测等级, 0-低, 1-中, 2-高, 3-最高。(只有扫描防护有此节点, 暴力破解不需要这个节点) "resp": 4224, //响应方式, 4224-邮件和短信, 4096-短信, 128-邮件, 0-无 "ipex_enable": 0, //IP 例外开关, 0-关闭, 1-开启</pre>
------	--

	<pre> "ipex_addr_obj_name":""," //IP 例外对象名, 只有当 ipex_enable 开启时可配置(地址对象名) }, "protect_url": [// 被保护的 url(暴力破解才有此节点) //此字段填空 { "url": "/abc", //被保护 url "usr": "test", //用户参数 "pwd": "test"//密码参数, 明文 }] } </pre>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据:</p> <pre>{ "result" : "0" }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.8.8 查看慢速攻击

请求接口	http://ip:port/v2/slowAttack?action=show&profile=xx
请求方式	GET

请求参数	需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。 profile为对应的站点安全名
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" , "profile": "default", // 站点名称 "enable": "1," //开关, 0-关闭, 1-开启 "action": "0" //动作, 0-通过, 1-丢弃 }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.8.9 修改慢速攻击

请求接口	http://ip:port/v2/slowAttack?action=mod
请求方式	POST
请求参数	需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。 POST参数

	<pre> { "profile": "default", // 站点名称 "enable": 1, //开关, 0-关闭, 1-开启 "action": 0, //动作, 0-通过, 1-丢弃 //以下为默认值 "log_enable": 1, //日志开关, 0-关闭, 1-开启 "log_level": 6, //日志级别, 6-信息, 5-通知, 4-警示, 1-告警 "detect_sensitive_level ": 0, //检测敏感度, 0-低, 1- 中, 2-高, 3-自定义 "detect_type ": 0, // "detect_cycle ": 0, //异常报文间隔 (只能是 1-120 单位 秒) , 只有检测敏感度是 3 时, 才填写此字段 "packet_count ": 0, //整型, 异常报文个数(只能是 1- 30, 单位个) , 只有检测敏感度是 3 时, 才填写此字段 "resp": 4224, //响应方式, 4224-邮件和短信, 4096-短 信, 128-邮件, 0-无 "ipex_enable": 0, //IP 例外开关, 0-关闭, 1-开启 "ipex_param":"" //IP 例外对象名, 只有当 ipex_enable 开启时可配置(地址对象名) } </pre>
--	--

返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.8.10 查看 SQL 注入防护

请求接口	http://ip:port/v2/sqlProtect?action=show&profile=xx&type=SQL
请求方式	GET
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <p>profile为对应的站点安全名</p> <p>type为SQL</p>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" , "profile": "default", // 站点名称</pre>

	<pre> "sign_enable": "1", //开关, 0-关闭, 1-开启 "sign_action": "0" //动作, 0-通过, 1-丢弃, 4-返回错误 页面 6-返回重定向 URL } 错误数据返回请参见返回错误数据对应内容 </pre>
--	---

3.8.11 修改 SQL 注入防护

请求接口	http://ip:port/v2/sqlProtect?action=mod
请求方式	POST
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <p>POST参数</p> <pre> { "profile": "default", // 站点名称 "sign_enable": 1, //开关, 0-关闭, 1-开启 "sign_action": 1, //动作, 0-通过, 1-丢弃, 4-返回错误 页面 6-返回重定向 URL //以下为默认值 "log_enable": 1, //日志开关, 0-关闭, 1-开启 "log_level": 1, //日志级别 </pre>

	<pre> "raw_pkt_enable": 0, //是否提取原始报文 "raw_pkt_time": 60, //提取最长时间 "raw_pkt_size": 1024, //提取文件大小 "record_header_enable": 0, //是否提取请求头信息 "database": 31, // "acl_block_time": 0, // "resp": 4224, //响应方式, 4224-邮件和短信, 4096-短信, 128-邮件, 0-无 "ipex_enable": 0, //IP 例外开关, 0-关闭, 1-开启 "ipex_param":"" //IP 例外对象名, 只有当 ipex_enable 开启时可配置(地址对象名) "exception_url": ""// } </pre>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据:</p> <pre>{ "result" : "0" }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.8.12 查看 XSS 攻击防护

请求接口	http://ip:port/v2/xssProtect?action=show&profile=xx&type=XSS
请求方式	GET
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <p>profile为对应的站点安全名</p> <p>type为XSS</p>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" , "profile": "default", // 站点名称 "sign_enable": "1" , //开关, 0-关闭, 1-开启 "sign_action": "1" //动作, 0-通过, 1-丢弃, 4-返回 错误页面 6-返回重定向 URL }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.8.13 修改 XSS 攻击防护

请求接口	http://ip:port/v2/sqlProtect?action=mod
请求方式	POST
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <p>POST参数</p> <pre>{ "profile": "default", // 站点名称 "sign_enable": 1, //开关, 0-关闭, 1-开启 "sign_action": 0, //动作, 0-通过, 1-丢弃, 4-返回错误页面 6-返回重定向 URL //以下为默认值 "log_enable": 1, //日志开关, 0-关闭, 1-开启 "log_level": 1, //日志级别 "raw_pkt_enable": 0, //是否提取原始报文 "raw_pkt_time": 60, //提取最长时间 "raw_pkt_size": 1024, //提取文件大小 "record_header_enable": 0, //是否提取请求头信息 "database": 65535, // "acl_block_time": 0, //</pre>

	<p>"resp": 4224, //响应方式, 4224-邮件和短信, 4096-短信, 128-邮件, 0-无</p> <p>"ipex_enable": 0, //IP 例外开关, 0-关闭, 1-开启</p> <p>"ipex_param":"" //IP 例外对象名, 只有当 ipex_enable 开启时可配置(地址对象名)</p> <p>"exception_url": ""//</p> <p>}</p>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据:</p> <p>{ "result" : "0" }</p> <p>错误数据返回请参见返回错误数据对应内容</p>

3.8.14 查看敏感信息防护

请求接口	http://ip:port/v2/appdPsm?action=show&profile=xx
请求方式	GET
请求参数	<p>需携带ts、sign两个参数, 具体见认证流程 (这两个参数建议放到url里) 。</p> <p>profile为对应的站点安全名</p>

返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" , "profile": "default", // 站点名称 "enable": "1" , //总开关, 0-关闭, 1-开启 "os_hidden": "1" , //操作系统信息防护开关, 0-关闭, 1-开启 "web_server_hidden": "1" , //服务器信息防护开关, 0-关闭, 1-开启 "web_error_hidden": "0" , //错误页面信息防护开关, 0-关闭, 1-开启 "errorcode_customize": "503" , //错误码, 只能填写 200,403,404,503 "card_hidden": "0" , //银行卡信息防护开关, 0-关闭, 1-开启 "czn_hidden": "0" //身份证信息防护开关, 0-关闭, 1- 开启 }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.8.15 修改敏感信息防护

请求接口	http://ip:port/v2/appdPsm?action=mod
请求方式	POST
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <p>POST参数</p> <pre>{ "profile": "default", // 站点名称 "enable": 1, //总开关, 0-关闭, 1-开启 "os_hidden": 1, //操作系统信息防护开关, 0-关闭, 1-开启 "web_server_hidden": 1, //服务器信息防护开关, 0-关闭, 1-开启 "web_error_hidden": 0, //错误页面信息防护开关, 0-关闭, 1-开启 "errorcode_customize": 503, //错误码, 只能填写200,403,404,503 "card_hidden": 0, //银行卡信息防护开关, 0-关闭, 1-开启 "czn_hidden": 0, //身份证信息防护开关, 0-关闭, 1-开启</pre>

	<p>//以下为默认值</p> <p>"resp": 4224, //响应方式, 4224-邮件和短信, 4096-短信, 128-邮件, 0-无</p> <p>"ftp_enable_flag": 0,</p> <p>"psm_log": 1,</p> <p>"psm_level": 6,</p> <p>"psm_replace_word": "x",</p> <p>"reg_pro": 0,</p> <p>"ftpserverinfo_hide": 0,</p> <p>"wag_page_flag": 0, //</p> <p>"reg_list": {}</p> <p>}</p>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据:</p> <p>{ "result" : "0" }</p> <p>错误数据返回请参见返回错误数据对应内容</p>

3.8.16 修改事件引擎

请求接口	http://ip:port/v2/detectEvt?action=mod
请求方式	POST
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <p>POST参数</p> <pre>{ "set_name": "default", // 站点名称，必填 "first_class_id": [//需要开启的一级事件集 一共 1-8 个一级事件分别对应 拒绝服务(1)、木马蠕虫(2)、爬虫扫描(3)、通用攻击(4)、信 息泄露(5)、溢出攻击(6)、注入攻击(7)、其他类型(8)。如想 开启哪个事件，请将 level_id 按照如下形式填写。不填写的 即为不启用。如下， 开启 1, 5, 6, 8 {"level_id": 1}, {"level_id": 5}, {"level_id": 6}, {"level_id": 8}], //以下字段无需关注，不需要传输 "enable": 1, //总开关， 0-关闭， 1-开启</pre>

	<pre> "domainname": "", //填写空即可 "mode": 3, //模式, 下发默认值 "search_str": "", //需要搜索的事件名称, 下发默认值 "action": "", //需要搜索的动作, 下发默认值 "sig_level": , //事件级别, 下发默认值 "sec_class_id": , //下发默认值 "sig_evt_id": , //下发默认值 "unchange_list": //下发默认值 } </pre>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据:</p> <pre>{ "result" : "0" }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.9 SSL 证书配置

3.9.1 查看证书

请求接口	http://ip:port/v2/certInfo?action=show
请求方式	GET

请求参数	需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" "certs" : [{ // 证书 1 "local_cert_name": "no1", //证书名称 "local_cert_state": 1, //证书状态， 1-正常， 0-未确定 "local_cert_locate": 0, //位置， 1-USB key, 0-本地文件 "issuer": "C=cn, ST=Some-State, O=Internet Widgits Pty Ltd, CN=ca", //证书发行者 "subject": "C=cn, ST=Some-State, O=Internet Widgits Pty Ltd, CN=no1", //主题 "start_time": "Dec 15 16:33:27 2014 GMT", //开始时间 "end_time": "Mar3 16:33:27 2023 GMT", //结束时间</pre>

	<p>"version ": "3", //版本</p> <p>"serial_num": "2102112123", //序列号</p> <p>"ext_info": "X509v3 Subject Key Identifier:&#xD;%9", //序列号</p> <p>"ref": "1", //证书引用次数, 如果大于 0 则改证书允许删除</p> <p>},</p> <p>{</p> <p>// 证书 2</p> <p>"local_cert_name": "no2", //证书名称</p> <p>"local_cert_state": 1, //证书状态, 1-正常, 0-未确定</p> <p>"local_cert_locate": 0, //位置, 1-USB key, 0-本地文件</p> <p>"issuer": "C=cn, ST=Some-State, O=Internet Widgits Pty Ltd, CN=ca_user", //证书发行者</p> <p>"subject": "C=cn, ST=Some-State, O=Internet Widgits Pty Ltd, CN=no2", //主题</p> <p>"start_time": "Dec 15 16:33:27 2014 GMT", //开始时间</p> <p>"end_time": "Mar3 16:33:27 2023 GMT", //结束时间</p> <p>"version ": "3", //版本</p> <p>"serial_num": "2102112126", //序列号</p>
--	---

	<pre>"ext_info": "X509v3 Subject Key Identifier: &#xD;%9", // 序列号 "ref": "1", // 证书引用次数, 如果大于 0 则改证书允许删除 }] }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>
--	--

3.9.2 删除证书

请求接口	http://ip:port/v2/certInfo?action=del&name=xxx
请求方式	GET
请求参数	需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。 name为证书名称
返回码	200
返回格式	application/json;charset=utf-8
返回数据	正确数据： { "result" : "0" } 错误数据返回请参见 返回错误数据对应内容

3.9.3 导入证书

请求接口	http://ip:port/v2/certInfo?action=mod
请求方式	POST
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <p>POST参数</p> <pre>{ "cert_file_name": "no1.crt", //证书文件名 "key_file_name": "no1.key", //密钥文件名 "type": 3, //证书类型, 2-PKCS12, 3-证书密钥分离 "password": "xxxx", //证书密码 "cert_file_content": "xxxx", //证书内容, 格式为读取文件后 base64 编码后的内容 "key_file_content": "xxxx", //密钥内容, 同上 "upload_location": 0, //上传路径, 0-本地, 1-USB key }</pre>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" }</pre>

	错误数据返回请参见 返回错误数据对应内容
--	--------------------------------------

3.10 事件库升级

3.10.1 事件库立即升级

请求接口	http://ip:port/v2/eventbaseupdate?action=add
请求方式	POST
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <p>POST参数</p> <pre>{ "server_style": 0, //服务器类型，0-默认升级服务器，1-指定升级服务器 "server_addr": "", //升级地址，如果 style 为 0，此字段为空 }</pre>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.10.2 获取事件库升级日志

请求接口	http://ip:port/v2/eventbaselogs?action=show
请求方式	GET
请求参数	需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" , "logs" : [{ "version": "V0700R0703B20170309", //更新版本 "up_time": "2017-03-09 19:00:15", //升级时间 "up_name": 0 //0-系统软件, 1-预定义事件库升级, 2- 恶意 URL 云库升级 }] }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.11 安全事件统计

3.11.1 获取安全事件统计

请求接口	http://ip:port/v2/securityEventStat?action=show
请求方式	GET
请求参数	需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" "attack" : [//按事件名称统计top10 { "HTTP_SQL注入攻击 " : "180", //事件数 "HTTP业务合规" : "65", //事件数 "HTTP_url躲避" : "10"//事件数 }] }</pre> <p>备注中文为 unicode</p>

	<p>例如业务合规\u4e1a\u52a1\u5408\u89c4</p> <p>错误数据返回请参见返回错误数据对应内容</p>

3.12 Flood 防护

3.12.1 查看智能 TCP FLOOD 防御配置

请求接口	http://ip:port/v2/antiAttack?action=show
请求方式	GET
请求参数	需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" , "anti_attack": { "sys_cookie_enable": 1, //智能 tcp 防御功能开关, 0-关闭, 1-开启 } }</pre>

	<p>"tcp_half": 2000, //TCP Flood 识别阈值(10-10000), 单位秒</p> <p>"log_enable": 1, //日志开关, 0-关闭, 1-开启</p> <p>"log_level": 6, //日志级别, 6-信息, 5-通知, 4-警示, 1-告警</p> <p>"resp": 4224, //响应方式, 4224-邮件和短信, 4096-短 信, 128-邮件, 0-无</p> <p>}</p> <p>}</p> <p>错误数据返回请参见返回错误数据对应内容</p>
--	---

3.12.2 修改智能 TCP FLOOD 防御配置

请求接口	http://ip:port/v2/antiAttack?action=mod
请求方式	POST
请求参数	<p>需携带ts、sign两个参数, 具体见认证流程 (这两个参数建议放到url里) 。</p> <p>POST参数</p> <p>{</p> <p>"sys_cookie_enable": 1, //智能 tcp 防御功能开关, 0-关闭, 1-开启</p>

	<p>"tcp_half": 2000, //TCP Flood 识别阈值(10-10000), 单位秒</p> <p>"log_enable": 1, //日志开关, 0-关闭, 1-开启</p> <p>"log_level": 6, //日志级别, 6-信息, 5-通知, 4-警示, 1-告警</p> <p>"resp": 4224, //响应方式, 4224-邮件和短信, 4096-短 信, 128-邮件, 0-无</p> <p>}</p>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据:</p> <p>{ "result" : "0" }</p> <p>错误数据返回请参见返回错误数据对应内容</p>

3.13 软件 Bypass

3.13.1 修改软件 Bypass

请求接口	http://ip:port/v2/vsSoftBypass?action=mod
请求方式	POST
请求参数	<p>需携带ts、sign两个参数, 具体见认证流程 (这两个参数建议放到url里) 。</p> <p>POST参数</p>

	<pre>{ "bypass":1//开关, 0-关闭, 1-开启 }</pre>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据:</p> <pre>{ "result" : "0" }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.14 黑/白名单配置

3.14.1 获取所有黑/白名单

请求接口	<p>http://ip:port/v2/fwBlackList?action=show(黑名单)</p> <p>http://ip:port/v2/fwWhiteList?action=show(白名单)</p>
请求方式	GET
请求参数	需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。
返回码	200
返回格式	application/json;charset=utf-8

返回数据	<p>正确数据:</p> <pre>{ "result" : "0" , "fw_list" : [{ "name": "123", //名称 "if_in": "any", //作用域接口 "src_addr_type": "0", //源地址类型, 0-主机, 1-网段, 2- 地址范围, 10-ipv6 主机, 11-ipv6 网段, 12-ipv6 地址范围 "src_addr_host": "10.10.12.32", //源地址主机地址 "src_addr_net": "10.10.12.1/24", //源地址网段地址 "src_addr_range1": "11.24.53.1", //源地址范围开始地址 "src_addr_range2": "11.24.53.254", //源地址范围结束地址 "dst_addr_type": "0", //目的地址类型, 0-主机, 1-网段, 2-地址范围, 10-ipv6 主机, 11-ipv6 网段, 12-ipv6 地址范 围 "dst_addr_host": "10.10.12.32", //目的地址主机地址 "dst_addr_net": "10.10.12.1/24", //目的地址网段地址 "dst_addr_range1": "11.24.53.1", //目的地址范围开始地址 "dst_addr_range2": "11.24.53.254", //目的地址范围结束地 址 "dst_port": "80", //目的端口</pre>
------	---

	<p>"set_periodic": "0", //时间设置开关, 0-关闭, 1-开启</p> <p>"week_day": "1", //1、2、3、4、5、6、7 分别代表周一到周日</p> <p>"day_enable_time": "1-5", //时间段, 表示几点到几点(24小时制)</p> <p>"log": "1", //日志开关, 0-关闭, 1-开启</p> <p>"log_level": "6", //日志级别, 6-信息, 5-通知, 4-警示, 1-告警</p> <p>"enable": "1", //开关, 0-关闭, 1-开启</p> <p>}</p> <p>]</p> <p>}</p> <p>错误数据返回请参见返回错误数据对应内容</p>
--	--

3.14.2 添加/修改黑/白名单

请求接口	<p>http://ip:port/v2/fwBlackList?action=add(黑名单)</p> <p>http://ip:port/v2/fwBlackList?action=mod(黑名单)</p> <p>http://ip:port/v2/fwWhiteList?action=add(白名单)</p> <p>http://ip:port/v2/fwWhiteList?action=mod(白名单)</p>
请求方式	POST
请求参数	需携带ts、sign两个参数, 具体见认证流程 (这两个参数建

	<p>议放到url里) 。</p> <pre> { "name": "123", //名称 "if_in": "any", //作用域接口 "src_addr_type": 0, //源地址类型, 0-主机, 1-网段, 2-地址范围, 10-ipv6 主机, 11-ipv6 网段, 12-ipv6 地址范围 "src_addr_host": "10.10.12.32", //源地址主机地址 "src_addr_net": "10.10.12.1/24", //源地址网段地址 "src_addr_range1": "11.24.53.1", //源地址范围开始地址 "src_addr_range2": "11.24.53.254", //源地址范围结束地址 "dst_addr_type": 0, //目的地址类型, 0-主机, 1-网段, 2-地址范围, 10-ipv6 主机, 11-ipv6 网段, 12-ipv6 地址范围 "dst_addr_host": "10.10.12.32", //目的地址主机地址 "dst_addr_net": "10.10.12.1/24", //目的地址网段地址 "dst_addr_range1": "11.24.53.1", //目的地址范围开始地址 "dst_addr_range2": "11.24.53.254", //目的地址范围结束地址 </pre>
--	---

	<p>"dst_port": 80, //目的端口</p> <p>"set_periodic": 0, //时间设置开关, 0-关闭, 1-开启</p> <p>"week_day": 1, //1、2、3、4、5、6、7 分别代表周一到周日</p> <p>"day_enable_time": "1-5", //时间段, 表示几点到几点(24 小时制)</p> <p>"log": 1, //日志开关, 0-关闭, 1-开启</p> <p>"log_level": 6, //日志级别, 6-信息, 5-通知, 4-警示, 1-告警</p> <p>"enable": 1//开关, 0-关闭, 1-开启</p> <p>}</p>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据:</p> <p>{ "result" : "0" }</p> <p>错误数据返回请参见返回错误数据对应内容</p>

3.14.3 删除黑/白名单

请求接口	http://ip:port/v2/fwBlackList?action=del&name=xx(黑名单)
------	---

	http://ip:port/v2/fwWhiteList?action= del&name=xx (白名单)
请求方式	GET
请求参数	需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。 name为黑/白名单的名称
返回码	200
返回格式	application/json;charset=utf-8
返回数据	正确数据： { "result" : "0" } 错误数据返回请参见 返回错误数据对应内容

3.14.4 开启/关闭黑/白名单

请求接口	http://ip:port/v2/fwListState?action=mod
请求方式	POST
请求参数	需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。 { "result" : "0" , "mode" : 2, //1-白名单, 2-黑名单 "name" : "test", //需要开启/关闭名单的名称，不能为空

	<pre>"enable" : 1, //开关, 0-关闭, 1-开启 }</pre>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据:</p> <pre>{ "result" : "0" }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.15 网关配置

3.15.1 获取所有网关

请求接口	http://ip:port/v2/gateList?action=show
请求方式	GET
请求参数	需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据:</p> <pre>{</pre>

	<pre>"result" : "0" , "gate_list" :[//可以是多个网关 { "gate_ip":"1.1.1.1", //网关 IP 地址 "oif ":"", //出接口, 无 "get_style": 0, //默认值 "distance": 1, //管理距离(1-255) "weight":1, //权重(1-100) "ip_ver":4//IP 类型, 4-IPv4, 6-IPv6 }] }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>
--	--

3.15.2 添加网关

请求接口	http://ip:port/v2/gateList?action=add
请求方式	POST
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <pre>{ "gate_ip":"1.1.1.1", //网关 IP 地址</pre>

	<pre> "distance": 1, //管理距离(1-255) "weight":1, //权重(1-100) "ip_ver":4//IP 类型, 4-IPv4, 6-IPv6 } </pre>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" ,}</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.15.3 删除网关

请求接口	http://ip:port/v2/gateList?action=del
请求方式	POST
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <pre> { "gate_ip":"1.1.1.1", //网关 IP 地址 "oif ":"", //出接口, 保留值, 不填写值 "ip_ver":4//IP 类型, 4-IPv4, 6-IPv6 } </pre>

返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" ,}</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.16 静态路由配置

3.16.1 获取所有静态路由

请求接口	http://ip:port/v2/staticRouteList?action=show
请求方式	GET
请求参数	需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" , "static_route_list" : [//可以是多个静态路由</pre>

	<pre>{ "dst_ip": "0.0.0.0/0", //网段及掩码 "nh_type": "0", //下一跳类型, 0-下一跳, 1-出接口 "nh_ip": "192.168.1.2", //如果 nh_type=0, 则表示下一 跳 IP 地址; 如果 nh_type=1, 则表示出接口名称, 比如 ETH1 "distance": "1", //管理距离(1-255) "weigh": "1", //权重(1-100) }] }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>
--	--

3.16.2 添加静态路由

请求接口	http://ip:port/v2/staticRouteList?action=add
请求方式	POST
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <pre>{ "dst_ip": "0.0.0.0/0", //网段及掩码 "nh_type": 0, //下一跳类型, 0-下一跳, 1-出接口</pre>

	<pre> "nh_ip": "192.168.1.2", //如果 nh_type=0, 则表示下一跳 IP 地址; 如果 nh_type=1, 则表示出接口名称, 比如 ETH1 "distance": 1, //管理距离(1-255) "weight":1, //权重(1-100) "ip_ver":4//IP 类型, 4-IPv4, 6-IPv6 } </pre>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据:</p> <pre>{ "result" : "0" ,}</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.16.3 修改路由

请求接口	http://ip:port/v2/staticRouteList?action=mod
请求方式	POST
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <p>只允许修改权重和管理距离，其他项必须在路由表里有</p> <pre>{</pre>

	<pre> "dst_ip": "0.0.0.0/0", //网段及掩码(修改时不能改此项) "nh_type": 0, //下一跳类型, 0-下一跳, 1-出接口(修改时不能改此项) "nh_ip": "192.168.1.2", //如果 nh_type=0, 则表示下一跳 IP 地址; 如果 nh_type=1, 则表示出接口名称, 比如 ETH1 (修改时不能改此项) "distance": 1, //管理距离(1-255) "weigh": 1, //权重(1-100) "ip_ver": 4 //IP 类型, 4-IPv4, 6-IPv6(修改时不能改此项) } </pre>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据:</p> <pre>{ "result" : "0" ,}</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.16.4 删除路由

请求接口	http://ip:port/v2/staticRouteList?action=del
请求方式	POST

请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <pre> { "dst_ip": "0.0.0.0/0", //网段及掩码 "nh_type": 0, //下一跳类型， 0-下一跳， 1-出接口 "nh_ip": "192.168.1.2", //如果 nh_type=0，则表示下一跳 IP 地址；如果 nh_type=1，则表示出接口名称，比如 ETH1 "ip_ver": 4 //IP 类型， 4-IPv4， 6-IPv6 } </pre>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.17 设备参数

3.17.1 设备重启

请求接口	http://ip:port/v2/powerOff?action=mod
------	---------------------------------------

请求方式	POST
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p> <p>POST参数</p> <pre>{ "operation": "0" //重启参数，必须是 0, 0 必须带引号为字符型 }</pre>
返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>

3.17.2 保存配置

请求接口	http://ip:port/v2/saveConfig?action=mod
请求方式	GET
请求参数	<p>需携带ts、sign两个参数，具体见认证流程（这两个参数建议放到url里）。</p>

返回码	200
返回格式	application/json;charset=utf-8
返回数据	<p>正确数据：</p> <pre>{ "result" : "0" }</pre> <p>错误数据返回请参见返回错误数据对应内容</p>