中新金盾抗拒绝服务系统

（API 接口说明）

中新网络信息安全股份有限公司

文档编码：ZXS-TD-DMS API 接口说明-v4.0

目 录

1 登陆

1.1 功能说明

通过用户名和密码登陆设备，获取会话 sid，之后每次请求在 cookie 中须携带此 sid 以通过验证。

1.2 接口调用 URL

http://[域名]/cgi-bin/login.cgi

1.3 输入参数

以 POST 方式传递以下参数：

表 1.1 登录 POST 参数

参数名称	是否必须	说明
param_type	是	固定值：login
param_username	是	登陆用户名；例如：admin
param_password	是	登陆密码；例如：123

说明

1. 登录过程需要将字段和字段值组合成字符串提交到接口；
2. 后面所有接口的获取或者提交都需要带登录过程中返回的 COOKIE 信息。

1.4 输出参数

- 登陆成功

登陆成功输出信息为 XML，跳转到/cgi-bin/status_global.cgi。

```
<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/xsl" version="1.0" href="/redirect.xsl"?>
<redirect>
 <page>/cgi-bin/status_global.cgi</page>
</redirect>
```

➢ 登陆失败

登陆失败输出信息为 XML，错误提示并跳转到/index.html。

```
<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/xsl" version="1.0" href="/zh-cn/xsl/failure.xsl"?>


<failure>
 <info>.....</info>
 <url>/index.html</url>
 <params></params>
</failure>
```

1.5 示例

➢ 请求

```
POST /cgi-bin/login.cgi HTTP/1.1
Host: 192.168.59.220:28099
.....
param_type=login&param_username=admin&param_password=123
```

➢ 返回

```
HTTP/1.1 200 OK
……
Set-Cookie:
sid=%07o%B4%88O%EE%0Ca%07%DA%D8i%D36HE%AF%28%BC%3C%BE%D5s%DFv%A6%
D83%D9%3E%16%96%09%1Dq%CF%D0d%85%98f%04%27%5DX%14%9DM
Content-Length: 173
```

```
Date: Fri, 04 May 2018 03:29:09 GMT
Server: HTTP-SRV


<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/xsl" version="1.0" href="/redirect.xsl"?>
<redirect>
 <page>/cgi-bin/status_global.cgi</page>
</redirect>
```

2 状态监控

2.1 全局统计

2.1.1 接口调用 URL

http://[域名]/cgi-bin/status_global.cgi

2.1.2 输入参数

GET 方式请求。

2.1.3 输出参数

全局统计标签为< status_global>。

表 2.1 全局统计标签

参数名称	说明
wan_input_bps	输入 bps
wan_input_pps	输入 pps
wan_submit_bps	输入过滤后 bps
wan_submit_pps	输入过滤后 pps
lan_input_bps	输出 bps（串联特有）
lan_input_pps	输出 pps（串联特有）
lan_submit_bps	输出过滤后 bps（串联特有）
lan_submit_pps	输出过滤后 bps（串联特有）
anonymous_incoming_bps	外网匿名流量 bps（串联特有）
anonymous_incoming_submit_bps	外网匿名流量过滤后 bps（串联特有）

anonymous_outgoing_bps	内网匿名流量 bps（串联特有）
anonymous_outgoing_submit_bps	内网匿名流量过滤后 bps（串联特有）
tcp_conn_in	TCP 进链接
tcp_conn_out	TCP 出链接
udp_conn	UDP 链接

2.1.4 示例

- 请求

```
GET /cgi-bin/status_global.cgi HTTP/1.1
```

- 返回

```
HTTP/1.1 200 OK
…

<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/xsl" version="1.0" href="/zh-cn/xsl/status_global.xsl"?>

<status_global>
    <wan_input_bps>0.00</wan_input_bps>
    <wan_input_pps>0</wan_input_pps>
    <wan_submit_bps>0.00</wan_submit_bps>
    <wan_submit_pps>0</wan_submit_pps>
    <lan_input_bps>0.00</lan_input_bps>
    <lan_input_pps>0</lan_input_pps>
    <lan_submit_bps>0.00</lan_submit_bps>
    <lan_submit_pps>0</lan_submit_pps>
    <anonymous_incoming_bps>0.00</anonymous_incoming_bps>
    <anonymous_incoming_submit_bps>0.00</anonymous_incoming_submit_bps>
    <anonymous_outgoing_bps>0.00</anonymous_outgoing_bps>
    <anonymous_outgoing_submit_bps>0.00</anonymous_outgoing_submit_bps>
    <tcp_conn_in>0</tcp_conn_in>
    <tcp_conn_out>0</tcp_conn_out>
```

```
    <udp_conn>0</udp_conn>
</status_global>
```

2.2 系统负载

2.2.1 接口调用 URL

http://[域名]/cgi-bin/status_health.cgi

2.2.2 输入参数

Get 方式获取。

2.2.3 输出参数

系统负载标签为< status_health>。

表 2.2 系统负载标签

一级标签	二级标签	说明
rack_unit_list		硬件单元标签（ATCA 独有）
	this_rack_unit	当前硬件单元
	rack_unit	其他硬件单元，依次排列
cpu_usage		CPU 占用率
memory_usage		内存使用
device_stat		网络接口统计（每个接口一个标签）
	name	接口名称
	recv_flow	接收流量（Mbps）
	recv_pps	接收报文（pps）
	recv_err	接收错误报文（pps）
	send_flow	发送流量（Mbps）
	send_pps	发送报文（pps）
	send_err	发送错误报文（pps）

2.2.4 示例

- 请求

```
GET /cgi-bin/status_health.cgi HTTP/1.1
```

- 返回

```
HTTP/1.1 200 OK
……
<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/xsl" version="1.0" href="/zh-cn/xsl/status_health.xsl"?>

<status_health>
    <rack_unit_list>
        <this_rack_unit>1</this_rack_unit>
        <rack_unit>1</rack_unit>
        <rack_unit>2</rack_unit>
    </rack_unit_list>

    <cpu_usage>3.5% </cpu_usage>
    <memory_usage>16626 MB total, 25.1% used</memory_usage>
    <device_stat>
        <name>xgbe1</name>
        <recv_flow>0.00</recv_flow>
        <recv_pps>0</recv_pps>
        <recv_err>0</recv_err>
        <send_flow>0.00</send_flow>
        <send_pps>0</send_pps>
        <send_err>0</send_err>
    </device_stat>
    …
    <device_stat>
        …
    </device_stat>
</status_health>
```

2.3 防护范围

2.3.1 接口调用 URL

http://[域名]/cgi-bin/status_pranges.cgi

2.3.2 输入参数

- Post 方式提交以下参数：

表 2.3 防护范围 POST 输入参数

参数	说明
param_submit_type	操作方式 1. submit：提交； 2. delete：删除 3. import：导入 4. export：导出
param_prange	地址范围（格式：x.x.x.x-x.x.x.x/xx）
param_import_pranges	范围列表
filename	导入配置文件名称
param_import_pranges2	导入配置文件路径

- Get 请求防护范围页面。

2.3.3 输出参数

防护范围输出标签为：<status_pranges>。

表 2.4 防护范围 GET 回应标签

一级标签	二级标签	说明

prange		范围标签
	address	开始地址
	address2	结束地址
	prefix	地址前缀

2.3.4 示例

- POST 提交

```
POST /cgi-bin/status_pranges.cgi HTTP/1.1
……
-----------------------------126082629511250
Content-Disposition: form-data; name="param_submit_type"
submit
-----------------------------126082629511250
Content-Disposition: form-data; name="param_prange"
1.1.1.1-1.1.1.2/24
-----------------------------126082629511250
Content-Disposition: form-data; name="param_import_pranges"; filename=""
Content-Type: application/octet-stream
-----------------------------126082629511250
Content-Disposition: form-data; name="param_import_pranges2"
-----------------------------126082629511250--
```

- GET 请求

```
GET /cgi-bin/status_pranges.cgi HTTP/1.1
```

- 返回

```
HTTP/1.1 200 OK
…
<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/xsl" version="1.0" href="/zh-cn/xsl/status_pranges.xsl"?>
```

```
<status_pranges>
    <prange>
        <address>1.1.1.1</address>
        <address2>1.1.1.2</address2>
        <prefix>24</prefix>
    </prange>
</status_pranges>
```

2.4 主机管理

2.4.1 主机列表

2.4.1.1 功能说明

获取主机各参数报文频率和连接数等，添加、删除、操作主机。

2.4.1.2 接口调用 URL

http://[域名] /cgi-bin/status_host.cgi

2.4.1.3 输入参数

POST 方式提交以下参数（查询、排序等均是 post 方式）：

表 2.5 主机状态 POST 提交

参数	说明
param_submit_type	1. query-host：查询 2. add-host：添加 3. 空：其他操作（如排序）
param_netaddr	需要添加或者查询的地址，格式： 1. 单个 IP：x.x.x.x 2. 范围：x.x.x.x-x.x.x.x

	3. 范围+前缀：x.x.x.x-x.x.x.x/xx 4. 空：非添加操作
param_this_sort	排列类型 1. -1：按主机地址排列 2. -2：按带宽排列 3. -5：按频率排列 4. -6：按连接排列 5. 1：默认排列
param_switch_auto_protection	“自动防御”变量： 1. on：勾选 2. 无：不勾选
param_switch_manual_protection	“手动防御”变量： 1. on：勾选 2. 无：不勾选
param_switch_extra_protection	“其他状态”变量： 1. on：勾选 2. 无：不勾选
param_flow_threshold	“流量阈值”变量： 1. 0：全部（默认） 2. 1：任意流量 3. 125：大于 1Kbps 4. 1250：大于 10Kbps 5. 12500：大于 100Kbps 6. 125000：大于 1Mbps 7. 1250000：大于 10Mbps 8. 12500000：大于 100Mbps 9. 125000000：大于 1000Mbps
param_view	“视图”变量： 1. -1：全部 2. 0：总流量前 100 3. 1：输入流量前 100 4. 2：输出流量前 100 5. 3：攻击频率前 100 6. 4：总连接前 100

	7. 5：新建连接前 100

- Get 请求主机列表。

表 2.6 GET 提交

参数	说明
param_view	1. -1：全部 2. 0：总流量前 100 3. 1：输入流量前 100 4. 2：输出流量前 100 5. 3：攻击频率前 100 6. 4：总连接前 100 7. 5：新建连接前 100

2.4.1.4 输出参数

主机状态返回标签为：<status_host >。

表 2.7 主机状态返回标签

一级标签	二级标签	说明
host_address		主机列表
sort_type		排列类型
netaddr		查询的主机
flow_treshold		流量阈值
switch_auto_protection		自动防御
switch_manual_protection		手动防御
switch_extra_protection		其他状态
host		主机标签
	type	主机类型： 1. full：全部主机 2. subnet：网段（子网段） 3. host：主机
	address	具体主机：

		1. 空：全部主机或者查询结果为空 2. x.x.x.x/xx：子网段 3. x.x.x.x：具体主机
	input_bps	输入 bps
	input_pps	输入 pps
	input_submit_bps	输入过滤后 bps
	input_submit_pps	输入过滤后 pps
	output_bps	输出 bps
	output_pps	输出 pps
	output_submit_bps	输出过滤后 bps
	output_submit_pps	输出过滤后 pps
	baseline_reference	基线因子
	syn_rate	Syn 报文频率
	ack_rate	Ack 报文频率
	udp_rate	Udp 报文频率
	icmp_rate	Icmp 报文频率
	frag_rate	碎片报文频率
	nonip_rate	Nonip 报文频率
	new_tcp_rate	新建 tcp 频率
	new_udp_rate	新建 udp 频率
	tcp_conn_in	Tcp 进连接数
	tcp_conn_out	Tcp 出连接数
	udp_conn	Udp 连接数
	icmp_conn	Icmp 连接数
	status	防护状态

2.4.1.5 示例

- POST 提交

```
POST /cgi-bin/status_host.cgi HTTP/1.1
....
```

```
param_submit_type=query-host&param_host_addr=&param_this_sort=1&param_netaddr=&param_flow_threshold=0
```

- GET 请求

```
GET /cgi-bin/status_host.cgi HTTP/1.1
```

- 返回

```
HTTP/1.1 200 OK
。。。
<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/xsl" version="1.0" href="/zh-cn/xsl/status_host.xsl"?>

<status_host>
 <host_address></host_address>
 <sort_type>1</sort_type>
 <netaddr></netaddr>
 <flow_threshold>0</flow_threshold>
 <switch_auto_protection></switch_auto_protection>
 <switch_manual_protection></switch_manual_protection>
 <switch_extra_protection></switch_extra_protection>
 <host>
        <type>host</type>
        <address>1.1.1.1</address>
        <input_bps>0.00</input_bps>
        <input_pps>0</input_pps>
        <input_submit_bps>0.00</input_submit_bps>
        <input_submit_pps>0</input_submit_pps>
        <output_bps>0.00</output_bps>
        <output_pps>0</output_pps>
        <output_submit_bps>0.00</output_submit_bps>
        <output_submit_pps>0</output_submit_pps>
        <baseline_reference>0</baseline_reference>
        <syn_rate>0</syn_rate>
        <ack_rate>0</ack_rate>
        <udp_rate>0</udp_rate>
        <icmp_rate>0</icmp_rate>
        <frag_rate>0</frag_rate>
```

```
        <nonip_rate>0</nonip_rate>
        <new_tcp_rate>0</new_tcp_rate>
        <new_udp_rate>0</new_udp_rate>
        <tcp_conn_in>0</tcp_conn_in>
        <tcp_conn_out>0</tcp_conn_out>
        <udp_conn>0</udp_conn>
        <icmp_conn>0</icmp_conn>
        <status></status>
        <protect_credits>0</protect_credits>
    </host>
    。。。
    <host>
        。。。
    </host>

</status_host>
```

2.4.2 主机设置

2.4.2.1 功能说明

针对主机设置流量策略、忽略、屏蔽等。

2.4.2.2 接口调用 URL

http://[域名] /cgi-bin/status_hostset.cgi

2.4.2.3 输入参数

POST 方式提交以下参数：

表 2.8 主机设置 POST 提交

参数	说明
param_setting_addr	主机 IP 地址（范围）： 1. 单个 IP：x.x.x.x

	2. 范围：x.x.x.x-x.x.x.x
param_prefix	地址前缀
param_exist	有效： 1. ON：勾选“有效” 2. 无：不勾选“有效”（则会删除主机或者范围）
param_record_flow	记录（串联）： 1. ON：勾选“记录” 2. 无：不勾选“记录”
param_force_protect	防护（旁路或者分析器特有字段）： 1. ON：勾选 2. 无：不勾选
param_gateway_ip	网关 IP 地址
param_gateway_mac	网关 MAC 地址
param_flowlimit_incoming_bps	输入 Mbps
param_flowlimit_incoming_pps	输入 PPS
param_flowlimit_outgoing_bps	输出 Mbps
param_flowlimit_outgoing_pps	输出 PPS
param_ignore	忽略所有流量 3. ON：勾选 4. 无：不勾选
param_forbid	屏蔽所有流量 1. ON：勾选 2. 无：不勾选
param_forbid_overflow	流量超出屏蔽 1. ON：勾选 2. 无：不勾选
param_reject_foreign_access	拒绝国外访问 1. ON：勾选 2. 无：不勾选
param_param_set	防护参数集
param_filter_set	过滤规则集

param_portpro_set_tcp	TCP 端口集
param_portpro_set_udp	UDP 端口集
param_plugin_tcp_0	WEB Service Protection xx 1. ON：勾选 2. 无：不勾选
param_plugin_tcp_1	Game Service Protection xx 1. ON：勾选 2. 无：不勾选
param_plugin_tcp_2	Misc Service Protection xx 1. ON：勾选 2. 无：不勾选
param_plugin_tcp_3	TCP DNS Service Protection xx 1. ON：勾选 2. 无：不勾选
Param_plugin_tcp_5	SSL|TLS Service Protection xx 1. ON：勾选 2. 无：不勾选
param_ssl_cert_list	SSL 插件证书
param_plugin_udp_1	UDP DNS Service Protection xx 1. ON：勾选 2. 无：不勾选
param_plugin_udp_4	UDP App Protection xx 1. ON：勾选 2. 无：不勾选

GET 请求输入参数：

表 2.9 主机设置 GET 请求参数

参数	说明
hostaddr	主机 IP 地址

2.4.2.4 输出参数

返回标签为< status_hostset>。

表 2.10 主机设置返回标签

一级标签	二级标签	说明
setting_address		主机列表
address		主机 IP 地址
prefix		地址前缀
exist		有效
record_flow		记录
param_force_protect		防护： 1. on：勾选 2. 空：不勾选
gateway_ip		网关 IP 地址
gateway_mac		网关 MAC 地址
flow_incoming_bps		输入 Mbps
flow_outgoing_bps		输入 PPS
flow_incoming_pps		输出 Mbps
flow_outgoing_pps		输出 PPS
ignore		忽略所有流量
forbid		屏蔽所有流量
forbid_overflow		流量超出屏蔽
reject_foreign		拒绝国外访问
param_set		防护参数集
filter_set		过滤规则集
portpro_set_tcp		TCP 端口集
portpro_set_udp		UDP 端口集
plugin		插件标签
	protocol	插件协议类型： 1. TCP：TCP 协议

		2. UDP：UDP 协议
	id	插件序号，配合 Protocol 使用： 1. 0:WEB Service xx 2. 1:Game Service xx 3. 2:Misc Service xx 4. 3:DNS Service xx（TCP） 5. 5:SSL|TLSServiceProtection 6. 1:DNS Service xx（UDP） 7. 4:UDP APP xx
	name	插件名称：和 id 对应
	enabled	是否开启插件： 1. Checked：开启了插件 2. 空：未开启插件

2.4.2.5 示例

- POST 提交

```
POST /cgi-bin/status_hostset.cgi HTTP/1.1
.....
param_setting_addr=1.1.1.1&param_prefix=24&param_exist=ON&param_gateway_ip=1.1.1.0&param_gateway_mac=&param_flowlimit_incoming_bps=&param_flowlimit_incoming_pps=&param_flowlimit_outgoing_bps=&param_flowlimit_outgoing_pps=&param_param_set=0&param_filter_set=0&param_portpro_set_tcp=0&param_portpro_set_udp=0
```

- GET 请求

```
http://192.168.59.220:28099/cgi-bin/status_hostset.cgi?hostaddr=1.1.1.1
```

- 返回

```
<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/xsl" version="1.0" href="/zh-cn/xsl/status_hostset.xsl"?>

<status_hostset>
    <setting_address>1.1.1.1</setting_address>
    <address>1.1.1.1</address>
```

```
<prefix>24</prefix>
<exist>checked</exist>
<record_flow>checked</record_flow>
<gateway_ip>1.1.1.0</gateway_ip>
<gateway_mac></gateway_mac>
<flow_incoming_bps></flow_incoming_bps>
<flow_outgoing_bps></flow_outgoing_bps>
<flow_incoming_pps></flow_incoming_pps>
<flow_outgoing_pps></flow_outgoing_pps>
<ignore></ignore>
<forbid></forbid>
<forbid_overflow></forbid_overflow>
<reject_foreign></reject_foreign>
<param_set>1</param_set>
<filter_set>0</filter_set>
<portpro_set_tcp>0</portpro_set_tcp>
<portpro_set_udp>0</portpro_set_udp>
<plugin>
    <protocol>tcp</protocol>
    <id>0</id>
    <name>WEB Service Protection v9.02</name>
    <enabled>checked</enabled>
</plugin>
<plugin>
    <protocol>tcp</protocol>
    <id>1</id>
    <name>Game Service Protection v4.1</name>
    <enabled>checked</enabled>
</plugin>
<plugin>
    <protocol>tcp</protocol>
    <id>2</id>
    <name>Misc Service Protection v3.2</name>
    <enabled>checked</enabled>
</plugin>
  <plugin>
    <protocol >tcp</protocol>
```

```
            <id>3</id>
            Service Protection v2.3</name>
          checked</enabled>
      </plugin>
      <plugin>
          <protocol>udp</protocol>
          <id>1</id>
          <name>DNS Service Protection v2.3</name>
          <enabled>checked</enabled>
      </plugin>
      <plugin>
          <protocol>udp</protocol>
          <id>4</id>
          <name>UDP App Protection v1.1</name>
          <enabled>checked</enabled>
      </plugin>
      <captured_files>
      </captured_files>
  </status_hostset>
```

2.5 连接监控

2.5.1 接口调用 URL

http://[域名] /cgi-bin/status_link.cgi

2.5.2 输入参数

POST 提交参数：

表 2.11 连接列表 POST 提交参数

参数	说明
param_submit_type	操作方式 1. select：查询；

	2. reset：重置 3. download：下载 4. show：排序
param_page	页数（第几页）
param_this_sort	排序方式： 1. -1：按本地地址排序 2. 1：默认排序 3. 2：按远程地址排序 4. 3：按活动连接排序 5. 4：按全部连接排序
param_filter	筛选条件（即界面选择连接内容） 1. 空：筛选条件为空 2. 其他：具体的筛选内容
link_conn_in	输入连接： 1. on：勾选输入连接 2. 无：不勾选
link_conn_out	输出连接： 1. on：勾选输出连接 2. 无：不勾选

- Get 请求连接列表。

2.5.3 输出参数

返回标签< status_link >。

表 2.12 返回标签

一级标签	二级标签	说明
filter		筛选条件
page		当前页数
page_title		翻页标签
sort_type		排序类型
link_conn_in		输入连接：

		1. true：勾选 2. 空：未勾选
link_conn_out		输出连接： 1. true：勾选 2. 空：未勾选
link		每条连接记录标签
	local_address	本地地址
	remote_address	远程地址
	port_links	活动连接
	total_links	全部连接

2.5.4 示例

- POST 提交

```
POST /cgi-bin/status_link.cgi HTTP/1.1
……
param_submit_type=select&param_page=0&param_this_sort=1&param_filter=&link_conn_in=on&link_conn_out=on
```

- 请求

```
GET /cgi-bin/status_link.cgi HTTP/1.1
```

- 返回

```
HTTP/1.1 200 OK
。。。
<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/xsl" version="1.0" href="/zh-cn/xsl/status_link.xsl"?>

<status_link>
    <filter></filter>
    <page>0</page>
```

```
<page_title>首页 前一页 - <a style="font-weight:bold;font-size:14px;">0</a> - <a href="javascript:select_page(1)">1</a> - <a href="javascript:select_page(2)">2</a> - <a href="javascript:select_page(3)">3</a> - <a href="javascript:select_page(4)">4</a> - <a href="javascript:add_page(1)">后一页</a> <a href="javascript:select_page(1000000000)">末页</a> 全部 95 页</page_title>
        <sort_type>1</sort_type>
        <link_conn_in></link_conn_in>
        <link_conn_out>true</link_conn_out>
        <link>
            <local_address>1.1.1.1:56344</local_address>
            <remote_address>2.2.2.2:5656</remote_address>
            <port_links>0</port_links>
            <total_links>410</total_links>
        </link>
    </status_link>
```


2.6 屏蔽列表

2.6.1 接口调用 URL

http://[域名] /cgi-bin/status_fblink.cgi

2.6.2 输入参数

POST 提交参数：

表 2.13 屏蔽列表 POST 提交参数

参数	说明
param_submit_type	操作方式 1. select：查询； 2. reset：重置 3. download：下载 4. show：排序
param_page	页数（第几页）

param_this_sort	排序方式： 1. -1：按本地地址排序 2. 1：默认排序 3. 2：按远程地址排序 4. 3：按当前状态排序 5. 4：按屏蔽原因排序
param_filter	筛选条件（即界面选择连接内容） 1. 空：筛选条件为空 2. 其他：具体的筛选内容

- Get 请求域名列表。

2.6.3 输出参数

返回标签< status_fblink>。

表 2.14 返回标签

一级标签	二级标签	说明
filter		筛选条件
page		当前页数
page_title		翻页标签
sort_type		排序类型
fblink		每条连接记录标签
	local_address	本地地址
	remote_address	远程地址
	release_time	屏蔽时间
	forbid_reason	屏蔽原因

2.6.4 示例

- POST 提交

```
POST /cgi-bin/status_fblink.cgi HTTP/1.1
……
param_submit_type=select&param_page=0&param_this_sort=3&param_filter=1.1.1.1
```

➢ 请求

```
GET /cgi-bin/status_fblink.cgi HTTP/1.1
```

➢ 返回

```
HTTP/1.1 200 OK
。。。
<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/xsl" version="1.0" href="/zh-cn/xsl/status_link.xsl"?>
<status_fblink>
    <filter>1.1.1.1</filter>
    <page>0</page>
    <page_title>首页 前一页 - <a style="font-weight:bold;font-size:14px;">0</
a> - 后一页 末页 全部 1 页</page_title>
    <sort_type>1</sort_type>
    <fblink>
        <local_address>1.1.1.1</local_address>
        <remote_address>2.2.2.2</remote_address>
        <release_time>禁止 45 秒</release_time>
        <forbid_reason>集群同步屏蔽 + 规则匹配</forbid_reason>
    </fblink>

</status_fblink>
```

2.7 IP 黑白名单设置

2.7.1 接口调用 URL

http://[域名] /cgi-bin/status_bwlist.cgi

2.7.2 输入参数

POST 方式提交参数：

表 2.15 黑白名单 POST 参数

参数名称	说明
param_submit_type	操作方式 1. submit：提交； 2. delete：删除 3. select：查询 4. import：导入 5. export：导出 6. show：排序
param_page	页数（第几页）
param_this_sort	排序方式： 1. 1：按地址排列 2. 2：按类型排列 3. 3：按匹配数排列
param_address	添加的地址
param_comments	备注
param_bwlist_file	名单列表
filename	配置文件名称
param_bwlist_file2	配置文件路径

- Get 请求黑白名单。

2.7.3 输出参数

返回标签<status_bwlist>。

表 2.16 黑白名单返回标签

一级标签	二级标签	说明
address		需要操作的 IP 地址

page		当前页数
page_title		翻页标签
sort_type		排序类型
bwlist		每条记录标签
	address	IP 地址
	flags	类型（黑名单、白名单）
	hits	匹配次数
	comment	备注

2.7.4 示例

- POST 提交

```
POST /cgi-bin/status_bwlist.cgi HTTP/1.1
……
-----------------------------146591551219569
Content-Disposition: form-data; name="param_submit_type"

submit
-----------------------------146591551219569
Content-Disposition: form-data; name="param_page"

1
-----------------------------146591551219569
Content-Disposition: form-data; name="param_this_sort"

1
-----------------------------146591551219569
Content-Disposition: form-data; name="param_address"

4.4.4.4
-----------------------------146591551219569
Content-Disposition: form-data; name="param_comments"
```

```
----------------------------146591551219569
Content-Disposition: form-data; name="param_bwlist_file"; filename=""
Content-Type: application/octet-stream


----------------------------146591551219569
Content-Disposition: form-data; name="param_bwlist_file2"


----------------------------146591551219569--
```

- GET 请求

```
GET /cgi-bin/status_bwlist.cgi HTTP/1.1
。。。
```

- 返回

```
HTTP/1.1 200 OK
<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/xsl" version="1.0" href="/zh-cn/xsl/status_bwlist.xsl"?>

<status_bwlist>
        <address></address>
        <page>0</page>
        <page_title>首页 前一页 - <a style="font-weight:bold;font-
size:14px;">0</a> - 后一页 末页 全部 1 页<       /page_title>
        <sort_type>1</sort_type>
        <bwlist>
                <address>1.1.1.1</address>
                <flags>黑名单</flags>
                <hits>0</hits>
                <comment></comment>
        </bwlist>

</status_bwlist>
```

2.8 域名管理

2.8.1 接口调用 URL

http://[域名] /cgi-bin/status_domains.cgi

2.8.2 输入参数

表 2.17 域名管理 POST 提交参数

参数	说明
param_submit_type	操作方式 1. submit：提交； 2. delete：删除 3. select：查询（按域名查询） 4. clear：清除自动获取的域名 5. import：导入 6. export：导出 7. show：排序 8. show_flags：类型筛选
param_page	页数（第几页）
param_show_flags	查询类型 1. blacklist+whitelist+collect：黑+白+自动 2. blacklist+whitelist：黑+白 3. blacklist：黑名单 4. whitelist：白名单 5. collect：自动收集
param_this_sort	排序方式： 1. -1：按域名排序 2. 2：按类型排序

	3. 3：按地址排序 4. 4：按匹配次数排序 5. 按备注排序
param_domain_name	需要操作的域名
param_domain_comment	备注
param_import_domains	导入的域名列表
filename	配置文件名称
param_import_domains2	配置文件路径

- Get 请求域名列表。

2.8.3 输出参数

返回标签< status_domains>。

表 2.18 返回标签

一级标签	二级标签	说明
page		当前页数
page_title		翻页标签
show_flags		筛选类型
domain_name		查询的域名
sort_type		排序类型
domain_host		每条记录标签
	name	域名
	flags	类型（黑名单、白名单）
	address	对应 IP 地址
	hits	匹配次数
	comment	备注

2.8.4 示例

- POST 提交

```
POST /cgi-bin/status_domains.cgi HTTP/1.1
……
------WebKitFormBoundary7F2JWjEhTFlubjA4
Content-Disposition: form-data; name="param_submit_type"

submit
------WebKitFormBoundary7F2JWjEhTFlubjA4
Content-Disposition: form-data; name="param_page"

0
------WebKitFormBoundary7F2JWjEhTFlubjA4
Content-Disposition: form-data; name="param_show_flags"

blacklist+whitelist+collect
------WebKitFormBoundary7F2JWjEhTFlubjA4
Content-Disposition: form-data; name="param_domain_name"


------WebKitFormBoundary7F2JWjEhTFlubjA4
Content-Disposition: form-data; name="param_domain_comment"


------WebKitFormBoundary7F2JWjEhTFlubjA4
Content-Disposition: form-data; name="param_import_domains"; filename=""
Content-Type: application/octet-stream


------WebKitFormBoundary7F2JWjEhTFlubjA4
Content-Disposition: form-data; name="param_import_domains2"


------WebKitFormBoundary7F2JWjEhTFlubjA4--
```

- 请求

```
GET /cgi-bin/status_domains.cgi HTTP/1.1
```

- 返回

```
HTTP/1.1 200 OK
。。。
<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/xsl" version="1.0" href="/zh-cn/xsl/status_domains.xsl"?>

<status_domains>
    <page>0</page>
    <page_title>..... ..... 0 ..... ..... .....1...</page_title>
    <show_flags>blacklist+whitelist+collect</show_flags>
    <domain_name></domain_name>
    <domain_host>
        <name>test.com</name>
        <flags>.....</flags>
        <address></address>
        <hits>0</hits>
        <comment>test</comment>
    </domain_host>
</status_domains>
```

3 攻击防御

3.1 全局防护参数

3.1.1 接口调用 URL

http://[域名] /cgi-bin/params_global.cgi

3.1.2 输入参数

POST 提交参数：

表 3.1 全局参数 POST 提交

参数	说明
param_submit_type	操作方式 1. submit：提交； 2. default：默认
param_flowctrl	流量策略 1. protect：攻击防御模式（旁路自动牵引） 2. passthrough：透明直通 3. manualProtect：手动牵引（旁路特有）
param_switch_discover_host	自动获取主机地址（串联特有） 1. on：勾选 2. 无：不勾选
param_switch_multiple_gateway	记录主机路由选择（串联特有） 1. on：勾选 2. 无：不勾选
param_switch_resolve_host	主机探测（旁路特有）： 1. on：勾选 2. 无：不勾选
param_switch_anti_spoof_retrans_syn	SYN 重传验证（旁路特有）：

	1. on：勾选 2. 无：不勾选
param_switch_anti_spoof_retrans_ack	ACK 重传验证（旁路特有）： 1. on：勾选 2. 无：不勾选
param_switch_anti_spoof_proxy1	验证方式一（旁路特有）： 1. on：勾选 2. 无：不勾选
param_switch_anti_spoof_proxy2	验证方式二（旁路特有）： 1. on：勾选 2. 无：不勾选
param_switch_proxy_response	代理主机路由（云防特有）： 1. on：勾选 2. 无：不勾选
param_critical_packet_rate_threshold	报文频率紧急状态
param_network_segment_packet_rate_threshold	单网段报文频率阀值
param_anonymous_flow_limit_wan_ip	外网匿名流量
param_anonymous_flow_limit_lan_ip	内网匿名流量（/IP）
param_anonymous_flow_limit_lan_mac	内网匿名流量（/MAC）
param_content_filter_flow_limit	简单流量过滤限制
param_ignore_host_flow_limit	忽略主机流量限制
param_malice_forbid_time	屏蔽持续时间
param_host_param_set	参数集序号
param_tcp_syn	SYN Flood 保护
param_tcp_syn_urgent	SYN Flood 高压保护
param_tcp_syn_host	SYN Flood 单机保护
param_tcp_ack_rst	ACK&RST Flood 保护
param_udp	UDP 保护触发
param_icmp	ICMP 保护触发
param_frag	碎片保护触发

param_nonip	Nonip 保护触发
param_close_port	关闭端口触发
param_baseline_factor	基线因子
param_tcp_max_host_connections_in	TCP 连接数量限制（输入/主机）
param_tcp_max_host_connections_out	TCP 连接数量限制（输出/主机）
param_tcp_max_link_connections	TCP 连接数量限制（/IP）
param_tcp_max_access_rate	TCP 连接频率保护
param_tcp_expire_timeout	TCP 连接空闲超时
param_udp_max_host_links	UDP 连接数量保护
param_udp_expire_timeout	UDP 连接空闲超时
param_icmp_expire_timeout	ICMP 连接空闲超时
param_bwlist_flags	黑白名单策略 blacklist：黑名单 whitelist：白名单 {0:blacklist 1:whitelist}：黑名单+白名单
variable_DomainAudit.AuditMode	域名变量
variable_DomainAudit.Redirect	域名跳转
variable_DNS.Mode	DNS 变量
variable_Misc.CustomData	Misc 变量
variable_WEB.Special	WEB.secial 变量
variable_WEB.AuthorizePage	WEB.AuthorizePage 变量

- Get 请求全局参数。

3.1.3 输出参数

全局参数返回标签为<params_global>。

表 3.2 全局参数返回标签

一级标签	二级标签	说明
param_submit_type		操作方式 1. submit：提交；

		2. default：默认
set_index		集序号标签
	value	集序号标签选值（0-15）
host_param_set		当前集序号
flowctrl		流量控制 Protect：攻击防御（自动牵引） Passthrough：透明直通 ManualProtect：手动牵引
time		系统时间
switch_discover_host		自动获取主机地址（串联） 1. checked：勾选 2. 空：不勾选
switch_multiple_gateway		记录主机路由选择（串联） 1. checked：勾选 2. 空：不勾选
param_switch_resolve_host		主机探测：（旁路） 1. checked：勾选 2. 空：不勾选
param_switch_anti_spoof_retrans_syn		SYN 重传验证：（旁路） 1. checked：勾选 2. 空：不勾选
param_switch_anti_spoof_retrans_ack		ACK 重传验证：（旁路） 1. checked：勾选 2. 空：不勾选
param_switch_anti_spoof_proxy1		验证方式一：（旁路） 1. checked：勾选 2. 空：不勾选
param_switch_anti_spoof_proxy2		验证方式一：（旁路） 1. checked：勾选 2. 空：不勾选
param_switch_proxy_response		代理主机路由：（云） 1. checked：勾选 2. 空：不勾选

critical_packet_rate_threshold		报文频率紧急状态： 1. checked：勾选 2. 空：不勾选
network_segment_packet_rate_threshold		单网段报文频率阀值
anonymous_flow_limit_wan_ip		外网匿名流量
anonymous_flow_limit_lan_ip		内网匿名流量（/IP）
anonymous_flow_limit_lan_mac		内网匿名流量（/MAC）
content_filter_flow_limit		简单流量过滤限制
ignore_host_flow_limit		忽略主机流量限制
malice_forbid_time		屏蔽持续时间
tcp_syn_protect		SYN Flood 保护
tcp_syn_urgent_protect		SYN Flood 高压保护
tcp_syn_host_protect		SYN Flood 单机保护
tcp_ack_rst_protect		ACK&RST Flood 保护
udp_protect		UDP 保护触发
icmp_protect		ICMP 保护触发
frag_protect		碎片保护触发
nonip_protect		Nonip 保护触发
close_port_protect		关闭端口触发
tcp_max_host_connections_in		TCP 连接数量限制（输入/主机）
tcp_max_host_connections_out		TCP 连接数量限制（输出/主机）
tcp_max_link_connections		TCP 连接数量限制（/IP）
tcp_max_access_rate		TCP 连接频率保护
tcp_conn_timeout		TCP 连接空闲超时
udp_max_host_links		UDP 连接数量保护
udp_expire_timeout		UDP 连接空闲超时
icmp_expire_timeout		ICMP 连接空闲超时
bwlist_flags		黑白名单策略 Blacklist：黑名单

		Whitelist：白名单
baseline_factor		基线因子
variable		变量设置标签（共 6 个）
	name	变量名称
	value	变量参数值

3.1.4 示例

- POST 提交

```
POST /cgi-bin/params_global.cgi HTTP/1.1
。。。

param_submit_type=submit&param_flowctrl=Protect&param_switch_discover_host=on&param_switch_multiple_gateway=on&param_critical_packet_rate_threshold=1500000&param_anonymous_flow_limit_wan_ip=100&param_anonymous_flow_limit_lan_ip=100&param_anonymous_flow_limit_lan_mac=100&param_content_filter_flow_limit=10&param_ignore_host_flow_limit=10&param_malice_forbid_time=10000&param_host_param_set=0&param_tcp_syn=10000&param_tcp_syn_urgent=500000&param_tcp_syn_host=10000&param_tcp_ack_rst=10000&param_udp=1000&param_icmp=100&param_frag=100&param_nonip=10000&param_close_port=1000&param_baseline_factor=0.00&param_tcp_max_host_connections_in=100000&param_tcp_max_host_connections_out=1000&param_tcp_max_link_connections=300&param_tcp_max_access_rate=300&param_tcp_expire_timeout=300&param_udp_max_host_links=100000&param_udp_expire_timeout=100&param_icmp_expire_timeout=30&param_bwlist_flags=blacklist&param_bwlist_flags=whitelist&variable_DomainAudit.AuditMode=0&variable_DomainAudit.Redirect=&variable_DNS.Mode=&variable_Misc.CustomData=&variable_WEB.Special=&variable_WEB.AuthorizePage=
```

- 请求

```
GET /cgi-bin/params_global.cgi?set=0 HTTP/1.1
。。。
```

- 返回

```
HTTP/1.1 200 OK
。。。
```

```
<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/xsl" version="1.0" href="/zh-cn/xsl/params_global.xsl"?>
<params_global>
    <set_index>
        <value>0</value>
        <value>1</value>
        <value>2</value>
        <value>3</value>
        <value>4</value>
        <value>5</value>
        <value>6</value>
        <value>7</value>
        <value>8</value>
        <value>9</value>
        <value>10</value>
        <value>11</value>
        <value>12</value>
        <value>13</value>
        <value>14</value>
        <value>15</value>
    </set_index>

    <host_param_set>0</host_param_set>
    <flowctrl>Protect</flowctrl>
    <time>2018-05-09 00:11:30 CST</time>
    <switch_discover_host>checked</switch_discover_host>
    <switch_multiple_gateway></switch_multiple_gateway>
    <critical_packet_rate_threshold>5000000</critical_packet_rate_threshold>

<network_segment_packet_rate_threshold>1000001</network_segment_packet_rate_threshold>
    <anonymous_flow_limit_wan_ip>100</anonymous_flow_limit_wan_ip>
    <anonymous_flow_limit_lan_ip>100</anonymous_flow_limit_lan_ip>
    <anonymous_flow_limit_lan_mac>100</anonymous_flow_limit_lan_mac>
    <content_filter_flow_limit>10</content_filter_flow_limit>
    <ignore_host_flow_limit>10</ignore_host_flow_limit>
    <malice_forbid_time>10000</malice_forbid_time>
    <tcp_syn_protect>10000</tcp_syn_protect>
```

```
<tcp_syn_urgent_protect>500000</tcp_syn_urgent_protect>
<tcp_syn_host_protect>10000</tcp_syn_host_protect>
<tcp_ack_rst_protect>10000</tcp_ack_rst_protect>
<udp_protect>1000</udp_protect>
<icmp_protect>100</icmp_protect>
<frag_protect>100</frag_protect>
<nonip_protect>10000</nonip_protect>
<close_port_protect>1000</close_port_protect>
<tcp_max_host_connections_in>100000</tcp_max_host_connections_in>
<tcp_max_host_connections_out>1000</tcp_max_host_connections_out>
<tcp_max_link_connections>300</tcp_max_link_connections>
<tcp_max_access_rate>300</tcp_max_access_rate>
<tcp_conn_timeout>300</tcp_conn_timeout>
<udp_max_host_links>100000</udp_max_host_links>
<udp_expire_timeout>100</udp_expire_timeout>
<icmp_expire_timeout>30</icmp_expire_timeout>
<bwlist_flags>blacklist+whitelist</bwlist_flags>
<baseline_factor>0.00</baseline_factor>
<variable>
    <name>DomainAudit.AuditMode</name>
    <value>10</value>
</variable>
<variable>
    <name>DomainAudit.Redirect</name>
    <value></value>
</variable>
<variable>
    <name>DNS.Mode</name>
    <value></value>
</variable>

<variable>
    <name>Misc.CustomData</name>
    <value></value>
</variable>
<variable>
    <name>WEB.Special</name>
```

```
            <value>googlebot baiduspider </value>
        </variable>
        <variable>
            <name>WEB.AuthorizePage</name>
            <value></value>
        </variable>
    </params_global>
```

3.2 规则管理

3.2.1 规则列表

3.2.1.1 接口调用 URL

http://[域名] /cgi-bin/params_filter.cgi

3.2.1.2 输入参数

POST 提交参数：

表 3.3 规则列表提交参数

参数	说明
param_submit_type	操作方式 1. reset：重置所有 2. delete：删除 3. enable：启用 4. disable：禁用
param_filter_set	规则集序号
param_index	规则序号

- Get 请求规则列表。

3.2.1.3 输出参数

返回标签为<params_filter>。

表 3.4 规则列表返回标签

一级标签	二级标签	说明
set		当前集序号
set_index		集序号索引（0-15）
	value	集序号值
filter		每条规则标签
	index	规则序号
	enabled	是否应用
	protocol	协议
	address	地址
	description	细节
	stat	匹配

3.2.1.4 示例

- POST 提交

```
POST /cgi-bin/params_filter.cgi HTTP/1.1
。。。
param_submit_type=delete&param_index=11&param_set_index=0
```

- 请求

```
GET /cgi-bin/params_filter.cgi?set_index=0 HTTP/1.1
```

- 返回

```
HTTP/1.1 200 OK
。。。
<?xml version="1.0" encoding="utf-8"?>
```

```
<?xml-stylesheet type="text/xsl" version="1.0" href="/zh-cn/xsl/params_filter.xsl"?>

<params_filter>
    <set>0</set>
    <set_index>
        <value>0</value>
        <value>1</value>
        <value>2</value>
        <value>3</value>
        <value>4</value>
        <value>5</value>
        <value>6</value>
        <value>7</value>
        <value>8</value>
        <value>9</value>
        <value>10</value>
        <value>11</value>
        <value>12</value>
        <value>13</value>
        <value>14</value>
        <value>15</value>
    </set_index>

    <filter>
        <index>0</index>
        <enabled></enabled>
        <protocol>TCP</protocol>
        <address>any == any (RSDrop)</address>
        <description>Disable Windows RPC ports from WAN</description>
        <stat>0</stat>
    </filter>
</params_filter>
```

3.2.2 规则设置

3.2.2.1 接口调用 URL

http://[域名] /cgi-bin/params_filter_edit.cgi?set=x

3.2.2.2 输入参数

POST 提交参数：

表 3.5 规则设置提交参数

参数	说明
param_filter_set/param_set_index	规则集序号 2019.08 以前版本：param_set_index 2019.08 以后版本：param_filter_set
param_rule_index	当前规则序号
param_system	是否是系统自带规则 1. y：是 2. 空：否
param_index	修改后规则序号
param_desc	规则描述
param_length	报文长度
param_laddr	本地地址
param_raddr	远程地址
param_protocol	协议类型
param_protocol_num	协议号
param_lport	本地端口
param_rport	远程端口
param_tcp_flags	TCP 标志位
param_tcp_window_size	TCP 窗口大小
param_icmp_type	ICMP type
param_icmp_code	ICMP code

param_keywords	模式匹配内容
param_keywords_sequential	顺序匹配
param_keywords_ignore_case	忽略大小写
param_send	发送方向
param_recv	接收方向
param_action	规则行为 filter：过滤 drop：拦截 pass：放行 forbid：屏蔽 ratelimit：频率限制
param_record	记录到日志
param_stream_index	频率限制统计 ID
param_stream_connection_limit	频率限制连接限制
param_stream_access_rate_limit	频率限制访问频率

- Get 请求规则设置。

3.2.2.3 输出参数

返回标签为<params_filter_edit>。

表 3.6 规则设置返回标签

参数	说明
set	规则集序号
index	当前规则序号
system	是否是系统自带规则
desc	规则描述
length	报文长度
laddr	本地地址
raddr	远程地址

protocol	协议类型
protocol_num	协议号
lport	本地端口
rport	远程端口
tcp_flags	TCP 标志位
tcp_window_size	TCP 窗口大小
icmp_type	ICMP type
icmp_code	ICMP code
keywords	模式匹配内容
sequential	顺序匹配
ignore_case	忽略大小写
send	发送方向
recv	接收方向
record	规则行为
action	记录到日志
stream_index	频率限制统计 ID
stream_connection_limit	频率限制连接限制
stream_access_rate_limit	频率限制访问频率

3.2.2.4 示例

- 提交

```
POST /cgi-bin/params_filter_edit.cgi HTTP/1.1
。。。
param_filter_set=0&param_rule_index=0&param_system=y&param_index=0&param_desc=Disable+Windows+RPC+ports+from+WAN&param_length=&param_laddr=&param_raddr=&param_protocol=tcp&param_protocol_num=6&param_lport=135%2C+137%2C+139%2C+445&param_rport=&param_tcp_window_size=&param_icmp_type=&param_icmp_code=&param_keywords=&param_send=ON&param_recv=ON&param_action=drop&param_stream_index=&param_stream_connection_limit=&param_stream_access_rate_limit=
```

- 请求

```
GET /cgi-bin/params_filter_edit.cgi?set_index=0&index=0 HTTP/1.1
。。。
```

➢ 返回

```
HTTP/1.1 200 OK
<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/xsl" version="1.0" href="/zh-cn/xsl/params_filter_edit.xsl"?>

<params_filter_edit>
    <set>0</set>
    <index>-1</index>
    <system></system>
    <desc></desc>
    <length></length>
    <laddr></laddr>
    <raddr></raddr>
    <protocol></protocol>
    <protocol_num></protocol_num>
    <lport></lport>
    <rport></rport>
    <tcp_flags></tcp_flags>
    <tcp_window_size></tcp_window_size>
    <icmp_type></icmp_type>
    <icmp_code></icmp_code>
    <keywords></keywords>
    <sequential></sequential>
    <ignore_case></ignore_case>
    <send></send>
    <recv></recv>
    <record></record>
    <action></action>
    <stream_index></stream_index>
    <stream_connection_limit></stream_connection_limit>
    <stream_access_rate_limit></stream_access_rate_limit>
</params_filter_edit>
```

3.3 TCP 端口设置

3.3.1 接口调用 URL

http://[域名] /cgi-bin/params_portpro_tcp.cgi

3.3.2 输入参数

POST 提交参数：

表 3.7 TCP 端口集提交参数

参数	说明
param_submit_type	操作方式 1. submit：提交 2. default：默认
param_portpro_set	端口集序号
param_start_port	起始端口
param_end_port	结束端口
param_attack_detection	连接攻击检测
param_connection_limit	连接数量限制
param_server_kick_weight	踢出权重
param_port_probe_weight	探测权重
param_protocol_pattern	协议类型
param_flags_timeout_connection	超时连接： 1. on：勾选 2. 无：不勾选
param_flags_defer_indication	延时提交： 1. on：勾选 2. 无：不勾选
param_flags_forbid_overrun	超出屏蔽： 1. on：勾选

	2. 无：不勾选
param_flags_trust_only	关联信任： 1. on：勾选 2. 无：不勾选
param_flags_domain_audit	域名审计： 1. on：勾选 2. 无：不勾选
param_flags_accept_protocol	接收协议 1. on：勾选 2. 无：不勾选
param_protect_plugin	防护模块（插件）： 1. 255：默认 2. 0：WEB Service xx 3. 1：GAME Service xx 4. 2：MISC Service xx 5. 3：DNS Service xx 6. 5：SSL|TLS Service xx
param_module_params	模块参数（插件参数） 注意：多个参数英文+号连接。

- Get 请求 TCP 端口列表。

3.3.3 输出参数

返回标签为< params_portpro_tcp >。

表 3.8 TCP 端口集返回标签

一级标签	二级标签	说明
portpro_set		当前集序号
set_index		集序号索引
	value	集序号值（0-15）
port_protection		每条端口防护记录
	start_port	起始端口

	end_port	结束端口
	attack_detection	连接攻击检测
	connection_limit	连接数量限制
	port_protect_limit	踢出/探测权重
	protect_plugin	防护模块（插件）
	plugin_params	模块参数（插件参数）
	protect_flags	协议类型选择
protocol_pattern		协议定义标签
	name	每条协议名称
protect_plugin		插件标签
	id	插件序号标识
	name	插件名称

3.3.4 示例

- POST 提交

```
POST /cgi-bin/params_portpro_tcp.cgi HTTP/1.1
。。。
param_submit_type=submit&param_portpro_set=0&param_start_port=39&param_end_port=40&param_attack_detection=&param_connection_limit=&param_server_kick_weight=&param_port_probe_weight=&param_protocol_pattern=BlueskyVChat&param_flags_timeout_connection=ON&param_protect_plugin=3&param_module_params=3+100+100+100+
```

- 请求

```
GET /cgi-bin/params_portpro_tcp.cgi?set=0 HTTP/1.1
。。。
```

- 返回

```
HTTP/1.1 200 OK
。。。
<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/xsl" version="1.0" href="/zh-cn/xsl/params_portpro_tcp.xsl"?>
```

```
<params_portpro_tcp>
    <portpro_set>0</portpro_set>
    <set_index>
        <value>0</value>
        <value>1</value>
        <value>2</value>
        <value>3</value>
        <value>4</value>
        <value>5</value>
        <value>6</value>
        <value>7</value>
        <value>8</value>
        <value>9</value>
        <value>10</value>
        <value>11</value>
        <value>12</value>
        <value>13</value>
        <value>14</value>
        <value>15</value>
    </set_index>

    <port_protection>
        <start_port>0</start_port>
        <end_port>38</end_port>
        <attack_detection>max</attack_detection>
        <connection_limit>max</connection_limit>
        <port_protect_limit>---/---</port_protect_limit>
        <protect_plugin>DNS Service Protection v2.3</protect_plugin>
        <plugin_params>2 100 100 100 </plugin_params>
        <protect_flags>超时连接|----------|----------|----------|----------|拒绝
BlueskyVChat</protect_flags>
    </port_protection>

    <protocol_pattern>
        <name>FTP&amp;amp;POP3</name>
    </protocol_pattern>
```

```
<protocol_pattern>
    <name>SMTP</name>
</protocol_pattern>
<protocol_pattern>
    <name>SSH</name>
</protocol_pattern>
<protocol_pattern>
    <name>HTTP</name>
</protocol_pattern>
<protocol_pattern>
    <name>SSL|TLS</name>
</protocol_pattern>
<protocol_pattern>
    <name>MSTS</name>
</protocol_pattern>
<protocol_pattern>
    <name>RADMIN</name>
</protocol_pattern>
<protocol_pattern>
    <name>BlueskyVChat</name>
</protocol_pattern>
<protocol_pattern>
    <name>CamfrogVChat</name>
</protocol_pattern>
<protect_plugin>
    <id>0</id>
    <name>WEB Service Protection v9.02</name>
</protect_plugin>
<protect_plugin>
    <id>1</id>
    <name>Game Service Protection v4.1</name>
</protect_plugin>
<protect_plugin>
    <id>2</id>
    <name>Misc Service Protection v3.2</name>
</protect_plugin>
<protect_plugin>
```

```
            <id>3</id>
            <name>DNS Service Protection v2.3</name>
        </protect_plugin>
    </params_portpro_tcp>
```

3.4 UDP 端口设置

3.4.1 接口调用 URL

http://[域名] /cgi-bin/params_portpro_udp.cgi

3.4.2 输入参数

POST 请求参数：

表 3.9 POST 请求参数

参数	说明
param_submit_type	操作方式 1. submit：提交 2. default：默认
param_portpro_set	端口集序号
param_start_port	起始端口
param_end_port	结束端口
param_attack_detection	攻击频率检测
param_packet_rate_limit	报文频率限制
param_protocol_pattern	协议类型选择
param_flags_open_port	开放端口 1. on：勾选 2. 无：不勾选
param_flags_sync_connect	同步连接 1. on：勾选

	2. 无：不勾选
param_flags_defer_indication	延时提交 1. on：勾选 2. 无：不勾选
param_flags_check_ttl	验证 TTL 1. on：勾选 2. 无：不勾选
param_protect_plugin	防护模块 1. 255：默认 2. 1：DNS Service xx 3. 4：UDP APP xx
param_module_params	模块参数

- Get 请求 UDP 端口列表。

3.4.3 输出参数

返回标签为< params_portpro_udp >。

表 3.10 UDP 端口集返回标签

一级标签	二级标签	说明
param_submit_type		操作方式 1. submit：提交 2. default：默认
portpro_set		TCP 端口集序号
set_index		集序号索引
	value	集序号值（0-15）
port_protection		每条端口防护记录
	start_port	起始端口
	end_port	结束端口
	attack_detection	攻击频率检测
	packet_rate_limit	报文频率限制

	protect_plugin	防护模块（插件）
	plugin_params	模块参数（插件参数）
	protect_flags	协议类型选择
protocol_pattern		协议定义标签
	name	每条协议名称
protect_plugin		插件标签
	id	插件序号标识
	name	插件名称

3.4.4 示例

- 提交

```
POST /cgi-bin/params_portpro_udp.cgi HTTP/1.1
。。。

param_submit_type=submit&param_portpro_set=0&param_start_port=1100&param_end_port=1101&param_attack_detection=100&param_packet_rate_limit=100&param_protocol_pattern=BlueskyVoice&param_flags_open_port=ON&param_flags_sync_connect=ON&param_flags_defer_indication=ON&param_flags_check_ttl=ON&param_protect_plugin=4&param_module_params=15
```

- 请求

```
GET /cgi-bin/params_portpro_udp.cgi?set=0 HTTP/1.1
。。。
```

- 返回

```
HTTP/1.1 200 OK
。。。
<params_portpro_udp>
    <portpro_set>0</portpro_set>
    <set_index>
        <value>0</value>
        <value>1</value>
```

```
            <value>2</value>
            <value>3</value>
            <value>4</value>
            <value>5</value>
            <value>6</value>
            <value>7</value>
            <value>8</value>
            <value>9</value>
            <value>10</value>
            <value>11</value>
            <value>12</value>
            <value>13</value>
            <value>14</value>
            <value>15</value>
        </set_index>

        <port_protection>
            <start_port>0</start_port>
            <end_port>122</end_port>
            <attack_detection>max</attack_detection>
            <packet_rate_limit>max</packet_rate_limit>
            <protect_plugin>UDP App Protection v1.1</protect_plugin>
            <plugin_params></plugin_params>
            <protect_flags>开放端口|------------|------------|---------</protect_flags>
        </port_protection>

        <protocol_pattern>
            <name>BlueskyVoice</name>
        </protocol_pattern>

        <protocol_pattern>
            <name>QEShow</name>
        </protocol_pattern>

        <protect_plugin>
            <id>1</id>
            <name>DNS Service Protection v2.3</name>
```

```
        </protect_plugin>

        <protect_plugin>
            <id>4</id>
            <name>UDP App Protection v1.1</name>
        </protect_plugin>

    </params_portpro_udp>
```

3.5 牵引设置

3.5.1 接口调用 URL

http://[域名] /cgi-bin/params_flowdiv.cgi

3.5.2 输入参数

POST 提交参数：

表 3.11 牵引设置提交参数

参数	说明
param_submit_type	操作方式 1. submit：提交 2. flowdiv_logs：牵引日志 3. flowdiv_execute：手动牵引 4. flowdiv_cancel：取消牵引
param_ctrl_division_notify_mail	主机牵引告警 1. ON：勾选 2. 无：不勾选
param_ctrl_flow_division	异常流量牵引 1. ON：勾选 2. 无：不勾选
param_ctrl_overflow_division	流量限制模式牵引

	1. ON：勾选 2. 无：不勾选
param_flowdiv_acl_start_id	ACL 规则开始 ID
param_flowdiv_acl_end_id	ACL 规则结束 ID
param_flowdiv_action_script	牵引脚本
param_flowdiv_global_flow	全局总流量
param_flowdiv_host_count	批量牵引主机个数
param_flowdiv_mannual_address	手动牵引 IP 地址
param_flowdiv_mannual_release_time	手动牵引释放时间
param_flowdiv_release_time	自动牵引释放时间
param_flowdiv_release_type	自动牵引释放方式 1. 0：牵引超时 2. 1：主机状态
param_flowdiv_trigger_flow	牵引触发流量

- Get 请求牵引配置。

3.5.3 输出参数

返回标签为< params_flowdiv >。

表 3.12 牵引设置返回标签

一级标签	二级标签	说明
flowdiv_host_list		牵引列表标签
	address	牵引 IP
	start_time	牵引开始时间
	release_time	牵引剩余时间
ctrl_division_mode		牵引模式
ctrl_flow_division		异常流量牵引
ctrl_division_notify		主机牵引告警
ctrl_overflow_division		流量限制模式牵引
flowdiv_acl_start_id		ACL 规则开始 ID

flowdiv_acl_end_id		ACL 规则结束 ID
flowdiv_trigger_flow		牵引触发流量
flowdiv_release_type		牵引释放方式
flowdiv_release_time		自动牵引释放时间
flowdiv_host_count		批量牵引主机数
flowdiv_global_flow		全局总流量
flowdiv_action_script		牵引脚本

3.5.4 示例

- 提交

```
POST /cgi-bin/params_flowdiv.cgi HTTP/1.1
。。。
param_submit_type=submit&param_ctrl_flow_division=ON&param_flowdiv_global_flow=123&param_flowdiv_host_count=5&param_flowdiv_trigger_flow=123&param_flowdiv_release_type=0&param_flowdiv_release_time=3600&param_flowdiv_acl_start_id=2&param_flowdiv_acl_end_id=222&param_flowdiv_mannual_address=&param_flowdiv_mannual_release_time=&param_flowdiv_action_script=%5B-TELNET+192.168.59.253-%5D%0D%0Ahuawei5300%0D%0Ahuawei5300%0D%0Asystem%0D%0A%3CFLOWDIV_CANCEL_KEYWORD%3Eundo+%3C%2FFLOWDIV_CANCEL_KEYWORD%3Eip+route-static+%3CHOST_ADDRESS%3E%2F32+null0%0D%0Aquit%0D%0Aquit
```

- 请求

```
GET /cgi-bin/params_flowdiv.cgi HTTP/1.1
```

- 返回

```
HTTP/1.1 200 OK
<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/xsl" version="1.0" href="/zh-cn/xsl/params_flowdiv.xsl"?>

<params_flowdiv>
    <flowdiv_host_list>
        <address>2.2.2.2</address>
        <start_time>1525597856</start_time>
        <release_time>9999</release_time>
    </flowdiv_host_list>
```

```
<ctrl_division_mode>2147483648</ctrl_division_mode>
<ctrl_flow_division></ctrl_flow_division>
<ctrl_division_notify></ctrl_division_notify>
<ctrl_overflow_division></ctrl_overflow_division>
<flowdiv_acl_start_id>2</flowdiv_acl_start_id>
<flowdiv_acl_end_id>222</flowdiv_acl_end_id>
<flowdiv_trigger_flow>123</flowdiv_trigger_flow>
<flowdiv_release_type>0</flowdiv_release_type>
<flowdiv_release_time>3600</flowdiv_release_time>
<flowdiv_host_count>5</flowdiv_host_count>
<flowdiv_global_flow>123</flowdiv_global_flow>
<flowdiv_action_script>
    xxxxxxxxxxxxxxxxx
</flowdiv_action_script>
</params_flowdiv>
```

3.6 变量设置

3.6.1 接口调用 URL

http://[域名] /cgi-bin/params_variables.cgi

3.6.2 输入参数

POST 提交参数：

表 3.13 变量设置提交参数

参数	说明
param_submit_type	操作方式 1. export：导出 2. import：导入

- Get 请求牵引配置。

3.6.3 输出参数

返回标签为< params_variables>。

表 3.14 牵引设置返回标签

一级标签	二级标签	说明
varlist		变量列表标签
	fname	配置文件名称
	Md5	配置文件 md5 值

3.6.4 示例

- 返回

```
<params_variables>
    <varlist>
     <fname>udpfilter.Data</fname>
     <md5>d41d8cd98f00b204e9800998ecf8427e</md5>
    </varlist>
</params_variables>
```

4 日志分析

4.1 日志列表

4.1.1 接口调用 URL

http://[域名] /cgi-bin/logs_list.cgi

4.1.2 输入参数

POST/GET 请求参数：

表 4.1 提交参数

参数	说明
param_submit_type	操作方式 1. query：查询 2. download：下载 3. clear：清除 4. submit：提交 5. level：日志级别查询 6. show：翻页查询
param_start_date	开始时间
param_end_date	结束时间
param_level	日志级别： 1. -1：全部（默认） 2. 0：重要事件 3. 1：防护事件 4. 2：普通事件
param_page	指定查询的页数（第几页）

param_logs_server	日志服务器(2019.8 月前)
param_remote_logs_all	全部事件日志(2019.8 月后)
param_remote_logs_critical	重要事件日志(2019.8 月后)
param_remote_logs_protect	防护事件日志(2019.8 月后)
param_remote_logs_notice	普通事件日志(2019.8 月后)
param_remote_logs_user	用户事件日志(2019.8 月后)
param_keyword	关键字

- Get 请求日志列表。

4.1.3 输出参数

返回标签为< logs_list>。

表 4.2 日志返回标签

一级标签	二级标签	说明
level		日志级别
keyword		搜索关键字
start_date		开始时间
end_date		结束时间
logs_server		日志服务器
page		当前页数（第几页）
page_title		翻页标签
page_total		共多少页标签
log		每条日志标签
	time	日志记录时间
	event	日志记录内容

4.1.4 示例

- 提交

```
POST /cgi-bin/logs_list.cgi HTTP/1.1
。。。
param_submit_type=query&param_page=0&param_level=-1&param_start_date=2018-05-07&param_end_date=2018-05-09&param_keyword=&param_logs_server=
```

- 请求

```
//查询 1.1.1.1，第二页
GET /cgi-bin/logs_list.cgi HTTP/1.1?param_keyword=1.1.1.1&param_page=1
```

- 返回

```
HTTP/1.1 200 OK
。。。
<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/xsl" version="1.0" href="/zh-cn/xsl/logs_list.xsl"?>

<logs_list>
    <level>-1</level>
    <keyword></keyword>
    <start_date>2018-05-07</start_date>
    <end_date>2018-05-09</end_date>
    <logs_server></logs_server>
    <page>0</page>
    <page_title>首页&amp;#160;前一页&amp;#160;-&amp;#160;<a style="font-weight:bold;font-size:14px;">0</a>&amp;#160;-&amp;#160;后一页&amp;#160;末页&amp;#160;全部 1 页<      /page_title>
    <page_total>1</page_total>
    <log>
        <time>2018-05-09 10:55:17</time>
        <event>report : network [ input 0/0 Mbps 0/14 pps, submit 0/0 Mbps ], trackers [ host 101 tcp 0/0 udp 0 links 0 ], load min/max/     mem : 0/0/15 %</event>
    </log>
</logs_list>
```

4.2 攻击分析

4.2.1 接口调用 URL

http://[域名] /cgi-bin/logs_report_attack.cgi

4.2.2 输入参数

POST/GET 请求参数：

表 4.3 提交参数

参数	说明
param_submit_type	操作方式 1. submit：查询 2. show：翻页查询
param_start_date	开始时间
param_end_date	结束时间
param_address	查询主机
param_flag	攻击类型： 1. 0：全部 2. 65535：SYN 3. 131072：ACK 4. 262144：UDP 5. 524288：ICMP 6. 1048576：FRAG 7. 2097152：NonIP
param_status	防护状态 1. 0：全部 2. 1：保护中 3. 2：结束

4.2.3 输出参数

返回标签为< logs_report_accack>。

表 4.4 攻击分析返回标签

一级标签	二级标签	说明
address		查询的 IP
start_date		查询开始时间
end_date		查询结束时间
cur_flags		查询攻击类型
cur_status		查询防护状态
page		当前页数（第几页）
page_title		翻页标签
page_total		共多少页标签
report		每条攻击分析标签
	sid	序号
	dst_address	目的地址
	dst_port	目的端口
	begin	开始时间
	end	结束时间
	last	持续时间
	flags	攻击类型
	bps_in	最大流量
	from_address	攻击源地址
	status	攻击状态
	archive	攻击报文名称
	highproto	高层协议

4.2.4 示例

- 返回

```
<logs_report_attack>
 <address></address>
 <start_date>2019-08-01 00:00:00</start_date>
 <end_date>2019-09-02 23:59:59</end_date>
 <cur_flags>65536</cur_flags>
 <cur_status>0</cur_status>
 <page>0</page>
 <page_title>xxx</page_title>
 <report>
  <sid>33</sid>
  <dst_address>172.17.2.2</dst_address>
  <dst_port>tcp 80</dst_port>
  <begin>2019-08-28 14:03:25</begin>
  <end>2019-08-28 14:08:25</end>
  <last>300</last>
  <flags>[SYN]</flags>
  <bps_in>0.93</bps_in>
  <from_address>172.16.2.2/32</from_address>
  <status>2</status>
  <archive>172.17.2.2_20190828140327.tgz</archive>
  <highproto></highproto>
 </report>
</logs_report_attack>
```

4.3 分析报告

4.3.1 接口调用 URL

http://[域名] /cgi-bin/logs_report.cgi

4.3.2 输入参数

POST/GET 请求参数：

表 4.5 提交参数

参数	说明
param_address	查询主机

4.3.3 输出参数

返回标签为< logs_report>。

表 4.6 分析报告返回标签

一级标签	二级标签	说明
address		查询的 IP
forbidden_counter		屏蔽统计
max_input		最大输入流量
max_output		最大输出流量
average_input		平均输入流量
average_output		平均输出流量
max_input_submit		最大输入过滤后流量
max_output_submit		最大输出过滤后流量
average_input_submit		平均输入流量
average_output_submit		平均输出流量
input_submit_percent		输入过滤比率
output_submit_percent		输出过滤比率
max_tcp_rate		最大 TCP 连接频率
average_tcp_rate		平均 TCP 连接频率
max_udp_rate		最大 UDP 连接频率
average_udp_rate		平均 UDP 连接频率
attack_type		攻击防护类型

4.3.4 示例

- 返回

```
<logs_report>
<address>172.16.2.2</address>
<forbidden_counter>0</forbidden_counter>
<max_input>0.00</max_input>
<max_output>0.00</max_output>
<average_input>0.00</average_input>
<average_output>0.00</average_output>
<max_input_submit>0.00</max_input_submit>
<max_output_submit>0.00</max_output_submit>
<average_input_submit>0.00</average_input_submit>
<average_output_submit>0.00</average_output_submit>
<input_submit_percent>0</input_submit_percent>
<output_submit_percent>0</output_submit_percent>
<max_tcp_rate>0</max_tcp_rate>
<average_tcp_rate>0</average_tcp_rate>
<max_udp_rate>0</max_udp_rate>
<average_udp_rate>0</average_udp_rate>
<attack_type></attack_type>
</logs_report>
```

4.4 TOP 统计

4.4.1 接口调用 URL

http://[域名] /cgi-bin/logs_report_top.cgi

4.4.2 输入参数

POST/GET 请求参数：

表 4.7 提交参数

参数	说明
level（GET）	统计级别： 1. 1：5 分钟内 2. 2：一小时内 3. 3：一天内
top（GET）	统计 TOP 数： 1. 10：TOP 10 2. 50：TOP 50 3. 100：TOP 100 4. 500：TOP 500
param_submit_type	提交方式： top：查询，指定时间段内查询时使用
param_top_num	统计 TOP 数： 1. 10：TOP 10 2. 50：TOP 50 3. 100：TOP 100 500：TOP 500
param_level	统计级别： 1. 1：5 分钟内 2. 2：一小时内 3. 3：一天内
param_start_date	开始时间
param_end_date	结束时间

4.4.3 输出参数

返回标签为< logs_report_top>。

表 4.8 TOP 统计返回标签

一级标签	二级标签	说明
start_date		查询开始时间

end_date		查询结束时间
level		查询级别
top_num		查询统计个数
scan_level		
scan_address		平均输出流量
top		列表
	index	序号
	date_time	时间
	address	主机地址
	input_bps_max	输入最大值 bps
	input_pps_max	输入最大值 pps
	input_bps_acc	输入累计值 bps
	input_bps_submit	输入过滤后 bps
	output_bps_max	输出最大值 bps
	output_pps_max	输出最大值 pps
	output_bps_acc	输出累计 bps
	output_bps_submit	输出过滤后 bps
	sps_max	sps 最大值

4.4.4 示例

- 返回

```
<logs_report_top>
 <start_date>2019-08-02 00:00:00</start_date>
 <end_date>2019-09-02 14:34:29</end_date>
 <level>4</level>
 <top_num>10</top_num>
 <scan_level>3</scan_level>
 <scan_address>0.0.0.0</scan_address>
 <top>
  <index>1</index>
```

```
<date_time>2019-08-15</date_time>
<address>172.17.2.2</address>
<input_bps_max>256.40</input_bps_max>
<input_pps_max>381552</input_pps_max>
<input_bps_acc>33937.98</input_bps_acc>
<input_bps_submit>318.44</input_bps_submit>
<output_bps_max>0.00</output_bps_max>
<output_pps_max>2</output_pps_max>
<output_bps_acc>684.59</output_bps_acc>
<output_bps_submit>797.53</output_bps_submit>
<sps_max>0</sps_max>
</top>

</logs_report_top>
```

4.5 流量分析

4.5.1 接口调用 URL

http://[域名] /cgi-bin/logs_report_flow.cgi

4.5.2 输入参数

POST/GET 请求参数：

表 4.9 提交参数

参数	说明
param_submit_type	统计级别： level：流量图级别切换查询 空：提交查询
param_level	级别： 1. 1：查看每分流量 2. 2：查看每时流量 3. 3：查看每日流量

	4. 4：查看每月流量
param_address	查询地址

4.5.3 输出参数

返回标签为< logs_report_flow>。

表 4.10 流量分析返回标签

一级标签	二级标签	说明
address		查询 IP 地址
level		查询级别
page		当前页数（第几页）
page_title		翻页标签
page_total		共多少页标签
report		列表
	date_time	日期
	date_time_max	时间
	input_bps_max	输入最大值 bps
	input_pps_max	输入最大值 pps
	input_bps_ave	平均输入 bps
	input_pps_ave	平均输入 pps
	output_bps_max	输出最大值 bps
	output_pps_max	输出最大值 pps
	output_bps_ave	平均输出 bps
	output_pps_ave	平均输出 bps
	sps_max	sps 最大值
	sps_ave	sps 平均值
	input_sum	输入累计
	output_sum	输出累计

4.5.4 示例

- 返回

```
<logs_report_flow>
 <address></address>
 <level>1</level>
 <sort_type>-1</sort_type>
 <start_date>1970-01-01 08:00:00</start_date>
 <end_date>2019-09-02 23:59:59</end_date>
 <page>0</page>
 <page_title>xxx</page_title>
 <report>
  <date_time>2019-09-02</date_time>
  <date_time_max>15:00</date_time_max>
  <input_bps_max>0.00</input_bps_max>
  <input_pps_max>1</input_pps_max>
  <input_bps_ave>0.00</input_bps_ave>
  <input_pps_ave>1</input_pps_ave>
  <output_bps_max>0.00</output_bps_max>
  <output_pps_max>1</output_pps_max>
  <output_bps_ave>0.00</output_bps_ave>
  <output_pps_ave>1</output_pps_ave>
  <sps_max>0</sps_max>
  <sps_ave>0</sps_ave>
  <input_sum>0.02</input_sum>
  <output_sum>0.01</output_sum>
 </report>
</logs_report_flow>
```

4.6 连接分析

4.6.1 接口调用 URL

http://[域名] /cgi-bin/logs_report_link.cgi

4.6.2 输入参数

POST/GET 请求参数：

表 4.11 提交参数

参数	说明
param_submit_type	统计级别： level：流量图级别切换查询 空：提交查询
param_level	级别： 1. 1：查看每分流量 2. 2：查看每时流量 3. 3：查看每日流量 4. 4：查看每月流量
param_address	查询地址

4.6.3 输出参数

返回标签为< logs_report_link>。

表 4.12 连接分析返回标签

一级标签	二级标签	说明
address		查询 IP 地址
level		查询级别
page		当前页数（第几页）
page_title		翻页标签
page_total		共多少页标签
report		列表
	date_time	日期
	date_time_max	时间
	tcp_in_max	TCP 进最大值
	tcp_in_ave	TCP 进平均值

	tcp_out_max	TCP 出最大值
	tcp_out_ave	TCP 出平均值
	udp_max	UDP 最大值
	udp_ave	UDP 平均值
	input_bps_max	输入最大值
	output_bps_max	输出最大值

4.6.4 示例

- 返回

```
<logs_report_link>
 <address></address>
 <level>1</level>
 <sort_type>-1</sort_type>
 <start_date>1970-01-01 08:00:00</start_date>
 <end_date>2019-09-02 23:59:59</end_date>
 <page>0</page>
 <page_title>###</page_title>
 <report>
  <date_time>2019-08-31</date_time>
  <date_time_max>21:50</date_time_max>
  <tcp_in_max>0</tcp_in_max>
  <tcp_in_ave>0</tcp_in_ave>
  <tcp_out_max>0</tcp_out_max>
  <tcp_out_ave>0</tcp_out_ave>
  <udp_max>0</udp_max>
  <udp_ave>0</udp_ave>
  <input_bps_max>0.00</input_bps_max>
  <output_bps_max>0.00</output_bps_max>
 </report>

</logs_report_link>
```

4.7 事件分析

4.7.1 接口调用 URL

http://[域名] /cgi-bin/logs_report_ event.cgi

4.7.2 输入参数

POST/GET 请求参数：

表 4.13 提交参数

参数	说明
param_submit_type	统计级别： level：流量图级别切换查询 空：提交查询
param_level	级别： 1. 1：查看每分流量 2. 2：查看每时流量 3. 3：查看每日流量 4. 4：查看每月流量
param_address	查询地址

4.7.3 输出参数

返回标签为< logs_report_event>。

表 4.14 事件分析返回标签

一级标签	二级标签	说明
address		查询 IP 地址
level		查询级别
page		当前页数（第几页）
page_title		翻页标签
page_total		共多少页标签

report		列表
	date_time	日期
	event_address	IP 地址
	event_desc	事件类型
	bps_max	最大流量 bps
	pps_max	最大流量 pps
	sps_max	最大 sps
	bps_ave	平均 bps
	sps_ave	平均 sps
	input_sum	输入累计流量
	output_sum	输出累计流量

4.7.4 示例

- 返回

```
<logs_report_event>
<address></address>
<level>1</level>
<sort_type>-1</sort_type>
<start_date>1970-01-01 08:00:00</start_date>
<end_date>2019-09-03 23:59:59</end_date>
<page>0</page>
<page_title>###</page_title>



<report>
 <date_time>2019-09-01 15:00</date_time>
 <event_address>global</event_address>
 <event_desc>&lt;TCP&gt;</event_desc>
 <bps_max>0.00</bps_max>
 <pps_max>1</pps_max>
 <sps_max>0</sps_max>
 <bps_ave>0.00</bps_ave>
```

```
<pps_ave>1</pps_ave>
<sps_ave>0</sps_ave>
<input_sum>0.02</input_sum>
<output_sum>0.01</output_sum>
</report>

</logs_report_event>
```

4.8 性能分析

4.8.1 接口调用 URL

http://[域名] /cgi-bin/logs_report_ health.cgi

4.8.2 输入参数

POST/GET 请求参数：

表 4.15 提交参数

参数	说明
param_submit_type	统计级别： level：流量图级别切换查询
param_level	级别： 1. 1：查看每分流量 2. 2：查看每时流量 3. 3：查看每日流量 4. 4：查看每月流量

4.8.3 输出参数

返回标签为< logs_report_ health>。

表 4.16 性能返回标签

一级标签	二级标签	说明
level		查询级别
page		当前页数（第几页）
page_title		翻页标签
page_total		共多少页标签
report		列表
	date_time	日期
	date_time_max	时间
	cpu_max	CPU 最大值
	mem_max	内存最大值
	input_bps_max	输入最大流量 bps
	input_pps_max	输入最大流量 pps
	output_bps_max	输出最大流量 bps
	output_pps_max	输出最大流量 pps
	sps_max	最大 sps
	cpu_ave	平均 cpu
	mem_ave	平均内存

4.8.4 示例

- 返回

```
<logs_report_health>
 <start_date>1970-01-01 08:00:00</start_date>
 <end_date>2019-09-03 23:59:59</end_date>
 <level>2</level>
 <sort_type>-1</sort_type>
 <page>0</page>
 <page_title></page_title>
 <report>
  <date_time>2019-09-03 07:00</date_time>
  <date_time_max>07:00</date_time_max>
```

```
<cpu_max>0.0</cpu_max>
<mem_max>35.0</mem_max>
<input_bps_max>0.00</input_bps_max>
<input_pps_max>1</input_pps_max>
<output_bps_max>0.00</output_bps_max>
<output_pps_max>1</output_pps_max>
<sps_max>0</sps_max>
<cpu_ave>0.0</cpu_ave>
<mem_ave>35.0</mem_ave>
</report>

</logs_report_health>
```

4.9 攻击档案

4.9.1 接口调用 URL

http://[域名] /cgi-bin/logs_attack_archives.cgi

4.9.2 输入参数

POST/GET 请求参数：

表 4.17 提交参数

参数	说明
param_submit_type	统计级别： query：查询 delete：删除 export：导出
param_filename	文件名称
param_start_date	开始时间
param_end_date	结束时间
param_address	查询地址

4.9.3 输出参数

返回标签为< logs_attack_archives>。

表 4.18 性能返回标签

一级标签	二级标签	说明
start_date		查询开始时间
end_date		查询结束时间
address		查询地址
filename		文件名称
page		当前页数（第几页）
page_title		翻页标签
page_total		共多少页标签
captured_files（archive）		列表
	time	时间
	name	文件
	size	大小

4.9.4 示例

- 返回

```
<logs_attack_archives>
 <start_date>2019-08-01</start_date>
 <end_date>2019-09-03</end_date>
 <page>0</page>
 <page_title>xxx</page_title>
 <address>172.17.2.2</address>
 <filename></filename>
 <captured_files>
  <archive>
   <time>2019-08-27 12:18:23</time>
   <name>172.17.2.2_20190827121823.tgz</name>
   <size>16872</size>
```

```
</archive>
</captured_files>
</logs_attack_archives>
```

4.10 报表管理

4.10.1 接口调用 URL

http://[域名] /cgi-bin/logs_report_manager.cgi

4.10.2 输入参数

POST/GET 请求参数：

表 4.19 提交参数

参数	说明
param_submit_type	统计级别： submit：提交 download：导出
param_manual_download_level	导出统计区间 1. 1：按分统计 2. 2：按时统计 3. 3：按天统计
param_manual_download_start_ts	导出开始时间
param_manual_download_end_ts	导出结束时间
param_sync_mail_type	邮件传递开关，ON：开启，空：不开启
param_sync_tftp_type	TFTP 传递开关，ON：开启，空：不开启
param_sync_tftp_server	TFTP 服务器
param_sync_report_level	同步周期 1. 2：按时同步 2. 3：按日同步 3. 3：按周同步
param_logs_report_type	日志列表开关，ON：开启，空：不开启

param_flows_report_type	流量分析开关，ON：开启，空：不开启
param_link_report_type	连接分析开关，ON：开启，空：不开启
param_event_report_type	事件分析开关，ON：开启，空：不开启
param_health_report_type	性能分析开关，ON：开启，空：不开启
param_attack_report_type	攻击分析开关，ON：开启，空：不开启

4.10.3 输出参数

返回标签为< logs_report_manager >。

表 4.20 性能返回标签

一级标签	二级标签	说明
sync_mail_type		邮件同步
sync_tftp_type		TFTP 同步
sync_tftp_server		TFTP 地址
sync_report_level		同步周期
sync_logs_report		日志列表
sync_flows_report		流量分析
sync_link_report		连接分析
sync_event_report		事件分析
sync_health_report		性能分析
sync_attack_report		攻击分析

4.10.4 示例

- 返回

```
<logs_report_manager>
<sync_mail_type>on</sync_mail_type>
<sync_tftp_type></sync_tftp_type>
<sync_tftp_server>ftp://1.1.1.1</sync_tftp_server>
<sync_report_level>3</sync_report_level>
```

```
<sync_logs_report>on</sync_logs_report>
<sync_flows_report>on</sync_flows_report>
<sync_link_report>on</sync_link_report>
<sync_event_report>on</sync_event_report>
<sync_health_report></sync_health_report>
<sync_attack_report>on</sync_attack_report>
</logs_report_manager>
```

5 系统配置

5.1 保存配置

5.1.1 接口调用 URL

http://[域名] /cgi-bin/setting_config.cgi

5.1.2 输入参数

POST/GET 请求参数：

表 5.1 提交参数

参数	说明
param_submit_type	统计级别： submit：保存配置 download：下载配置 delete：删除配置
param_devaddr	网络设备地址，ON：开启，空：不开启
param_global	全局防护参数，ON：开启，空：不开启
param_portpro	TCP/UDP 端口保护，ON：开启，空：不开启
param_host	主机及配置参数，ON：开启，空：不开启
param_filter	规则列表，ON：开启，空：不开启
param_import_settings	导入文件名称

5.2 系统设备

5.2.1 接口调用 URL

http://[域名] /cgi-bin/setting_device.cgi

5.2.2 输入参数

POST 提交参数：

表 5.2 提交参数

参数	说明
param_submit_type	操作方式 1. add-addr：添加地址 2. del-addr：删除地址 3. gateway：设置网关 4. set-dns：设置 DNS 5. peer-addr：设置对端 6. default：默认 7. reboot：重启
param_set_dev	设备接口
param_set_vlan_id	VLAN ID
param_set_label	子接口 ID
param_set_address	地址

- Get 请求系统设备列表。

5.2.3 输出参数

返回标签为<setting_device>。

表 5.3 系统设备列表返回标签

一级标签	二级标签	说明
rack_unit_list		硬件单元标签

	this_rack_unit	当前硬件单元
	rack_unit	硬件单元值（有几个单元就显示几个）
device		接口信息标签
	dev	接口名称
	link	接口状态
	address	接口地址
	gateway	接口网关
	function	接口功能标识
	peer_addr	对端地址
name_servers		DNS 地址

5.2.4 示例

- 提交

```
POST /cgi-bin/setting_device.cgi HTTP/1.1
。。。
param_submit_type=add-addr&param_set_dev=eth3&param_set_vlan_id=&param_set_label=&param_set_address=192.168.105.1%2F24
```

- 请求

```
GET /cgi-bin/setting_device.cgi HTTP/1.1
```

- 返回

```
HTTP/1.1 200 OK
<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/xsl" version="1.0" href="/zh-cn/xsl/setting_device.xsl"?>

<setting_device>
    <rack_unit_list>
        <this_rack_unit>1</this_rack_unit>
        <rack_unit>1</rack_unit>
        。。。
```

```
        </rack_unit_list>
        <device>
            <dev>eth0</dev>
            <link>no link</link>
            <address>192.168.100.1/24</address>
            <gateway></gateway>
            <function>同步设备</function>
            <peer_addr></peer_addr>
        </device>
                。。。
        <name_servers>114.114.114.114</name_servers>
    </setting_device>
```

5.3 集群配置

5.3.1 接口调用 URL

http://[域名] /cgi-bin/setting_cluster.cgi

5.3.2 输入参数

POST 提交参数：

表 5.4 提交参数

参数	说明
param_submit_type	操作方式 1. save：保存 2. start：启动 3. delete：删除
param_target_device	集群同步设备
param_sync_settings	同步到集群，ON：开启，空：不开启
param_messenger_nodes	集群通信地址
param_target_address_x	集群同步地址 x：表示集群节点数，取值 0-31

param_ha_enable	启用主备模式，ON：开启，空：不开启
param_ha_active	主激活模式，ON：开启，空：不开启
param_ha_multi_active	多线路激活模式，ON：开启，空：不开启
param_ha_switch_if_any_link_failed	任一链路异常则切换，ON：开启，空：不开启
param_ha_shutdown_inactive_link	备用模式下断开网络接口，ON：开启，空：不开启
param_ha_active_timeout	激活状态超时时间
param_ha_standby_timeout	备用状态超时时间
param_ha_alive_check_address1	上行链路检测地址
param_ha_alive_check_address2	下行链路检测地址

5.3.3 输出参数

返回标签为<setting_cluster >。

表 5.5 返回标签

一级标签	二级标签	说明
sync_device		集群同步设备
messenger_nodes		集群通信地址
ha_enable		启用主备模式
ha_active		主激活模式
ha_multi_active		多线路激活模式
ha_switch_if_any_link_failed		任一链路异常则切换
ha_shutdown_inactive_link		备用链路断开接口
ha_active_timeout		激活状态超时时间
ha_standby_timeout		备用状态超时时间
ha_alive_check_address1		上行链路检测地址
ha_alive_check_address2		下行链路检测地址
device_list		接口列表

	device	接口标识
cluster_node		同步地址列表
	id	同步地址 ID
	address	同步 IP 地址

5.3.4 示例

- 返回

```
<setting_cluster>
 <sync_device></sync_device>
 <messenger_nodes></messenger_nodes>
 <ha_enable></ha_enable>
 <ha_active></ha_active>
 <ha_multi_active></ha_multi_active>
 <ha_switch_if_any_link_failed></ha_switch_if_any_link_failed>
 <ha_shutdown_inactive_link></ha_shutdown_inactive_link>
 <ha_active_timeout>3</ha_active_timeout>
 <ha_standby_timeout>30</ha_standby_timeout>
 <ha_alive_check_address1></ha_alive_check_address1>
 <ha_alive_check_address2></ha_alive_check_address2>
 <device_list>
  <device>-</device>
  <device>eth0</device>
  <device>eth1</device>
  <device>eth2</device>
  <device>eth3</device>
  <device>eth4</device>
  <device>eth5</device>
  <device>eth6</device>
  <device>eth7</device>
  <device>lo</device>
 </device_list>

 <cluster_node>
  <id>0</id>
  <address></address>
```

```
</cluster_node>
</setting_cluster>
```

5.4 控管属性

5.4.1 接口调用 URL

http://[域名] /cgi-bin/setting_ctrlcfg.cgi

5.4.2 输入参数

POST 请求参数：

表 5.6 控管属性提交参数

参数	说明
param_submit_type	操作方式 1. submit：提交 2. test：测试邮箱
param_ctrl_attack_analysis	异常攻击分析 1. ON：勾选 2. 无：未勾选
param_ctrl_archive_packets	攻击报文归档 1. ON：勾选 2. 无：未勾选
param_ctrl_status_notify_mail	攻击状态告警 1. ON：勾选 2. 无：未勾选
param_ctrl_flow_notify_mail	异常流量告警 1. ON：勾选 2. 无：未勾选
param_notify_flow_threshold	异常流量告警阀值
param_log_host_flow_threshold	主机日志流量
param_password_modes	密码复杂度

param_password_min_length	密码最小长度
param_password_expire_time	密码过期时间
param_password_history_size	密码历史记录
param_user_idle_logout_time	登陆空闲超时
param_login_failure_trigger	登陆失败限制
param_login_failure_timelimit	登陆屏蔽时间
param_weak_password_list	弱密码字典
param_mail_smtp_server	SMTP 服务器
param_mail_sender	发送用户名
param_mail_password	登陆密码
param_old_mail_password	登录密码(加密)
param_mail_recipients	接收地址列表
param_mail_subject	邮件主题
param_mail_content	邮件内容
param_preserve_rate_min_days	分钟统计保存
param_preserve_rate_hour_days	小时统计保存
param_preserve_rate_day_days	每日统计保存
param_preserve_syslog_items	系统日志保存
param_preserve_attack_items	攻击记录保存
param_preserve_flowdiv_items	牵引日志保存
param_minimum_disk_space	磁盘自动清理阀值
param_nfs_storage_option	NFS 服务开关 1. ON：开启 2. 无：关闭
param_nfs_storage_server	NFS 服务器地址
param_nfs_storage_path	NFS 服务目录
param_nfs_storage_proto	NFS 服务协议，TCP/UDP

- Get 请求系统控管属性。

5.4.3 输出参数

控管属性返回标签为<setting_ctrlcfg>。

表 5.7 返回标签

一级标签	二级标签	说明
notify_flow_threshold		异常流量告警阀值
log_host_flow_threshold		主机日志流量阀值
ctrl_attack_analysis		异常攻击分析
ctrl_archive_packets		攻击报文归档
ctrl_notify_mail		攻击状态告警
ctrl_flow_notify		异常流量告警
ctrl_status_notify		异常流量告警阀值
mail_config		邮箱配置
	smtp_server	SMTP 服务器
	sender	发送用户名
	password	登陆密码
	recipients	接收地址列表
	subject	邮件主题
	content	邮件内容
password_modes		密码复杂度
password_min_length		密码最小长度
password_expire_time		密码过期时间
password_history_size		密码历史记录
user_idle_logout_time		登陆空闲超时
login_failure_trigger		登陆失败限制
login_failure_timelimit		登陆屏蔽时间
weak_password_list		弱密码字典
preserve_rate_min_days		分钟统计保存
preserve_rate_hour_days		小时统计保存

preserve_rate_day_days		每日统计保存
preserve_syslog_items		系统日志保存
preserve_attack_items		攻击记录保存
preserve_fblink_items		屏蔽记录保存
preserve_flowdiv_items		牵引日志保存
minimum_disk_space		磁盘自动清理阀值
nfs_storage_option		NFS 服务
nfs_storage_server		NFS 服务器地址
nfs_storage_proto		NFS 服务协议
nfs_storage_path		NFS 服务目录

5.4.4 示例

- 提交

```
POST /cgi-bin/setting_ctrlcfg.cgi HTTP/1.1
。。。
param_submit_type=submit&param_old_mail_password=4bUAido%2BQCFr0sGRimg0Sw%3D%3D&param_ctrl_attack_analysis=ON&param_ctrl_status_notify_mail=ON&param_notify_flow_threshold=100&param_log_host_flow_threshold=&param_password_modes=0&param_password_min_length=0&param_password_expire_time=0&param_password_history_size=0&param_user_idle_logout_time=0&param_login_failure_trigger=0&param_login_failure_timelimit=0&param_weak_password_list=&param_mail_smtp_server=smtp.sina.com&param_mail_sender=zxsoft&param_mail_password=4bUAido%2BQCFr0sGRimg0Sw%3D%3D&param_mail_recipients=zxsoft_jishu%40sina.com&param_mail_subject=%E4%B8%AD%E6%96%B0%E7%BD%91%E5%AE%89&param_mail_content=&param_preserve_rate_min_days=3&param_preserve_rate_hour_days=30&param_preserve_rate_day_days=365&param_preserve_syslog_items=500000&param_preserve_attack_items=500000&param_preserve_flowdiv_items=500000&param_minimum_disk_space=10
```

- 请求

```
GET /cgi-bin/setting_ctrlcfg.cgi HTTP/1.1
```

- 返回

```
<setting_ctrlcfg>
```

```
<notify_flow_threshold>100</notify_flow_threshold>
<log_host_flow_threshold></log_host_flow_threshold>
<ctrl_attack_analysis>on</ctrl_attack_analysis>
<ctrl_archive_packets></ctrl_archive_packets>
<ctrl_notify_mail>on</ctrl_notify_mail>
<ctrl_flow_notify></ctrl_flow_notify>
<ctrl_status_notify></ctrl_status_notify>
<mail_config>
 <smtp_server>smtp.sina.com</smtp_server>
 <sender>zxsoft_jishu@sina.com</sender>
 <password>6gUkM923aZMzc5ax2bqrhA==</password>
 <recipients>zxsoft_jishu@sina.com</recipients>
 <subject>192.168.60.216 测试</subject>
 <content></content>
</mail_config>

<password_modes>1</password_modes>
<password_min_length>0</password_min_length>
<password_expire_time>0</password_expire_time>
<password_history_size>0</password_history_size>
<user_idle_logout_time>0</user_idle_logout_time>
<login_failure_trigger>0</login_failure_trigger>
<login_failure_timelimit>0</login_failure_timelimit>
<weak_password_list><![CDATA[]]></weak_password_list>
<preserve_rate_min_days>3</preserve_rate_min_days>
<preserve_rate_hour_days>29</preserve_rate_hour_days>
<preserve_rate_day_days>365</preserve_rate_day_days>
<preserve_syslog_items>500000</preserve_syslog_items>
<preserve_attack_items>500000</preserve_attack_items>
<preserve_fblink_items>500000</preserve_fblink_items>
<preserve_flowdiv_items>500000</preserve_flowdiv_items>
<minimum_disk_space>10</minimum_disk_space>
<nfs_storage_option></nfs_storage_option>
<nfs_storage_server></nfs_storage_server>
<nfs_storage_proto>tcp</nfs_storage_proto>
<nfs_storage_path></nfs_storage_path>
</setting_ctrlcfg>
```

5.5 用户组管理

5.5.1 接口调用 URL

用户组展示页面：http://[域名] /cgi-bin/setting_group.cgi

用户组编辑页面：http://[域名] /cgi-bin/setting_group_edit.cgi

5.5.2 输入参数

POST 请求参数：

表 5.8 提交参数

参数	说明
param_submit_type	操作方式 1. submit：提交
group_name	组名称
group_desc	组描述
status_pranges	防护范围，ON：勾选 无：未勾选
status_host	主机状态，ON：勾选 无：未勾选
status_link	连接监控，ON：勾选 无：未勾选
status_forbidden	屏蔽列表 ，ON：勾选 无：未勾选
status_bwlist	黑白名单，ON：勾选 无：未勾选
status_domains	域名管理，ON：勾选 无：未勾选
params_global	全局参数，ON：勾选 无：未勾选
params_filter	规则设置，ON：勾选 无：未勾选
params_tcp	TCP 保护，ON：勾选 无：未勾选
params_udp	UDP 保护，ON：勾选 无：未勾选
params_ssl_cert	SSL 证书，ON：勾选 无：未勾选
params_flowdiv	牵引设置，ON：勾选 无：未勾选
params_variables	变量设置，ON：勾选 无：未勾选

logs_list	日志列表，ON：勾选 无：未勾选
logs_attack_archives	攻击档案，ON：勾选 无：未勾选
logs_report_manager	报表管理，ON：勾选 无：未勾选
setting_config	保存配置，ON：勾选 无：未勾选
setting_device	系统设备，ON：勾选 无：未勾选
setting_cluster	集群参数，ON：勾选 无：未勾选
setting_ctrlcfg	控管属性，ON：勾选 无：未勾选
setting_time	时间设定，ON：勾选 无：未勾选
setting_snmp_system	SNMP 系统，ON：勾选 无：未勾选
setting_snmp_trap	SNMP Trap，ON：勾选 无：未勾选
setting_snmp_user	SNMP 用户，ON：勾选 无：未勾选
setting_snmp_view	SNMP 视图，ON：勾选 无：未勾选
setting_aaa	AAA 认证，ON：勾选 无：未勾选
setting_group	用户组管理，ON：勾选 无：未勾选
setting_user	用户管理，ON：勾选 无：未勾选
service_version	版本信息，ON：勾选 无：未勾选
service_capture	报文捕捉，ON：勾选 无：未勾选
service_update	产品升级，ON：勾选 无：未勾选
service_systools	系统工具，ON：勾选 无：未勾选

5.5.3 输出参数

用户组列表返回标签：<setting_group>

用户组编辑返回标签：<setting_group_edit>

表 5.9 用户组列表返回标签

一级标签	二级标签	说明
group_list		列表
group_name		用户组名称
group_desc		用户组描述

users		下属用户

表 5.10 用户组编辑返回标签

一级标签	二级标签	说明
group_name		用户组名称
group_desc		用户组描述
status_pranges		防护范围
status_host		主机状态
status_link		连接监控
status_forbidden		屏蔽列表
status_bwlist		黑白名单
status_domains		域名管理
params_global		全局参数
params_filter		规则设置
params_tcp		TCP 保护
params_udp		UDP 保护
params_ssl_cert		SSL 证书
params_flowdiv		牵引设置
params_variables		变量设置
logs_list		日志列表
logs_attack_archives		攻击档案
logs_report_manager		报表管理
setting_config		保存配置
setting_device		系统设备
setting_cluster		集群参数
setting_ctrlcfg		控管属性
setting_time		时间设定
setting_snmp_system		SNMP 系统
setting_snmp_trap		SNMP Trap

setting_snmp_user		SNMP 用户
setting_snmp_view		SNMP 视图
setting_aaa		AAA 认证
setting_group		用户组管理
setting_user		用户管理
service_version		版本信息
service_capture		报文捕捉
service_update		产品升级
service_systools		系统工具

5.5.4 示例

- 返回

```
<setting_group>
 <group_list>
  <group_name>monitor</group_name>
  <group_desc>网络观察员--仅可以查看当前系统状态，无权更改</group_desc>
  <users></users>
 </group_list>

</setting_group>
```

5.6 用户管理

5.6.1 接口调用 URL

http://[域名] /cgi-bin/setting_user.cgi

5.6.2 输入参数

POST 请求参数：

表 5.11 提交参数

参数	说明
param_submit_type	操作方式 1. submit：提交 2. delete：删除
param_username	用户名称
param_password	用户密码
param_login_mode_web	WEB 登录模式，ON：勾选 空：未勾选
param_login_mode_cli	CLI 登录模式，ON：勾选 空：未勾选
param_login_address	登录地址
param_group_list	用户组

5.6.3 输出参数

返回标签：< setting_user >

表 5.12 返回标签

一级标签	二级标签	说明
user		列表
name		用户名
mode		登录模式
login_address		登录地址
group_list		用户组

5.6.4 示例

- 返回

```
<setting_user>
 <user>
  <name>admin</name>
  <mode>web,cli</mode>
  <login_address></login_address>
  <group_list>administrator</group_list>
 </user>
</setting_user>
```

5.7 时间设置

5.7.1 功能说明

时间查看和设置。

5.7.2 接口调用 URL

http://[域名] /cgi-bin/setting_time.cgi

5.7.3 输入参数

POST 请求参数：

表 5.13 提交参数

参数	说明
param_submit_type	操作方式 1. submit：提交
param_time	设置时间
param_time_zone	设置时区

5.7.4 输出参数

返回标签：< setting_time>

表 5.14 返回标签

一级标签	二级标签	说明
time		当前时间
uptime		启动时间
server		NTP 服务器
time_zone		当前时区
zone_list		时区列表
	zone	时区名称

5.7.5 示例

- 返回

```
<setting_time>
 <time>2019-09-03 13:16:43 CST</time>
 <uptime>1 day 19 hours 43 minutes </uptime>
 <server></server>
 <time_zone>Asia/Shanghai</time_zone>
 <zone_list>
  <zone>Africa/Abidjan</zone>
 </zone_list>
</setting_time>
```

5.8 SNMP 管理

5.8.1 接口调用 URL

SNMP 系统：http://[域名] /cgi-bin/setting_snmp_system.cgi

SNMP Trap：http://[域名] /cgi-bin/setting_snmp_trap.cgi

SNMP 用户：http://[域名] /cgi-bin/setting_snmp_user.cgi

SNMP 视图：http://[域名] /cgi-bin/setting_snmp_view.cgi

5.8.2 输入参数

表 5.15 SNMP 系统提交参数

参数	说明
param_submit_type	操作方式 1. submit：提交
param_snmp_service	SNMP 服务
param_sys_contact	联系信息
param_sys_location	物理地址
param_sys_description	系统描述
param_sys_objectid	系统 OID

表 5.16 SNMP Trap 提交参数

参数	说明
param_submit_type	操作方式 1. set：提交 2. clear：清空
param_trap_authenticationFailure	SNMP 验证失败
param_trap_portstat	端口状态改变
param_trap_system	系统状态改变
param_trap_attack	网络攻击
param_trap_config	配置改变

表 5.17 SNMP 用户提交参数

参数	说明
param_submit_type	操作方式 1. add：添加 2. delete：删除
param_version	SNMP 版本 1. v1 2. v2c

	3. v3
param_user_community	团体名称
param_source_network	访问源地址
param_access_type	访问权限 1. readonly：只读 2. readwrite：读写
param_access_view	访问视图

表 5.18 SNMP 视图提交参数

参数	说明
param_submit_type	操作方式 1. add：提交 2. delete：删除
param_view_name	视图名称
param_view_rule	视图规则 1. included：包含 2. excluded：排除
param_view_mib	MIB 子树

5.8.3 输出参数

表 5.19 SNMP 系统返回标签< setting_snmp_system >

一级标签	二级标签	说明
enabled		是否开启
sys_contact		联系信息
sys_location		物理地址
sys_description		系统描述
sys_objectid		系统 OID

表 5.20 SNMP TRAP 返回标签< setting_snmp_trap >

一级标签	二级标签	说明
param_trap_authenticationFailure		SNMP 验证失败
param_trap_portstat		端口状态改变
param_trap_system		系统状态改变
param_trap_attack		网络攻击
param_trap_config		配置改变
trap_address		接收主机地址
user_list		SNMP 用户列表
	name	SNMP 用户名称

表 5.21 SNMP 用户返回标签< setting_snmp_user>

一级标签	二级标签	说明
user		用户列表
	name	用户
	security	安全
	privilege	访问权限
	view	视图

表 5.22 SNMP 视图返回标签< setting_snmp_view >

一级标签	二级标签	说明
view		视图列表
	name	视图名称
	mode	视图规则
	mibs	mib 子树

5.8.4 示例

- 返回

```
<setting_snmp_view>
<view>
```

```
    <name>zxsoft</name>
    <mode>Included</mode>
    <mibs>.1</mibs>
  </view>
</setting_snmp_view>
```

6 服务支持

6.1 版本信息

6.1.1 接口调用 URL

http://[域名] /cgi-bin/service_version.cgi

6.1.2 输入参数

GET 请求方式。

6.1.3 输出参数

系统版本信息标签为<service_version>。

表 6.1 系统版本信息标签

一级标签	二级标签	说明
rack_unit_list		硬件单元标签（ATCA 独有）
	this_rack_unit	当前硬件单元
	rack_unit	其他硬件单元，依次排列
product_model		产品型号
version_str		版本号
serial		序列号
expire		授权期限

6.1.4 示例

- 返回

```
<service_version>
<product_model>ZX-DMS 6121</product_model>
```

```
<version_str>#138,2018-09-29  9:49:45</version_str>
<serial>vKGERR5Y3jn7s6H9ceMdR</serial>
<expire></expire>
</service_version>
```

6.2 报文捕捉

6.2.1 接口调用 URL

http://[域名] /cgi-bin/ service_capture.cgi

6.2.2 输入参数

POST 请求参数：

表 6.2 提交参数

参数	说明
param_submit_type	操作方式 1. submit：提交 2. download：下载
param_capture_mac_address	捕捉 MAC 地址
param_capture_ip_address	捕捉 IP 地址
param_capture_flags	捕捉方向 s:源地址，t:目的地址
param_capture_protocol	协议类型，可选值：IP、tcp、udp、icmp、icmpv6、igmp、空
param_protocol_num	协议号
param_capture_dev_name	接口
param_capture_sample_rate	采样比
param_capture_count	捕捉报文数
param_capture_tftp_file	tftp 服务器

6.2.3 输出参数

返回标签：< service_capture>

表 6.3 返回标签

一级标签	二级标签	说明
capture_device		当前选择的捕捉接口
capture_dev_name		接口列表
	dev_name_id	接口 ID 标识
	dev_name	接口名称
mac_address		捕捉 mac 地址
ip_address		捕捉 IP 地址
flags		捕捉方向
count		捕捉报文数
file		tftp 服务器
size		数据大小
protocol		协议
protocol_num		协议号
sample_rate		采样比

6.2.4 示例

- 返回

```
<service_capture>
 <capture_device>all</capture_device>
 <capture_dev_name>
  <dev_name_id></dev_name_id>
  <dev_name>all</dev_name>
 </capture_dev_name>

 <mac_address></mac_address>
 <ip_address></ip_address>
```

```
<flags></flags>
<count></count>
<file></file>
<size></size>
<protocol>0</protocol>
<protocol_num>0</protocol_num>
<sample_rate></sample_rate>
</service_capture>
```