

Supernova 测试仪 SSL 卸载用例说明

网测科技

2021/01/21

目录

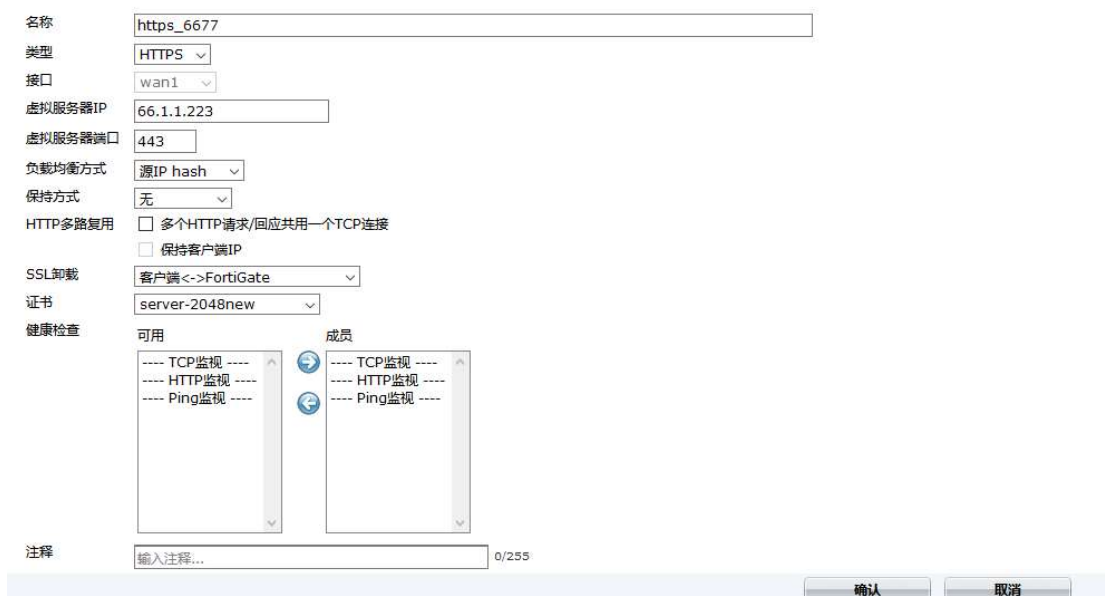
引言	3
1.配置负载均衡，并启用 ssl 卸载功能	3
2.配置 Supernova 测试仪	4
3.运行用例	6
4.报文验证	7
5.https 并发用例特殊配置	8

引言

Supernova 测试仪支持 HTTPS 用例的 SSL 卸载功能，只需要在卸载 ssl 设备上配置好即可。除 https 并发用例外，测试仪上不需要做任何其它特殊配置，https 并发用例在“参数”中有启用 ssl 卸载功能按钮，打开后可使并发连接数量的范围*2。

此处以负载均衡设备举例说明：

1.配置负载均衡，并启用 ssl 卸载功能



名称: https_6677

类型: HTTPS

接口: wan1

虚拟服务器IP: 66.1.1.223

虚拟服务器端口: 443

负载均衡方式: 源IP hash

保持方式: 无

HTTP多路复用: ☐ 多个HTTP请求/回应共用一个TCP连接
☐ 保持客户端IP

SSL卸载: ☒ 客户端<->FortiGate

证书: server-2048new

健康检查: 可用

成员: TCP监视, HTTP监视, Ping监视

注释: 输入注释... 0/255

确认 取消



编辑真实服务器

虚拟服务器: https_6677

IP地址: 77.1.1.200

端口: 80

权重: 1

最大连接数: 0

HTTP主机:

模式: 活动

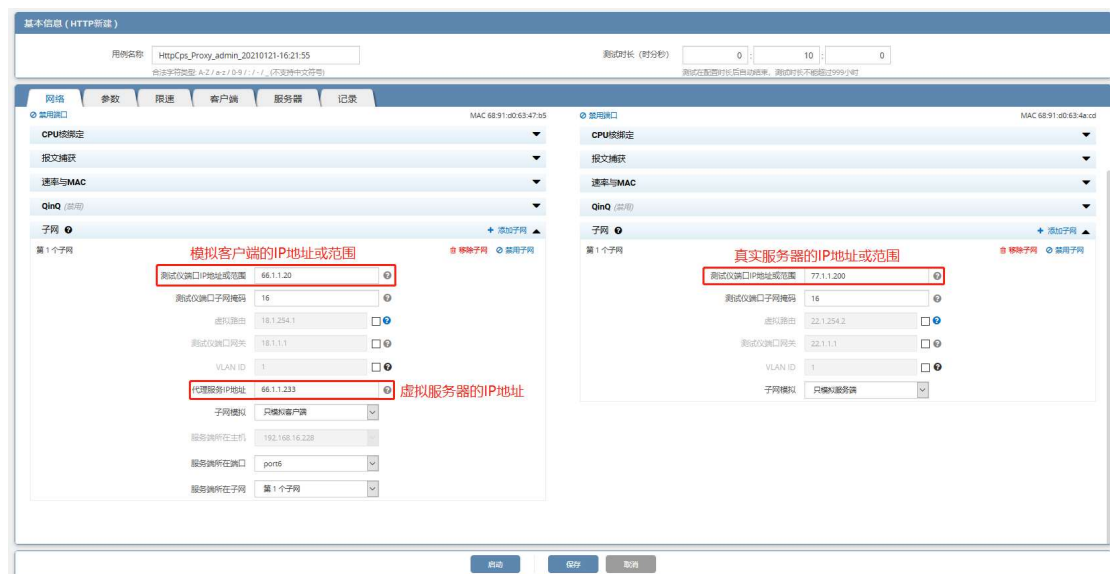
确认 取消

2.配置 Supernova 测试仪

1) 登录系统，依次点击，用例->代理设备测试->HTTP->新建服务->增加，单击增加，在弹出的选择用例选项中，编辑用例网络选项，根据需要修改配置参数，然后点击确定，进入用例配置页面。



2) 点击确定，进入用例配置界面，配置子网信息。



3) 点击参数，配置用例参数。



基本信息 (HTTPS新建)

用例名称: HttpsCps_Proxy_admin_20210121-16:34:10 测试时长 (时:分:秒): 0 : 10 : 0

网络 参数 限速 客户端 服务器 记录

HTTPS服务器端口: 443
HTTP服务器端口: 80 **真实的服务器端口号**

服务器证书配置: 默认1024key SSL套件
HTTP固定头: Server: nginx/1.9.10
Content-Type: text/html

4) 配置报文捕获查看用例运行报文交互过程。

基本信息 (HTTP新建)

用例名称: HttpCps_Proxy_admin_20210126-14:27:13 测试时长 (时:分:秒): 0 : 10 : 0

网络 参数 限速 客户端 服务器 记录

客户端

端口: port2
MAC: 68:91:d0:63:47:b5

CPU绑定

报文捕获

协议类型: 全部
IP地址: 源IP地址或目标的IP地址, 例如17.1.1.2
端口: 源端口或目标的端口, 例如80
Pcap文件大小: 50000
捕获包数: 50000

速率与MAC

QinQ (禁用)

子网

第1个子网: 测试源IP地址或范围: 17.1.2.2-17.1.2.200

服务端

端口: port6
MAC: 68:91:d0:63:4a:c8

CPU绑定

报文捕获

协议类型: 全部
IP地址: 源IP地址或目标的IP地址, 例如17.1.1.2
端口: 源端口或目标的端口, 例如80
Pcap文件大小: 50000
捕获包数: 50000

速率与MAC

QinQ (禁用)

子网

第1个子网: 测试源IP地址或范围: 18.1.1.100

启动 保存 取消

5) 用例编辑完成后, 可以点击启动直接运行用例, 也可以点击保存, 保存用例配置。

基本信息 (HTTPS新建)

用例名称: HttpsCps_Proxy_admin_20210121-16:38:06 测试时长 (时:分:秒): 0 : 10 : 0

网络 参数 限速 客户端 服务器 记录

客户端

端口: port1
MAC: 68:91:d0:63:47:b4

CPU绑定

报文捕获

协议类型: 全部
IP地址: 源IP地址或目标的IP地址, 例如17.1.1.2
端口: 源端口或目标的端口, 例如80
Pcap文件大小: 50000
捕获包数: 50000

速率与MAC

QinQ (禁用)

子网

第1个子网: 测试源IP地址或范围: 17.1.2.2-17.1.2.201

服务端

端口: port5
MAC: 68:91:d0:63:4a:cc

CPU绑定

报文捕获

协议类型: 全部
IP地址: 源IP地址或目标的IP地址, 例如17.1.1.2
端口: 源端口或目标的端口, 例如80
Pcap文件大小: 50000
捕获包数: 50000

速率与MAC

QinQ (禁用)

子网

第1个子网: 测试源IP地址或范围: 21.1.1.100

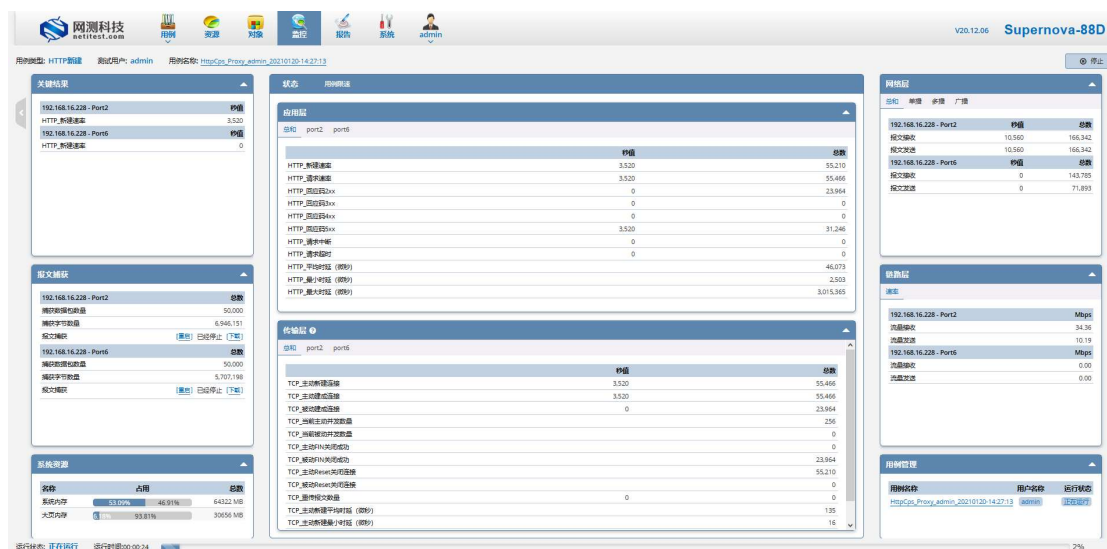
启动 保存 取消

3.运行用例

用例编辑保存后，点击运行按钮运行测试用例



用例运行监控数据页面：



用例运行结束，可以点击下载报告查看用例运行中报文交互



4.报文验证

No.	Time	Source	Destination	Protocol	Length	Info
138	2.128199	66.1.1.20	66.1.1.223	TCP	62	10014 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1452 SACK_PERM=1
142	2.128336	66.1.1.223	66.1.1.20	TCP	62	443 → 10014 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
143	2.128359	66.1.1.20	66.1.1.223	TLSv1.1	129	Client Hello
146	2.128443	66.1.1.223	66.1.1.20	TCP	60	443 → 10014 [ACK] Seq=1 Ack=76 Win=5840 Len=0
148	2.128692	66.1.1.223	66.1.1.20	TLSv1.1	1126	Server Hello, Certificate, Server Hello Done
150	2.129114	66.1.1.20	66.1.1.223	TLSv1.1	396	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
164	2.131707	66.1.1.223	66.1.1.20	TLSv1.1	60	Change Cipher Spec
166	2.131971	66.1.1.223	66.1.1.20	TLSv1.1	123	Encrypted Handshake Message
167	2.131974	66.1.1.20	66.1.1.223	TCP	60	10014 → 443 [ACK] Seq=418 Ack=1148 Win=65535 Len=0
168	2.132062	66.1.1.20	66.1.1.223	TLSv1.1	203	Application Data
172	2.132648	66.1.1.223	66.1.1.20	TLSv1.1	187	Application Data
173	2.132661	66.1.1.20	66.1.1.223	TCP	60	10014 → 443 [RST, ACK] Seq=567 Ack=1281 Win=65535 Len=0

> Frame 173: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: IntelCor_ee:92:50 (90:e2:ba:ee:92:50), Dst: Fortinet_35:cd:34 (08:5b:0e:35:cd:34)
> Internet Protocol Version 4, Src: 66.1.1.20, Dst: 66.1.1.223
> Transmission Control Protocol, Src Port: 10014, Dst Port: 443, Seq: 567, Ack: 1281, Len: 0

客户端为加密报文

No.	Time	Source	Destination	Protocol	Length	Info
32	2.123003	77.1.1.1	77.1.1.200	TCP	74	10011 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=92230810 TSecr=0 WS=2
33	2.123006	77.1.1.200	77.1.1.1	TCP	62	80 → 10011 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452 SACK_PERM=1
36	2.123097	77.1.1.1	77.1.1.200	TCP	60	10011 → 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0
50	2.127747	77.1.1.1	77.1.1.200	HTTP	157	GET /index_1bytes.html HTTP/1.1
51	2.127752	77.1.1.200	77.1.1.1	HTTP	140	HTTP/1.1 200 OK (text/html)
54	2.127813	77.1.1.1	77.1.1.200	TCP	60	10011 → 80 [ACK] Seq=104 Ack=87 Win=5840 Len=0
56	2.128266	77.1.1.1	77.1.1.200	TCP	60	10011 → 80 [FIN, ACK] Seq=104 Ack=87 Win=5840 Len=0
57	2.128269	77.1.1.200	77.1.1.1	TCP	60	80 → 10011 [FIN, ACK] Seq=87 Ack=105 Win=65535 Len=0
58	2.128345	77.1.1.1	77.1.1.200	TCP	60	10011 → 80 [ACK] Seq=105 Ack=88 Win=5840 Len=0

> Frame 56: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: Fortinet_35:cd:35 (08:5b:0e:35:cd:35), Dst: IntelCor_ed:b5:74 (90:e2:ba:ed:b5:74)
> Internet Protocol Version 4, Src: 77.1.1.1, Dst: 77.1.1.200
> Transmission Control Protocol, Src Port: 10011, Dst Port: 80, Seq: 104, Ack: 87, Len: 0

server端为http非加密报文

5.https 并发用例特殊配置

https 并发用例在“参数”中有启用 ssl 卸载功能按钮，打开后可使并发连接数量的范围*2。

基本信息 (HTTPS开发)

用例名称: HttpsCc_Proxy_admin_20210121-16:46:40

测试时长 (时:分:秒): 0 : 10 : 0

合法字符类型: A-Z/a-z/0-9/_/-/. (不支持中文符号)

测试在配置时长后自动结束, 测试时长不能超过999小时

网络 参数 限速 客户端 服务器 记录

用例参数 通用参数

用户admin占用内存: 60 GB

用户admin申请占用的内存数量, 可以设置--内存管理页面申请

用例运行占用内存: 60 GB

运行此用例占用的内存空间, 包括DPDK的大页内存, 以及SSL会话占用的普通系统内存, 范围: 2 - 60GB

DPDK大页内存占比: 50 %

DPDK大页内存占用指运行内存的百分比, 运行HTTPS并发用例时, 建议大页内存占比50%, 剩余内存用于建立SSL会话, 范围: 20% - 70%

虚拟用户数量: 256

范围: 1 - 16,384, 每个客户端端口和CPU核, 至少有一个虚拟用户

在还没有启用受测设备SSL卸载时, 并发范围为1-820000

受测设备SSL卸载: 启用

并发连接数量: 820000

范围: 1 - 820,000, 并发连接数大于等于客户端的所有cpu核数之和

Think Time: 0

发送HTTP请求: 每条连接建立成功后 所有连接建立成功后

HTTP请求次数: 0

每新建一条TCP连接, 发送HTTP请求的次数, 请求结束后会关闭TCP连接, 0表示无限制, 范围: 0 - 50000

请求添加Host字段: 是

HTTP请求头中, 是否自动添加Host字段, 配置正则代理和IP地址列表, 必选项

HTTP代理模式: 反向代理

启动 保存 取消

基本信息 (HTTPS开发)

用例名称: HttpsCc_Proxy_admin_20210121-16:46:40

测试时长 (时:分:秒): 0 : 10 : 0

合法字符类型: A-Z/a-z/0-9/_/-/. (不支持中文符号)

测试在配置时长后自动结束, 测试时长不能超过999小时

网络 参数 限速 客户端 服务器 记录

用例参数 通用参数

用户admin占用内存: 60 GB

用户admin申请占用的内存数量, 可以设置--内存管理页面申请

用例运行占用内存: 60 GB

运行此用例占用的内存空间, 包括DPDK的大页内存, 以及SSL会话占用的普通系统内存, 范围: 2 - 60GB

DPDK大页内存占比: 50 %

DPDK大页内存占用指运行内存的百分比, 运行HTTPS并发用例时, 建议大页内存占比50%, 剩余内存用于建立SSL会话, 范围: 20% - 70%

虚拟用户数量: 256

范围: 1 - 16,384, 每个客户端端口和CPU核, 至少有一个虚拟用户

启用受测设备SSL卸载后, 并发连接数量可设置范围为1-1640000, 可设置并发数量是原来的2倍

受测设备SSL卸载: 启用

并发连接数量: 1640000

范围: 1 - 1,640,000, 并发连接数大于等于客户端的所有cpu核数之和

Think Time: 0

发送HTTP请求: 每条连接建立成功后 所有连接建立成功后

HTTP请求次数: 0

每新建一条TCP连接, 发送HTTP请求的次数, 请求结束后会关闭TCP连接, 0表示无限制, 范围: 0 - 50000

请求添加Host字段: 是

HTTP请求头中, 是否自动添加Host字段, 配置正则代理和IP地址列表, 必选项

HTTP代理模式: 反向代理

启动 保存 取消