Supernova 测试仪

IPsec VPN 测试配置手册

网测科技

2021/01/26

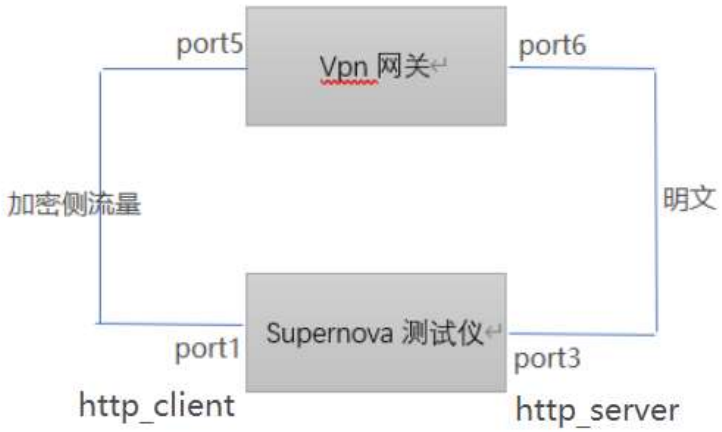
目录

1.文档说明

本文档主要介绍 IPsec VPN 的配置和测试过程。随着需求的不断改变，可能会对用例配置进行修改和升级，从而改变配置过程，所以有任何问题，请联系我们的售前或售后支持人员。

2.测试拓扑图

常见拓扑:



测试仪 port1 和被测设备 DUTport5 间建立 esp 加密 ipsec 隧道，测试仪 port3 和 DUT 的 port6 明文传输。

本次测试采用 Supernova-46E 为测试仪，Fortigate 防火墙为 VPN 网关。

3.支持秘钥和证书模式

IPsec VPN 支持 PSK 和 Signature 两种模式，也就是秘钥和证书，先讲述秘钥认证模式，再讲述证书认证模式。

4.配置防火墙为 VPN 网关

1）配置防护墙 port5 和 port6 的接口地址。

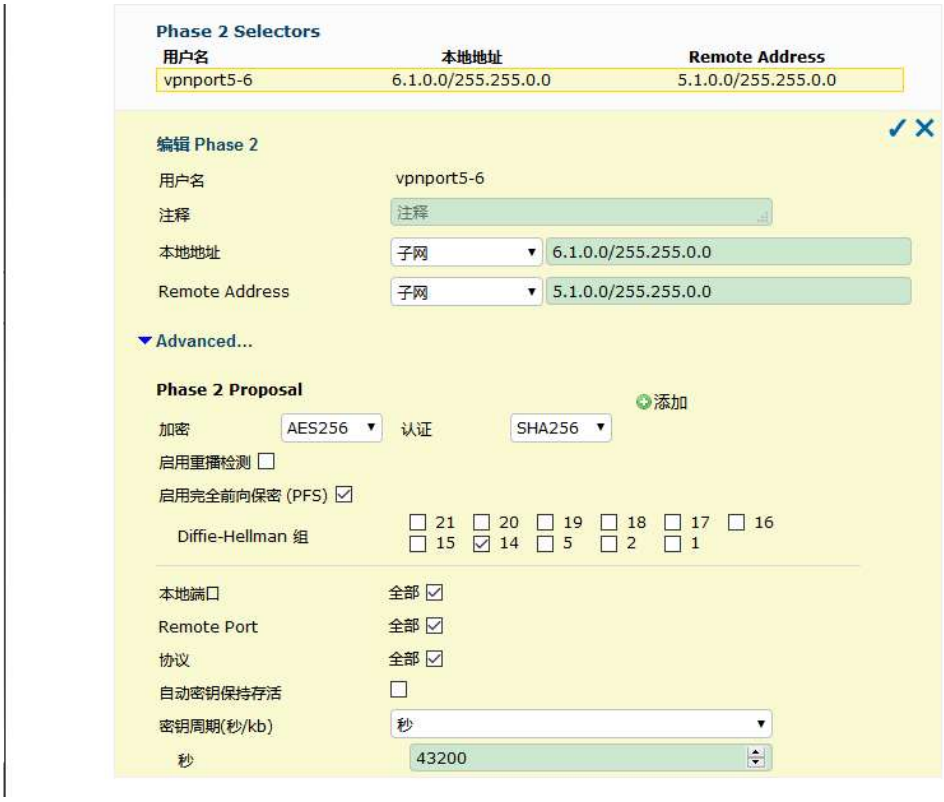
状态	Name	成员	IP/子网掩码	类型
物理 (13)				
	port1		192.168.16.248 255.255.255.0	物理
	port2		192.168.100.99 255.255.255.0	物理
	port3		3.1.1.1 255.255.0.0	物理
	port4		4.1.1.1 255.255.0.0	物理
	port5		5.1.1.1 255.255.0.0	物理
	port6		6.1.1.1 255.255.0.0	物理
	port7		7.1.1.1 255.255.0.0	物理
	port8		8.1.1.1 255.255.0.0	物理
	port9		9.1.1.1 255.255.0.0	物理
	port10		10.1.1.1 255.255.0.0	物理

2）选择远程网关的方式和 vpn 网关的接口地址。

3）选择认证方法为秘钥认证，秘钥两端需要保持一致。IKEv1 主模式。对等体任意即可。

第一阶段的安全关联加密认证算法，DH 组，禁用 XAUTH。

配置阶段二，本地地址和 remote 地址可以不填。



4）配置防火墙策略，策略放行。

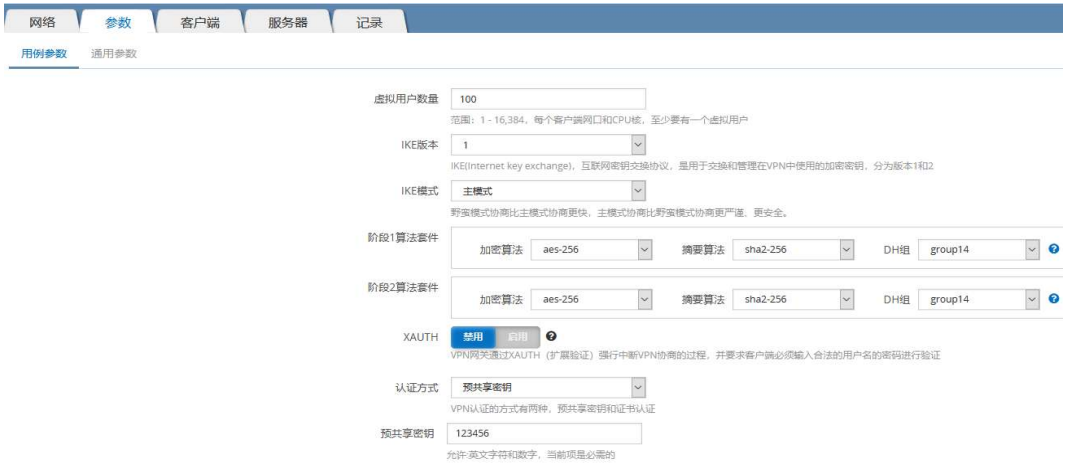
5.配置 Supernova 测试仪

1）添加 ipsec 新建或并发用例。

2）配置客户端对应 IP 地址，客户端就是隧道建立的发起者。

3）配置服务端对应 IP，服务器端就是 web 服务器（每条隧道建立成功都要 get 一次）。

4）配置用例“参数”中就是 ipsec vpn 的主要配置项，包括 IKE 版本、模式，阶段 1 和阶段 2 的加密、认证、DH 组，认证方式等，所有配置项和 vpn 网关一一对应。



5）用例配置完成，运行测试用例，查看用例运行界面

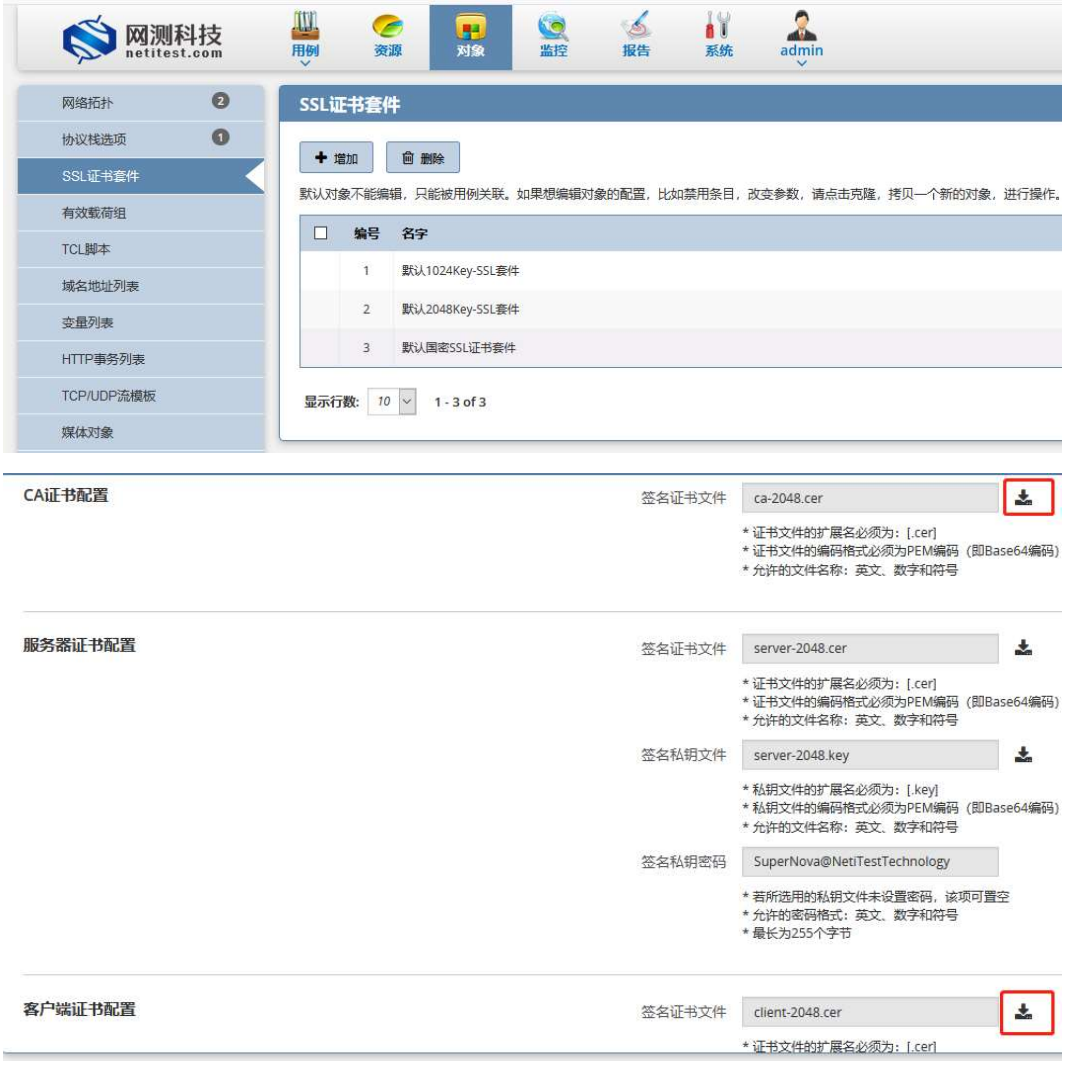
6.IPsec VPN 新建和并发设置

1）Ipsec 新建是虚拟用户控制新建数量，虚拟用户表示用多少用户去并发新建隧道

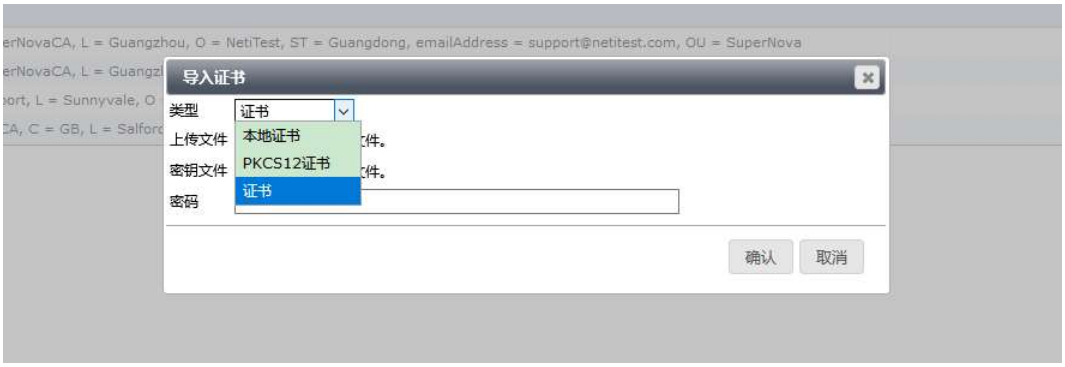
2）Ipsec 并发是隧道数控制并发隧道的数量

7.证书认证模式

1）获得测试仪客户端和 CA 证书



2）需要将客户端证书，和 CA 导入到 vpn 网关设备中



3）在配置 IPsec 中选择证书认证，并关联上传到本地的客户端证书、CA 证书


```
FG300C3913605314 # show user peer
config user peer
    edit "ssluser1"
        set ca "CA_Cert_2"
    next
    edit "yliu_rsa2048_user1"
        set ca "CA_Cert_1"
    next
    edit "yliu_rsa_2048_client"
        set ca "CA_Cert_1"
    next
end

FG300C3913605314 #
```

4）Spernova 配置证书配置，本地证书必须是同一 CA 颁发

其它配置与 PSK 配置方法相同，不在赘述。