

Supernova 测试仪

IPsec VPN 测试配置手册

网测科技

2021/01/26

目录

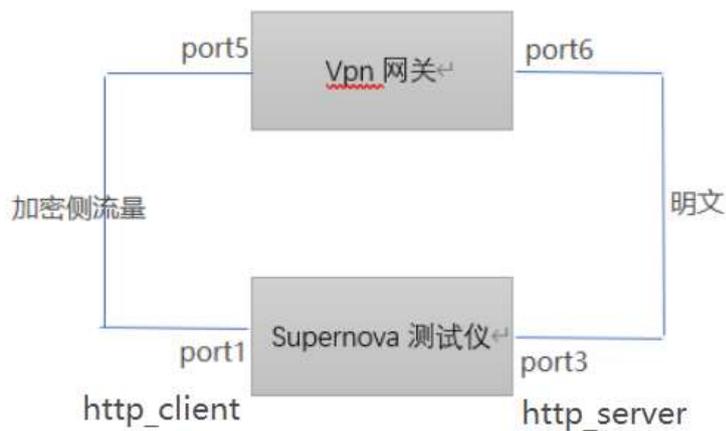
1.文档说明.....	3
2.测试拓扑图.....	3
3.支持秘钥和证书模式.....	3
4.配置防火墙为 VPN 网关.....	4
5.配置 Supernova 测试仪.....	6
6.IPsec VPN 新建和并发设置.....	8
7.证书认证模式.....	9

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.支持密钥和证书模式

IPsec VPN 支持 PSK 和 Signature 两种模式，也就是密钥和证书，先讲述密钥认证模式，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。

系统管理

路由

策略 & 对象

安全配置文件

虚拟专网

- IPsec
 - 隧道
 - 向导
 - 隧道模板
- SSL
- 监视器

用户名: vpnport5-6
10000 concurrent user(s) will be supported

注释: 注释

网络

IP 版本: IPv4

远程网关: 拨号用户

接口: port5

模式配置:

NAT穿越:

对等体状态探测:

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

认证 ✓ ✕

方法: 预共享密钥

预共享密钥: ●●●●● 显示密钥

IKE

版本: 1 2

Mode: Aggressive 主模式(ID保护)

对等体选项

访问类型: 任意对端 ID

第一阶段的安全关联加密认证算法，DH 组，禁用 XAUTH。

Phase 1 Proposal [添加] [X]

加密: AES256 认证: SHA256

Diffie-Hellman 组: 21 20 19 18 17 16
 15 14 5 2 1

密钥生存时间 (秒): 86400

本地ID: []

XAUTH [编辑]

类型: 已禁用

配置阶段二，本地地址和 remote 地址可以不填。

Phase 2 Selectors

用户名	本地地址	Remote Address
vpnport5-6	6.1.0.0/255.255.0.0	5.1.0.0/255.255.0.0

编辑 Phase 2 [添加] [X]

用户名: vpnport5-6

注释: []

本地地址: 子网 6.1.0.0/255.255.0.0

Remote Address: 子网 5.1.0.0/255.255.0.0

▼ Advanced...

Phase 2 Proposal [添加]

加密: AES256 认证: SHA256

启用重播检测:

启用完全前向保密 (PFS):

Diffie-Hellman 组: 21 20 19 18 17 16
 15 14 5 2 1

本地端口: 全部

Remote Port: 全部

协议: 全部

自动密钥保持存活:

密钥周期(秒/kb): 秒 []

秒: 43200

4) 配置防火墙策略，策略放行。

流入接口: vpnport5-6 []

源地址: all []

用户: 点击添加... []

设备: 点击添加... []

流出接口: port6 []

目的地址: all []

时间表: always []

服务: ALL []

动作: ACCEPT []

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



用例类型: Vpn新建 测试用户: admin 用例名称: IPsecRemoteAccess_TP_admin_20201203-14:54:03 运行结果: ● 用户中断 [查看历史] 异常信息: ● 测试被用户中断

关键结果

192.168.16.216 - Port1	总数
IPSec隧道新建	1,811
IPSec隧道建立	1,763

报文捕获

192.168.16.216 - Port1	总数
捕获数据包数量	5,000
捕获字节数量	1,067,873
报文捕获	[重抓] [已经停止] [下载]

192.168.16.216 - Port3	总数
捕获数据包数量	5,000
捕获字节数量	1,049,785
报文捕获	[重抓] [已经停止] [下载]

状态

应用层

总和 port1	秒值
HTTP_请求速率	59
HTTP_响应码2xx	59
HTTP_响应码3xx	0
HTTP_响应码4xx	0
HTTP_响应码5xx	0
HTTP_新建速率	59

传输层

总和 port1	总数	秒值
IPSec隧道新建	1,811	59
IPSec隧道建立	1,763	82
IPSec隧道并发		52

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



网络 参数 客户端 服务器 记录

用例参数 通用参数

虚拟用户数量

范围：1 - 1,024，每个客户端网口和CPU核，至少要有有一个虚拟用户

IKE版本

IKE(Iternet key exchange)，互联网密钥交换协议，是用于交换和管

IKE模式

野蛮模式协商比主模式协商更快，主模式协商比野蛮模式协商更严道

2) Ipsec 并发是隧道数控制并发隧道的数量



网络 参数 客户端 服务器 记录

用例参数 通用参数

IPSec并发隧道数

范围：1 - 1,000,000，并发的IPsec隧道个数，每个隧道内都会有流量发送和接收

Think Time

发送HTTP请求并接收响应后，到再次发送HTTP请求的等待时长，单位为秒

IKE版本

7.证书认证模式

1) 获得测试仪客户端和 CA 证书

The screenshot displays the NetiTest web interface for configuring SSL certificates. The top navigation bar includes icons for '用例', '资源', '对象', '监控', '报告', '系统', and 'admin'. The left sidebar shows a menu with 'SSL证书套件' selected. The main content area is titled 'SSL证书套件' and contains a table of certificates:

编号	名字
1	默认1024Key-SSL套件
2	默认2048Key-SSL套件
3	默认国密SSL证书套件

Below the table, there are '增加' and '删除' buttons, and a note: '默认对象不能编辑, 只能被用例关联. 如果想编辑对象的配置, 比如禁用条目, 改变参数, 请点击克隆, 拷贝一个新的对象, 进行操作.' The '显示行数' is set to 10, showing 1-3 of 3 items.

The 'CA证书配置' section shows the '签名证书文件' field set to 'ca-2048.cer' with a download icon. Below it are instructions: '* 证书文件的扩展名必须为: [.cer]', '* 证书文件的编码格式必须为PEM编码 (即Base64编码)', and '* 允许的文件名称: 英文、数字和符号'.

The '服务器证书配置' section shows the '签名证书文件' field set to 'server-2048.cer' and the '签名私钥文件' field set to 'server-2048.key', both with download icons. The '签名私钥密码' field is set to 'SuperNova@NetiTestTechnology'. Instructions include: '* 私钥文件的扩展名必须为: [.key]', '* 私钥文件的编码格式必须为PEM编码 (即Base64编码)', '* 允许的文件名称: 英文、数字和符号', '* 若所选用的私钥文件未设置密码, 该项可置空', and '* 最长的密码格式: 英文、数字和符号', '* 最长为255个字节'.

The '客户端证书配置' section shows the '签名证书文件' field set to 'client-2048.cer' with a download icon. The instruction '* 证书文件的扩展名必须为: [.cer]' is shown below.

2) 需要将客户端证书, 和 CA 导入到 vpn 网关设备中

The screenshot shows the '导入证书' (Import Certificate) dialog box. The background shows the CA configuration details: 'erNovaCA, L = Guangzhou, O = NetiTest, ST = Guangdong, emailAddress = support@netitest.com, OU = SuperNova'. The dialog box has the following fields:

- 类型: A dropdown menu with '证书' selected.
- 上传文件: A text input field with '本地证书' entered.
- 密钥文件: A text input field with 'PKCS12证书' entered.
- 密码: A text input field with '证书' entered.

At the bottom of the dialog are '确认' and '取消' buttons.



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

虚拟用户数量
范围: 1 - 16,384, 每个客户端网口和CPU核, 至少要有有一个虚拟用户

IKE版本
IKE(Internet key exchange), 互联网密钥交换协议, 是用于交换和管理在VPN中使用的加密密钥, 分为版本1和2

IKE模式
野蛮模式协商比主模式协商更快, 主模式协商比野蛮模式协商更严谨, 更安全。

阶段1算法套件
加密算法 摘要算法 DH组

阶段2算法套件
加密算法 摘要算法 DH组

XAUTH 禁用 启用
VPN网关通过XAUTH (扩展验证) 强行中断VPN协商的过程, 并要求客户端必须输入合法的用户的密码进行验证

认证方式
VPN认证的方式有两种, 预共享密钥和证书认证

证书认证
 部分

其它配置与 PSK 配置方法相同，不在赘述。