

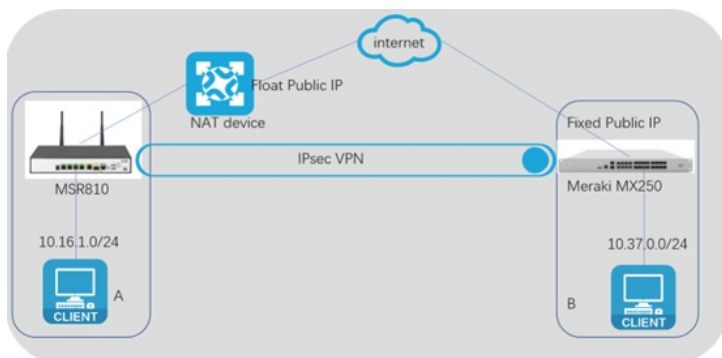
知 H3C MSR810与Cisco Meraki MX250的IPsec VPN主模式NAT穿越场景对接案例

IPSec VPN

IPSec VPN

zhiliao_1qRBai 2023-04-26 发表

组网及说明



说明：

1. B侧Meraki MX250与A侧MSR810建立隧道方式的IPsec VPN,IKE协商模式为Main模式。
2. 第一阶段协商为预共享密钥认证。
3. B所在的子网（10.37.0.0/24）与Host A所在的子网（10.16.1.0/24）之间的数据流进行安全保护。
4. MSR810版本为H3C Comware Software, Version 7.1.064, Release 0821P18。

配置步骤

二、实验步骤：

接口IP，底层路由信息等不在此做描述，只显示IPsec VPN协商参数部分配置。

1. 由于B侧设备为友商设备，需要确定第一阶段与第二阶段协商协商参数。

Pre-share KEY	test
IKE version	IKEv1
DH	Group2
Encryption	AES-128
HASH	SHA1
Exchange-mode	Main
封装类型	ESP
第二阶段	AES-128/SHA-1
PFS	PFS Grupo 2
协商超时	28800 s

Meraki配置截图为：



其中custom的参数配置为：

Choose a Preset: Custom

Phase 1

Encryption: AES 128
Authentication: SHA1
Diffie-Hellman group: 2
Lifetime (seconds): 28800

Phase 2

Encryption: AES 128 x
Authentication: SHA1 x
PFS group: 2
Lifetime (seconds): 28800

Cancel Update

2. MSR810上的配置如下：

- (1) 完成接口IP/路由配置；
- (2) 定义需要保护的数据流

acl advanced 3001

rule 0 permit ip source 10.16.1.0 0.0.0.255 destination 10.37.0.0 0.0.0.255

- (3) 配置IPsec安全提议，协商封装报文使用的各种安全协议

ipsec transform-set tran1

esp encryption-algorithm aes-cbc-128

esp authentication-algorithm sha1

pfs dh-group2

封装模式默认为ESP。

- (4) 配置IKE keychain，约定通信双方使用的密钥信息

ike keychain keychain1

pre-shared-key address x.x.x.x 255.255.255.0 key simple test

- (5) 配置IKE profile，约定建立IKE SA所需的安全参数：

ike profile profile1

keychain keychain1

local-identity user-fqdn www.msr.com

match remote identity address x.x.x.x 255.255.255.0 //对端公网IP

proposal 1

- (6) 配置IPsec安全策略，建立IPsec隧道，保护需要防护的数据流：

```
ipsec policy map1 10 isakmp
transform-set tran1
security acl 3001
remote-address x.x.x.x
```

配置关键点

验证 on time-based 28800

通过A侧主接口上配置IPsec安全策略，对接口上的流量进行保护：

```
interface GigabitEthernet0/0
Haciendo ping a 10.37.0.254 con 32 bytes de datos:
Respuesta desde 10.37.0.254: bytes=32 tiempo=7ms TTL=252
Respuesta desde 10.37.0.254: bytes=32 tiempo=5ms TTL=252
Respuesta desde 10.37.0.254: bytes=32 tiempo=6ms TTL=252
Respuesta desde 10.37.0.254: bytes=32 tiempo=6ms TTL=252

Estadísticas de ping para 10.37.0.254:
  Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
  Mínimo = 5ms, Máximo = 7ms, Media = 6ms

C:\WINDOWS\system32>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet 2:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::42eb:f970:b82:e3bd%21
    Dirección IPv4. . . . . : 10.16.1.2
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . : 10.16.1.1
```

Ping通过后，查看IKE协商

```
<T016>display ike sa
Connection-ID Local Remote Flag DOI
-----
116 192.168.1.1 192.168.1.2 RD IPsec
115 192.168.1.1 192.168.1.2 RD|RL IPsec
Flags:
RD--READY RL--REPLACED FD--FADING RK--REKEY
<T016>
```

```
<T016>display ike sa verbose
-----
Connection ID: 116
Outside VPN:
Inside VPN:
Profile: profile1
Transmitting entity: Responder
Initiator cookie: 74a966628257e2f7
Responder cookie: f53e78ad99df7cf6
-----
Local IP/port: 192.168.1.1/4500
Local ID type: FQDN
Local ID: www.msr.com

Remote IP/port: 192.168.1.2/4500
Remote ID type: IPV4_ADDR
Remote ID: 192.168.1.2

Authentication-method: PRE-SHARED-KEY
Authentication-algorithm: SHA1
Encryption-algorithm: AES-CBC-128

Life duration(sec): 28800
Remaining key duration(sec): 27212
Exchange-mode: Main
Diffie-Hellman group: Group 2
NAT traversal: Detected

Extend authentication: Disabled
Assigned IP address:
Vendor ID index:0xffffffff
Vendor ID sequence number:0x0
-----
```

通过display ipsec sa可以查看IPsec VPN建立情况：

```
IPsec policy: map1
Sequence number: 10
Mode: ISAKMP
```

附件下载: [H3C MSR10与Cisco Meraki MX250的IPsec VPN对接案例V0.1.docx](#)

```
-----
Encapsulation mode: tunnel
Perfect Forward Secrecy: dh-group2
Inside VPN:
Extended Sequence Numbers enabled: N
```