

知 F1000-AK系列使用IKEV2主模式建立IPSEC VPN典型配置

IPSec VPN IPSec VPN zhiliao_8mkdB 2018-11-24 发表

组网及说明

1 配置需求及说明

1.1 适用的产品系列

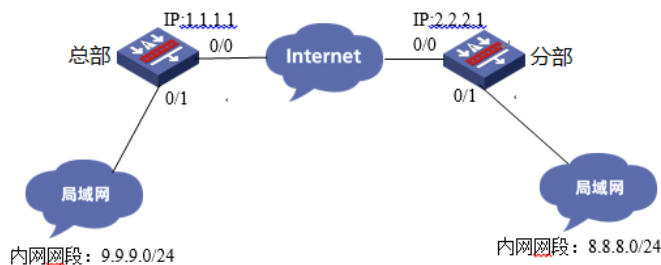
本案例适用于如F1000-AK180、F1000-AK170等F1000-AK系列的防火墙。

1.2 配置需求及实现的效果

用户需求两台V7防火墙使用IKEV2协议对接IPSEC VPN，IP地址及接口规划如下表所示：

公司名称	外网接口	公网地址/掩码	公网网关	内网接口	内网地址/掩码
总部	0/0	1.1.1.1/24	1.1.1.2	0/1	9.9.9.0/24
分部	0/0	2.2.2.1/24	2.2.2.2	0/1	8.8.8.0/24

2 组网图



配置步骤

3 两端防火墙上网配置

防火墙上网配置略，本文只针对IPSEC VPN配置进行介绍。

3.1 总部侧创建IPSEC兴趣流匹配到分部的数据

创建IPSEC的感兴趣流，用于匹配IPSEC数据。

system

```
[H3C]acl advanced 3000
```

```
[H3C-acl-ipv4-adv-3000]rule permit ip source 9.9.9.0 0.0.0.255 destination 8.8.8.0 0.0.0.255
```

```
[H3C-acl-ipv4-adv-3000]quit
```

创建acl 3001调用在外网接口用于排除IPSEC兴趣流不做NAT。

```
[H3C]acl advanced 3001
```

```
[H3C-acl-ipv4-adv-3001]rule deny ip source 9.9.9.0 0.0.0.255 destination 8.8.8.0 0.0.0.255
```

```
[H3C-acl-ipv4-adv-3001]rule permit ip source any
```

```
[H3C-acl-ipv4-adv-3001]quit
```

3.2 总部侧创建IPSEC安全提议

加密类型设置为3des-cbc，认证类型设置为md5。

```
[H3C]ipsec transform-set 1
```

```
[H3C-ipsec-transform-set-1] esp encryption-algorithm 3des-cbc
```

```
[H3C-ipsec-transform-set-1] esp authentication-algorithm md5
```

```
[H3C-ipsec-transform-set-1] quit
```

3.3 总部侧创建IKEV2安全提议

设备存在默认的IKE V2安全提议，所以不需要配置也存在参数。

```
[H3C]ikev2 proposal 1
```

```
[H3C-ikev2-proposal-1]quit
```

以下为IKE V2默认的加密及认证算法。

```
display ikev2 proposal
```

```
IKEv2 proposal : default
```

```
Encryption: AES-CBC-128 3DES-CBC
```

```
Integrity: SHA1 MD5
```

```
PRF: SHA1 MD5
```

```
DH Group: MODP1536/Group5 MODP1024/Group2
```

3.4 总部侧创建IKE V2安全密钥

创建IKE V2密钥，地址填写分部侧设备的公网IP，密码设置为123。

```
[H3C]ike keychain 1
[H3C-ike-keychain-1-peer2]peer 2
[H3C-ike-keychain-1-peer2] address 2.2.2.1 255.255.255.255
[H3C-ike-keychain-1-peer2] identity address 2.2.2.1
[H3C-ike-keychain-1-peer2] pre-shared-key plaintext 123
[H3C-ike-keychain-1-peer2]quit
```

3.5 总部侧创建IKE安全框架

创建IKE安全框架，将对端地址、keychain、proposal关联起来。

```
[H3C]ikev2 profile 1
[H3C-ikev2-profile-1]keychain 1
[H3C-ikev2-profile-1] authentication-method local pre-share
[H3C-ikev2-profile-1] authentication-method remote pre-share
[H3C-ikev2-profile-1] match remote identity address 2.2.2.1 255.255.255.255
[H3C-ikev2-profile-1]quit
```

3.6 总部侧创建IPSEC安全策略

创建IKE安全策略GE0/0将transform-set、acl、ikev2-profile、对端地址关联起来。

```
[H3C]ipsec policy GE0/0 1 isakmp
[H3C-ipsec-policy-isakmp- GE0/0-1]transform-set 1
[H3C-ipsec-policy-isakmp- GE0/0-1]security acl 3000
[H3C-ipsec-policy-isakmp- GE0/0-1]remote-address 2.2.2.1
[H3C-ipsec-policy-isakmp- GE0/0-1]ikev2-profile 1
[H3C-ipsec-policy-isakmp- GE0/0-1]quit
```

3.7 总部侧在外网接口调用NAT及IPSEC策略

```
[H3C]interface GigabitEthernet 0/0
[H3C-GigabitEthernet 0/0]ipsec apply policy GE0/0
[H3C-GigabitEthernet 0/0]nat outbound 3001
[H3C-GigabitEthernet 0/0]quit
```

3.8 分部侧创建IPSEC兴趣流匹配到分部的数据

创建IPSEC的兴趣流，用于匹配IPSEC数据。

```
system
[H3C]acl advanced 3000
[H3C-acl-ipv4-adv-3000]rule permit ip source 8.8.8.0 0.0.0.255 destination 9.9.9.0 0.0.0.255
[H3C-acl-ipv4-adv-3000]quit
创建acl 3001调用在外网接口用于排除IPSEC兴趣流不做NAT。
[H3C]acl advanced 3001
[H3C-acl-ipv4-adv-3001]rule deny ip source 8.8.8.0 0.0.0.255 destination 9.9.9.0 0.0.0.255
[H3C-acl-ipv4-adv-3001]rule permit ip source any
[H3C-acl-ipv4-adv-3001]quit
```

3.9 分部侧创建IPSEC安全提议

加密类型设置为3des-cbc，认证类型设置为md5。

```
[H3C]ipsec transform-set 1
[H3C-ipsec-transform-set-1] esp encryption-algorithm 3des-cbc
[H3C-ipsec-transform-set-1] esp authentication-algorithm md5
[H3C-ipsec-transform-set-1] quit
```

3.10 分部侧创建IKEV2安全提议

设备存在默认的IKE V2安全提议,所以不需要配置也存在参数。

```
[H3C]ikev2 proposal 1
[H3C-ikev2-proposal-1]quit
```

以下为IKE V2默认的加密及认证算法。

```
display ikev2 proposal
IKEv2 proposal : default
Encryption: AES-CBC-128 3DES-CBC
Integrity: SHA1 MD5
PRF: SHA1 MD5
DH Group: MODP1536/Group5 MODP1024/Group2
```

3.11 分部侧创建IKE V2安全密钥

创建IKE V2密钥，地址填写分部侧设备的公网IP，密码设置为123。

```
[H3C]ike keychain 1
[H3C-ike-keychain-1-peer1]peer 1
[H3C-ike-keychain-1-peer1] address 1.1.1.1 255.255.255.255
[H3C-ike-keychain-1-peer1] identity address 1.1.1.1
[H3C-ike-keychain-1-peer1] pre-shared-key plaintext 123
[H3C-ike-keychain-1-peer1]quit
```

3.12 分部侧创建IKE安全框架

创建IKE安全框架，将本端地址、对端地址、keychain、proposal关联起来。

```
[H3C]ikev2 profile 1
[H3C-ikev2-profile-1]keychain 1
[H3C-ikev2-profile-1] authentication-method local pre-share
[H3C-ikev2-profile-1] authentication-method remote pre-share
[H3C-ikev2-profile-1] match remote identity address 1.1.1.1 255.255.255.255
[H3C-ikev2-profile-1]quit
```

3.13 分部创建IPSEC安全策略

创建IKE安全策略GE0/0将transform-set、acl、ikev2-profile、对端地址关联起来。

```
[H3C]ipsec policy GE0/0 1 isakmp
[H3C-ipsec-policy-isakmp- GE0/0-1]transform-set 1
[H3C-ipsec-policy-isakmp- GE0/0-1]security acl 3000
[H3C-ipsec-policy-isakmp- GE0/0-1]remote-address 1.1.1.1
[H3C-ipsec-policy-isakmp- GE0/0-1]ikev2-profile 1
[H3C-ipsec-policy-isakmp- GE0/0-1]quit
```

3.14 分部侧在外网接口调用NAT及IPSEC策略

```
[H3C]interface GigabitEthernet 0/0
[H3C-GigabitEthernet 0/0]ipsec apply policy GE0/0
[H3C-GigabitEthernet 0/0]nat outbound 3001
[H3C-GigabitEthernet 0/0]quit
```

4 保存配置

```
[H3C]quit
save force
```

5 隧道验证

通过如下显示信息查看到总部上IKEv2协商成功后生成的IKEv2 SA。

```
[H3C] display ikev2 sa
Tunnel ID   Local           Remote           Status
-----
1   1.1.1.1/500     2.2.2.1/500     EST
```

通过命令行查看dis ipsec sa可以看到隧道状态已经建立完成。

```
dis ipsec sa
-----
Interface: GigabitEthernet0/0
-----

IPsec policy: 1
Sequence number: 1
Mode: ISAKMP
-----

Tunnel id: 0
Encapsulation mode: tunnel
Perfect Forward Secrecy:
Inside VPN:
Extended Sequence Numbers enable: N
Traffic Flow Confidentiality enable: N
Path MTU: 1444
Tunnel:
    local address: 1.1.1.1
```

remote address: 2.2.2.1

Flow:

sour addr: 9.9.9.9/255.255.255.255 port: 0 protocol: ip

dest addr: 8.8.8.8/255.255.255.255 port: 0 protocol: ip

[Inbound ESP SAs]

SPI: 2831964167 (0xa8cc5807)

Connection ID: 12884901889

Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5

SA duration (kilobytes/sec): 1843200/3600

SA remaining duration (kilobytes/sec): 1843199/1475

Max received sequence-number: 4

Anti-replay check enable: Y

Anti-replay window size: 64

UDP encapsulation used for NAT traversal: N

Status: Active

[Outbound ESP SAs]

SPI: 662015886 (0x27758f8e)

Connection ID: 55834574848

Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5

SA duration (kilobytes/sec): 1843200/3600

SA remaining duration (kilobytes/sec): 1843199/1475

Max sent sequence-number: 4

UDP encapsulation used for NAT traversal: N

Status: Active

通过如下显示信息查看到分部上IKEv2协商成功后生成的IKEv2 SA。

[H3C] display ikev2 sa

Tunnel ID	Local	Remote	Status
-----------	-------	--------	--------

1	2.2.2.1/500	1.1.1.1/500	EST
---	-------------	-------------	-----

通过命令行查看dis ipsec sa可以看到隧道状态已经建立完成。

dis ipse sa

Interface: GigabitEthernet0/0

IPsec policy: 1

Sequence number: 1

Mode: ISAKMP

Tunnel id: 0

Encapsulation mode: tunnel

Perfect Forward Secrecy:

Inside VPN:

Extended Sequence Numbers enable: N

Traffic Flow Confidentiality enable: N

Path MTU: 1444

Tunnel:

local address: 2.2.2.1

remote address: 1.1.1.1

Flow:

sour addr: 8.8.8.8/255.255.255.255 port: 0 protocol: ip

dest addr: 9.9.9.9/255.255.255.255 port: 0 protocol: ip

[Inbound ESP SAs]

SPI: 662015886 (0x27758f8e)

Connection ID: 12884901889

Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5

SA duration (kilobytes/sec): 1843200/3600

SA remaining duration (kilobytes/sec): 1843199/1431

Max received sequence-number: 4

Anti-replay check enable: Y

Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: Active

[Outbound ESP SAs]

SPI: 2831964167 (0xa8cc5807)
Connection ID: 12884901888
Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/1431
Max sent sequence-number: 4
UDP encapsulation used for NAT traversal: N
Status: Active

配置关键点