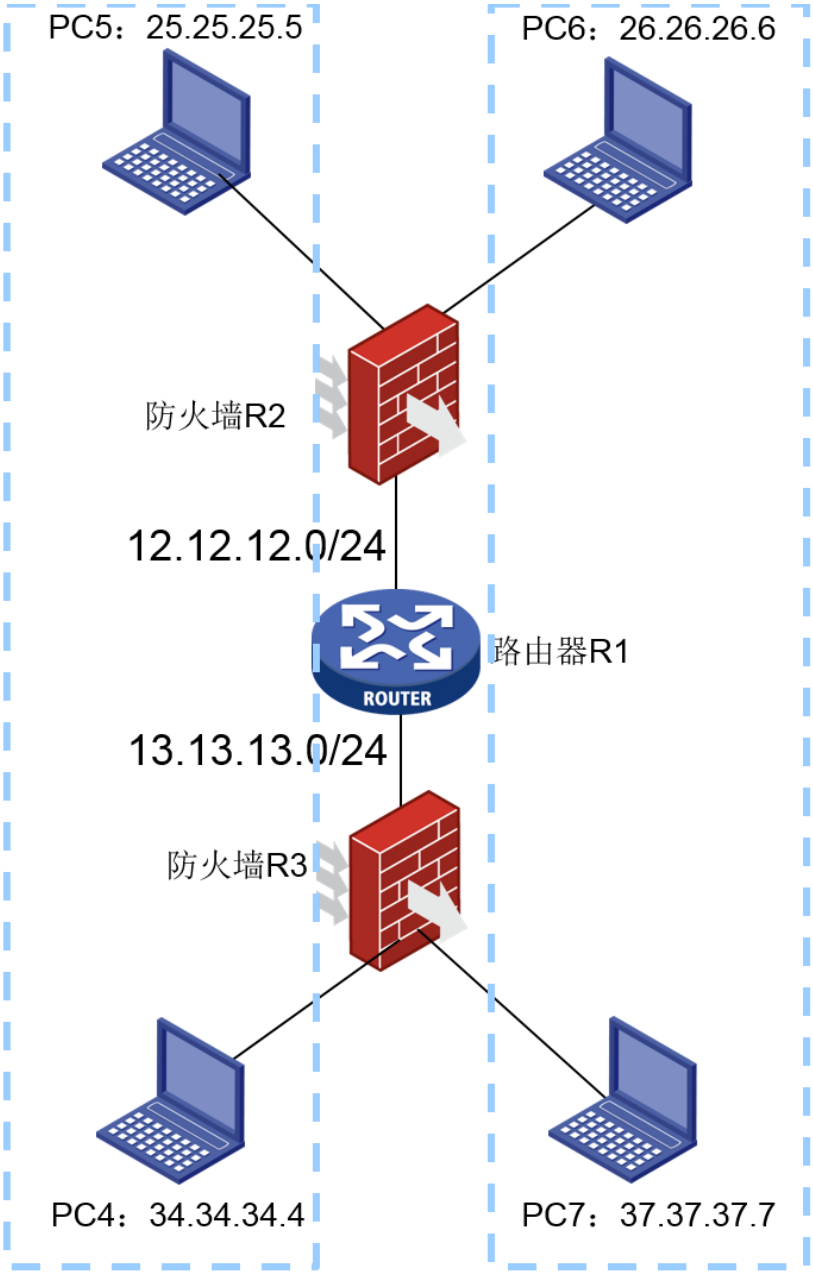
V7防火墙同一对端点，单条物理路径下，建立ipsec隧道，对两端私网的两种不同互访流量，使用不同的加密方式处理的典型配置

IPSec VPN 徐猛 2020-11-29 发表

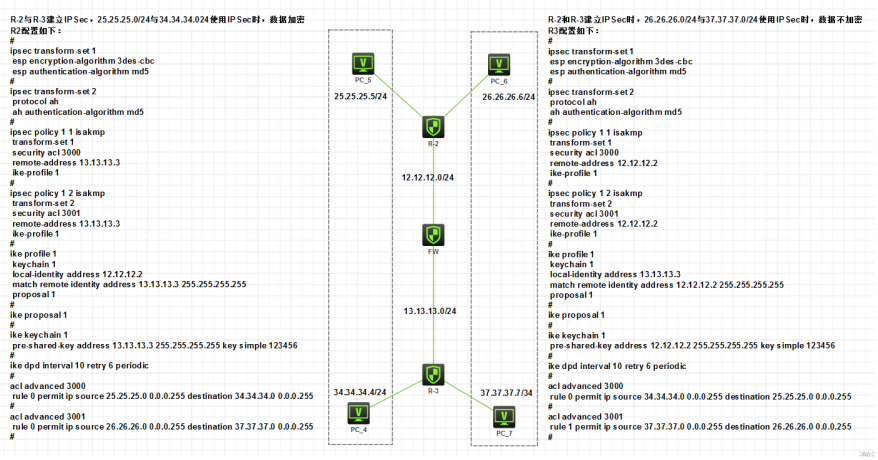
组网及说明

组网情况如下图，两端私网出口分别为R2和R3：
R-2与R-3建立IPSec，25.25.25.0/24与34.34.34.024互访使用IPSec时，数据需要加密。
同时，26.26.26.0/24与37.37.37.0/24互访使用IPSec时，数据不加密。



配置步骤

对于现场的需求，我们制定了方案是，针对不同的流量加密需求，我们在同一ipsec策略下，创建两个编号，分别保护不同的流量，并对于需要加密的流量，使用ESP方式的ipsec安全提议；对于不需要加密的流量，使用AH方式（只做数据完整性校验等，不做加密）的安全提议。为便于清晰的理解配置逻辑，这边将拓扑图和配置做了左右对比图，可以先大致看下图：



1.现场需求和详细配置罗列：

（1）需求：两端私网出口分别为R2和R3:

R-2与R-3建立IPSec，25.25.25.0/24与34.34.34.024互访使用IPSec时，数据需要加密。

R-2和R-3建立IPSec，26.26.26.0/24与37.37.37.0/24互访使用IPSec时，数据不加密。

（2）R2详细配置：

```
#
ipsec transform-set 1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec transform-set 2
 protocol ah
 ah authentication-algorithm md5
#
ipsec policy 1 1 isakmp
 transform-set 1
 security acl 3000
 remote-address 13.13.13.3
 ike-profile 1
#
ipsec policy 1 2 isakmp
 transform-set 2
 security acl 3001
 remote-address 13.13.13.3
 ike-profile 1
#
ike profile 1
 keychain 1
 local-identity address 12.12.12.2
 match remote identity address 13.13.13.3 255.255.255.255
 proposal 1
#
ike proposal 1
#
ike keychain 1
 pre-shared-key address 13.13.13.3 255.255.255.255 key cipher
$c$3$VXLgC1uUD9eeLugp8kwhpeZpVyvp/A==
#
ike dpd interval 10 retry 6 periodic
#
acl advanced 3000
 rule 0 permit ip source 25.25.25.0 0.0.0.255 destination 34.34.34.0 0.0.0.255
#
acl advanced 3001
 rule 0 permit ip source 26.26.26.0 0.0.0.255 destination 37.37.37.0 0.0.0.255
#
```

（3）R3详细配置：

```
#
```

```
ipsec transform-set 1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec transform-set 2
 protocol ah
 ah authentication-algorithm md5
#
ipsec policy 1 1 isakmp
 transform-set 1
 security acl 3000
 remote-address 12.12.12.2
 ike-profile 1
#
ipsec policy 1 2 isakmp
 transform-set 2
 security acl 3001
 remote-address 12.12.12.2
 ike-profile 1
#
ike profile 1
 keychain 1
 local-identity address 13.13.13.3
 match remote identity address 12.12.12.2 255.255.255.255
 proposal 1
#
ike proposal 1
#
ike keychain 1
 pre-shared-key address 12.12.12.2 255.255.255.255 key cipher
$c$3$FNY1oCdahtwgcp6NaWTB8DnB0O/Oog==
#
ike dpd interval 10 retry 6 periodic
#
acl advanced 3000
 rule 0 permit ip source 34.34.34.0 0.0.0.255 destination 25.25.25.0 0.0.0.255
#
acl advanced 3001
 rule 1 permit ip source 37.37.37.0 0.0.0.255 destination 26.26.26.0 0.0.0.255
#
```

2.如上配置后，经测试， 34.34.34.4和 25.25.25.5能够正常互访， 37.37.37.7 和 26.26.26.6也能够正常互访 。

3.查看对应的ike sa和ipsec sa的建立情况：

（1）查看ike sa情况如下：

```
[R-3]dis ike sa
   Connection-ID   Remote              Flag        DOI
-------------------------------------------------------------------------
   1               12.12.12.2          RD          IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
```

（2）查看ipsec sa的情况如下，发现建立起了两种不同类型和不同tunnel id的ipsec隧道，分别由tunnel 1保护 34.34.34.0/24和25.25.25.0/24之间的流量，以及tunnel 2保护 37.37.37.0/24和26.26.26.0/24之间的流量：

```
[R-3]dis ipsec sa
-------------------------------
Interface: GigabitEthernet0/0
-------------------------------

  -----------------------------
  IPsec policy: 1
  Sequence number: 1
```

Mode: ISAKMP

Tunnel id: 1

Encapsulation mode: tunnel

Perfect Forward Secrecy:

Inside VPN:

Extended Sequence Numbers enable: N

Traffic Flow Confidentiality enable: N

Path MTU: 1444

Tunnel:

local address: 13.13.13.3

remote address: 12.12.12.2

Flow:

sour addr: 34.34.34.0/255.255.255.0 port: 0 protocol: ip

dest addr: 25.25.25.0/255.255.255.0 port: 0 protocol: ip

[Inbound ESP SAs]

SPI: 3515239723 (0xd1864d2b)

Connection ID: 4294967298

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

SA duration (kilobytes/sec): 1843200/3600

SA remaining duration (kilobytes/sec): 1843199/3585

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: 227170458 (0x0d8a589a)

Connection ID: 4294967299

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

SA duration (kilobytes/sec): 1843200/3600

SA remaining duration (kilobytes/sec): 1843199/3585

Max sent sequence-number: 4

UDP encapsulation used for NAT traversal: N

Status: Active

IPsec policy: 1

Sequence number: 2

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: 1456

Tunnel:

local address: 13.13.13.3

remote address: 12.12.12.2

Flow:

sour addr: 37.37.37.0/255.255.255.0 port: 0 protocol: ip

dest addr: 26.26.26.0/255.255.255.0 port: 0 protocol: ip

[Inbound AH SAs]

SPI: 4037884367 (0xf0ad39cf)

Connection ID: 4294967296

Transform set: AH-MD5

SA duration (kilobytes/sec): 1843200/3600

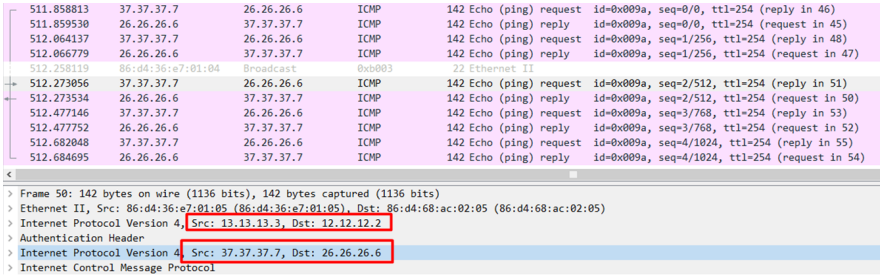
SA remaining duration (kilobytes/sec): 1843199/3566

Max received sequence-number: 4

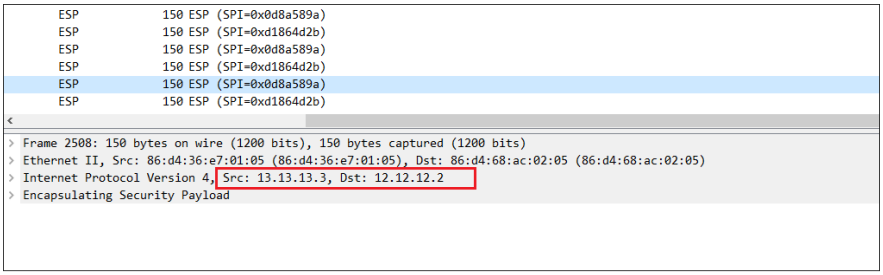
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: Active

[Outbound AH SAs]
SPI: 80191694 (0x04c7a0ce)
Connection ID: 4294967297
Transform set: AH-MD5
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/3566
Max sent sequence-number: 4
UDP encapsulation used for NAT traversal: N
Status: Active
[R-3]

4.对不同类型的业务流抓包对比，来判断报文的加密/不加密是否成功：
（1）使用 37.37.37.7和26.26.26.6进行互访测试，走的是tunnel 2的AH类型封装的隧道，抓包发现报文未进行加密，可以看到报文内层私网数据报内容。



（2） 使用 34.34.34.4和25.25.25.5 进行互访测试，走的是tunnel 1的ESP类型封装的隧道，抓包发现报文内容已被ESP加密，无法看到报文内层私网数据报内容。



配置关键点