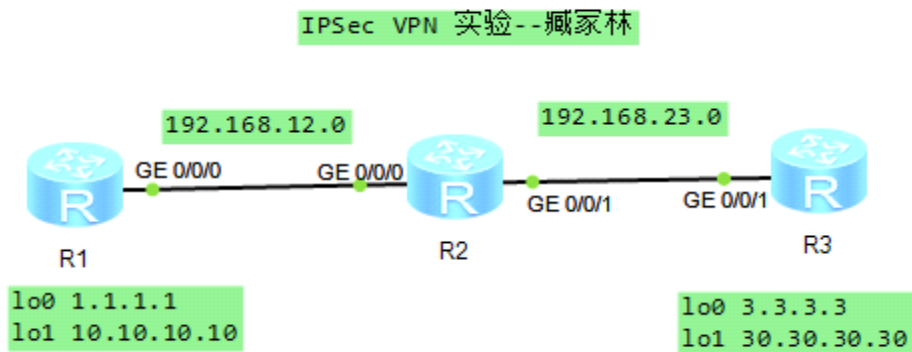


## HCIP-Datacom 分解实验 - VPN 技术

臧家林制作



### VPN 技术 实验 1：IPSec VPN



#### 基础配置

R1 :  
undo ter mo  
sy  
sys R1  
int loo0  
ip add 1.1.1.1 24  
int loo1  
ip add 10.10.10.10 24  
int g0/0/0

```
ip add 192.168.12.1 24
q
```

```
ospf 1 router-id 1.1.1.1
area 0
net 1.1.1.1 0.0.0.0
net 10.10.10.10 0.0.0.0
net 192.168.12.1 0.0.0.0
q
```

```
R2:
undo ter mo
sy
sys R2
int g0/0/0
ip add 192.168.12.2 24
int g0/0/1
ip add 192.168.23.2 24
q
```

```
ospf 1 router-id 2.2.2.2
area 0
net 192.168.12.2 0.0.0.0
net 192.168.23.2 0.0.0.0
q
```

```
R3:
undo ter mo
sy
sys R3
int lo0
ip add 3.3.3.3 24
int loo1
ip add 30.30.30.30 24
```

```

int g0/0/1
ip add 192.168.23.3 24
q

ospf 1 router-id 3.3.3.3
area 0
net 3.3.3.3 0.0.0.0
net 30.30.30.30 0.0.0.0
net 192.168.23.3 0.0.0.0
q

```

待 OSPF 收敛完成后，查看 OSPF 邻居以及路由表  
R1 R3 之间可以通信

```
[R2]dis ospf peer bri
```

```

      OSPF Process 1 with Router ID 2.2.2.2
      Peer Statistic Information
-----
Area Id      Interface      Neighbor id    State
0.0.0.0      GigabitEthernet0/0/0    1.1.1.1       Full
0.0.0.0      GigabitEthernet0/0/1    3.3.3.3       Full
-----

```

=====

## 配置 ACL 定义感兴趣流

配置高级 ACL 来定义 IPsec VPN 的感兴趣流。高级 ACL 能够基于特定的参数来匹配流量

R1 R3 的源地址，目的地址相反

```

R1:
acl 3000
rule permit ip source 1.1.1.0 0.0.0.255 destination
3.3.3.0 0.0.0.255

```

```
R3:
acl 3000
rule permit ip source 3.3.3.0 0.0.0.255 destination
1.1.1.0 0.0.0.255
```

=====

## 配置 IPsec VPN 提议

创建 IPsec 提议，并进入 IPsec 提议视图来指定安全协议。  
注意确保隧道两端的设备使用相同的安全协议

```
encapsulation-mode (transport ) (tunnel)    配置报文的封装模式，默认为 tunnel 模式
esp authentication-algorithm sha1            配置 IPS 协议使用的认证算法
esp encryption-algorithm 3des               配置 ESP 加密算法
```

R1 R3 配置相同

```
R1:
ipsec proposal tun
esp authentication-algorithm sha1
esp encryption-algorithm 3des
```

```
R3:
ipsec proposal tun
esp authentication-algorithm sha1
esp encryption-algorithm 3des
```

执行 display ipsec proposal 命令，验证配置结果

```
[R1]dis ipsec proposal
```

```
Number of proposals: 1
```

```
IPSec proposal name: tun
Encapsulation mode: Tunnel
Transform           : esp-new
ESP protocol        : Authentication SHA1-HMAC-96
                    : Encryption    3DES
```

```
=====
```

## 创建 IPsec 策略

手工创建 IPsec 策略，每一个 IPsec 安全策略都使用唯一的名称和序号来标识，IPsec 策略中会应用 IPsec 提议中定义的安全协议、认证算法、加密算法和封装模式，手工创建的 IPsec 策略还需配置安全联盟（SA）中的参数

执行 ipsec policy	创建策略
执行 ipsec-policy	指定 SA 建立方式 可使用 IKE
或是手工建立	
执行 security ACL	指定 IPSEC 策略所引用的访问控制列表
执行 proposal	指定 IPSEC 策略所引用的提议
执行 tunnel local	用来指定安全隧道的本端地址
执行 tunnel remote	指定隧道的对端地址
执行 sa spi	指定安全索引参数
执行 sa string-key	指定安全联盟的认证密钥

R1 :

```
ipsec policy p1 10 manual
security acl 3000
proposal tun
tunnel remote 192.168.23.3
tunnel local 192.168.12.1
sa spi outbound esp 54321
sa spi inbound esp 12345
sa string-key outbound esp simple huawei
sa string-key inbound esp simple huawei
q
```

R3 :

```
ipsec policy p1 10 manual
security acl 3000
proposal tun
tunnel remote 192.168.12.1
tunnel local 192.168.23.3
sa spi outbound esp 12345
sa spi inbound esp 54321
sa string-key outbound esp simple huawei
sa string-key inbound esp simple huawei
q
```

执行 display ipsec policy 命令，验证配置结果

```
[R1]dis ipsec policy
```

```
=====
```

```
IPSec policy group: "p1"
```

```
Using interface:
```

```
=====
```

```
Sequence number: 10
```

```
Security data flow: 3000
```

```
Tunnel local address: 192.168.12.1
```

```
Tunnel remote address: 192.168.23.3
```

```
Qos pre-classify: Disable
```

```
Proposal name:tun
```

```
Inbound AH setting:
```

```
AH SPI:
```

```
AH string-key:
```

```
AH authentication hex key:
```

```
Inbound ESP setting:
```

```
ESP SPI: 12345 (0x3039)
```

```
ESP string-key: huawei
```

```
ESP encryption hex key:
```

```
=====
```

### 在接口下应用 IPSec 策略

在物理接口应用 IPSec 策略，接口将对感兴趣流量进行 IPSec 加密处理

R1:

```
int g0/0/0
```

```
ipsec policy p1
```

```
R3:
int g0/0/1
ipsec policy p1
```

验证设备将对感兴趣流量进行 IPSec 加密处理

```
R1:ping -a 1.1.1.1 3.3.3.3
```

```
R1 : display ipsec statistics esp
```

```
[R1]display ipsec statistics esp
Inpacket count           : 5
Inpacket auth count      : 0
Inpacket decap count      : 0
Outpacket count           : 5
Outpacket auth count      : 0
Outpacket encap count     : 0
Inpacket drop count       : 0
```

ping 之后，会有加密解密的报文

不是感兴趣流量不加解密

```
ping -a 10.10.10.10 30.30.30.30
```

```
[R1]ping -a 10.10.10.10 30.30.30.30
PING 30.30.30.30: 56 data bytes, press CTRL_C to break
  Reply from 30.30.30.30: bytes=56 Sequence=1 ttl=254 time=40 ms
  Reply from 30.30.30.30: bytes=56 Sequence=2 ttl=254 time=30 ms
  Reply from 30.30.30.30: bytes=56 Sequence=3 ttl=254 time=30 ms
  Reply from 30.30.30.30: bytes=56 Sequence=4 ttl=254 time=30 ms
  Reply from 30.30.30.30: bytes=56 Sequence=5 ttl=254 time=20 ms
```

加密解密的报文 还是 5

=====

配置动态 IKE v2 IPSec VPN



R1:  
int g0/0/0  
undo ipsec policy  
q  
  
undo ipsec policy p1 10  
undo ipsec proposal tran

R3:  
int g0/0/1  
undo ipsec policy  
q  
  
undo ipsec policy p1 10  
undo ipsec proposal tran

=====

R1:  
ipsec proposal tran1  
  
ike peer huawei v2  
pre-shared-key simple huawei  
remote-address 192.168.23.3  
q

ipsec policy p1 10 isakmp  
security acl 3000  
proposal tran1  
ike-peer huawei  
q

int g0/0/0  
ipsec policy p1

R3:

ipsec proposal tran1

ike peer huawei v2  
pre-shared-key simple huawei  
remote-address 192.168.12.1  
q

ipsec policy p1 10 isakmp  
security acl 3000  
proposal tran1  
ike-peer huawei  
q

int g0/0/1  
ipsec policy p1

=====

dis ike proposal  
display ipsec sa