

第十二章隧道和 VPN

12.1. 创建 Tunnel

提问 通过隧道的方式在网络中传输 IP 数据

回答

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#interface Tunnel1
```

```
Router1(config-if)#ip address 192.168.35.6 255.255.255.252
```

```
Router1(config-if)#tunnel source 172.25.1.5
```

```
Router1(config-if)#tunnel destination 172.25.1.7
```

```
Router1(config-if)#exit
```

```
Router1(config)#end
```

```
Router1#
```

```
Router5#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router5(config)#interface Tunnel3
```

```
Router5(config-if)#ip address 192.168.35.5 255.255.255.252
```

```
Router5(config-if)#tunnel source 172.25.1.7
```

```
Router5(config-if)#tunnel destination 172.25.1.5
```

```
Router5(config-if)#exit
```

```
Router5(config)#end
```

```
Router5#
```

注释 Tunnel 的配置中也可以使用 tunnel source Ethernet0 的方式来捆绑到端口。产生出来的虚拟隧道接口通常会一直 UP，即使对端关机，12.2(8)T 后引入了 keepalive 参数可以对隧道的状态进行监控，keepalive 3 2 每隔 3 秒一个 Keepalive，如果两次没收到就认为端口当掉。如果对数据包的完整性或者防

止乱序包，可以配置 `tunnel checksum`, `tunnel sequence-datagrams`，但需要注意的是 GRE 不是 TCP，数据包丢弃了不会重传。缺省情况下隧道的模式 GRE，也可以通过 `tunnel mode ipip` 命令来改变其模式。由于 GRE 是封装 IP 数据包所以不可避免地产生了 MTU 的问题，对于 TCP 连接可以使用 `ip tcp path-mtu-discovery`，但对于非 TCP 的 GRE，需要使用 `tunnel path-mtu-discovery`。在 12.2(13)T 以后引入了 `tunnel path-mtu-discovery min-mtu 500` 来定义最小的 MTU 从而保证安全

12.2. 其他协议隧道至 IP

提问 通过隧道的方式在 IP 网络中传输其他协议数据，比如 IPX

回答

```
Router1#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router1(config)#ipx routing AAAA.BBBB.0001
```

```
Router1(config)#interface Tunnel1
```

```
Router1(config-if)#ipx network AAA
```

```
Router1(config-if)#tunnel source 172.25.1.5
```

```
Router1(config-if)#tunnel destination 172.25.1.7
```

```
Router1(config-if)#exit
```

```
Router1(config)#end
```

```
Router1#
```

```
Router5#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router2(config)#ipx routing AAAA.BBBB.0002
```

```
Router5(config)#interface Tunnel3
```

```
Router5(config-if)#ipx network AAA
```

```
Router5(config-if)#tunnel source 172.25.1.7
```

```
Router5(config-if)#tunnel destination 172.25.1.5
```

```
Router5(config-if)#exit
```

```
Router5(config)#end
```

```
Router5#
```

注释 注意的是隧道模式里面只有 GRE 模式是支持 IPX 的。同时可以在隧道接口下配置多个不同的协议从而支持在隧道中封装多个协议

```
Router1(config)#interface Tunnel1
```

```
Router1(config-if)#ip address 192.168.35.6 255.255.255.252
```

```
Router1(config-if)#ipx network AAA
```

```
Router1(config-if)#tunnel source 172.25.1.5
```

```
Router1(config-if)#tunnel destination 172.25.1.7
```

```
Router1(config-if)#exit
```

```
Router1(config)#end
```

```
Router1#
```

12.3. 隧道和动态路由协议

提问 在隧道中传递路由协议

回答

怎么解决到 tunnel destination 的路由不是通过 tunnel 接口的问题，第一种方法是静态路由

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#interface Tunnel1
```

```
Router1(config-if)#ip address 192.168.35.6 255.255.255.252
```

```
Router1(config-if)#tunnel source 172.25.1.5
```

```
Router1(config-if)#tunnel destination 172.22.1.2
```

```
Router1(config-if)#exit
```

```
Router1(config)#ip route 172.22.1.2 255.255.255.255 172.25.1.1
```

```
Router1(config)#router eigrp 55
```

```
Router1(config-router)#network 192.168.35.0
```

```
Router1(config-router)#exit
```

```
Router1(config)#end
```

```
Router1#
```

第二种对 tunnel 接口采用另外的路由协议，从而排除此地址在互联的路由协议中

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#interface Tunnel1
```

```
Router1(config-if)#ip address 192.168.35.6 255.255.255.252
```

```
Router1(config-if)#tunnel source 172.25.1.5
```

```
Router1(config-if)#tunnel destination 172.22.1.2
```

```
Router1(config-if)#exit
```

```
Router1(config)#router eigrp 55
```

```
Router1(config-router)#network 172.22.0.0
```

```
Router1(config-router)#network 172.25.0.0
```

```
Router1(config-router)#end
```

```
Router1(config)#router rip
```

```
Router1(config-router)#network 192.168.35.0
```

```
Router1(config-router)#exit
```

```
Router1(config)#end
```

```
Router1#
```

第三种方法路由过滤

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#interface Tunnel1
```

```
Router1(config-if)#ip address 192.168.35.6 255.255.255.252
```

```
Router1(config-if)#tunnel source 172.25.1.5
```

```
Router1(config-if)#tunnel destination 172.22.1.2
```

```
Router1(config-if)#exit
```

```
Router11(config)#ip prefix-list TUNNELROUTES seq 10 permit 192.168.0.0/16 ge 17
```

```
Router1(config)#router eigrp 55
```

```
Router1(config-router)#network 172.22.0.0
```

```
Router1(config-router)#network 172.25.0.0
```

```
Router1(config-router)#network 192.168.35.0
```

```
Router1(config-router)#distribute-list prefix TUNNELROUTES out Tunnel1
```

```
Router1(config-router)#exit
```

```
Router1(config)#end
```

```
Router1#
```

注释 前两种很简单但是冗余性和扩展性不好，推荐第三种

12.4. 查看隧道状态

提问 查看隧道状态

回答

```
Router1#show interface Tunnel5
```

```
Router1#ping 192.168.66.6
```

```
Router1#ping 172.22.1.4
```

注释

12.5. 在 GRE 隧道中创建一个加密的路由器到路由器的 VPN

提问 通过预共享密钥的方法创建互联网连接路由器的加密 VPN

回答

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#crypto isakmp policy 10
```

```
Router1(config-isakmp)#encr aes 256
```

```
Router1(config-isakmp)#authentication pre-share
```

```
Router1(config-isakmp)#group 2
```

```
Router1(config-isakmp)#exit
```

```
Router1(config)#crypto isakmp key TUNNELKEY01 address 172.16.2.1 no-xauth
```

```
Router1(config)#crypto ipsec transform-set TUNNEL-TRANSFORM ah-sha-hmac esp-aes 256
```

```
Router1(cfg-crypto-trans)#mode transport
```

```
Router1(cfg-crypto-trans)#exit
```

```
Router1(config)#crypto map TUNNELMAP 10 ipsec-isakmp
```

% NOTE: This new crypto map will remain disabled until a peer

and a valid access list have been configured.

```
Router1(config-crypto-map)#set peer 172.16.2.1
```

```
Router1(config-crypto-map)#set transform-set TUNNEL-TRANSFORM
```

```
Router1(config-crypto-map)#match address 102
```

```
Router1(config-crypto-map)#exit
```

```
"EN-US">Router1(config)#access-list 102 permit gre host 172.16.1.1 host 172.16.2.1
```

```
Router1(config)#interface Tunnel1
```

```
Router1(config-if)#ip address 192.168.1.1 255.255.255.252

Router1(config-if)#tunnel source 172.16.1.1

Router1(config-if)#tunnel destination 172.16.2.1

Router1(config-if)#exit

Router1(config)#interface FastEthernet0/0

Router1(config-if)#ip address 172.16.1.1 255.255.255.0

Router1(config-if)#ip access-group 101 in

Router1(config-if)#crypto map TUNNELMAP

Router1(config-if)#exit

Router1(config)#access-list 101 permit gre host 172.16.2.1 host 172.16.1.1

Router1(config)#access-list 101 permit esp host 172.16.2.1 host 172.16.1.1

Router1(config)#access-list 101 permit udp host 172.16.2.1 host 172.16.1.1 eq isakmp

Router1(config)#access-list 101 permit ahp host 172.16.2.1 host 172.16.1.1

Router1(config)#access-list 101 deny ip any any log

Router1(config)#interface Loopback0

Router1(config-if)#ip address 192.168.16.1 255.255.255.0

Router1(config-if)#exit

Router1(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2

Router1(config)#ip route 192.168.15.0 255.255.255.0 192.168.1.2

Router1(config)#end

Router1#

Router2#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#crypto isakmp policy 10
```

```
Router2(config-isakmp)#encr aes 256

Router2(config-isakmp)#authentication pre-share

Router2(config-isakmp)#group 2

Router2(config-isakmp)#exit

Router2(config)#crypto isakmp key TUNNELKEY01 address 172.16.1.1

Router2(config)#crypto ipsec transform-set TUNNEL-TRANSFORM ah-sha-hmac esp-aes 256

Router2(cfg-crypto-trans)#mode transport

Router2(cfg-crypto-trans)#exit

Router2(config)#crypto map TUNNELMAP 10 ipsec-isakmp

% NOTE: This new crypto map will remain disabled until a peer

       and a valid access list have been configured.

Router2(config-crypto-map)#set peer 172.16.1.1

Router2(config-crypto-map)#set transform-set TUNNEL-TRANSFORM

Router2(config-crypto-map)#match address 102

Router2(config-crypto-map)#exit

Router2(config)#access-list 102 permit gre host 172.16.2.1 host 172.16.1.1

Router2(config)#interface Tunnel1

Router2(config-if)#ip address 192.168.1.2 255.255.255.252

Router2(config-if)#tunnel source 172.16.2.1

Router2(config-if)#tunnel destination 172.16.1.1

Router2(config-if)#exit

Router2(config)#interface FastEthernet0/0

Router2(config-if)#ip address 172.16.2.1 255.255.255.0

Router2(config-if)#ip access-group 101 in
```



```

Router2(config-if)#crypto map TUNNELMAP

Router2(config-if)#exit

Router2(config)#access-list 101 permit gre host 172.16.1.1 host 172.16.2.1

Router2(config)#access-list 101 permit esp host 172.16.1.1 host 172.16.2.1

Router2(config)#access-list 101 permit udp host 172.16.1.1 host 172.16.2.1 eq isakmp

Router2(config)#access-list 101 permit ahp host 172.16.1.1 host 172.16.2.1

Router2(config)#access-list 101 deny ip any any log

Router2(config)#interface Loopback0

Router2(config-if)#ip address 192.168.15.1 255.255.255.0

Router2(config-if)#exit

Router2(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2

Router2(config)#ip route 192.168.16.0 255.255.255.0 192.168.1.1

Router2(config)#end

Router2#

```

注释 第一步首先使用 ISAKMP 来生成合适的密钥交换策略，当双方协商 SA 参数时，先从优先级低的策略开始，使用 `show crypto isakmp policy` 来查看当前策略。然后定义初始的密钥 `crypto isakmp key`，这里可以基于 IP 地址也可以基于主机名，如果基于主机名对端要配置 `crypto isakmp identity hostname`，用 `show crypto isakmp key` 来验证。`show crypto isakmp sa` 用来查看协商的 ISAKMP SA 状态，而最后 IPSec SA 通过 `show crypto ipsec sa` 来查看。下一步是定义 IPSec 的 transform set，是定义如何处理符合的数据包，并且要定义 Ipsec 的透明模式，缺省使用隧道模式，对于 GRE 使用透明模式，GRE 隧道比传统的 IPSec 隧道好 在更简单和更灵活，比如可以传递动态路由协议等。最后使用 `crypto map` 命令整合。最后要注意的是 `crypto map` 应用于接收 GRE 数据包的接口而不是 tunnel 接口。

`show crypto engine connections active` 显示当前连接情况

12.6. 在两个路由器的 Lan 接口之间创建加密 VPN

提问 使用预共享密钥的方式创建加密 VPN 通过互联网连接的两个 LAN 接口

回答

R1

Router1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#crypto isakmp policy 10

Router1(config-isakmp)#encr aes 256

Router1(config-isakmp)#authentication pre-share

Router1(config-isakmp)#group 2

Router1(config-isakmp)#exit

Router1(config)#crypto isakmp key TUNNELKEY01 address 172.16.2.1 no-xauth

Router1(config)#crypto ipsec transform-set LAN2LAN-TRANSFORM ah-sha-hmac esp-aes 256

Router1(cfg-crypto-trans)#exit

Router1(config)#access-list 102 permit gre host 172.16.1.1 host 172.16.2.1

Router1(config)#crypto map LAN2LANMAP 10 ipsec-isakmp

% NOTE: This new crypto map will remain disabled until a peer

and a valid access list have been configured.

Router1(config-crypto-map)#set peer 172.16.2.1

Router1(config-crypto-map)#set transform-set LAN2LAN-TRANSFORM

Router1(config-crypto-map)#match address 103

Router1(config-crypto-map)#exit

Router1(config)#access-list 103 permit ip 192.168.16.0 0.0.0.255 192.168.15.0 0.0.0.255

Router1(config)#interface FastEthernet0/1

Router1(config-if)#ip address 192.168.16.1 255.255.255.0

Router1(config-if)#exit

Router1(config)#interface FastEthernet0/0

```
Router1(config-if)#ip address 172.16.1.1 255.255.255.0
```

```
Router1(config-if)#ip access-group 101 in
```

```
Router1(config-if)#crypto map LAN2LANMAP
```

```
Router1(config-if)#exit
```

```
Router1(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2
```

```
Router1(config)#access-list 101 permit esp host 172.16.2.1 host 172.16.1.1
```

```
Router1(config)#access-list 101 permit udp host 172.16.2.1 host 172.16.1.1 eq isakmp
```

```
Router1(config)#access-list 101 permit ahp host 172.16.2.1 host 172.16.1.1
```

```
Router1(config)#access-list 101 deny ip any any log
```

```
Router1(config)#end
```

```
Router1#
```

```
R2
```

```
Router2#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router2(config)#crypto isakmp policy 10
```

```
Router2(config-isakmp)#encr aes 256
```

```
Router2(config-isakmp)#authentication pre-share
```

```
Router2(config-isakmp)#group 2
```

```
Router2(config-isakmp)#exit
```

```
Router2(config)#crypto isakmp key TUNNELKEY01 address 172.16.1.1
```

```
Router2(config)#crypto ipsec transform-set LAN2LAN-TRANSFORM ah-sha-hmac esp-aes 256
```

```
Router2(cfg-crypto-trans)#exit
```

```
Router2(config)#crypto map LAN2LANMAP 10 ipsec-isakmp
```

% NOTE: This new crypto map will remain disabled until a peer

and a valid access list have been configured.

```
Router2(config-crypto-map)#set peer 172.16.1.1
```

```
Router2(config-crypto-map)#set transform-set LAN2LAN-TRANSFORM
```

```
Router2(config-crypto-map)#match address 103
```

```
Router2(config-crypto-map)#exit
```

```
Router2(config)#access-list 103 permit ip 192.168.15.0 0.0.0.255 192.168.16.0 0.0.0.255
```

```
Router2(config)#interface FastEthernet0/1
```

```
Router2(config-if)#description Internal LAN
```

```
Router2(config-if)#ip address 192.168.15.1 255.255.255.0
```

```
Router2(config-if)#exit
```

```
Router2(config)#interface FastEthernet0/0
```

```
Router2(config-if)#description Connection to Internet
```

```
Router2(config-if)#ip address 172.16.2.1 255.255.255.0
```

```
Router2(config-if)#crypto map LAN2LANMAP
```

```
Router2(config-if)#exit
```

```
Router2(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2
```

```
Router2(config)#access-list 101 permit esp host 172.16.1.1 host 172.16.2.1
```

```
Router2(config)#access-list 101 permit udp host 172.16.1.1 host 172.16.2.1 eq isakmp
```

```
Router2(config)#access-list 101 permit ahp host 172.16.1.1 host 172.16.2.1
```

```
Router2(config)#access-list 101 deny ip any any log
```

```
Router2(config)#end
```

```
Router2#
```

注释 这里跟前节区别在于 12.5 建立的是可路由的加密 VPN。前面配置了 mode transport 而这里使用了 IPSec 隧道缺省的隧道模式。在 ACL 配置上前者允许的是 GRE 的数据包，这里是内部 LAN 接口之间的数据包，所以这里两个互联是桥接，前者两个互联是路由。通常我们更喜欢路由模式多一些

12.7. 生成 RSA 密钥

提问 生成共享的 RSA 密钥用于加密或者认证

回答

先在 R1 上生成自己的 pubkey

```
Router1#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router1(config)#crypto key generate rsa
```

```
The name for the keys will be: Router1.oreilly.com
```

```
Choose the size of the key modulus in the range of 360 to 2048 for your
```

```
General Purpose Keys. Choosing a key modulus greater than 512 may take  
a few minutes.
```

```
How many bits in the modulus [512]: 1024
```

```
Generating RSA keys ...
```

```
[OK]
```

```
Router1(config)#end
```

```
Router1#show crypto key mypubkey rsa
```

```
% Key pair was generated at: 01:19:45 EST Mar 1 2003
```

```
Key name: Router1.oreilly.com
```

```
Usage: General Purpose Key
```

```
Key Data:
```

```
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00E68338

D561B2D1 7B8B75D6 7B34F6AF 1710B00B 5B6E9E8D D7183BE6 F08A6342 054EADFC

B764DF9C 4592B891 522727F2 14233B47 8F757134 24F03DB3 833C5988 312B11E9

FB6E0E20 4579C0A4 F2062353 4F1C8CE4 410EE57B 9FCEE784 DA7E3852 408E9742

2584DF56 67293F3F F76B6A96 C4D518FB 1A0114BF E2449838 BE5794E2 37020301 0001
```

% Key pair was generated at: 01:19:52 EST Mar 1 2003

Key name: Router1.oreilly.com.server

Usage: Encryption Key

Key Data:

```
307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00BD928A BD5637E6

2265621C 3AC57138 911CA27D 11F40AA1 E657EA26 6EBF654C 952A3319 D421A33C

E2ECA87E CD7E050C 8A8FE64D B73954EA BF2ED639 BC6A8F74 5B9550EA 4119E796

IT">A97430E2 4B1BF7D3 ED1469FF AEA83690 A0FEA871 BBFBEB8AD 19020301 0001
```

Router1#

然后拷贝粘贴到对端路由器

Router2#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#crypto key pubkey-chain rsa

Router2(config-pubkey-chain)#addressed-key 192.168.99.1

Router2(config-pubkey-key)#address 192.168.99.1

Router2(config-pubkey-key)#key-string

Enter a public key as a hexadecimal number

Router2(config-pubkey)#30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00E68338

```
Router2(config-pubkey)#D561B2D1 7B8B75D6 7B34F6AF 1710B00B 5B6E9E8D D7183BE6 F08A6342 054EADFC
```

```
Router2(config-pubkey)#B764DF9C 4592B891 522727F2 14233B47 8F757134 24F03DB3 833C5988 312B11E9
```

```
Router2(config-pubkey)#FB6E0E20 4579C0A4 F2062353 4F1C8CE4 410EE57B 9FCEE784 DA7E3852 408E9742
```

```
Router2(config-pubkey)#2584DF56 67293F3F F76B6A96 C4D518FB 1A0114BF E2449838 BE5794E2 37020301  
0001
```

```
Router2(config-pubkey)#quit
```

```
Router2(config-pubkey-key)#exit
```

```
Router2(config-pubkey-chain)#exit
```

```
Router2(config)#end
```

```
Router2#show crypto key pubkey-chain rsa address 192.168.99.1
```

```
Key address: 192.168.99.1
```

```
Usage: General Purpose Keyass="MsoNormal"> Source: Manually entered
```

```
Data:
```

```
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00E68338
```

```
D561B2D1 7B8B75D6 7B34F6AF 1710B00B 5B6E9E8D D7183BE6 F08A6342 054EADFC
```

```
B764DF9C 4592B891 522727F2 14233B47 8F757134 24F03DB3 833C5988 312B11E9
```

```
FB6E0E20 4579C0A4 F2062353 4F1C8CE4 410EE57B 9FCEE784 DA7E3852 408E9742
```

```
2584DF56 67293F3F F76B6A96 C4D518FB 1A0114BF E2449838 BE5794E2 37020301 0001
```

```
Router2#
```

注释 由于密匙里面包含路由器名和域名，所以必须首先配置

```
Router1(config)#hostname Router1
```

```
Router1(config)#ip domain-name oreilly.com
```

如果修改上面配置则密钥无效。通过命令 `crypto key zeroize rsa` 来删除当前密钥

12.8. 使用 RSA 密钥创建路由器到路由器的 VPN

提问 利用 RSA 密钥创建一个加密的 VPN

回答

R1

```
Router1#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router1(config)#crypto key pubkey-chain rsa
```

```
Router1(config-pubkey-chain)#addressed-key 172.16.2.1
```

```
Router1(config-pubkey-key)#address 172.16.2.1
```

```
Router1(config-pubkey-key)#key-string
```

```
Enter a public key as a hexadecimal number ....
```

```
Router1(config-pubkey)#30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00EB0AB2
```

```
Router1(config-pubkey)#EA33B519 0CD95EFF EDFD4723 BED73640 97981CC0 1FC83FBF 5C6DF97C 8CB8CE0A
```

```
Router1(config-pubkey)#C5FE959D 1E055002 83B92EF4 35B69545 C3217E5F E0C32A73 44FD2373 15979E77
```

```
Router1(config-pubkey)#75598BE0 B4A4E7B2 3C318C2D 3BF3B192 8B71D8C9 A1E0F929 0E84BDAD EC909833
```

```
Router1(config-pubkey)#BC425170 400BD26A 319E632F 4E9649F5 BA7ADA40 5A94B09C 05F8414E 33020301  
0001
```

```
Router1(config-pubkey)#quit
```

```
Router1(config-pubkey-key)#exit
```

```
Router1(config-pubkey-chain)#exit
```

```
Router1(config)#crypto isakmp policy 100
```

```
Router1(config-isakmp)#encryption aes 256
```



```
Router1(config-isakmp)#authentication rsa-encl

Router1(config-isakmp)#group 2

Router1(config-isakmp)#exit

Router1(config)#crypto ipsec transform-set TUNNEL-TRANSFORM ah-sha-hmac esp-aes 256

Router1(cfg-crypto-trans)#mode transport

Router1(cfg-crypto-trans)#exit

Router1(config)#crypto map TUNNEL-RSA 10 ipsec-isakmp

% NOTE: This new crypto map will remain disabled until a peer

        and a valid access list have been configured.

Router1(config-crypto-map)#set peer 172.16.2.1

Router1(config-crypto-map)#set transform-set TUNNEL-TRANSFORM

Router1(config-crypto-map)#match address 102

Router1(config-crypto-map)#exit

Router1(config)#access-list 102 permit gre host 172.16.1.1 host 172.16.2.1

Router1(config)#interface Tunnel1

Router1(config-if)#ip address 192.168.1.1 255.255.255.252

Router1(config-if)#tunnel source 172.16.1.1

Router1(config-if)#tunnel destination 172.16.2.1

Router1(config-if)#exit

Router1(config)#interface FastEthernet0/0

Router1(config-if)#ip address 172.16.1.1 255.255.255.0

Router1(config-if)#ip access-group 101 in

Router1(config-if)#crypto map TUNNEL-RSA

Router1(config-if)#exit
```

```
Router1(config)#access-list 101 permit gre host 172.16.2.1 host 172.16.1.1
```

```
Router1(config)#access-list 101 permit esp host 172.16.2.1 host 172.16.1.1
```

```
Router1(config)#access-list 101 permit udp host 172.16.2.1 host 172.16.1.1 eq isakmp
```

```
Router1(config)#access-list 101 permit ahp host 172.16.2.1 host 172.16.1.1
```

```
Router1(config)#access-list 101 deny ip any any log
```

```
Router1(config)#end
```

```
Router1#
```

```
R2
```

```
Router2#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router2(config)#crypto key pubkey-chain rsa
```

```
Router2(config-pubkey-chain)#addressed-key 172.16.1.1
```

```
Router2(config-pubkey-key)#address 172.16.1.1
```

```
Router2(config-pubkey-key)#key-string
```

```
-US~>Enter a public key as a hexadecimal number ....
```

```
Router2(config-pubkey)#30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00A0830E
```

```
Router2(config-pubkey)#01E4B6E1 08823E41 8A98A7F4 DB0E6277 1E7AA500 F7B620CA 49BCBEBA B0A0455A
```

```
Router2(config-pubkey)#114BA6B9 5ADE0D2E 7DC3EFC1 D7D07015 01C83E08 7305ED3C 71F04B44 31A1C574
```

```
Router2(config-pubkey)#C0E6ACA2 C191DB07 3D347F88 2D2884BF 99C2AF80 45BC1BE9 6D2BF684 B60C04E6
```

```
Router2(config-pubkey)#0F3D5C09 7C26694F 8FB75F90 2FA1DF46 94401D54 82ACA366 E621DD04 4B020301  
0001
```

```
Router2(config-pubkey)#quit
```

```
Router2(config-pubkey-key)#exit
```

```
Router2(config-pubkey-chain)#exit

Router2(config)#crypto isakmp policy 100

Router2(config-isakmp)#encryption aes 256

Router2(config-isakmp)#authentication rsa-encr

Router2(config-isakmp)#group 2

Router2(config-isakmp)#exit

Router2(config)#crypto ipsec transform-set TUNNEL-TRANSFORM ah-sha-hmac esp-aes 256

Router2(cfg-crypto-trans)#mode transport

Router2(cfg-crypto-trans)#exit

Router2(config)#crypto map TUNNEL-RSA 10 ipsec-isakmp

Router2(config-crypto-map)#set peer 172.16.1.1

Router2(config-crypto-map)#set transform-set TUNNEL-TRANSFORM

Router2(config-crypto-map)#match address 102

Router2(config-crypto-map)#exit

Router2(config)#access-list 102 permit gre host 172.16.2.1 host 172.16.1.1

Router2(config)#interface Tunnel1

Router2(config-if)#ip address 192.168.1.2 255.255.255.252

Router2(config-if)#tunnel source 172.16.2.1

Router2(config-if)#tunnel destination 172.16.1.1

Router2(config-if)#exit

Router2(config)#interface FastEthernet0/0

Router2(config-if)#ip address 172.16.1.1 255.255.255.0

Router2(config-if)#ip access-group 101 in

Router2(config-if)#crypto map TUNNEL-RSA
```

```
Router2(config-if)#exit
```

```
Router2(config)#access-list 101 permit gre host 172.16.1.1 host 172.16.2.1
```

```
Router2(config)#access-list 101 permit esp host 172.16.1.1 host 172.16.2.1
```

```
Router2(config)#access-list 101 permit udp host 172.16.1.1 host 172.16.2.1 eq isakmp
```

```
Router2(config)#access-list 101 permit ahp host 172.16.1.1 host 172.16.2.1
```

```
Router2(config)#access-list 101 deny ip any any log
```

```
Router2(config)#end
```

```
Router2#
```

注释 类似 12.3 和 12.6

12.9. 创建主机到路由器的 VPN

提问 从远端主机到路由器的 VPN 连接

回答

只有路由器的配置，没有主机上软件的配置

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#aaa new-model
```

```
Router1(config)#aaa authentication login default group tacacs+
```

```
Router1(config)#aaa authentication enable default group tacacs+
```

```
Router1(config)#tacacs-server host 172.25.1.1
```

```
Router1(config)#tacacs-server key NEOSHI
```

```
Router1(config)#crypto isakmp policy 10
```

```
Router1(config-isakmp)#encryption 3des
```

```
Router1(config-isakmp)#authentication pre-share
```

```
Router1(config-isakmp)#group 2
```

```

Router1(config-isakmp)#exit

Router1(config)#crypto ipsec transform-set VPN-TRANSFORMS ah-sha-hmac esp-sha-hmac esp-3des

Router1(cfg-crypto-trans)#mode tunnel

Router1(cfg-crypto-trans)#exit

Router1(config)#crypto dynamic-map VPN-USER-MAP 50

Router1(config-crypto-map)#description A dynamic crypto map for VPN users

Router1(config-crypto-map)#match address 115

Router1(config-crypto-map)#set transform-set VPN-TRANSFORMS

Router1(config-crypto-map)#exit

Router1(config)#access-list 115 deny any 224.0.0.0 35.255.255.255

Router1(config)#access-list 115 deny any 172.25.1.255 0.0.0.0

Router1(config)#access-list 115 permit any any

Router1(config)#crypto map CRYPTOMAP 10 ipsec-isakmp dynamic
>VPN-USER-MAP

Router1(config)#interface FastEthernet0/1

Router1(config-if)#ip address 172.25.1.5 255.255.255.0

Router1(config-if)#crypto map CRYPTOMAP

Router1(config-if)#exit

Router1(config)#exit

Router1#

```

注释 由于主机可能来自任意地址所以这里使用过了 dynamic crypto maps

12.10. 创建 SSL VPN

提问 使用路由器的 WebVPN 服务来创建 SSL VPN

回答

Core#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Core(config)#hostname Core

Core(config)#ip domain-name oreilly.com

Core(config)#aaa new-model

Core(config)#aaa authentication login local_auth local

Core(config)#username ijbrown secret ianspassword

Core(config)#username kdooley secret kevinspassword

Core(config)#crypto pki trustpoint WEBVPN

Core(ca-trustpoint)#enrollment selfsigned

Core(ca-trustpoint)#rsa-keypair WEBVPN 1024

Core(ca-trustpoint)#subject-name CN=WEBVPN OU=cookbooks O=oreilly

Core(ca-trustpoint)#exit

Core(config)#crypto pki enroll WEBVPN

The router has already generated a Self Signed Certificate for

trustpoint TP-self-signed-3299111097.

If you continue the existing trustpoint and Self Signed Certificate

will be deleted.

Do you want to continue generating a new Self Signed Certificate? [yes/no]:yes

% Include the router serial number in the subject name? [yes/no]: no

% Include an IP address in the subject name? [no]: no

Generate Self Signed Router Certificate? [yes/no]: yes

Router Self Signed Certificate successfully created

```
Core(config)#interface Loopback0
```

```
Core(config-if)#ip address 172.25.100.2 255.255.255.255
```

```
Core(config-if)#exit
```

```
Core(config)#webvpn enable gateway-addr 172.25.100.2
```

```
Core(config)# Core(config)#webvpn
```

```
Core(config-webvpn)#ssl trustpoint WEBVPN
```

```
Core(config-webvpn)#ssl encryption 3des-sha1
```

```
Core(config-webvpn)#title "Cisco Cookbook WebVPN Portal"
```

```
Core(config-webvpn)#url-list COOKBOOKURLS
```

```
Core(config-webvpn-url)#heading "Cookbook URLs"
```

```
Core(config-webvpn-url)#url-text "Cisco Cookbook" url-value  
"http://www.oreilly.com/catalog/ciscockbk/"
```

```
Core(config-webvpn-url)#url-text "Perl Cookbook" url-value  
"http://www.oreilly.com/catalog/perlckbk2/"
```

```
Core(config-webvpn-url)#heading "Cisco URLs"
```

```
Core(config-webvpn-url)#url-text "The Books" url-value  
"http://www.oreilly.com/pub/topic/cisco"
```

```
Core(config-webvpn-url)#exit
```

```
Core(config-webvpn)#port-forward list SERVERLOGIN local-port 20003 remote-server 172.25.1.1  
remote-port 23
```

```
Core(config-webvpn)#exit
```

```
Core(config)#end
```

```
Core#
```

注释 12.3(14)T 引入了 WebVPN 服务，但是只能在特定的平台上，只能支持 SSLv3，不支持 TLS，不支持思科 SSL VPN 客户端软件。附带说一下最后的 port forward 配置，当用户连接上 WebVPN 后，使用 telnet 到本地的 20003 端口就会转发至 172.25.1.1 的 23 端口

<!--[if !supportLists]-->12.11. <!--[endif]-->查看 IPSec 协议状态

提问 查看 VPN 状态

回答

显示 ISAKMP security associations.

```
Router1#show crypto isakmp sa
```

IPSec security associations

```
Router1#show crypto ipsec sa
```

查看活动的 IPSec 连接

```
Router1#show crypto engine connections active
```

S">

```
Router1#show crypto engine connections dropped-packet
```

查看配置的 IPSec crypto maps

```
Router1#show crypto map
```

对于 dynamic crypto maps

```
Router1#show crypto dynamic-map
```