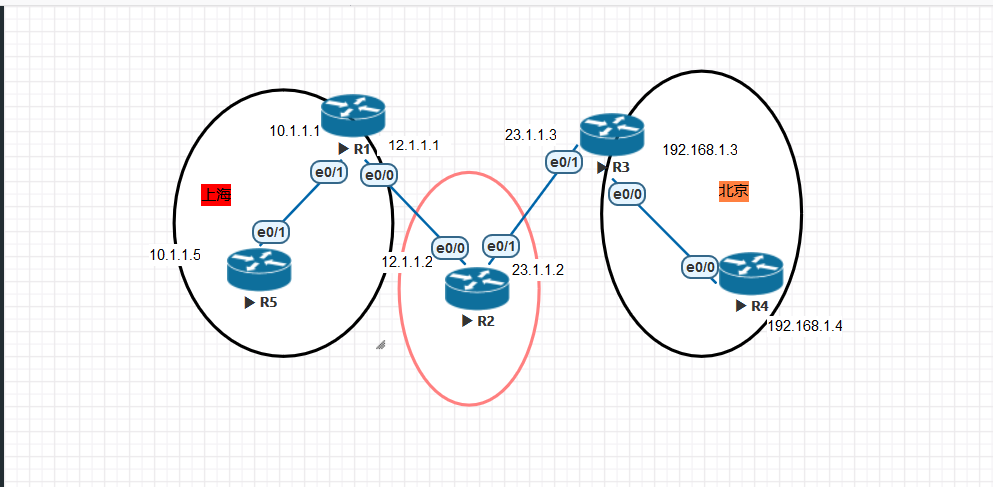
**IPSec配置实例（实验题需要导入到eve-ng模拟器）**

**拓扑图：**

**·**

1. **IP地址配置：**

**R1路由器上的配置：**

**Router(config)#int e0/1**

**Router(config-if)#ip add 10.1.1.1 255.255.255.0**

**Router(config-if)#no shut**

**Router(config-if)#int e0/0**

**Router(config-if)#ip address 12.1.1.1 255.255.255.0**

**Router(config-if)#no shut**

**Router(config-if)#**

**Router(config)#ip route 0.0.0.0 0.0.0.0 12.1.1.2**

**R2配置：**

**Router(config)#int e0/0**

**Router(config-if)#ip address 12.1.1.2 255.255.255.0**

**Router(config-if)#no shut**

**Router(config-if)#int e0/1**

**Router(config-if)#ip add 23.1.1.2 255.255.255.0**

**Router(config-if)#no shut**

**R3配置：**

**Router(config)#int e0/1**

**Router(config-if)#ip add 23.1.1.3 255.255.255.0**

**Router(config-if)#no shut**

**Router(config-if)#int e0/0**

**Router(config-if)#ip address 192.168.1.3 255.255.255.0**

**Router(config-if)#no shut**

**Router(config)#ip route 0.0.0.0 0.0.0.0 23.1.1.2**

**R4的配置：**

**Router(config)#int e0/0**

**Router(config-if)#ip address 192.168.1.4 255.255.255.0**

**Router(config-if)#no shut**

**Router(config-if)#exit**

**Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.3**

**Router(config)#**

**R5的配置：**

**Router(config)#int e0/0**

**Router(config-if)#ip address 192.168.1.4 255.255.255.0**

**Router(config-if)#no shut**

**Ethernet0/0, changed state to up**

**Router(config-if)#do write**

**Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.3**

**测试：**

**Router(config)#do ping 192.168.1.4**

**Type escape sequence to abort.**

**Sending 5, 100-byte ICMP Echos to 192.168.1.4, timeout is 2 seconds:**

**.....**

**Success rate is 0 percent (0/5)**

**Router(config)#end**

**Router#**

**\*Jun 25 13:12:25.001: %SYS-5-CONFIG\_I: Configured from console by console**

**Router#ping 23.1.1.3**

**Type escape sequence to abort.**

**Sending 5, 100-byte ICMP Echos to 23.1.1.3, timeout is 2 seconds:**

**!!!!!**

**Success rate is 100 percent (5/5), round-trip min/avg/max = 1/14/39 ms**

**Router#ping 192.168.1.4**

**Type escape sequence to abort.**

**Sending 5, 100-byte ICMP Echos to 192.168.1.4, timeout is 2 seconds:**

**U.U.U**

**Success rate is 0 percent (0/5)**

1. **配置IPSec vpn**

**R1路由器的配置**

**Router(config)#crypto isakmp policy 1**

**Router(config-isakmp)#encryption 3des**

**Router(config-isakmp)#hash sha**

**Router(config-isakmp)#authentication pre-share**

**Router(config-isakmp)#group 2**

**Router(config-isakmp)#exit**

**Router(config)#crypto isakmp key 0 cisco123 address 23.1.1.3**

**Router(config)#crypto ipsec transform-set ccie esp-3des esp-sha-hmac**

**Router(cfg-crypto-trans)#exit**

**Router(config)#access-list 100 permit ip 10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.255**

**Router(config)#crypto map |2| 1 ipsec-isakmp**

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

**and a valid access list have been configured**

**Router(config-crypto-map)#set peer 23.1.1.3**

**Router(config-crypto-map)#set transform-set ccie**

**Router(config-crypto-map)#match address 100**

**Router(config-crypto-map)#int e0/0**

**Router(config-if)#crypto map |2|**

**Router(config-if)#**

**\*Jun 25 13:17:50.311: %CRYPTO-6-ISAKMP\_ON\_OFF: ISAKMP is ON**

**Router(config-if)#exit**

**R3路由器的配置：**

**Router(config)#crypto isakmp policy 1**

**Router(config-isakmp)#encryption 3des**

**Router(config-isakmp)#hash sha**

**Router(config-isakmp)#authentication pre-share**

**Router(config-isakmp)#group 2**

**Router(config-isakmp)#exit**

**Router(config)#crypto isakmp key 0 cisco123 address 12.1.1.1**

**Router(config)#crypto ipsec transform-set ccie esp-3des esp-sha-hmac**

**Router(cfg-crypto-trans)#exit**

**Router(config)# access-list 100 permit ip 192.168.1.0 0.0.0.255 10.1.1.0 0.0.0.255**

**Router(config)#crypto map |2| 1 ipsec-isakmp**

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

**and a valid access list have been configured.**

**Router(config-crypto-map)#set peer 12.1.1.1**

**Router(config-crypto-map)#set transform-set ccie**

**Router(config-crypto-map)#match address 100**

**Router(config-crypto-map)#exit**

**Router(config)#int e0/1**

**Router(config-if)#crypto map |2|**

**Router(config-if)#**

**\*Jun 25 13:23:36.340: %CRYPTO-6-ISAKMP\_ON\_OFF: ISAKMP is ON**

**测试VPN：**

**（1）在R1上查看IKE（isakmp）策略：**

Global IKE policy  
Protection suite of priority 1  
encryption algorithm: Three key triple DES  
hash algorithm: Secure Hash Standard  
authentication method: Pre-Shared Key  
Diffie-Hellman group: #2 (1024 bit)  
lifetime: 86400 seconds, no volume limit  
Default protection suite  
encryption algorithm: DES - Data Encryption Standard (56 bit keys).  
hash algorithm: Secure Hash Standard  
authentication method: Rivest-Shamir-Adleman Signature  
Diffie-Hellman group: #1 (768 bit)  
lifetime: 86400 seconds, no volume limit  
r1#  
说明： 上面列出了 IKE（ISAKMP）策略中默认的加密算法（Encryption）， Hash 算  
法（HMAC），密钥算法（Diffie-Hellman），认证方式（Authentication），以及我们配  
置的参数。

**（ 2）查看 Phase One 时的认证密码：**  
r1#show crypto isakmp key  
Keyring Hostname/Address Preshared Key  
default 23.1.1.3 cisco123  
r1#  
说明： 可以看出我们配置的与 peer 23.1.1.3 之间的认证密码是 csico123。  
**（ 3）查看 IKE SA（ ISAKMP SA）：**  
r1#show crypto isakmp sa  
IPv4 Crypto ISAKMP SA  
dst src state conn-id slot status  
IPv6 Crypto ISAKMP SA  
r1#  
说明： 虽然在 R1 与 R3 之间已经配置足够的 VPN 命令，但 IKE SA 仍然没有建立，  
这是因为，在没有用户流量的传输来初始化的情况下， IKE SA 通常是无法自动建立  
的。  
**（ 4）查看 R1 上 IKE SA 的 peer：**  
r1#show crypto isakmp peers  
r1#  
r1#  
说明： 可以看见目前没有任何 IKE SA peer。  
**（ 5）查看 R1 上的 IPsec Transform:**r1#show crypto ipsec transform-set  
Transform set ccie: { esp-3des esp-sha-hmac }  
will negotiate = { Tunnel, },  
r1#  
说明： IPsec Transform 显示了数据封装使用 esp 加 3des 加密，并且使用 esp 结合  
sha 做 hash 计算，默认配置时没有指定 IPsec mode，所以默认的 mode 和预期一样  
是 tunnel。  
**（ 6）查看 R1 上的 IPsec SA：**  
r1#show crypto ipsec sa  
interface: FastEthernet0/0  
Crypto map tag: l2l, local addr 12.1.1.1  
protected vrf: (none)  
local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)  
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)  
current\_peer 23.1.1.3 port 500  
PERMIT, flags={origin\_is\_acl,}  
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0  
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0  
#pkts compressed: 0, #pkts decompressed: 0  
#pkts not compressed: 0, #pkts compr. failed: 0  
#pkts not decompressed: 0, #pkts decompress failed: 0  
#send errors 0, #recv errors 0  
local crypto endpt.: 12.1.1.1, remote crypto endpt.: 23.1.1.3  
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0  
current outbound spi: 0x0(0)  
inbound esp sas:  
inbound ah sas:  
inbound pcp sas:  
outbound esp sas:  
outbound ah sas:  
outbound pcp sas:  
r1#  
说明： 可以看见当前 R1 上 IPsec SA 的信息，但目前的 SA 并非活动状态，并且 SA  
显示了正确的数据信息，即从本地 10.1.1.0/24 发往 192.168.1.0/24 的。  
**（ 7）查看 R1 上的 IPsec SA 的 Lifetime：**  
r1#show crypto ipsec security-association  
Security association lifetime: 4608000 kilobytes/3600 seconds  
r1#  
说明： 默认的 IPsec SA 的 Lifetime 为 3600 seconds，即 1 小时；默认 volume limit  
为 4,608,000 Kbytes，即 4.608 Gbyte。  
**（ 8）查看 R1 上的 crypto map：**  
r1#show crypto map  
Crypto Map "l2l" 1 ipsec-isakmp  
Peer = 23.1.1.3  
Extended IP access list 100  
access-list 100 permit ip 10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.255  
Current peer: 23.1.1.3  
Security association lifetime: 4608000 kilobytes/3600 seconds  
PFS (Y/N): N  
Transform sets={  
ccie,  
}  
Interfaces using crypto map l2l:  
FastEthernet0/0  
r1#  
说明： crypto map 显示了指定加密数据发往的对端为 23.1.1.3，即和 23.1.1.3 建  
立 IPsec 隧道，调用的 IPsec transform 为 ccie，并且指定 ACL 100 中的流量为被保护  
的流量。  
**（ 9）从上海公司 R5 向北京公司 R4 发送流量：**  
r5#ping 192.168.1.4  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.1.4, timeout is 2 seconds:  
.!!!!  
Success rate is 80 percent (4/5), round-trip min/avg/max = 64/125/212 ms  
r5#  
说明： 上海公司R5 向北京公司 R4 发送的 5 个数据包，有 4 个成功穿越了 Internet，  
说明该流量激活了 IKE SA，并且在双方应该成功建立了 IPsec 隧道，所以才实现了  
VPN 的功能。

**（ 10）再次查看 R1 上 IKE SA 的 peer：**  
r1#show crypto isakmp peers  
Peer: 23.1.1.3 Port: 500 Local: 12.1.1.1  
Phase1 id: 23.1.1.3  
r1#  
说明： R1 已经成功与 R3 建立 IKE peer，说明 IKE SA 也应该成功建立， R1 本地源  
地址为 12.1.1.1，目标为 23.1.1.3，目标端口号为 500。  
（ 11）再次查看 R1 上的 IKE SA（ISAKMP SA）：  
r1#show crypto isakmp sa  
IPv4 Crypto ISAKMP SA  
dst src state conn-id slot status  
23.1.1.3 12.1.1.1 QM\_IDLE 1001 0 ACTIVE  
IPv6 Crypto ISAKMP SA  
r1#  
说明： IKE SA 已经成功建立， R1 本地源地址为 12.1.1.1，目标为 23.1.1.3，并且  
为激活状态，如为(delete)状态，则不可用。  
**（ 12）再次查看 R1 上的 IPsec SA：**  
r1#show crypto ipsec sa  
interface: FastEthernet0/0  
Crypto map tag: l2l, local addr 12.1.1.1  
protected vrf: (none)  
local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)  
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)  
current\_peer 23.1.1.3 port 500  
PERMIT, flags={origin\_is\_acl,}  
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4  
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4  
#pkts compressed: 0, #pkts decompressed: 0  
#pkts not compressed: 0, #pkts compr. failed: 0  
#pkts not decompressed: 0, #pkts decompress failed: 0  
#send errors 1, #recv errors 0  
local crypto endpt.: 12.1.1.1, remote crypto endpt.: 23.1.1.3  
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0  
current outbound spi: 0x84D01C7D(2228231293)  
inbound esp sas:  
spi: 0xEB838CF1(3951267057)  
transform: esp-3des esp-sha-hmac ,  
in use settings ={Tunnel, }  
conn id: 1, flow\_id: SW:1, crypto map: l2l  
sa timing: remaining key lifetime (k/sec): (4537199/3427)  
IV size: 8 bytes  
replay detection support: Y  
Status: ACTIVE  
inbound ah sas:  
inbound pcp sas:  
outbound esp sas:  
spi: 0x84D01C7D(2228231293)  
transform: esp-3des esp-sha-hmac ,  
in use settings ={Tunnel, }  
conn id: 2, flow\_id: SW:2, crypto map: l2l  
sa timing: remaining key lifetime (k/sec): (4537199/3425)  
IV size: 8 bytes  
replay detection support: Y  
Status: ACTIVE  
outbound ah sas:  
outbound pcp sas:  
r1#  
说明： IPsec SA 中显示了之前通了的 4 个包成功被 IPsec 加密，并且可以看出该  
SA 为 Active 状态，特别要注意的是，目前的 IPsec mode 工作在 Tunnel 模式。