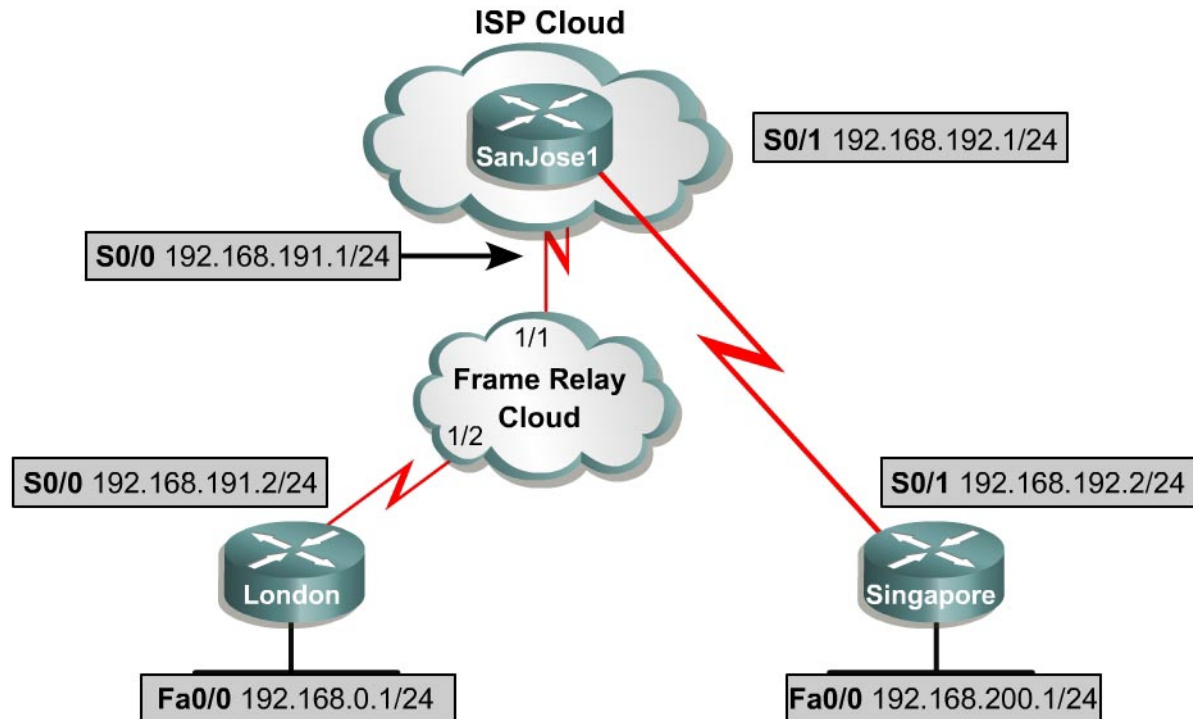


Lab 13.8.1 Configuring a Site-to-Site IPsec VPN Using Pre-Shared Keys



Objective

Plan and configure VPN connections between two sites using IKE and IPSEC.

Scenario

The International Travel Agency (ITA) has decided that communications between the London and Singapore branch offices require a method of insuring that sensitive corporate data is not being intercepted. ITA has decided to implement a site-to-site VPN solution. The solution that will be implemented will enable a site-to-site IPsec based VPN to ensure confidentiality, integrity, and authentication. In this scenario, the SanJose1 site will act as the Internet Service Provider (ISP).

Step 1

Before beginning this lab, it is recommended that each router be reloaded after erasing its startup configuration. This prevents problems that may be caused by residual configurations. Cable the network according to the diagram. This lab assumes an Adtran Atlas 550 will be used to emulate the Frame Relay cloud. Be sure to connect the serial interfaces on the router to the port as labeled in the diagram. On each router, configure their respective hostname and FastEthernet address.

On the SanJose1 router, configure the following:

```
SanJose1(config)#int s 0/0
SanJose1(config-if)#ip address 192.168.191.1 255.255.255.0
SanJose1(config-if)#encapsulation frame-relay
```

```

SanJose1(config-if)#frame-relay lmi-type ansi
SanJose1(config-if)#no shut

SanJose1(config)#int s 0/1
SanJose1(config-if)#ip address 192.168.192.1 255.255.255.0
SanJose1(config-if)#no shut
SanJose1(config-if)#exit

SanJose1(config)#ip route 192.168.0.0 255.255.255.0 192.168.191.2
SanJose1(config)#ip route 192.168.200.0 255.255.255.0 192.168.192.2

```

On the London and Singapore routers, configure their serial interfaces and default routes as follows:

```

London(config)#int s0/0
London(config-if)#ip add 192.168.191.2 255.255.255.0
London(config-if)#encapsulation frame-relay
London(config-if)#frame-relay lmi-type ansi
London(config-if)#no shut
London(config-if)#exit
London(config)#ip route 0.0.0.0 0.0.0.0 192.168.191.1

Singapore(config)#int s0/1
Singapore(config-if)#ip add 192.168.192.2 255.255.255.0
Singapore(config-if)#clock rate 56000
Singapore(config-if)#no shut
Singapore(config-if)#exit
Singapore(config)#ip route 0.0.0.0 0.0.0.0 192.168.192.1

```

Verify connectivity between the FastEthernet LANs on London and Singapore with an extended ping.

Step 2

Plan the parameters for IKE.

Parameter	Singapore Site	London Office
Key distribution method—manual or isakmp	isakmp	isakmp
Encryption algorithm— DES or 3DES	DES	DES
Hash algorithm—MD5 or SHA-1	SHA-1	SHA-1
Authentication method—Pre-share or RSA	pre-share	pre-share
Key exchange—D-H Group 1 or 2	Group 1	Group 1
IKE SA Lifetime— 86400 seconds or less	86400	86400

Note: The default values are in bold.

Enable IKE on the Singapore router. Create an IKE policy with a priority of 100 using pre-shared keys as the method of authentication. Configure a pre-shared key of **cisco1234** and use the Serial interface IP address on the London router as the peer's address.

```

Singapore(config)#crypto isakmp policy 100
Singapore(config-isakmp)#authentication pre-share
Singapore(config-isakmp)#crypto isakmp key cisco1234 address 192.168.191.2

```

A given pre-shared key is a private key shared between two peers. As a given peer, the same key could be specified to share with multiple remote peers. However, a more secure approach is to specify different keys to share between different pairs of peers.

Verify the IKE policy for the Singapore router, as follows:

```
Singapore#show crypto isakmp policy
```

The configuration output should look similar to the following:

```
Protection suite of priority 100
  encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
  hash algorithm:        Secure Hash Standard
  authentication method: Pre-Shared Key
  Diffie-Hellman group:  #1 (768 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
```

Step 3

Enable IKE on the London router. Create an IKE policy with a priority of 100 using pre-shared keys as the method of authentication. Configure a pre-shared key of **cisco1234** and use the Serial interface IP address on the Singapore router as the peer's address.

```
London(config)#crypto isakmp policy 100
London(config-isakmp)#authentication pre-share
London(config-isakmp)#crypto isakmp key cisco1234 address 192.168.192.2
```

Verify the IKE policy for the London router, as follows:

```
London#show crypto isakmp policy
```

The configuration output should look similar to Singapore's output

Step 4

Plan and configure IPSec policies on the Singapore and London routers.

Policy	Singapore	London
Transform set	esp-des	esp-des
Traffic type to be encrypted	IP	IP
SA establishment	ipsec-isakmp	ipsec-isakmp

An access list needs to be configured on each router to specify which traffic is to be encrypted. In this lab, only the LAN traffic between sites is to be protected. On the Singapore router, configure an extended access list 120 that will define this traffic going to the London router as follows:

```
Singapore(config)#access-list 120 permit ip 192.168.200.0 0.0.0.255 192.168.0.0
0.0.0.255
```

Now, configure an IPSec transform set called MYSET and specify that ESP with DES will be used.

```
Singapore(config)#crypto ipsec transform-set MYSET esp-des
```

Note: Up to three transform sets can be in a set. Sets are limited to one AH and up to two ESP transforms.

Configure an IPSec crypto map using a map name of MYMAP and a sequence number of **110**. This crypto map is to use `ipsec-isakmp`.

```
Singapore(config)#crypto map MYMAP 110 ipsec-isakmp
```

Configure the crypto map to match the access list 120, set the transform set MYSET upon the match condition, and set the peer address as the Serial Interface IP address on the London router.

```
Singapore(config-crypto-map)#match address 120
Singapore(config-crypto-map)#set transform-set MYSET
Singapore(config-crypto-map)#set peer 192.168.191.2
```

Finally, apply crypto map MYMAP to the serial interface on the Singapore router.

```
Singapore(config)#int s0/1
Singapore(config-if)#crypto map MYMAP
```

Use the `show crypto ipsec sa` command and verify the configuration settings.

```
Singapore#show crypto ipsec sa

interface: Serial0/1
  Crypto map tag: MYMAP, local addr. 192.168.192.2

  local ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.0.0/255.255.255.0/0/0)
  current_peer: 192.168.191.2
    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 decompress failed: 0
    #send errors 0, #recv errors 0

    local crypto endpt.: 192.168.192.2, remote crypto endpt.: 192.168.191.2
    path mtu 1500, media mtu 1500
    current outbound spi: 0
  <Output omitted>
```

Record the number of packets encrypted _____ and the number of packets decrypted _____

Apply the similar settings to the London router as follows:

```
London(config)#access-list 120 permit ip 192.168.0.0 0.0.0.255 192.168.200.0
0.0.0.255
London(config)#crypto ipsec transform-set MYSET esp-des
London(config)#crypto map MYMAP 110 ipsec-isakmp
London(config-crypto-map)#match address 120
```

```
London(config-crypto-map)#set transform-set MYSET
London(config-crypto-map)#set peer 192.168.192.2
```

Finally, apply crypto map MYMAP to the serial interface on the London router.

```
London(config)#int s0/0
London(config-if)#crypto map MYMAP
```

Use the **show crypto ipsec sa** command and verify the configuration settings. The output should be similar to that of the Singapore router.

Step 5

Test and verify the VPN operation. From the Singapore router enable debugging to observe the ISAKMP and IPsec negotiation and security association creation as follows:

```
Singapore#debug crypto ipsec
Crypto IPSEC debugging is on
Singapore#debug crypto isakmp
Crypto ISAKMP debugging is on
```

Since the encryption is performed between LAN interfaces, an extended ping must be used. From the Singapore router, do an extended ping to the London router LAN interface IP address from the LAN interface IP address of the Singapore router.

Was any debug information seen? _____

Now verify the security associations by using the **show crypto ipsec sa** and **show crypto isakmp sa** commands. Output should be similar to the following:

```
Singapore#show crypto ipsec sa

interface: Serial0/1
  Crypto map tag: MYMAP, local addr. 192.168.192.2

  local ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.0.0/255.255.255.0/0/0)
  current_peer: 192.168.191.2
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 0
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

  local crypto endpt.: 192.168.192.2, remote crypto endpt.: 192.168.191.2
  path mtu 1500, media mtu 1500
  current outbound spi: E1F92A37

inbound esp sas:
  spi: 0xAA42D3DF(2856506335)
    transform: esp-des ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2000, flow_id: 1, crypto map: MYMAP
    sa timing: remaining key lifetime (k/sec): (4607999/3441)
    IV size: 8 bytes
    replay detection support: N
```

Complete the following information from the **show** commands:

Packets encrypted _____ Packets decrypted _____

To observe the process again, clear the SAs by using the `clear crypto sa` and the `clear crypto isakmp` commands. Then generate interesting traffic by doing additional extended pings between routers.