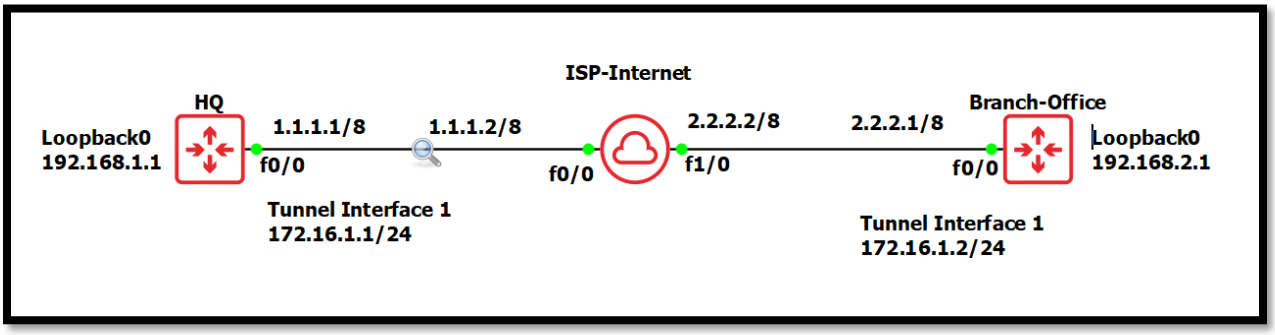

Networkforyou
Welcome
To
Network for you
IPSEC_S2S_VPN
Networkforyou

Site to Site IPSec VPN Tunnel in CISCO IOS Routers:



Step 1. Configuring IPSec Phase 1 (ISAKMP Policy):

crypto isakmp policy 5
authentication pre-share
encryption 3des
group 2
hash sha
lifetime 86400
exit
crypto isakmp key 0 cisco123 address 2.2.2.1

crypto isakmp policy 5	Creates ISAKMP policy number 5. Can create multiple policies, for example 7, 8, 9 with different configuration. Router will check list of policies one by one, if any matched, IPSec negotiation move to Phase 2
authentication pre-share	Authentication method is pre-shared key.
encryption 3DES	3DES encryption algorithm will be used for Phase 1.
group 2	Diffie-Hellman group to be used is group 2.
hash sha	SHA algorithm will be used.
lifetime 86400	Phase 1 lifetime is 86400 seconds which is 1 day.
crypto isakmp key cisco123 address 2.2.2.1	The Phase 1 password is cisco123 and remote peer IP address is 2.2.2.1

Step 2. Configuring IPSec Phase 2 (Transform Set):

crypto ipsec transform-set TSET esp-aes 128 esp-md5-hmac
exit
crypto ipsec security-association lifetime seconds 3600

crypto ipsec transform-set TSET	Creates transform-set called TSET
esp-aes	AES 128-bit encryption method and ESP IPSec protocol will be used.
esp-md5-hmac	MD5 hashing algorithm will be used.
crypto ipsec security-association lifetime seconds 3600	This is the amount to time that the phase 2 sessions exists before re-negotiation.

Step 3. Configuring ACL for Interesting Traffic:

ip access-list extended VPN-TRAFFIC
permit ip host 192.168.1.1 host 192.168.2.1

ACL defines interesting traffic that needs to go through the VPN tunnel. Traffic originating from 192.168.1.1 host to 192.168.2.1. host will go via VPN tunnel.

Step 4. Configure Crypto Map:

Crypto Map ties together & connect above defined ISAKMP and IPSec configuration together

crypto map CMAP 10 ipsec-isakmp
match address **VPN-TRAFFIC**
set peer 2.2.2.1
set transform-set TSET

crypto map CMAP 10 ipsec-isakmp	Creates new crypto map with sequence number 10. Can create more sequence numbers with same crypto map name if you

	have multiple sites.
match address VPN-TRAFFIC	Its matches interesting traffic from ACL named VPN-TRAFFIC.
set peer 2.2.2.1	This is public IP address of BO.
set transform-set TSET	This links the transform-set in this crypto map configuration.

Step 5. Apply Crypto Map to Outgoing Interface of HQ:

The final step is to apply the crypto map to the outgoing interface of the router (HQ). Here, the outgoing interface is FastEthernet 0/0. You can have multiple crypto maps defined in the configuration of a router, but you can only have one applied to an interface at once time. If you have a router that needs to connect to multiple peers from the same interface, the peers will need to be defined in the single crypto map. You would can another numbered entry to the crypto map with different transform-sets and match ACLs. Site 1 configuration is Completed.

int fa0/0

crypto map CMAP

Site-2, BO Configuration:

Move to the Site-2 Router to complete the VPN configuration. The settings for BO are identical, with the only difference being the peer IP Addresses and Access Lists:

Step 1. Configuring IPSec Phase 1 (ISAKMP Policy):
config t crypto isakmp policy 5 authentication pre-share encryption 3des group 2 hash sha lifetime 86400 exit crypto isakmp key 0 cisco123 address **1.1.1.1**

Step 2. Configuring IPSec Phase 2 (Transform Set):
crypto ipsec transform-set TSET esp-aes 128 esp-md5-hmac crypto ipsec security-association lifetime seconds 3600

Step 3. Configuring ACL for Interesting Traffic:
ip access-list extended VPN-TRAFFIC permit ip host **192.168.2.1** host **192.168.1.1**

Step 4. Configure Crypto Map:
crypto map CMAP 10 ipsec-isakmp match address VPN-TRAFFIC set peer **1.1.1.1** set transform-set TSET

Step 5. Apply Crypto Map to outgoing interface of BO:
int fa0/0 crypto map CMAP exit

Note: Red color need to change in BO router.