SITE-T0-SITE VPN CONFIGURATION

Configuring VPN (Virtual Private Network) with ISP network. The purpose of a VPN is to create protect or create high security to a network traffic. VPN helps encrypt information and all traffic on a network for it to be safe from attackers or whoever is trying to monitor the network. It is a modern day security technology required by most organization for the security of their networks.

This will be done in a LAB of connecting two offices together, head office and branch office, the purpose is for both to be able to communicate or share data or information through network protocols through routing traffics between the branches with an encryptions with the use of VPN and it will also encrypt over a public IP.

The LAB will be done by placing 2811 Cisco router and 2960 Cisco switch in each office. The routers will serve as a DHCP server and will connect both office together and each router in the office will be connected to the switch to provide network to all LAN devices from the router, VPN will be configured to secure all traffics passing through both branches. The project will be done using Cisco Packet Tracer.

Please have in mind that this is a practical Lab, in real world to connect the 2 branches together the organization will have to lay a fiber optic cable or use a fixed wireless internet (fixed wireless transmit signal through the air from a nearby tower which means they provide a cable free connection.

Starting the configuration: (HQ-Router)

```
# en

# conf t

# hostname HQ-Router

# int f0/0

# ip add 197.149.90.1 255.255.255.0

# no shutdown

# int f0/1

# ip add 192.168.4.1 255.255.255.0
```

no shutdown

end

wr

(BO-Router)

en

conf t

hostname BO-Router

int f0/0

ip add 197.149.90.2 255.255.255.0

no shutdown

int f0/1

ip add 192.168.5.1 255.255.255.0

no shutdown

end

wr

Configuration DHCP (HQ-Router)

en

conf t

ip dhcp pool HQ-Router

network 192.168.4.0 255.255.255.0

default-router 192.168.4.1

dns-server 192.168.4.1

end

wr

Configuration DHCP (BO-Router)

en

conf t

ip dhcp pool HQ-Router

network 192.168.5.0 255.255.255.0

default-router 192.168.5.1

dns-server 192.168.5.1

end

wr

Configuration IP routing (HQ-Router)

en

conf t

router ospf 100

router-id 0.0.0.1

network 192.168.4.0 0.0.0.255 area 0

network 197.149.90.0 0.0.0.255 area 0

end

wr

Configuration IP routing (BO-Router)

en

conf t

router ospf 100

router-id 0.0.0.2

network 192.168.5.0 0.0.0.255 area 0

network 197.149.90.0 0.0.0.255 area 0

end

wr

Configuration VPN (HQ-Router)

en

conf t

crypto isakmp enable

crypto isakmp policy 1

encr aes 128

hash sha

authentication pre-share

group 2

lifetime 86400

exit

crypto isakmp key cisco123 address 197.149.90.2

crypto ipsec transform-set TS esp-aes 128 esp-sha-hmac

ip route 192.168.5.0 255.255.255.0 197.149.90.2

ip access-list extended VPN-TRAFFIC

permit ip 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255

crypto map CMAP 10 ipsec-isakmp

set peer 197.149.90.2

set transform-set TS

match address VPN-TRAFFIC

interface FastEthernet0/1

crypto map CMAP

end

wr

Configuration VPN (BO-Router)

en

conf t

crypto isakmp enable

crypto isakmp policy 1

encr aes 128

hash sha

authentication pre-share

group 2

lifetime 86400

exit

crypto isakmp key cisco123 address 197.149.90.1

crypto ipsec transform-set TS esp-aes 128 esp-sha-hmac

ip route 192.168.4.0 255.255.255.0 197.149.90.1

ip access-list extended VPN-TRAFFIC

permit ip 192.168.5.0 0.0.0.255 192.168.4.0 0.0.0.255

crypto map CMAP 10 ipsec-isakmp

set peer 197.149.90.1

set transform-set TS

match address VPN-TRAFFIC

interface FastEthernet0/1

crypto map CMAP

end

wr

TO Check VPN Status

show crypto isakmp sa

show crypto ipsec sa

That is the end of the configuration

You have to put all device to auto get IP in order for DHCP server to assign IP to them all. Ping from each devices to see if they will communication with each other as it is important to check if all process are working fine.

VPN create a secure connection over a public network which serves as a mask for network and protect network from exposing to bad intention individuals, VPN will mask the network location, the IP address and encrypt all traffic passing through the network.

NOTE: Port numbers in this Lab are the numbers of port we connected our cables, this can be different in your situation if you connect your cables to a different port. Therefore you have to use the port numbers during the configuration.