A site-to-site VPN connects users in different locations within an entire network.

Through this network, the users can exchange data from their own locations while that

information is encrypted and secured through the VPN. Users working in separate offices can still be connected to one another and all of their internal resources. This keeps all users connected even when they are working remotely while securing the information exchanged

between them

Many organizations have multiple physical sites, each with their own corporate local area network (LAN). While geographically separated, these multiple sites need a single corporate WAN to support secure cross-site communication.

A site-to-site Virtual Private Network (VPN) provides this by creating an encrypted link between VPN gateways located at each of these sites. A site-to-site VPN tunnel encrypts traffic at one end and sends it to the other site over the public Internet where it is decrypted and routed on to its destination.

Benefits of Site-to-Site VPN

Site-to-site VPNs are in use by many organizations. The reason for this is that they provide a number of benefits to enterprises and their employees, such as:

Secure Connectivity: All traffic flowing over a site-to-site VPN is encrypted. This means that any business data crossing over the public Internet is encrypted, protecting it against eavesdropping and modification.

Simplified Network Architecture

Access Control: Some network resources are intended to only be accessible internally, meaning that employees at other sites should have access but not external users. Since site-to-site VPN users are “internal” users, access control rules are simpler to define because any traffic not originating from inside the network or entering via VPN tunnels can be blocked from accessing these resources.

Connect all devices and assign IP addresses as shown below

Set IP route as shown below in the ISP router

ip route 172.16.1.0 255.255.255.0 10.10.10.1

ip route 192.168.10.0 255.255.255.0 11.11.11.1

Try pinging from PC0 or PC1 to check the connection.

ping 192.168.10.10

Step 4: Configure iskamp policy and define IPsec transform set by entering the commands given below in the HQ router

crypto isakmp enable

crypto isakmp policy 20

authentication pre-share

encryption 3des

hash md5

group 1

lifetime 3600

exit

crypto isakmp key cisco123 address 11.11.11.1

crypto ipsec transform-set myset esp-3des esp-md5-hmac

: Create access list and crypto map in the HQ router CLI

access-list 100 permit ip 172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255

create crypto map for ipsec

crypto map mymap 20 ipsec-isakmp

set peer 11.11.11.1

set transform-set myset

match address 100

exit

apply crypto map to outgoing interface of VPN device

int s0/0/0

crypto map mymap

Branch routr:

ip route 0.0.0.0 0.0.0.0 11.11.11.2

crypto isakmp enable

crypto isakmp policy 20

authentication pre-share

encryption 3des

hash md5

group 1

lifetime 3600

exit

crypto isakmp key cisco123 address 10.10.10.1

crypto ipsec transform-set myset esp-3des esp-md5-hmac

access-list 100 permit ip 192.168.10.0 0.0.0.255 172.16.1.0 0.0.0.255

crypto map mymap 20 ipsec-isakmp

set peer 10.10.10.1

set transform-set myset

match address 100

exit

int s0/0/0

crypto map mymap

Verify the created isakmp policies with the following command

HQ

exit

exit

show crypto isakmp sa

show crypto isakmp policy

show crypto map

show crypto ipsec sa