Site to Site VPN

It helps to connect two different braches or remote locations. It ensure that connectivity between between two public networks and with security.

Implementaion Stages

Phase 1: Internet security association key management protocols (ISAKMP).

Phase 2: Internet protocol security. It is having ESP and AH.

Phase 3: Interesting traffic will configured by ACL.

Phase 4: Mapping (Crypto Map).

Phase 5: Apply map on interface.

Here Pre share key will be used for trust worthiness between two branches.

Encryption:

It will convert plain text into sifar text. It classified into 3 types.

1. DES-Data encryption standard
2. 3 DES
3. AES-Advanced encryption standard

Hash:

It is used for checksum. It is having two types

1. MD5-Message Digest
2. SHA-Secure hashing Algorithm

Ockley:

It is responsible to carry the message from Router 1 to Router 2.

If we are using both sites of routers are cisco vendors, then it is operated in main mode, In this 6 messages will be exchanged. For different vendors of router in both sites, It will be operated in Aggressive Mode only 3 messages exchanged.

In this VPN, we have 2 Tunnels. Those are

1. ISAKMP
2. IPSEC

ISAKMP: By using this tunnel session keys will be exchanged. Generated by the **Diffie**–**Hellman** Algorithm. ISAKMP tunnel is responsible for IPSEC tunnel up and running.

IPSEC: This tunnel is used for actual data transmission. ESP and AH are responsible for carry data in IPSEC tunnel.

Crypto Map:

It is used to identify the router the packet belongs to which network. Only one crypto map can be applied for single interface.

HMac: Hamc is used for sequence number. To also add the Tags.

VPN CONFIGUARATION:

Router-1

crypto isakmp policy 10

encr 3des

hash md5

authentication pre-share

group 2

crypto isakmp key cisco address 1.1.1.2

crypto isakmp key juniper address 1.1.1.3

!

!

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

crypto ipsec transform-set lenovo esp-aes esp-sha-hmac

!

crypto map irfan 110 ipsec-isakmp

set peer 1.1.1.2

set transform-set dell

match address 101

crypto map irfan 111 ipsec-isakmp

set peer 1.1.1.3

set transform-set lenovo

match address 102

!

!

!

!

!

interface Loopback0

ip address 10.1.1.1 255.0.0.0

!

interface FastEthernet0/0

ip address 1.1.1.1 255.0.0.0

duplex auto

speed auto

crypto map irfan

!

interface FastEthernet0/1

no ip address

shutdown

duplex auto

speed auto

!

ip route 0.0.0.0 0.0.0.0 FastEthernet0/0

!

!

no ip http server

no ip http secure-server

!

access-list 101 permit ip host 10.1.1.1 host 20.1.1.1

access-list 101 permit ip host 1.1.1.1 host 1.1.1.2

access-list 102 permit ip host 10.1.1.1 host 30.1.1.1

!

control-plane

!

!

!

line con 0

exec-timeout 0 0

privilege level 15

logging synchronous

line aux 0

exec-timeout 0 0

privilege level 15

logging synchronous

line vty 0 4

login

!

!

End

Router-2

crypto isakmp policy 10

encr 3des

hash md5

authentication pre-share

group 2

crypto isakmp key cisco address 1.1.1.1

!

!

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

!

crypto map irfan 110 ipsec-isakmp

set peer 1.1.1.1

set transform-set dell

match address 101

!

!

!

!

!

interface Loopback0

ip address 20.1.1.1 255.0.0.0

!

interface FastEthernet0/0

ip address 1.1.1.2 255.0.0.0

duplex auto

speed auto

crypto map irfan

!

interface FastEthernet0/1

no ip address

shutdown

duplex auto

speed auto

!

ip route 0.0.0.0 0.0.0.0 1.1.1.1

!

!

no ip http server

no ip http secure-server

!

access-list 101 permit ip host 20.1.1.1 host 10.1.1.1

access-list 101 permit ip host 1.1.1.2 host 1.1.1.1

!

!

control-planel!

!

line con 0

exec-timeout 0 0

privilege level 15

logging synchronous

line aux 0

exec-timeout 0 0

privilege level 15

logging synchronous

line vty 0 4

login

End

**OUTPUT**

R1#sh crypto isakmp sa

dst src state conn-id slot status

1.1.1.2 1.1.1.1 QM\_IDLE 1 0 ACTIVE

R1#sh crypto ipsec sa

interface: FastEthernet0/0

Crypto map tag: irfan, local addr 1.1.1.1

protected vrf: (none)

local ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)

remote ident (addr/mask/prot/port): (1.1.1.2/255.255.255.255/0/0)

current\_peer 1.1.1.2 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.: 1.1.1.1, remote crypto endpt.: 1.1.1.2

path mtu 1500, ip mtu 1500

current outbound spi: 0x0(0)

inbound esp sas:

inbound ah sas:

inbound pcp sas:

outbound esp sas:

outbound ah sas:

outbound pcp sas:

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.1.1/255.255.255.255/0/0)

remote ident (addr/mask/prot/port): (20.1.1.1/255.255.255.255/0/0)

current\_peer 1.1.1.2 port 500

PERMIT, flags={origin\_is\_acl,}

#pkts encaps: 14, #pkts encrypt: 14, #pkts digest: 14

#pkts decaps: 14, #pkts decrypt: 14, #pkts verify: 14

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 6, #recv errors 0

local crypto endpt.: 1.1.1.1, remote crypto endpt.: 1.1.1.2

path mtu 1500, ip mtu 1500

current outbound spi: 0x65DCEB8B(1708977035)

inbound esp sas:

spi: 0xDA81E22F(3665945135)

transform: esp-3des esp-md5-hmac ,

in use settings ={Tunnel, }

conn id: 2004, flow\_id: SW:4, crypto map: irfan

sa timing: remaining key lifetime (k/sec): (4441307/3533)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

