CONFIGURING SITE TO SITE VPN

Network Security Report:

Executive Summary:

Networking is a vast concept, in basic terms, network is the group of computers that are connected to each other and is used to share the information or communicate with each other. Local area network is the network which consists of the small number network devices may belong to specific person or organization, whereas wide area network is the group of LAN networks. Even though, network is categorized into different forms depending on the size and purpose everything can be connected to each other which forms the giant structure, which is known as 'internet' which incontrovertibly has a great impact in mankind. In my view, people unaware with internet can be counted in fingers because from the birth (hospital) to the death (cemetery), in this time everything is connected to the network. Internet of things has proved, basically every device can be connected to the network and can be controlled, monitored from a specific device, which is leading to automation, prediction, and evaluation. From these we can simply generalize that importance of network is beyond words, however on the other side, the consequence is also devastating, depending on the data and usage. A secure, redundant, scalable, that can maintain confidentiality, integrity, and accessibility triad, incidence response network can be achieved by aligning the network with secure network frameworks such as AAA and response framework like NIST. Data loss can lead to huge physical, economic, and reputational consequences; therefore, network should be maintained from the end devices to the end point router. Depending on the structure, usage and risk of an organisation, Firewalls, anti-malwares, spywares, IDS (detects the intrusion), IPS(detects and also prevents the intrusions), ACLs, VPN, ESA/WSA devices can be used for the security of the data and network devices. For example, as cisco ASA5505, ASA5506 firewalls (provides many features listed above and can be used as a router). Limiting the access and exposure of the network to the outside network is must for securing end devices and hosts, to prevent the intrusion not only from outside but also from the inside of the network.

In this report as well, I have tried to explain the procedure to configure the site-to-site VPN, in an Enterprise Organization, which helps to limit the exposure of data in the Internet protecting the Confidentiality and integrity of the data of an organization even having two sites at two ends of the world. From this report, the reader will be able to analyse the concept of the VPN, and configuration of the VPN devices. I have tried to explain the basic security practices for the basic configuration for the end devices. Overall, I have explained from the basic router configurations to the VPN set up for head and the branch office in an organization. I have also included the references for many topics if interested to learn more about those terms.

Thank you!

Table of Contents

• Introduction

Virtual Private Network (VPN) is a private network over the public network (internet). VPN uses the virtual connection routed through the internet instead of the dedicated physical network, from one site to the other. Although, the information is transported through the public network, it is encapsulated or tunnelled from one end to other end which creates private and virtual connection. The modern VPN devices use the strong encryption algorithm and strong authentication mechanisms to protect the integrity of data. VPNs saves huge cost by reducing connectivity cost and remote connection bandwidth can be increased, scalable without needing to set up new infrastructure, and compatible with variety of WAN links. VPNs connects two end devices which can be done in layer 2 and layer 3, also can be end-to-end connection such as GRE and IPsec or any-to-any connection like Multiprotocol level Switching (MPLS). However, in this report I will discuss about the layer 3 IPsec VPN.

IPsec is a secured protocol from which secure services can be achieved, which provides authentication, integrity, access control and confidentiality of information, allowing for site-to-site and remote access VPNs. Remote access VPNs are set up in the host level, which allows for dynamically changing the connection based on the locations and dynamic IP address. It can be enabled and disabled when needed. This type of VPNs is generally set up between an employee and Organization working from home, however in site-to-site VPN the VPN connection is configured in both sides gateway device, can be router, ASA firewalls, cisco VPN concentrators and found in network level, host inside the network are unaware of it. Generally, set up to connect branch and head offices.

More advance VPN technologies are also being developed and used in different purposes such as, Multiprotocol Label Switching VPN, Dynamic Multipoint VPN to interconnect a greater number of sites, and for the better costumer approach respectively etc. VPNs have features like Hairpinning (every traffic must pass from the VPN terminating device before connecting to the internet, and split Tunnelling (only the trusted traffic have to pass through VPN device other traffic can split and directly connect to the internet).

IETF standard (RFC 2401 – 2412) defines how a VPN can be secured across IP networks. IPsec can protect all traffic between layer 4 to 7 virtually and also authenticates IP packets between source and destination. IPsec does not have to follow specific rules, so that new security technologies can be easily upgraded as required. Following are the security function and choices for each function:

- Confidentiality using encryption, for example AES, 3DES
- Integrity using hashing algorithm for example SHA, SCRYPT, MD5 • Authentication using internet Key Exchange IKE for example PSK, RSA
- Secure Key exchange using Diffie-Hellman.

Security Association (SA) defines that to establish the VPN link both peers must have same SA structure with same choices for communication, hashing, Authentication and exchanging parameters. Following tables shows implementing SA for setting links

Site 1	Site 2
AH	AH
3DES	AES
SHA256	SCRYPT
PSK	PSK
DH2	DH3
This set up cannot create the link	

Site 1	Site 2		Framework
AH	AH	←	IPsec Protocol
3DES	3DES	←	Confidentiality
SHA256	SHA256	←	Integrity
PSK	PSK	←	Authentication
DH2	DH2	←	Diffie-Hellman
This setup can create the link			

This was the general intro of VPN, types, mechanism, structure. Because VPN is a vast subject itself, we will keep up to this for the basic introduction of VPN. We will face lot of terms, processes while configuring the actual links which we will be discussing at the same time. I believe, the concept will be clearer while we actually configure the links.

• Scenario

Topology:

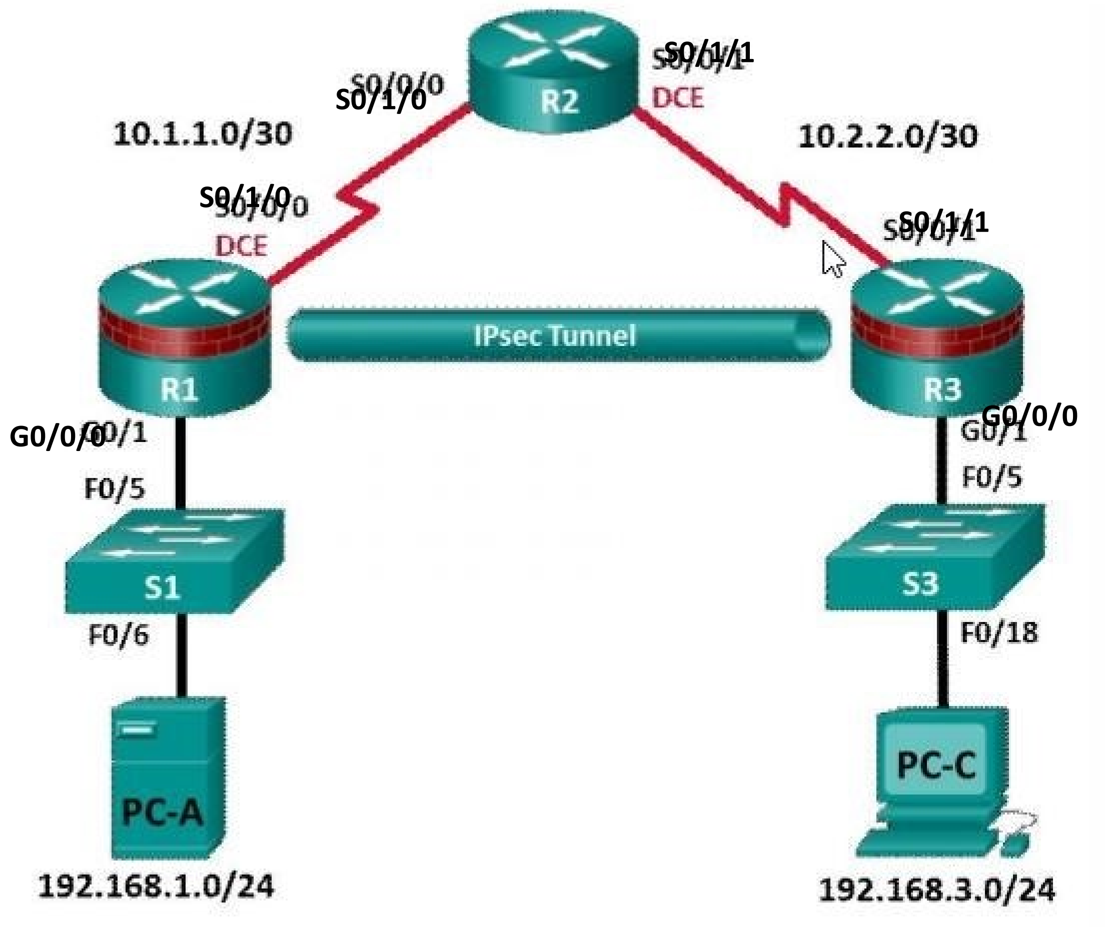

Fig: Topology taken from cisco 8.4.1.3 Lab -Configure Site-to-Site VPN using CLI

In this scenario, we have four different networks connected with each other. We can see, when we want to connect from PC-A to PC-C we have to route through R1, R2 and R3, however if we set a tunnel between R1 and R3 network we do not have to route through R2, which can be the internet. In brief we do not want to expose traffic from 192.168.1.0/24 network to 192.168.3.0/24 network to R2 network, so we will set up a link between R1 and R3, which will create virtual and private network between these two devices.

Resources Used:

- 3 routers (Cisco 1941 with iso 15.5(3) S4b, RELEASE SOFTWARE licence.
- 2 switches
- 2 Windows 10 machines.
- Serial and Ethernet Cables as shown
- Console cables to configure the networking devices

IP addressing Table

As I already mentioned we will use four different networks to configure the devices in the above topology. Following is the detailed scheme of IP addressing for each device.

Devices	Interfaces	IP address	Subnet Mask	Default gateway
R1	G0/1	192.168.1.1	255.255.255.0	
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	
R2	S0/0/0	10.1.1.2	255.255.255.252	
	S0/0/1	10.2.2.2	255.255.255.252	
R3	S0/0/1	10.2.2.1	255.255.255.252	
	G0/1	192.168.3.1	255.255.255.252	
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Objectives

- **To configure basic Device Settings**
- **To configure a Site-to-Site VPN**

Note: In this lab, I have used Cisco 1941 with iso 15.5(3) S4b, RELEASE SOFTWARE licence routers, you can choose the available routers to perform this lab, however the router should support hashing and encryption. You can check your router version issuing the **show version** command.

```
Router>en
Router#show version
Cisco IOS XE Software, Version 03.16.04b.S - Extended Support Release
Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 15.5
(3)S4b, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Mon 17-Oct-16 20:23 by mcpre
```

• Basic Device Configuration

Basically, basic device setting is the initial step to configure the networking devices, that will make sure the traffic flow and build up the connection between devices from same or different networks, which includes cabling the devices, configuring the hostname, assigning the ip addresses to the ports, and configuring the routing protocols for connection in different networks. I will briefly approach these cases step by step with the commands and output, troubleshooting the scenarios and so on.

Firstly, configure the cables as shown in the topology, routers are connected using the serial cables whilst other devices are configured using Ethernet cables. Firstly, it is a good practice to disable the DNS lookup to mitigate the dns lookup, in any mistyped command. We can verify the connections in router using the **show ip interface brief** command. **DCE** and **DTT** interfaces should identified and cabled accordingly, we can issue **show controllers 'serialname'** command to identify the DCE or DTT interfaces connected by the serial cable. I will set clock rate 64000 for the bandwidth In the DCE interface in each router.

```
Router#sh ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES unset  down                  down
GigabitEthernet0/0/1   unassigned      YES unset  up                    up
Serial0/1/0            unassigned      YES unset  up                    up
Serial0/1/1            unassigned      YES unset  up                    up
GigabitEthernet0       unassigned      YES unset  down                  down
Vlan1                  unassigned      YES unset  up                    down
Router#
Router#
```

Fig: show IP interface brief

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain lookup
Router(config)#
```

Fig: disable DNS lookup

```
Router#show controllers serial0/1/0

Serial0/1/0 - (NIM-2T) is up
 Encapsulation : HDLC
 Cable type: V.35 DCE
 mtu 1500, max_buffer_size 1524, max_pak_size 1608 enc 84
 loopback: Off,  crc: 16, invert_data: Off
 nrzi: Off, idle char: Flag
 dce_terminal_timing_enable: Off ignore_dtr: Off
 serial_clockrate: 2000000bps, serial_clock_index: 0
 serial_restartdelay:60000,  serial_restartdelay_def:60000

     RTS up, CTS up, DTR up, DCD up, DSR up
Router#
```

Fig: show controllers serial0/1/0

```
Router(config)#interface s0/1/0
Router(config-if)#clock rate 64000
Router(config-if)#
```

Fig: clock rate 64000

Configure the hostname:

Hostname can be configured using **#hostname 'NAME'** command.

```
Router(config)#hostname R1
R1(config)#
```

Fig: hostname 'R1'

Configure IP address

IP address is assigned in the routers and switches selecting the interface from global configuration mode and turning on the interface will allow the flow of traffic. Similarly, assign the IP address in the hosts similarly from the IP addressing table with the default gateway. In this report, I will not configure address of switches because we don't have VLANS, and traffic is forwarded by the native VLAN 0 to the gateway. Up to this part we should be able to send and receive packets form the devices in the same network.

```
R1(config)#interface s0/1/0
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#no shutdown
```

```
R1(config-if)#interface g0/0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut
```

```
R1#sh ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES unset  down                  down
GigabitEthernet0/0/1   192.168.1.1     YES manual up                    up
Serial0/1/0            10.1.1.1        YES manual up                    up
Serial0/1/1            unassigned      YES unset  up                    up
GigabitEthernet0       unassigned      YES unset  down                  down
Vlan1                  unassigned      YES unset  up                    down
R1#
```

FIG: Configure IP address.

Configure Routing Protocol:

To route in the different networks, we have to configure routing in the routers, there are different protocols by which we can configure routing such as static, OSPF, RIP and EIGRP are the major routing protocols. In this report, I will set up OSPF routing protocols in each router. Open Shortest Path First OSPF, is a link-state routing protocol, collects link state information from routers and forwards packets determining the routing table information, with is IETF open standard and comparatively suitable for the Large Networks. Following command is used to configure the OSPF routing.

#ip ospf <number>

#Network destination network wildcard mask area 'area Id'

```
R1(config)#router ospf 101
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#network 10.1.1.0 0.0.0.3 area 0
R1(config-router)#passive interface g0/0/1
                          ^
% Invalid input detected at '^' marker.

R1(config-router)#passive
R1(config-router)#passive-interface g0/0/1
R1(config-router)#
```

Fig: configuration of ospf in R1.

Note: All routers inside an area must have the same area ID to become OSPF neighbour We

can issue, **#no ip ospf <number>** to delete the ospf routing.

We can verify ospf using **ip route** and **show ospf neighbor** command.

```
R1#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface 10.2.2.2
0   FULL/  -        00:00:31    10.1.1.2        Serial0/1/0
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is not set
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/1/0
L        10.1.1.1/32 is directly connected, Serial0/1/0
O        10.2.2.0/30 [110/3124] via 10.1.1.2, 00:01:58, Serial0/1/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/0/1
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0/1
O     192.168.3.0/24 [110/3125] via 10.1.1.2, 00:00:58, Serial0/1/0
R1#
R1#
```

Fig: verify ospf in R1.

Similarly, configure the ospf in R2 and R3, and assign the ip address to the host devices and also the default gateway, at this point we should be able to ping PC-A to PC-B.

Verify connectivity

```
C:\Users\sysadmin>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.3.3: bytes=32 time=36ms TTL=125
Reply from 192.168.3.3: bytes=32 time=36ms TTL=125
Reply from 192.168.3.3: bytes=32 time=36ms TTL=125
Reply from 192.168.3.3: bytes=32 time=36ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 36ms, Maximum = 36ms, Average = 36ms

C:\Users\sysadmin>

C:\Users\sysadmin>
```

Fig: Ping PC-A to PC-C

```
C:\Users\sysadmin>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=36ms TTL=125
Reply from 192.168.1.3: bytes=32 time=36ms TTL=125
Reply from 192.168.1.3: bytes=32 time=36ms TTL=125

Ping statistics for 192.168.1.3:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 36ms, Maximum = 36ms, Average = 36ms
Control-C
^C
C:\Users\sysadmin>_
```

Fig: ping PC-C to PC-A save startup configuration to the

running configuration.

#copy running-config startup-config

• Limiting Access

We can limit the Access in the end devices by configuring and encrypting the passwords, I will recommend configuring at least 10 characters long complex password for the security and encrypting the password converts the plain text password into random string of the mixed characters and make it harder to crack the password.

We can use the security passwords command to set a minimum password length of 10 character and enable secret followed by the password also we can encrypt the password using secure hashing algorithm like (SCRYPT) for the security. we can also issue logging synchronous command to avoid the disruption in the CLI while typing the passwords. Further for the security concern we can deploy different users with their passwords encrypted and assigning the precedence level for limiting the access to the commands. Precedence level are between 0-15 where 15 gets the higher level of precedence which should be assigned to the main administrative credentials. Following figures shows the steps to configure and encrypt passwords. Security passwords restricts the unauthorized person to access the privileged exec mode. In addition, we can even set the console passwords to limit access to the console lines, vty lines password for remote connection, and auxiliary ports in the similar way. For the login credentials in Enterprise and large-scale organizations using AAA server for the login authentication, frustration to configure each end devices can be mitigated because AAA can be used to configure all the devices from one place, RADIUS is the protocol which make it possible. However, in the figures below we are using local database because for easy understanding.

```
R1(config)#security password min-length 10
R1(config)#enable algorithm-type scrypt secret complexpassword
R1(config)#
```

FIG: Configuring the security password using SCRYPT algorithm

```
R1(config)#username user01 algorithm-type scrypt secret user01pass
R1(config)#exit
R1#
```

FIG: Creating user and giving him credentials

```
R1(config)#line console 0
R1(config-line)#login local
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#service
R1(config)#service pass
R1(config)#service password-encryption
R1(config)#
```

FIG: Enabling console line password.

• VPN Configuration

As a recap we are configuring the IPsec VPN settings on two routers from our topology, R1 and R3 we will create a tunnel between them. For a normal understanding take R1 and R3 branch and head office and R2 as internet, we do not want the traffic of the organization to expose in the internet(R2). We have already setup the basic configuration and we can ping the hosts to each other.

Enable Internet Key Exchange IKE policies:

As we know IPsec is a framework which allows the exchange of security protocols as new technologies, and encryption algorithms. I have already talk about the security protocols, security association (SA) should be same in both peers for communication, hashing, encryption, Authentication and exchanging parameters. IKE is configured in two phases; first phase defines the key exchange method for the validation of IKE policies between the peers and phase 2 is all about exchanging the match IPsec policies for authentication and encryption of data.

In most cases, IKE is enabled by default, if not we can use the command **crypto isakmp enable** command. Some older version routers do not support IKE. Now, we will set up the security association, if both peers accept the SA, we can then proceed to phase 2.

To configure the ISAKMP policy issue **crypto isakmp policy** with a priority of **10**. For hashing we will use **sha, aes 256** for **encryption** algorithm, **pre-shared** key as **authentication** type**, lifetime** of **3600** seconds, and **Diffie-hellman** group **14**.

FIG: Issue the crypto isakmp number

We can view the Isakmp policy with **show crypto isakmp policy** command.

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#?
ISAKMP commands:
  authentication  Set authentication method for protection suite
  default         Set a command to its defaults
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults

R1(config-isakmp)#hash sha
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 14
R1(config-isakmp)#lifetime 3600
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#end
```

FIG: crypto isakmp policy on R1.

Configure same isakmp policy in R3 as well.

```
R3#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   AES - Advanced Encryption Standard (256 bit keys
).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #14 (2048 bit)
        lifetime:               3600 seconds, no volume limit
R3#
```

Configure pre-shared keys

IKE uses the pre-shared key as the authentication method, a key must be configured to an end point pointing to the other endpoint, which must match with each other. Use crypto isakmp key <key-string> address <Ip address of the other point). These IP addresses are also the end points for the remote VPN endpoint. We will configure a password <complexpassword> as the key.

```
R1(config)#crypto isakmp key complexpassword address 10.2.2.1
R1(config)#
```

FIG: configuration of pre-share key Router1:

```
R3(config)#crypto isakmp key complexpassword address 10.1.1.1
R3(config)#
```

FIG: configuration of pre-share key Router3:

Configure IPsec transform set and lifelines.

Another important crypto configuration parameter is to form the security Association. We will create **cyrpto ipsec transform-set <tag> 50, esp** transform using **aes 25**6 and **sha** hash function in both routers.

```
R3(config)#crypto isakmp key complexpassword address 10.1.1.1
R3(config)#crypto ip
R3(config)#crypto ipsec tran
R3(config)#crypto ipsec transform-set 50 ?
  ah-md5-hmac      AH-HMAC-MD5 transform
  ah-sha-hmac      AH-HMAC-SHA transform
  ah-sha256-hmac   AH-HMAC-SHA256 transform
  ah-sha384-hmac   AH-HMAC-SHA384 transform
  ah-sha512-hmac   AH-HMAC-SHA512 transform
  comp-lzs         IP Compression using the LZS compression algorithm
  esp-3des         ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes          ESP transform using AES cipher
  esp-des          ESP transform using DES cipher (56 bits)
  esp-gcm          ESP transform using GCM cipher
  esp-gmac         ESP transform using GMAC cipher
  esp-md5-hmac     ESP transform using HMAC-MD5 auth
  esp-null         ESP transform w/o cipher
  esp-seal         ESP transform using SEAL cipher (160 bits)
  esp-sha-hmac     ESP transform using HMAC-SHA auth
  esp-sha256-hmac  ESP transform using HMAC-SHA256 auth
  esp-sha384-hmac  ESP transform using HMAC-SHA384 auth
  esp-sha512-hmac  ESP transform using HMAC-SHA512 auth
```

```
R3(config)#crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
R3(cfg-crypto-trans)#exit
R3(config)#
```

```
R1(config)#crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
R1(cfg-crypto-trans)#exit
```

FIG: configuration of ipsec transform set in R1 and R3

We can also change the security association lifetime, lifetimes typically are session for the VPN link, which will redo this process after every lifetime and the associations should match in every processes for the uninterrupted connection.

```
R3(config)#crypto ipsec security-association lifetime seconds 1800
R3(config)#
```

```
R1(config)#crypto ipsec security-association lifetime seconds 1800
R1(config)#exit
R1#
```

FIG: config crypto ipsec security-association lifetime

Interesting traffic

In the network, we do not always send the important messages which we can send even without encryption to do so we will use extended ACL to define interesting traffic. The packet that is denied by this rule (ACL) is not dropped it is sent unencrypted. These VPN rules are outbound in both endpoints interfaces and must mirror each other.

R3(config)#access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255 R1(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

FIG: create rule to define the interesting traffic in R1 and R3.

Creating and applying a crypto map.

Crypto map associates with various IKE and IPsec settings and also the peer matching the traffic, which is applied to one or more interfaces and must facing towards the peer device. we will use the IKE to establish crypto map configurations. We will name the crypto map as **CMAP** and use 10 as the sequence number. Remember we had used crypto isakmp policy 10, and configured our first phase IKE, it is also the similar process.

Use **crypto map <name> <sequence-num> <type>** command, which will be disabled until a peer and a valid access list have been configured. We will **match address** with the created ACL with **command match address 101** and **set peer** with the **ip address of pointing peer device**, we will use **group14** for pfs, which was derived independently through separate deffie-hellman exchange, similarly **transformset 50** and lifetime **900** seconds. This IKE crypto set should be mirrored match in peer router, which then is assigned to the peer facing interfaces in both peer devices, using **crypto map 'map-name'** command selecting the interface in global configuration mode, which should create a link between the end devices which I will show in the results of this report.

```
R1(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid
access list have been configured. R1(config-crypto-map)#match address 101
R1(config-crypto-map)#set ?
 group            Set the san group parameters
 identity         Identity restriction.
 ikev2-profile    Specify ikev2 Profile
 ip               Interface Internet Protocol config commands
 isakmp-profile   Specify isakmp Profile
 nat              Set NAT translation  peer
Allowed Encryption/Decryption peer.
 pfs              Specify pfs settings
 reverse-route    Reverse Route Injection.
 security-association  Security association parameters
 transform-set    Specify list of transform sets in priority order
R1(config-crypto-map)#set peer 10.2.2.1
R1(config-crypto-map)#set pfs group14
R1(config-crypto-map)#set transform-set 50
R1(config-crypto-map)#set security-association lifetime seconds 900
R1(config-crypto-map)#exit
```

FIG: creating a crypto map R1

```
R3(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R3(config-crypto-map)#match address 101
R3(config-crypto-map)#set peer 10.1.1.1
R3(config-crypto-map)#set pfs group14
R3(config-crypto-map)#set transform-set 50
R3(config-crypto-map)#set security-association lifetime seconds 900
R3(config-crypto-map)#exit
R3(config)#
```

FIG: creating a crypto map R3

```
1(config)#interface s0/1/0
1(config-if)#crypto map CMAP
1(config-if)#
Jun  6 01:58:50.929: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
1(config-if)#end
1#
Jun  6 01:59:00.346: %SYS-5-CONFIG_I: Configured from console by console
1#
```

```
R3(config)#interface s0/1/1
R3(config-if)#crypto map CMAP
R3(config-if)#
*Feb  5 01:23:46.126: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)#end
R3#
```

FIG: Assigning the crypto map in accurate interfaces in R1 and R3.

• Results and Troubleshoot

Verify the site-to-site IPsec VPN configuration

We can use different show commands to verify the VPN configuration listed below:

- **Show crypto isakmp policy**

  It will display the configured ISAKMP policies on the router.

```
R1#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   AES - Advanced Encryption Standard (256 bit keys
).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #14 (2048 bit)
        lifetime:               3600 seconds, no volume limit
R1#
```

FIG: crypto isakmp policy on R1

```
R3#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   AES - Advanced Encryption Standard (256 bit keys
).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #14 (2048 bit)
        lifetime:               3600 seconds, no volume limit
R3#
```

FIG: crypto isakmp policy on R3

- **Show crypto ipsec transform-set**

It will display the configured transform set, unless the isakmp policy is matched and mirrored in both VPNs end device, we can analyse there is no link created

```
R1#show crypto ipsec transform-set
Transform set default: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set 50: { esp-256-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },

R1#
```

FIG: show crypto ipsec transform-set on R1

```
R3#show crypto ipsec transform-set
Transform set default: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set 50: { esp-256-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },

R3#
```

FIG: show crypto ipsec transform-set on R3

- **Show crypto map**
  It shows if the device is mapped with the peer device showing the configuration like peer, ACL, lifetime, DH group and rule linked to the interface which should map in both end points

FIG: show crypto map in R1

```
R3#show crypto map
Crypto Map IPv4 "CMAP" 10 ipsec-isakmp
        Peer = 10.1.1.1
        Extended IP access list 101
            access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.25
5
        Current peer: 10.1.1.1
        Security association lifetime: 4608000 kilobytes/900 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): Y
        DH group:  group14
        Mixed-mode : Disabled
        Transform sets={
                50:  { esp-256-aes esp-sha-hmac  } ,
        }
        Interfaces using crypto map CMAP:
                Serial0/1/1

        Interfaces using crypto map NiStTeSt1:

R3#
```

FIG: show crypto map in R3

```
R1#show crypto map
Crypto Map IPv4 "CMAP" 10 ipsec-isakmp
        Peer = 10.2.2.1
        Extended IP access list 101
            access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.25
5
        Current peer: 10.2.2.1
        Security association lifetime: 4608000 kilobytes/900 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): Y
        DH group:  group14
        Mixed-mode : Disabled
        Transform sets={
                50:  { esp-256-aes esp-sha-hmac  } ,
        }
        Interfaces using crypto map CMAP:
                Serial0/1/0

        Interfaces using crypto map NiStTeSt1:

R1#
```

Verify IPsec security associations

Display ISAKMP associations

- **Show crypto isakmp sa**
  This command at this phase will reveals that no IKE SAs exist yet, because we have not generated any interesting traffic to the connection

```
R3#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status

IPv6 Crypto ISAKMP SA
```

FIG: show isakmp sa

Display crypto security associations

- **Show crypto ipsec sa**

Similarly in the above phase we can see no security associations listed in the end of the command.

However, if we generate some interesting traffic the output will change.

R1#sh crypto ipsec sa
interface: Serial0/1/0
Crypto map tag: CMAP, local addr 10.1.1.1

protected vrf: (none)

local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)

current_peer 10.2.2.1 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.: 10.1.1.1, remote crypto endpt.: 10.2.2.1
    plaintext mtu 1500, path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
    current outbound spi: 0x0(0)
    PFS (Y/N): N, DH group: none
    inbound esp sas:
inbound ah sas:
    inbound pcp sas:
outbound esp sas:     outbound
ah sas:         outbound pcp
sas:
R1#
```

FIG: show crypto ipsec sa on R1

Generating some traffic:

As we look back, we had created the rule that define the **interesting traffic** that was, **access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255** in router 1. Let's first generate an uninteresting traffic just pinging from PC-A to R3 interface and issue the **show crypto isakmp sa** and **show crypto ipsec sa** command, we found no IKE SA and security associations because that was not the interesting traffic, we can verify the hello packets were not encrypted using debug command. Use **debug ip ospf hello** to start debugging and **no debug ip ospf hello** command to turn it off. However, if we produce any interesting traffic such as try pinging from pc-A to PC-C we can see the changed output of the command, and the packets were also encrypted, which verifies our VPN set up is working as expected.

```
C:\Users\sysadmin>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:
Request timed out.
Reply from 192.168.3.3: bytes=32 time=69ms TTL=126
Reply from 192.168.3.3: bytes=32 time=70ms TTL=126
Reply from 192.168.3.3: bytes=32 time=70ms TTL=126

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 69ms, Maximum = 70ms, Average = 69ms

C:\Users\sysadmin>
```

FIG: ping request form PC-A to PC-C

R1#sh crypto ipsec sa interface:
Serial0/1/0
  Crypto map tag: CMAP, local addr 10.1.1.1
protected vrf: (none)

```
  local   ident  (addr/mask/prot/port):  (192.168.1.0/255.255.255.0/0/0)
remote  ident  (addr/mask/prot/port):  (192.168.3.0/255.255.255.0/0/0)
current_peer 10.2.2.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
   #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3
   #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.: 10.1.1.1, remote crypto endpt.: 10.2.2.1
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
    current outbound spi: 0x9BC817CD(2613581773)
PFS (Y/N): Y, DH group: group14      inbound esp
sas:
     spi: 0x52F8E838(1392044088)
transform: esp-256-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2001, flow_id: ESG:1, sibling_flags FFFFFFFF80004048, crypto map: CMAP
       sa timing: remaining key lifetime (k/sec): (4607999/838)
IV size: 16 bytes        replay detection support: Y
       Status: ACTIVE(ACTIVE)

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0x9BC817CD(2613581773)
transform: esp-256-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2002, flow_id: ESG:2, sibling_flags FFFFFFFF80004048, crypto map: CMAP
       sa timing: remaining key lifetime (k/sec): (4607999/838)
IV size: 16 bytes        replay detection support: Y       Status:
ACTIVE(ACTIVE)      outbound ah sas:      outbound pcp sas:
```

FiG: show crypto isakmp sa

```
R3#sh crypto ipsec sa  interface
Serial0/1/1
Crypto map tag: CMAP, local addr 10.2.2.1protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
current_peer 10.1.1.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
    #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3
#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.: 10.2.2.1, remote crypto endpt.: 10.1.1.1
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/1
     current outbound spi: 0x52F8E838(1392044088)
     PFS (Y/N): Y, DH group: group14
inbound esp sas:
      spi: 0x9BC817CD(2613581773)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: ESG:1, sibling_flags FFFFFFFF80000048, crypto map: CMAP
        sa timing: remaining key lifetime (k/sec): (4607999/623)
        IV size: 16 bytes
        replay detection support: Y
Status: ACTIVE(ACTIVE)
inbound ah sas:      inbound
pcp sas:     outbound esp sas:
      spi: 0x52F8E838(1392044088)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: ESG:2, sibling_flags FFFFFFFF80000048, crypto map: CMAP
        IV size: 16 bytes                    sa timing: remaining key lifetime (k/sec): (4607999/623)
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
outbound ah sas:      outbound
pcp sas:
```

FIG: show crypto ipsec sa

• Conclusion

To sum up, in this report, I tried to explain the configuration detailed configuration of VPN link between the two routers as described in our scenario. Anyone, going through this report can briefly understand the VPNs, types of VPNs, and configuration of VPN from the scratch. From the basic configurations of our network devices to achieve the fully working site-to-site layer3 IPsec VPN, I believe, someone with little knowledge of networking can briefly understand, configure, verify, and troubleshoot the VPN concept.

• References

[1] [2] [3] [4] [5]

[1] s. kent, "security Architecture for the Internet Protocol," datatracker.ietf.org, cambridge, 1998.

[2] TechTarget Contibutor, "authentication, authorization, and accounting (AAA)," [Online]. Available: https://www.techtarget.com/searchsecurity/definition/authentication-authorizationand-accounting.

[3] E. Anderson, "How to Comply in 2020 With The 5 Functions of The NIST Cybersecurity Framework," 09 01 2020. [Online]. Available: https://www.forescout.com/blog/how-to-complywith-the-5-functions-of-the-nist-cybersecurity-framework/.

[4] cisco, "Cisco IOS VPN Configuration Guide," [Online]. Available: https://www.cisco.com/c/en/us/td/docs/security/vpn_modules/6342/vpn_cg/6342site3.html. [Accessed 2022 05 24].

[5] PRISMA, "What Is a Remote Access VPN?," [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-a-remote-accessvpn#:~:text=A%20remote%20access%20virtual%20private,the%20users%20send%20and%20rec eive.. [Accessed 27 05 2022].

[6] cisco networking academy, "Implementing virtual private network," in *CCNA security*, cisco networking academy.

[7] cisco networking academy, *8.4.1.3 - Configuring a Site-to-Site VPN Using Cisco IOS,* cisco netcad academy.