

**Purpose**

With growing networks, security and managing who can reach network resources is increasingly important. Virtual private networks (VPNs) provide a secure way to transfer data over the internet. VPNs typically provide a tunnel with which data can be sent securely by authenticating the sources and destination of origin, encrypting the data, and using algorithms to determine if the data had been modified in transmission. IPSecurity (IPSec) is a standard of VPNs that implements these functions for internet traffic. This lab explores the ability to use IPSec VPNs to securely connect two remote sites or buildings over the internet.

**Background Information**

IP Security Virtual Private Networks (IPSec VPN) is a standard to send data securely over connections. Important functions performed under this framework are authentication, secure key exchange, confidentiality, and integrity.

Authentication refers to verifying the senders. An important factor of secure data transfer is that the devices communicating know who they are communicating with. As a result, IPSec defines authentication through two methods, private pre-shared key and a public key. A private pre-shared key is a password that both endpoints know before starting the exchange. Then, to make sure they are communicating with each other, they repeat the secret handshake to each other. In a public key exchange, the Diffie-Hellman algorithm is used to generate a shared secret handshake over the internet. This new handshake is then used for the authentication process.

Secure key exchange refers to making sure that sending or negotiating key data to initialize the connection also remains secure. When sending secret handshakes over the internet, the security standards of IPSec must be applied as well. Sending secret handshakes over the internet without any security makes the subsequent VPN tunnel insecure as it is like giving a secret password to everyone. Thus, during this secure exchange for authentication, the messages sent must also value confidentiality and integrity.

Confidentiality refers to making sure that the data transferred cannot be read and understood by any user or device along the path of transmission. This is implemented in the IPSec standard through encryption using various encryption algorithms. Encryption works almost like converting the message to a made-up language between two devices. The source device converts their message into this made-up language and then sends it over to the end device. Since no one else understands this made-up language, it is only at the end device that the data can be converted back and decrypted to its original state.There are options such as DES, 3DES, and AES. DES and 3DES have been cracked, meaning that they are no longer securely hiding the contents of the data encrypted. As a result, AES should be used instead.

Integrity refers to making sure that the data transferred hasn’t been modified in the transmission process. It works by taking the message and running it through a function, called a hash, that calculates a long number corresponding to this exact message. When the message is received, the receiving device runs it through the same hash. If the computed number is the same at the endpoint as it was at the source, then the devices can confirm that the data has not been modified in between. The integrity protocols that can be used is MD5 and SHA, although for best security practices, SHA should be used, and the computed value should be at least 256-bits long.

IPSec defines two different headers when sending data, the AH header and the ESP header. The AH header provides authentication and integrity. The ESP header provides authentication, integrity, and confidentiality. As a result, the ESP header will be the more secure choice at a cost of using more computing resources.

A common VPN is the remote access VPN, where a host requests and initializes a secure connection with a remote network. This requires special VPN software on the host to handle this operation. The VPN configured in this lab is a site-to-site VPN, which is a network tunnel that is always activated and keeps data passing between two destinations secure always. Site-to-site VPNs do not require special VPN software. This is because a remote access VPN can be used anywhere remotely whereas the site-to-site VPN is specifically between two endpoints, meaning it can be statically configured on the networking devices connecting the endpoints. For this reason, site-to-site VPNs are useful for securely connecting two buildings of a company over the internet since they use known endpoints.

To configure a site-to-site VPN, the secure internet key exchange must be configured. In this process, the type of authentication, either pre-shared or public, encryption algorithm, hashing algorithm, and Diffie-Hellman group, if using public keys, must be defined. This configures the VPN for authentication and secure key exchange. Then a transform set must be made which defines which header, either AH or ESP, encryption algorithm, and hashing algorithm will be used for the actual data transfer. Then, a crypto access list must be configured, which tells the router which packets they should keep secure. In some cases, the data transferred might be more sensitive than others to security and this is where different packets can be held to different security standards. Finally, a crypto map must be configured which connects the authentication, secure key exchange, transform set, and crypto access list altogether. These same configurations must also be applied onto the adjacent router participating in IPSec.

**Lab Summary**

Two routers were connected. Both have a loopback address to simulate a connected network to the edge of each router. For authentication, IPSec is configured with a secure private pre-shared key exchange using AES encryption, SHA-256 integrity check and Diffie-Helman group 2. For data transfer, IPSec is configured using the ESP header, AES encryption, and SHA-256.

**Lab Commands**

**Router (config) # crypto isakmp policy <policy number>**

Creates a new secure crypto key exchange policy. Policy number can be any number.

**Router (config-isakmp) # authentication <authentication type>**

Configures the key exchange policy to use a specific authentication type. The authentication type can be pre-share, rsa-encr (encrypted RSA), or rsa-slg (RSA signatures).

**Router (config-isakmp) # encryption <encryption type>**

Configures the key exchange policy to use a specific encryption algorithm. The encryption type can be AES, DES, or 3DES. For best security, only use AES.

**Router (config-isakmp) # hash <hash type>**

Configures the key exchange policy to use a specific hashing algorithm. The encryption type can be MD5, SHA, SHA-256, or SHA-512. For best security practices, use either SHA-256 or SHA-512.

**Router (config-isakmp) # group <DH group number>**

Configures the key exchange policy to use a specific Diffie-Hellman group number. The DH group number can be 1, 2, 5, or 7. The default is 2.

**Router (config-isakmp) # lifetime <time in seconds>**

Configures the key exchange policy to have a specific lifetime. The default time is 86400 seconds, the equivalent of one day.

**Router (config) # crypto isakmp identity address <current router address>**

Configures the router to identify as a specific IP address for key exchange.

**Router (config) # crypto isakmp key <password> address <peer address>**

Configures the router to create a pre-shared key with a peer router. For best practices, follow good password creation rules. The peer address is the IP address of the router to have a pre-shared key with.

**Router (config) # access-list <list number> permit <ip address> <wildcard mask>**

Creates an access-list entry for the crypto access-list. A standard or extended access-list can be used for this purpose. Used to allow certain packets to be forwarded.

**Router (config) # crypto ipsec transform-set <name> <encryption> <hash>**

Creates the transform-set for the VPN tunnel. The name should be recognizable and should be fully capitalized to distinguish from Cisco IOS keywords. For encryption, DES, 3DES, or AES can be used but ultimately, the keyword esp-aes should be used for best security. For hash, esp-md5-hmac, esp-sha-hmac, esp-sha256-hmac, and esp-sha512-hmac can be used. If the ah header is to be used (not needing encryption), then only the hash needs to be defined by typing ah in place of esp, such as ah-sha-hmac.

**Router (cfg-crypto-trans) # mode tunnel**

Configures the IPsec to tunnel mode instead of transport mode, meaning that the headers in the data sent are encrypted. This means that the IP addresses are hidden during transmission.

**Router (config) # crypto map <name> <isakmp policy number> ipsec-isakmp**

Creates a crypto map which links all parts of the IPSec connection together. The name should be recognizable and should be fully capitalized to distinguish from Cisco IOS keywords. The ISAKMP policy number should be of a previously defined key exchange policy.

**Router (config-crypto-map) # match address <access list number>**

Configures the crypto map to only use VPN standards on packets that match the predefined access control list. Access list number should be of a previously configured access list.

**Router (config-crypto-map) # set peer <peer address>**

Configures the crypto map to use the defined VPN standards when sending data to the VPN peer. Peer address should be a 32-bit IPv4 address of the peer router.

**Router (config-crypto-map) # set transform-set <transform set name>**

Configures the crypto map to use the security standards defined in the transform set. Transform set name should be all capitalized and be an already configured transform set.

**Router (config-if) # crypto map <crypto map name>**

Configures the interface to use and apply the crypto map standards. The crypto map name should be all capitalized and be an already configured crypto map.

**Router # show crypto isakmp policy**

Shows information related to the secure key exchange including encryption algorithm, hash algorithm, authentication method, Diffie-Hellman group: and lifetime used.

**Router # show access-lists**

Shows all configured access-lists on the routers including how many matches each entry in each access-list has.

**Router # show crypto ipsec transform-set**

Shows all configured transform-sets on the routers including their encryption algorithms, hashing algorithms, IPSec header, and transmission mode, either transport or tunnel.

**Router # show crypto map**

Shows all configured crypto maps on the router including their corresponding peer, crypto access list, transform set, and key exchange policy number.

**Router # show crypto ipsec sa**

Shows transmission data for the IPSec connection including the packets encrypted and the standards used on the participating inbound and outbound interfaces.

**Network Diagram with IP’s**

**Shape, rectangle

Description automatically generated**

|  |  |  |
| --- | --- | --- |
| **Device Name** | Interface | IP Address |
| **R1** | G0/0/0 | 2.2.2.1/24 |
|  | Loopback0 | 1.1.1.1/24 |
|  |  |  |
| **R2** | G0/0/0 | 2.2.2.2/24 |
|  | Loopback0 | 3.3.3.1/24 |

**Configurations**

**Router 1**

**R1#show running-config**

Current configuration : 1932 bytes

version 15.5

service timestamps debug datetime msec

service timestamps log datetime msec

no platform punt-keepalive disable-kernel-core

hostname R1

boot-start-marker

boot-end-marker

vrf definition Mgmt-intf

address-family ipv4

exit-address-family

address-family ipv6

exit-address-family

no aaa new-model

subscriber templating

multilink bundle-name authenticated

license udi pid ISR4321/K9 sn FDO21491LXV

license accept end user agreement

license boot level securityk9

spanning-tree extend system-id

redundancy

mode none

vlan internal allocation policy ascending

crypto isakmp policy 1

encr aes

authentication pre-share

hash sha256

group 2

crypto isakmp key VPNPassword123 address 2.2.2.2

crypto ipsec transform-set VPN esp-aes esp-sha256-hmac

mode tunnel

crypto map VPNMap 1 ipsec-isakmp

set peer 2.2.2.2

set transform-set VPN

match address 101

interface Loopback0

ip address 1.1.1.1 255.255.255.0

interface GigabitEthernet0/0/0

ip address 2.2.2.1 255.255.255.0

negotiation auto

crypto map VPNMap

no shutdown

interface GigabitEthernet0/0/1

no ip address

shutdown

negotiation auto

interface Serial0/1/0

no ip address

shutdown

interface Serial0/1/1

no ip address

shutdown

interface GigabitEthernet0

vrf forwarding Mgmt-intf

no ip address

shutdown

negotiation auto

interface Vlan1

no ip address

shutdown

ip forward-protocol nd

no ip http server

no ip http secure-server

ip tftp source-interface GigabitEthernet0

ip route 3.3.3.0 255.255.255.0 GigabitEthernet0/0/0 2.2.2.2

access-list 101 permit tcp 1.1.1.0 0.0.0.255 3.3.3.0 0.0.0.255

access-list 101 permit ip 1.1.1.0 0.0.0.255 3.3.3.0 0.0.0.255

control-plane

line con 0

stopbits 1

line aux 0

stopbits 1

line vty 0 4

login

end

**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

1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C 1.1.1.0/24 is directly connected, Loopback0

L 1.1.1.1/32 is directly connected, Loopback0

2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C 2.2.2.0/24 is directly connected, GigabitEthernet0/0/0

L 2.2.2.1/32 is directly connected, GigabitEthernet0/0/0

3.0.0.0/24 is subnetted, 1 subnets

S 3.3.3.0 [1/0] via 2.2.2.2, GigabitEthernet0/0/0

**R1#show crypto isakmp policy**

Global IKE policy

Protection suite of priority 1

encryption algorithm: AES - Advanced Encryption Standard (128 bit keys).

hash algorithm: Secure Hash Standard 2 (256 bit)

authentication method: Pre-Shared Key

Diffie-Hellman group: #2 (1024 bit)

lifetime: 86400 seconds, no volume limit

**R1#show access-lists**

Extended IP access list 101

10 permit tcp 1.1.1.0 0.0.0.255 3.3.3.0 0.0.0.255

20 permit ip 1.1.1.0 0.0.0.255 3.3.3.0 0.0.0.255 (1 match)

**R1#show crypto ipsec transform-set**

Transform set default: { esp-aes esp-sha-hmac }

will negotiate = { Transport, },

Transform set VPN: { esp-aes esp-sha256-hmac }

will negotiate = { Tunnel, },

**R1#show crypto map**

Interfaces using crypto map NiStTeSt1:

Crypto Map IPv4 "VPNMap" 1 ipsec-isakmp

Peer = 2.2.2.2

Extended IP access list 101

access-list 101 permit tcp 1.1.1.0 0.0.0.255 3.3.3.0 0.0.0.255

access-list 101 permit ip 1.1.1.0 0.0.0.255 3.3.3.0 0.0.0.255

Current peer: 2.2.2.2

Security association lifetime: 4608000 kilobytes/3600 seconds

Responder-Only (Y/N): N

PFS (Y/N): N

Mixed-mode : Disabled

Transform sets={

VPN: { esp-aes esp-sha256-hmac } ,

}

Interfaces using crypto map VPNMap:

GigabitEthernet0/0/0

**Router 2**

**R2#show running-config**

Current configuration : 1932 bytes

version 15.5

service timestamps debug datetime msec

service timestamps log datetime msec

no platform punt-keepalive disable-kernel-core

hostname R2

boot-start-marker

boot-end-marker

vrf definition Mgmt-intf

address-family ipv4

exit-address-family

address-family ipv6

exit-address-family

no aaa new-model

subscriber templating

multilink bundle-name authenticated

license udi pid ISR4321/K9 sn FDO214420QQ

license accept end user agreement

license boot level securityk9

spanning-tree extend system-id

redundancy

mode none

vlan internal allocation policy ascending

crypto isakmp policy 1

encr aes

authentication pre-share

group 2

hash sha256

crypto isakmp key VPNPassword123 address 2.2.2.1

crypto ipsec transform-set VPN esp-aes esp-sha256-hmac

mode tunnel

crypto map VPNMap 1 ipsec-isakmp

set peer 2.2.2.1

set transform-set VPN

match address 101

interface Loopback0

ip address 3.3.3.1 255.255.255.0

interface GigabitEthernet0/0/0

ip address 2.2.2.2 255.255.255.0

negotiation auto

crypto map VPNMap

no shutdown

interface GigabitEthernet0/0/1

no ip address

shutdown

negotiation auto

interface Serial0/1/0

no ip address

shutdown

interface Serial0/1/1

no ip address

shutdown

interface GigabitEthernet0

vrf forwarding Mgmt-intf

no ip address

shutdown

negotiation auto

interface Vlan1

no ip address

shutdown

ip forward-protocol nd

no ip http server

no ip http secure-server

ip tftp source-interface GigabitEthernet0

ip route 1.1.1.0 255.255.255.0 GigabitEthernet0/0/0 2.2.2.1

access-list 101 permit tcp 3.3.3.0 0.0.0.255 1.1.1.0 0.0.0.255

access-list 101 permit ip 3.3.3.0 0.0.0.255 1.1.1.0 0.0.0.255

control-plane

line con 0

stopbits 1

line aux 0

stopbits 1

line vty 0 4

login

end

**R2#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

1.0.0.0/24 is subnetted, 1 subnets

S 1.1.1.0 [1/0] via 2.2.2.1, GigabitEthernet0/0/0

2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C 2.2.2.0/24 is directly connected, GigabitEthernet0/0/0

L 2.2.2.2/32 is directly connected, GigabitEthernet0/0/0

3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C 3.3.3.0/24 is directly connected, Loopback0

L 3.3.3.1/32 is directly connected, Loopback0

**R2#show access-lists**

Extended IP access list 101

10 permit tcp 3.3.3.0 0.0.0.255 1.1.1.0 0.0.0.255

20 permit ip 3.3.3.0 0.0.0.255 1.1.1.0 0.0.0.255

**R2#show crypto isakmp policy**

Global IKE policy

Protection suite of priority 1

encryption algorithm: AES - Advanced Encryption Standard (128 bit keys).

hash algorithm: Secure Hash Standard 2 (256 bit)

authentication method: Pre-Shared Key

Diffie-Hellman group: #2 (1024 bit)

lifetime: 86400 seconds, no volume limit

**R2#show crypto ipsec transform-set**

Transform set default: { esp-aes esp-sha-hmac }

will negotiate = { Transport, },

Transform set VPN: { esp-aes esp-sha256-hmac }

will negotiate = { Tunnel, },

**R2#show crypto map**

Interfaces using crypto map NiStTeSt1:

Crypto Map IPv4 "VPNMap" 1 ipsec-isakmp

Peer = 2.2.2.1

Extended IP access list 101

access-list 101 permit tcp 3.3.3.0 0.0.0.255 1.1.1.0 0.0.0.255

access-list 101 permit ip 3.3.3.0 0.0.0.255 1.1.1.0 0.0.0.255

Current peer: 2.2.2.1

Security association lifetime: 4608000 kilobytes/3600 seconds

Responder-Only (Y/N): N

PFS (Y/N): N

Mixed-mode : Disabled

Transform sets={

VPN: { esp-aes esp-sha256-hmac } ,

}

Interfaces using crypto map VPNMap:

GigabitEthernet0/0/0

**Verification**

**R1#ping 3.3.3.1 source loopback 0**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 3.3.3.1, timeout is 2 seconds:

Packet sent with a source address of 1.1.1.1

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 3/3/3 ms

**R1#show crypto ipsec sa**

interface: GigabitEthernet0/0/0

Crypto map tag: VPNMap, local addr 2.2.2.1

protected vrf: (none)

local ident (addr/mask/prot/port): (1.1.1.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (3.3.3.0/255.255.255.0/0/0)

current\_peer 2.2.2.2 port 500

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

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4

#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4

#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.: 2.2.2.1, remote crypto endpt.: 2.2.2.2

plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/0

current outbound spi: 0xAB764184(2876653956)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x7C5B020C(2086339084)

transform: esp-aes esp-sha256-hmac ,

in use settings ={Tunnel, }

conn id: 2001, flow\_id: ESG:1, sibling\_flags FFFFFFFF80004048, crypto map: VPNMap

sa timing: remaining key lifetime (k/sec): (4607999/3588)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0xAB764184(2876653956)

transform: esp-aes esp-sha256-hmac ,

in use settings ={Tunnel, }

conn id: 2002, flow\_id: ESG:2, sibling\_flags FFFFFFFF80004048, crypto map: VPNMap

sa timing: remaining key lifetime (k/sec): (4607999/3588)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

protected vrf: (none)

local ident (addr/mask/prot/port): (1.1.1.0/255.255.255.0/6/0)

remote ident (addr/mask/prot/port): (3.3.3.0/255.255.255.0/6/0)

current\_peer 2.2.2.2 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.: 2.2.2.1, remote crypto endpt.: 2.2.2.2

plaintext mtu 1500, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/0

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#ping 3.3.3.1 source GigabitEthernet0/0/0**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 3.3.3.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

**R1#show crypto ipsec sa**

interface: GigabitEthernet0/0/0

Crypto map tag: VPNMap, local addr 2.2.2.1

protected vrf: (none)

local ident (addr/mask/prot/port): (1.1.1.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (3.3.3.0/255.255.255.0/0/0)

current\_peer 2.2.2.2 port 500

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

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4

#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4

#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.: 2.2.2.1, remote crypto endpt.: 2.2.2.2

plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/0

current outbound spi: 0xAB764184(2876653956)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x7C5B020C(2086339084)

transform: esp-aes esp-sha256-hmac ,

in use settings ={Tunnel, }

conn id: 2001, flow\_id: ESG:1, sibling\_flags FFFFFFFF80004048, crypto map: VPNMap

sa timing: remaining key lifetime (k/sec): (4607999/3573)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0xAB764184(2876653956)

transform: esp-aes esp-sha256-hmac ,

in use settings ={Tunnel, }

conn id: 2002, flow\_id: ESG:2, sibling\_flags FFFFFFFF80004048, crypto map: VPNMap

sa timing: remaining key lifetime (k/sec): (4607999/3573)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

protected vrf: (none)

local ident (addr/mask/prot/port): (1.1.1.0/255.255.255.0/6/0)

remote ident (addr/mask/prot/port): (3.3.3.0/255.255.255.0/6/0)

current\_peer 2.2.2.2 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.: 2.2.2.1, remote crypto endpt.: 2.2.2.2

plaintext mtu 1500, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/0

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:

**R2#show crypto ipsec sa**

interface: GigabitEthernet0/0/0

Crypto map tag: VPNMap, local addr 2.2.2.2

protected vrf: (none)

local ident (addr/mask/prot/port): (3.3.3.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (1.1.1.0/255.255.255.0/0/0)

current\_peer 2.2.2.1 port 500

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

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4

#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4

#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.: 2.2.2.2, remote crypto endpt.: 2.2.2.1

plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/0

current outbound spi: 0x7C5B020C(2086339084)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0xAB764184(2876653956)

transform: esp-aes esp-sha256-hmac ,

in use settings ={Tunnel, }

conn id: 2001, flow\_id: ESG:1, sibling\_flags FFFFFFFF80000048, crypto map: VPNMap

sa timing: remaining key lifetime (k/sec): (4607999/3418)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x7C5B020C(2086339084)

transform: esp-aes esp-sha256-hmac ,

in use settings ={Tunnel, }

conn id: 2002, flow\_id: ESG:2, sibling\_flags FFFFFFFF80000048, crypto map: VPNMap

sa timing: remaining key lifetime (k/sec): (4607999/3418)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

protected vrf: (none)

local ident (addr/mask/prot/port): (3.3.3.0/255.255.255.0/6/0)

remote ident (addr/mask/prot/port): (1.1.1.0/255.255.255.0/6/0)

current\_peer 2.2.2.1 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.: 2.2.2.2, remote crypto endpt.: 2.2.2.1

plaintext mtu 1500, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/0

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:

**Problems**

The first problem was encountered when trying to configure the ISAKMP key exchange policy. The **crypto isakmp policy <policy number>** command was not recognized by the Cisco IOS version. It was found that for the Cisco 4321 router used, the securityk9 software packaged is not enabled by default. The solution for this was to create a new license boot registration for the two routers used in the VPN connection. After reloading the routers, all the commands were enabled on the router.

The second problem was that the wrong hashing algorithm was configured in both the key exchange policy and the transform set. Originally, the SHA algorithm was used for both but for best practices, at least SHA-256 should be used. As a result, using the **no hash sha** command and **hash sha-256** in the isakmp policy configuration mode reconfigured the right hashing algorithm. For the transform set, the **no transform-set VPN esp-aes esp-sha-hmac** was used to remove the existing transform-set and the command **transform-set VPN esp-aes esp-sha256-hmac** was used to reconfigure it to use SHA-256.

**Conclusion**

VPNs are an increasingly important topic as internet security becomes more of a concern. With sophisticated attacking tools developed, IPSec offers a framework for sending secure packets that implements authentication, confidentiality, and integrity. The configured site-to-site solution creates a static VPN connection between two static endpoints. This implementation is important for creating secure connections between two locations and can serve as an important configuration for businesses with multiple company sites.