# REPORT ON SITE-TO-SITE VPN IMPLEMENTATION FOR MM NETWORK

Krish Patel

# Table of Contents



# 1.0 Introduction

As MM expands its operations, the need for secure communication channels between its geographically dispersed sites becomes vital. This report addresses the requirement to establish a secure link between the main Headquarters (HQ) and the company's server

farm. The primary objective is to protect data confidentiality and integrity as data traverses over the potentially insecure public internet. This will be achieved by implementing a Site-to-Site Virtual Private Network (VPN).

This document serves as a comprehensive guide for the Information Officer. It begins with Task 1, providing foundational knowledge about VPNs, comparing different VPN technologies suitable for site-to-site links, and explaining the crucial role of symmetric and asymmetric encryption in securing VPN communications. Task 2 outlines the practical implementation of an Internet Protocol Security (IPSec) Site-to-Site VPN using Cisco routers within Cisco Packet Tracer. This section explains the configuration process step-by-step, analyses the commands used (referencing provided logs), and presents verification results using standard testing methodologies and Cisco CLI show commands. The successful implementation in the simulated environment validates the design before potential deployment on the live network.

# 2.0 VPN Concepts and Technologies

## 2.1 What is a VPN?

A Virtual Private Network (VPN) is a technology that creates a secure, encrypted connection over a less secure network, such as the public internet. The purpose of a VPN is to establish a network tunnel using encryption technology in a public network to safely carry out directional data transmission and prevent others from sniffing (Xu et al., 2020). The core purpose of a VPN is to provide confidentiality (preventing eavesdropping), integrity (ensuring data hasn't been tampered with), and authentication (verifying the identity of the communicating parties).

VPNs work by establishing a logical connection, often called a tunnel, between two endpoints. Data originating from one endpoint destined for the other is first encrypted using agreed-upon cryptographic algorithms and keys. Encryption is the foundation to secure internet packets. However, it needs high-speed processing for encryption algorithms, which may restrain the speed of data delivery via the networks (Mahmmod et al., 2020). This encrypted data is then encapsulated within standard IP packets for transmission across the public network. At the receiving end, the process is reversed: the packet is de-encapsulated, and the data is decrypted using the shared key, restoring it to its original form. Authentication mechanisms ensure that only authorised devices or users can establish the VPN connection. This procedure allows businesses to securely extend their private network reach across public infrastructure, effectively creating a wide area network (WAN) that is both flexible and secure.

## 2.2 Types of VPNs

VPNs generally fall into two main categories based on their use case:

- **Remote Access VPN:** This type allows individual users, such as remote workers or travelling employees, to securely connect to their business’s central network resources (servers, printers, internal applications) from their personal devices (laptops, smartphones). The user typically initiates the connection using VPN client software installed on their device, which establishes a secure tunnel to a VPN gateway (often a firewall) at the business’s network edge. Once a VPN tunnel has been established between a teleworker’s client device and the business’s VPN gateway, the teleworker can access many of the business’s computing resources through the tunnel (Nyakommitta, 2020).

- **Site-to-Site VPN:** This type connects entire networks at different geographical locations, creating a single, cohesive private network across multiple sites. Instead of individual users initiating connections, network gateways (typically routers or firewalls) at the edge of each site's network are configured. IPSec provides a secure tunnel between two devices such as two directly connected routers (Sholihah, 2019). All traffic flowing between the connected sites that matches predefined criteria is automatically encrypted and sent through the VPN tunnel. This is ideal for businesses like MM needing to securely link their HQ network with a remote server farm or branch offices, allowing seamless and secure resource sharing between the locations. This report focuses solely on the implementation of a Site-to-Site VPN.

## 2.3 Site-to-Site VPN Technologies Comparison

Many protocols can be used to establish VPN tunnels. For Site-to-Site connections, the most common are PPTP, L2TP, and IPSec. Each offers different trade-offs between speed, security, and ease of configuration.

- *2.3.1. PPTP (Point-to-Point Tunneling Protocol):* Developed by Microsoft and others, PPTP is one of the oldest VPN protocols. PPTP (Point-to-Point Tunneling Protocol) is a network protocol used in the implementation of Virtual Private Networks (VPN). PPTP uses a client-server design that operates at Layer 2 of the OSI model (Putra, 2018). Its primary advantage is speed, largely due to its relatively weak encryption. It is also generally easy to configure and is widely supported on older operating systems. However, PPTP suffers from significant known security vulnerabilities. The authentication protocols it uses have been compromised, making it susceptible to attacks. Due to these security flaws, PPTP is discouraged for any connection requiring high-level security and is unsuitable for MM's requirements.
- *2.3.2. L2TP (Layer 2 Tunneling Protocol):* L2TP was developed as a replacement to PPTP. By itself, L2TP does not provide any encryption or confidentiality; it only creates the tunnel. To provide security, L2TP is almost always implemented in conjunction with IPSec. IPSec handles the encryption, authentication, and integrity checking for the data passing through the L2TP tunnel. The key difference between IPSEC tunnelling IP directly and L2TP tunnelling IP by way of PPP is that with IPSEC, the protocol used to do the tunneling is directly aware of the IP processing (Shea, 2025). This combination offers significantly better security than PPTP. Configuration is moderately complex due to the involvement of two protocols. Performance is generally slower than PPTP because of the double encapsulation and the stronger encryption provided by IPSec. While secure when paired with IPSec, using IPSec directly often provides similar security with potentially less overhead.
- *2.3.3. IPSec (Internet Protocol Security):* IPSec is not a single protocol, but a group of protocols designed to provide comprehensive security at the IP layer (Layer 3). IPSec is a widely used network layer protocol by VPN services for securing internet communications by providing confidentiality, integrity, and authenticity (S, 2023). IPSec operates in two main modes: Tunnel mode (encrypting the entire original IP packet and adding a new IP header, typically used for Site-to-Site VPNs) and Transport mode (encrypting only the payload, usually used for end-to-end security between hosts). Key protocols within the group include Authentication Header (AH) for integrity and authentication, and Encapsulating Security Payload (ESP) for confidentiality, integrity, and authentication. The Internet Key Exchange (IKE) protocol (versions 1 and 2) is used to find security parameters and establish secure

keying material. IPSec supports high-level encryption algorithms like AES and robust hashing algorithms like SHA. While its configuration can be complex due to the number of options and phases involved, its high level of security and flexibility make it the industry standard for Site-to-Site VPNs. Speed can be impacted by the chosen encryption strength and hardware capabilities, but modern hardware often includes cryptographic acceleration to prevent this.

- *2.3.4. Technology Selection Rationale:*
  Comparing the options for MM's requirement:
    - *PPTP:* Unacceptable due to severe security vulnerabilities.
    - *L2TP/IPSec:* Offers good security but relies on IPSec for it and adds L2TP overhead.
    - *IPSec:* Provides the highest level of security directly at the IP layer, is highly configurable, and is the industry standard for enterprise Site-to-Site connections.

Given the requirement to securely link the HQ and server farm, protecting potentially sensitive corporate data, the security features of IPSec make it the most suitable choice, despite its relative configuration complexity. The implementation in this report will utilise IPSec in Tunnel mode using ESP for confidentiality and integrity.

## 2.4 Encryption in VPNs

Encryption is the foundation of VPN security, rendering transmitted data unreadable without the correct key. VPNs leverage two fundamental types of encryption during their operation: symmetric and asymmetric.

- *2.4.1. Symmetric Encryption:*
  In the symmetric key technique, both Encryption and decryption are done based on a single key called a private key. It is also referred to as a secret key (Alenezi, 2020). The sender and receiver must possess the same key before secure communication can begin.
    - **Process:** Sender encrypts data with the shared key -> Sends encrypted data -> Receiver decrypts data with the same shared key.
    - **Advantages:** Very fast and efficient, making it ideal for encrypting large volumes of data, such as the actual user traffic flowing through an established VPN tunnel.
    - **Disadvantages:** The main challenge is secure key distribution; how do the sender and receiver securely agree on the shared key without an interceptor intercepting it? If the key is compromised, all communication encrypted with it is compromised.
    - **Example:** AES (Advanced Encryption Standard) is a widely implemented, strong symmetric encryption algorithm. The configuration for MM uses AES-256, indicating a key length of 256 bits, which provides a very high level of security.
- *2.4.2. Asymmetric Encryption:*
  Asymmetric key encryption uses public keys for encryption and different key for decryption it is also called private key (Yassein, 2017). The public key can be freely

distributed without compromising security, while the private key must be kept secret by the owner.

- **Process:** Data encrypted with the public key can only be decrypted with the corresponding private key. Conversely, data encrypted with the private key can be verified (or decrypted) using the public key, which is useful for digital signatures and authentication.
- **Advantages:** Solves the key distribution problem found in symmetric encryption. Allows secure communication initiation without a pre-shared secret channel. Also enables digital signatures for authentication and non-repudiation.
- **Disadvantages:** Significantly slower and more intensive than symmetric encryption, making it unsuitable for encrypting large amounts of data directly.
- **Example:** While RSA is a common asymmetric algorithm often used for digital certificates, the Diffie-Hellman key exchange algorithm is crucial in the context of IPSec's IKE phase. DH allows two parties, who have never met, to securely establish a shared secret (which will become the symmetric key) over an insecure channel, even if an eavesdropper intercepts their entire exchange. This exchange is protected by the difficulty of solving the discrete logarithm problem, underlined by asymmetric principles. The group 5 configured in the IKE policy refers to a specific Diffie-Hellman group, which determines the strength of the key exchange process. Authentication in the setup relies on a Pre-Shared Key (PSK), a simpler mechanism than digital certificates (which use RSA/DSA), but the initial secure establishment of session keys still relies on the DH exchange secured by the PSK.

- *2.4.3. Role in VPN Establishment (IKE Phases):*
  IKE exchange consists of two phases. As refers, the phase 1 exchange is based on identities and secrets. Phase 1 exchange happens once, and then allows multiple phase 2 connections, which relies on the session key established in phase 1 (Zhuli, 2010). IPSec VPNs combine the strengths of both encryption types during the two phases of the Internet Key Exchange (IKE) process:
  - **IKE Phase 1 (Management Connection):** The primary goal of Phase 1 is to authenticate the VPN peers (routers) and establish a secure, authenticated channel between them. This is where asymmetric cryptography stands out. The peers use the DH exchange to generate identical shared secret keys securely. This phase also negotiates the security parameters (ISAKMP policy) for the Phase 1 tunnel itself. This secure channel established in Phase 1 is then used to protect the negotiations for Phase 2. Asymmetric cryptography (DH) is used here because it allows secure key establishment over the untrusted internet without initially needing to send the sensitive symmetric keys across the wire directly. Authentication is achieved either via pre-shared keys or digital certificates.
  - **IKE Phase 2 (Data Connection - IPSec SAs):** Once the secure Phase 1 tunnel exists, Phase 2 negotiations occur through this protected channel. The purpose of Phase 2 is to negotiate the specific IPSec security parameters (the "Transform Set") that will be used to encrypt the actual user data. These parameters include the specific symmetric encryption algorithm (e.g., AES-256), the data integrity algorithm (e.g., SHA-HMAC), the IPSec protocol (ESP

or AH), and the mode (Tunnel or Transport). Multiple Phase 2 Security Associations (SAs) can be established for different types of traffic, protected by the single Phase 1 SA.

- **Symmetric encryption (AES-256 in this case)** is used for encrypting the bulk user data in Phase 2 because it is much faster and more efficient than asymmetric encryption, suitable for handling potentially high volumes of network traffic passing through the VPN tunnel.

In summary, VPNs use the slow but secure asymmetric principles (DH) during Phase 1 to securely establish the fast symmetric keys, which are then used during Phase 2 for efficient encryption of the actual data traffic. This two-phase approach leverages the best of both worlds: secure key exchange and efficient data protection.

# 3.0 IPSec Site-to-Site VPN Implementation and Testing

## 3.1 Scenario Overview

This section details the configuration and testing of the IPSec Site-to-Site VPN connecting MM's HQ network and the remote server farm network. The objective is to ensure that all IP traffic flowing between the internal LAN segment at HQ and the internal LAN segment at the server farm is encrypted and protected while crossing the simulated public internet link between the edge routers of the two sites. The configuration was completed using Cisco Packet Tracer.

## 3.2 Network Topology and Addressing

- HQ Router: Edge router at the Headquarters site.
  - External (WAN) interface GigabitEthernet0/1/0 IP: 10.10.100.1/30.
  - Internal (LAN) interface GigabitEthernet0/0 IP: 129.100.100.1/23, connecting to the HQ LAN network 129.100.100.0/23.
- FARM Router: Edge router at the Server Farm site.
  - External (WAN) interface GigabitEthernet0/1/0 IP: 10.10.100.2/30.
  - Internal (LAN) interface GigabitEthernet0/0 IP: 192.168.100.1/24, connecting to the FARM LAN network 192.168.100.0/24.
- WAN Link: The connection between the routers uses the 10.10.100.0/30 subnet, linking GigabitEthernet0/1/0 on HQ to GigabitEthernet0/1/0 on FARM.
- VPN Peers: HQ Router (10.10.100.1) and FARM Router (10.10.100.2).

## 3.3 Configuration Process Explained

Configuring an IPSec Site-to-Site VPN on Cisco routers involves logical steps, ensuring both ends agree on how to secure the communication:

- *3.3.1. Phase 1: ISAKMP/IKE Policy Configuration:* Define the parameters for establishing the initial secure management tunnel (IKE Phase 1 SA). This policy matches on both devices. Key parameters include:
  - encryption: Algorithm for securing Phase 1 negotiations (AES-256).
  - hash: Algorithm for ensuring integrity of Phase 1 messages (SHA).

    - authentication: Method for verifying peer identity (pre-share).
    - group: Diffie-Hellman group for secure key exchange strength (group 5).
    - lifetime: How long the Phase 1 SA remains valid before renegotiation.
- *3.3.2. Pre-Shared Key Configuration:* Define the secret key shared between the two peers. This key is used during the authentication part of Phase 1. The key is identical on both routers and associated with the peer's IP address.
- *3.3.3. Phase 2: IPSec Policy (Transform Set):* Define how the actual user data will be protected (IKE Phase 2 SAs). This specifies the combination of protocols and algorithms. Key parameters include:
    - protocol: ESP (for confidentiality and integrity).
    - encryption algorithm: Symmetric algorithm for data encryption (esp-aes 256).
    - integrity algorithm: Hashing algorithm for data integrity (esp-sha-hmac).
- *3.3.4. Defining Interesting Traffic (Access Control List - ACL):* Create an ACL to identify the traffic that will be encrypted and sent through the VPN tunnel. Traffic matching a permit statement in this ACL triggers the VPN process. The source and destination should be the internal networks that need to communicate securely. Traffic not matching this ACL will be transmitted without encryption.
- *3.3.5. Crypto Map Configuration:* This links all the previous elements together. A crypto map entry links the ACL, the peer's IP address, and the IPSec transform sets. It also defines the complete IPSec policy to be applied.
- *3.3.6. Applying Crypto Map to Interface:* Apply the configured crypto map to the router's external-facing (WAN) interface. This activates the IPSec policy on that interface, causing the router to assess outbound traffic against the crypto map's ACL.
- *3.3.7. Routing Considerations:* Ensure the router knows how to reach the peer's external IP address. This could be via a default route to the internet or a specific static route. Additionally, the router needs to know that the remote internal network is reachable via the VPN peer.

## 3.4 Configuration Walkthrough (Based on Provided CLI - FARM Router)

The provided CLI log shows the configuration steps performed on the FARM router (10.10.100.2). A corresponding configuration, with relevant IP addresses and network definitions adjusted, was also applied to the HQ router (10.10.100.1) to establish the Site-to-Site VPN tunnel. The following analysis details the specific commands applied on the FARM router as shown in the log:

### 3.4.1. ISAKMP (IKE Phase 1) Policy:

```
FARM>enable
FARM#conf
FARM#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
FARM(config)#lic
FARM(config)#license b
FARM(config)#license boot m
FARM(config)#license boot module c
FARM(config)#license boot module c2900 te
FARM(config)#license boot module c2900 technology-package se
FARM(config)#license boot module c2900 technology-package securityk9
```

```
FARM(config)#exit
FARM#
%SYS-5-CONFIG_I: Configured from console by console

FARM#wr
Building configuration...
[OK]
FARM#rel
FARM#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO2911/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 72/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test

____________________
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x3bcd3d8
Self decompressing the image :
################################################
```

Copy

```
FARM>enab
FARM>enable
FARM#conf
FARM#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
FARM(config)#crypto isakmp policy 10
FARM(config-isakmp)#encryption aes 256
FARM(config-isakmp)#hash sha
FARM(config-isakmp)#authentication pre-share
FARM(config-isakmp)#group 5
FARM(config-isakmp)#lifetime 86400
FARM(config-isakmp)#exit
FARM(config)#
```

*Explanation:* As a requirement, the securityk9 technology package license is activated (license boot, wr, reload) to enable the necessary cryptographic features on the FARM router. Following this, the ISAKMP policy (priority 10) is configured using crypto isakmp policy 10. This command block defines the essential parameters for the IKE Phase 1 negotiation with the peer (10.10.100.1), specifying AES-256 encryption, SHA hashing, pre-shared key authentication, Diffie-Hellman group 5 for key exchange strength, and an 86400-second (1 day) lifetime for the security association. This policy matches the configuration on the HQ peer router for the initial secure tunnel (Phase 1 SA).

### *3.4.2. Pre-Shared Key:*

```
FARM(config)#crypto isakmp key VPNSECRETKEY address 10.10.100.1
```

*Explanation:* Sets the shared secret VPNSECRETKEY to be used when authenticating with the peer at IP address 10.10.100.1 (HQ Router).

### *3.4.3. IPSec Transform Set (IKE Phase 2):*

```
FARM(config)#crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac
```

*Explanation:* Defines the set of protocols/algorithms VPN-SET for protecting user data (Phase 2): ESP protocol using AES-256 for encryption and SHA-HMAC for integrity.

### *3.4.4. Access Control List (ACL):*

```
FARM(config)#ip access-list extended VPN-ACL
FARM(config-ext-nacl)#permit ip 192.168.100.0 0.0.0.255 10.10.100.0 0.0.0.3
FARM(config-ext-nacl)#exit
```

*Explanation*: This command configures an extended IP Access Control List named VPN-ACL. This ACL aims to identify the specific IP traffic flows that will be subject to the IPSec encryption policy defined in the associated crypto map. The permit statement defines this traffic as any IP packet originating from the 192.168.100.0/24 network (source address 192.168.100.0 with wildcard mask 0.0.0.255), corresponding to the FARM internal LAN segment. The destination specified is the 10.10.100.0/30 network (destination address 10.10.100.0 with wildcard mask 0.0.0.3), corresponds to the network segment applied for the direct WAN connection between the HQ and FARM routers. Consequently, IP traffic matching these source and destination network parameters is designated as "interesting traffic" for potential IPSec processing.

#### *3.4.5. Crypto Map:*

```
FARM(config)#crypto map VPN-MAP 10 ipsec-isakmp
FARM(config-crypto-map)#set peer 10.10.100.1
FARM(config-crypto-map)#set transform-set VPN-SET
FARM(config-crypto-map)#match address VPN-ACL
FARM(config-crypto-map)#exit
```

*Explanation:* Creates crypto map VPN-MAP, sequence 10. It connects the peer, transform set, and ACL together.

#### *3.4.6. Interface Application & Routing:*

```
FARM(config)#interface g0/1/0
FARM(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
FARM(config-if)#exit
FARM(config)#ip route 10.10.100.0 255.255.255.252 10.10.100.1
```

*Explanation:* Applies the crypto map VPN-MAP to the physical WAN interface GigabitEthernet0/1/0. ISAKMP process is activated. A static route is added, to ensure reachability to the peer's subnet via the peer itself.

## 3.5 Testing and Verification Strategy

To confirm the VPN is operational and securing traffic as intended, the following tests were performed:

1. **Connectivity Test (Ping):** Ping from a device on the HQ LAN (10.10.100.1) to a device on the FARM LAN (192.168.100.1), and vice-versa. Successful pings imply end-to-end reachability, via the tunnel.
2. **Path Verification (Traceroute):** Use traceroute from HQ LAN to FARM LAN. The output shows the packet going to the local router, then appearing at the remote router, hiding the public internet hops, indicating traffic is being tunnelled.
3. **VPN Status Verification (Show Commands):** Cisco IOS to show commands on both edge routers to check the status of the VPN tunnels.
    - show crypto isakmp sa: Verifies IKE Phase 1 Security Associations. Shows peer IP’s and state
    - show crypto ipsec sa: Verifies IKE Phase 2 Security Associations. Shows details about the actual data tunnel, including traffic encrypted/decrypted counts, peer IPs, Security Parameter Index (SPIs), transform set used, Non-zero packet counts confirm traffic is flowing through the tunnel.

## 3.6 Verification Results

The images below show the output of verification commands, run on the HQ router (10.10.100.1) after configuration and traffic initiation.

### *3.6.1. show crypto isakmp sa Output Analysis:*

```
HQ#show crypto is
HQ#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.10.100.2     10.10.100.1     QM_IDLE           1043    0 ACTIVE
```

*Explanation:* This output confirms:

- An IKE Phase 1 Security Association (SA) exists.
- The local endpoint (src) is 10.10.100.1 (HQ).
- The remote endpoint (dst) is 10.10.100.2 (FARM).
- The state is QM_IDLE. This is the expected state for a successfully established Phase 1 tunnel that is idle.
- The status is ACTIVE, indicating the Phase 1 SA is valid and operational.
- This confirms successful completion of IKE Phase 1 negotiation between the peers.

### *3.6.2. show crypto ipsec sa Output Analysis:*

```
local crypto endpt.: 10.10.100.1, remote crypto endpt.:10.10.100.2
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1/0
current outbound spi: 0x6D03B3D6(1828959190)

inbound esp sas:
 spi: 0x0062DE30(6479408)
   transform: esp-aes 256 esp-sha-hmac ,
   in use settings ={Tunnel, }
   conn id: 2008, flow_id: FPGA:1, crypto map: VPN-MAP
   sa timing: remaining key lifetime (k/sec): (4525504/3490)
   IV size: 16 bytes
   replay detection support: N
   Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
 spi: 0x6D03B3D6(1828959190)
   transform: esp-aes 256 esp-sha-hmac ,
   in use settings ={Tunnel, }
   conn id: 2009, flow_id: FPGA:1, crypto map: VPN-MAP
   sa timing: remaining key lifetime (k/sec): (4525504/3490)
   IV size: 16 bytes
   replay detection support: N
   Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

*Explanation:* This output confirms details about the IKE Phase 2 SAs:

- **Peers:** Confirms local (10.10.100.1) and remote (10.10.100.2) endpoints.
- **Interface:** Identifies the outbound interface associated with this SA (GigabitEthernet0/1/0).
- **Inbound SA:** Details for traffic received from the peer (10.10.100.2) and decrypted locally.
    - spi: Security Parameter Index used by the peer to send encrypted traffic *to* us.
    - transform: Shows the security protocols used (ESP with AES 256 encryption and SHA-HMAC integrity), matching our VPN-SET configuration.
    - in use settings: Confirms Tunnel mode is used.
    - crypto map: Shows the SA was established based on the VPN-MAP crypto map.
    - Status: ACTIVE: Confirms the inbound SA is operational.
- **Outbound SA:** Details for traffic being encrypted locally and sent to the peer (10.10.100.2).
    - spi: SPI that this router (10.10.100.1) uses to send encrypted traffic *to* the peer. This matches the current outbound spi.
    - transform, in use settings, crypto map, Status: ACTIVE: Confirms matching configuration and operational status for outbound traffic.
- **Lifetime:** Shows remaining key lifetime.
- **Replay Detection:** Shows 'N' (No).

Together, these show command outputs demonstrate that both Phase 1 and Phase 2 tunnels have been successfully established and are active between the HQ and FARM routers using the configured IPSec parameters. In addition, ping tests were successful, confirming the VPN is functional.

## 4.0 Conclusion

The implementation of the Site-to-Site IPSec VPN between MM's HQ and server farm has been successfully designed, configured, and tested within Cisco Packet Tracer. By leveraging the security features of the IPSec protocol suite, specifically ESP with AES-256 encryption and SHA-HMAC integrity, a secure tunnel has been established over the simulated public WAN link. The configuration process, involving the setup of IKE Phase 1 and Phase 2 policies, definition of traffic via ACLs, and application of crypto maps, was detailed and verified. The successful verification using ping, traceroute, and Cisco IOS show crypto isakmp sa and show crypto ipsec sa commands confirms that the VPN provides a secure, encrypted path for data transmission between the two sites, meeting the project's security objectives. This successful simulation provides confidence for deployment on the live network.

# 5.0 Recommendations

While the basic VPN functionality is confirmed, the following recommendations should be considered for improving security and manageability in a production environment:

1. **Enable Anti-Replay:** The show crypto ipsec sa output indicates replay detection is not enabled (replay detection support: N). Enabling anti-replay protection (usually default but can be enabled within the crypto map or globally) is recommended to prevent attackers from capturing and re-injecting old packets. Anti-replay protection allows a receiving node to identify replayed messages and discard them
2. **Stronger Authentication:** While Pre-Shared Keys (PSKs) are simple to configure, they represent a single point of failure if compromised and do not scale well. Consider migrating to digital certificates using RSA or ECDSA signatures for peer authentication, which provides a robust identity verification and better scalability.
3. **Perfect Forward Secrecy (PFS):** Ensure Perfect Forward Secrecy (PFS) is enabled for IKE Phase 2 (e.g., set pfs group5 within the crypto map). “PFS means that the leakage of a long-used master key does not lead to the leakage of a past session key” or in other words past session keys cannot be retrieved in the case that Phase 1 keys are compromised (Ge, 2022).
4. **Monitoring and Logging:** Implement monitoring of the VPN tunnel status (up/down) and traffic statistics. Configure routers to log significant VPN events (tunnel establishment, failures) to a central syslog server for auditing and troubleshooting.
5. **Redundancy:** For business stability, consider implementing a redundant VPN tunnel, potentially using a secondary internet connection or configuring failover mechanisms between primary and backup VPN gateways.
6. **Regular Policy Review:** Periodically review and update the encryption algorithms, hash functions, and DH groups used in the IKE and IPSec policies to ensure they align with current security best practices and standards.

# 6.0 References

**Works Cited**

Alenezi, Mohammed, et al. “Symmetric Encryption Algorithms: Review and Evaluation Study Haneen Alabdulrazzaq Public Authority for Applied Education and Training Symmetric Encryption Algorithms: Review and Evaluation Study.” *International Journal of Communication Networks and Information Security (IJCNIS*, vol. 767, no. 2, 2020, p. 256, www.researchgate.net/profile/Haneen-Alabdulrazzaq/publication/349324592_Symmetric_Encryption_Algorithms_Review_and_Evaluation_study/links/602acfa7a6fdcc37a82c0189/Symmetric-Encryption-Algorithms-Review-and-Evaluation-study.pdf.

Ge, Mingchang, et al. “AuthPFS: A Method to Verify Perfect Forward Secrecy in Authentication Protocols.” *Taiwan Ubiquitous Information*, vol. 7, no. 3, 2022, bit.kuas.edu.tw/~jni/2022/vol7/s3/12.JNI0401.pdf. Accessed 20 Apr. 2025.

Mahmmod, Khalid F., et al. “IPsec Cryptography for Data Packets Security within VPN Tunneling Networks Communications.” *2020 International Conference on Electrical Engineering and Informatics (ICELTICs)*, vol. 1, no. 1, 27 Oct. 2020, https://doi.org/10.1109/iceltics50595.2020.9315407. Accessed 15 July 2021.

Nyakomitta, P.S. and Abeka, S.O. (2020) 'Security investigation on remote access methods of virtual private network', *Global Journal of Computer Science and Technology: E Network, Web & Security*, 20(1), pp. 27-35.

Putra, Chrystia Aji, et al. “Point to Point Protocol Tunneling VPN Simulation and Analysis on Sniffing.” *Www.atlantis-Press.com*, Atlantis Press, 1 Dec. 2018, www.atlantis-press.com/proceedings/icst-18/55911005. Accessed 27 Sept. 2022.

Raymond, David R., et al. “Scalable, Cluster-Based Anti-Replay Protection for Wireless Sensor Networks.” *2007 IEEE SMC Information Assurance and Security Workshop*, vol. 1, no. 1, June 2007, pp. 127–134, ieeexplore.ieee.org/abstract/document/4267552, https://doi.org/10.1109/iaw.2007.381924. Accessed 20 Apr. 2025.

S, Amaldeep, and Sriram Sankaran. “Cross Protocol Attack on IPSec-Based VPN.” *IEEE Xplore*, 1 May 2023, ieeexplore.ieee.org/abstract/document/10131787.

Shea, Richard. “L2TP.” *Google Books*, 2025, books.google.co.uk/books?hl=en&lr=&id=ydKQ4YKc_xsC&oi=fnd&pg=PR13&dq=l2tp+tunneling+protocol&ots=i4QVdJfjc7&sig=RZm_vZJaS8a0VlvPSzhUMRszUJc&redir_esc=y#v=onepage&q=ipsec&f=false. Accessed 20 Apr. 2025.

Sholihah, W, et al. “Information and Communication System Technology with VPN Site-To-Site IPsec.” *Journal of Physics: Conference Series*, vol. 1193, no. 1, Apr. 2019, p. 012012, https://doi.org/10.1088/1742-6596/1193/1/012012.

Xu, Zhiwei, and Jie Ni. “Research on Network Security of VPN Technology.” *IEEE Xplore*, 1 Dec. 2020, ieeexplore.ieee.org/document/9418865/.

Yassein, Muneer Bani, et al. “Comprehensive Study of Symmetric Key and Asymmetric Key Encryption Algorithms.” *2017 International Conference on Engineering and Technology (ICET)*, vol. 1, no. 1, Aug. 2017, ieeexplore.ieee.org/document/8308215?arnumber=8308215, https://doi.org/10.1109/icengtechnol.2017.8308215.

Zhuli, Meng, et al. “Context Based Deep Packet Inspection of IKE Phase One Exchange in IPSec VPN.” *2010 International Conference on Innovative Computing and Communication and 2010 Asia-Pacific Conference on Information Technology and Ocean Engineering*, vol. 1, no. 1, 2010, pp. 3–6, ieeexplore.ieee.org/abstract/document/5439287, https://doi.org/10.1109/cicc-itoe.2010.8. Accessed 20 Apr. 2025.