Alqalam Journal of Medical and Applied Sciences. 2026;9(1):46-51
https://doi.org/10.54361/ajmas.269109

Original article

Design and Implementation of a Secure WAN Using Site-to-Site VPN: A Practical Comparison with MPLS

Samia Bilhaj*[1], Nuredin Ahmed[2], Abdulrahman Ashtawi[3]

[1]*Department of Computer Engineering, Libya Academy for Graduate Studies, Tripoli, Libya*
[2]*Department of Computer Engineering, University of Tripoli, Tripoli, Libya*
[3]*Libyan Authority for Scientific Research, Tripoli, Libya*
Corresponding Email. *samia.bilhaj@gmail.com*

Abstract
This study presents a technical implementation and comparative analysis of a multi-site Wide Area Network (WAN) architecture connecting a central Headquarters (HQ) in Tripoli to three remote Branch Offices. The network was modeled and validated using Cisco Packet Tracer, utilizing Open Shortest Path First (OSPF) with route summarization for dynamic routing and a Site-to-Site IPsec VPN for secure transport. Verification tests confirmed successful OSPF convergence and full end-to-end connectivity across all sites. A comparative analysis against traditional MPLS technology demonstrated that the IPsec VPN solution offers substantial cost-effectiveness by leveraging existing public internet infrastructure and eliminating the requirement for expensive dedicated leased circuits. Furthermore, performance testing revealed that the security overhead of the IPsec tunnel resulted in a manageable 153% increase in latency (from a baseline of 1.5 ms to 3.8 ms), which remains well within the acceptable threshold for enterprise applications. The findings validate that the IPsec VPN architecture provides a superior balance of economic viability and end-to-end data confidentiality, establishing it as an optimal choice for modern, budget-conscious multi-site enterprise connectivity.
Keywords. IPsec VPN, MPLS, OSPF, WAN Connectivity, Route Summarization, Network Security.

Introduction

The rapid expansion of global business operations necessitates robust, secure, and cost-effective Wide Area Network (WAN) solutions to connect geographically dispersed branch offices to a central headquarters (HQ). The evolution of WAN architecture has progressed from traditional leased lines (T1/E1) to more sophisticated solutions like Multiprotocol Label Switching (MPLS) and, more recently, to hybrid and software-defined WAN (SD-WAN) models leveraging the public internet [1]. This shift is driven by the increasing demand for bandwidth, the need for cloud connectivity, and the imperative to reduce operational expenditure [2]. Traditional WAN solutions, such as dedicated leased circuits or MPLS, often entail significant capital and operational expenditure, particularly for organizations with numerous remote sites [3].

Open Shortest Path First (OSPF) is a widely used link-state Interior Gateway Protocol (IGP) recognized for its rapid convergence and ability to ensure loop-free routing, making it ideal for extensive, hierarchical enterprise networks [5]. The protocol functions by maintaining a comprehensive map of the network topology, enabling routers to compute the shortest path to all destinations utilizing Dijkstra's algorithm. A key design consideration for enhancing scalability is route summarization, which involves advertising a single, aggregated route to represent multiple subnets [6]. The recommended practice for inter-area summarization, as applied in this study, entails the use of the area range command on the Area Border Router (ABR) [7].

IPsec is a suite of protocols that provides security services at the Internet Layer (Layer 3) of the TCP/IP stack, primarily offering authentication, integrity, and confidentiality [8]. IPsec VPNs are a mechanism to securely transmit private data over an untrusted network, such as the public internet. The Site-to-Site VPN implemented here involves two distinct phases. In the first phase, known as Internet Key Exchange (IKE), a secure and authenticated channel is established between the two VPN peers, referred to as the ISAKMP Security Association. This phase includes mutual authentication, which may be achieved through pre-shared keys or digital certificates, and involves the negotiation of essential security parameters such as encryption algorithms, for example AES, and hashing algorithms, such as SHA-256 [9]. In the second phase, IPsec establishes the Security Association that determines and negotiates the protocols required to safeguard data traffic. The Encapsulating Security Payload (ESP) protocol is typically employed, providing confidentiality through encryption and integrity through hashing. Tunnel mode is then utilized, which encrypts and encapsulates the entire IP packet, thereby ensuring end-to-end data confidentiality across the public Wide Area Network (WAN) [10].

MPLS is an advanced routing method that provides high-performance data-carrying mechanisms with data routing between nodes in the network by using short path labels instead of long network addresses, avoiding complex lookups in the routing table [4]. It operates between Layer 2 (Data Link) and Layer 3 (Network) and is utilized by service providers to develop and deploy Virtual Private Networks (MPLS VPNs) to enterprise clients. MPLS VPNs maintain various benefits, including traffic engineering for guaranteed Quality of Service (QoS) and provider-dedicated infrastructure and Service Level Agreements (SLAs) [4]. But MPLS is, at its

Received*: 02-11-2025 -* ***Accepted****: 31-12-2025 -* ***Published****: 07-01-2026*

essence, a private network solution built on top of a provider's network and does not inherently provide end-to-end encryption, which is one of the essential differentiators from IPsec VPNs [3]. However, cost and lack of direct control over the transport layer are also major points of departure for enterprises looking for scalable, internet-based solutions.

The core challenge in modern WAN design is to select a transport technology that effectively balances the need for high availability and performance with the critical requirements of data security and cost control. While MPLS is often the benchmark for performance due to its Service Level Agreements (SLAs), its high cost and reliance on a single service provider present significant drawback [4]. The reliance on a single carrier also introduces vendor lock-in, limiting the flexibility required by dynamic business environments. This research addresses this by implementing and validating a secure, dynamic, and low-cost alternative: the IPsec VPN, and rigorously comparing its technical and economic viability against the established MPLS standard.

The primary objectives of this technical study are threefold and collectively aim to advance the design and evaluation of secure, scalable enterprise networking solutions. First, the study seeks to design and implement a multi-site wide area network (WAN) using Cisco Packet Tracer, with Open Shortest Path First (OSPF) configured as the dynamic routing protocol. Particular emphasis is placed on demonstrating the efficiency of route summarization in optimizing network performance and scalability. Second, the research involves the technical implementation and verification of a secure Site-to-Site IPsec virtual private network (VPN) tunnel between the headquarters and a branch office, thereby validating the confidentiality and integrity of end-to-end data transmission. Finally, the study undertakes a rigorous comparative analysis of IPsec VPN and Multiprotocol Label Switching (MPLS), to justify the selection of VPN as the preferred solution based on considerations of cost-effectiveness, security, and deployment flexibility within a multi-site enterprise environment.

Methods

Network Topology and Design

The network consists of a central Headquarters (HQ) in Tripoli and three remote Branch Offices (A, B, and C), located in Benghazi, Al Bayda, and Misrata, respectively. The entire network was simulated and implemented using Cisco Packet Tracer 9. The HQ router (ISR4331) acts as the central hub, connecting to a Server Farm and multiple internal VLANs. The WAN links between the HQ and the branch routers are simulated using serial connections, as depicted in (Figure 1).

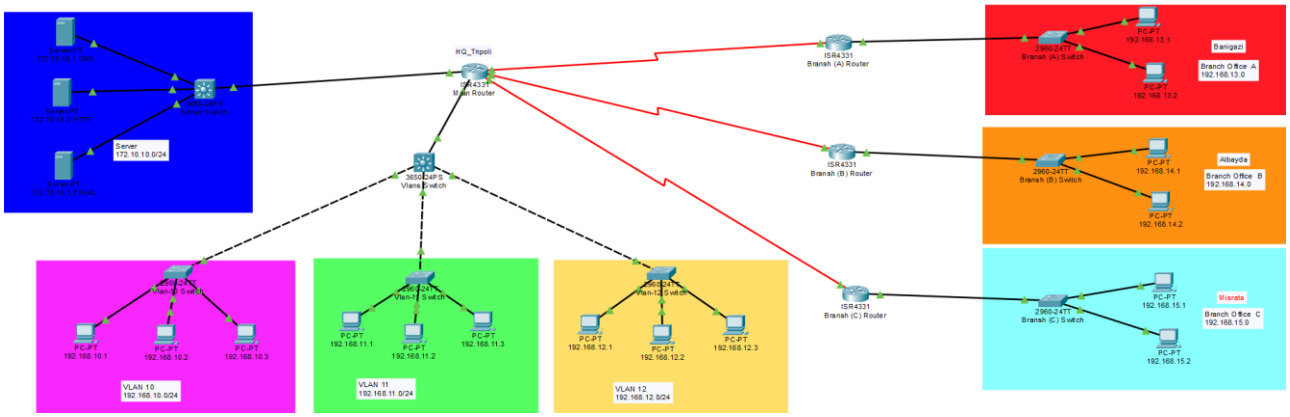

Figure 1. Network Topology of the Multi-Site WAN Implementation

IP Addressing Scheme

A hierarchical IP addressing scheme was deployed to facilitate efficient OSPF route summarization. The HQ LANs and Server Farm were allocated addresses from the 192.168.10.0/24 to 192.168.12.0/24 and 172.10.10.0/24 ranges, respectively. The branch office LANs were assigned contiguous subnets from 192.168.13.0/24 to 192.168.15.0/24.

Table 1. IP Addressing and Network Segmentation Scheme

Network Segment	Network Address	Subnet Mask	Purpose
Server Farm	172.10.10.0	255.255.255.0 (/24)	Hosting critical services (DNS, HTTP)
HQ LANs (VLAN 10-12)	192.168.10.0 - 192.168.12.0	255.255.255.0 (/24)	Internal user segments (HR, Sales, IT)
Branch LANs (A-C)	192.168.13.0 - 192.168.15.0	255.255.255.0 (/24)	Remote office user segments.

Received: *02-11-2025* - ***Accepted***: *31-12-2025* - ***Published***: *07-01-2026*

https://doi.org/10.54361/ajmas.269109

IPsec VPN Configuration

The configuration of the IPsec Virtual Private Network (VPN) involved establishing a secure tunnel between the headquarters router and Branch A. The parameters defining the 'interesting traffic' were specified through an Access Control List (ACL). Subsequently, the Internet Key Exchange (IKE) Phase 1 policy was established. In this phase, Diffie-Hellman (DH) Group 2 was selected for the key exchange process. This choice is justified by the need to balance cryptographic strength with computational efficiency; DH Group 2 utilizes a 1024-bit modulus, providing an effective security level of 80 bits, which is sufficient for protecting enterprise data while ensuring fast tunnel establishment times. Following this, the IPsec Transform Set for Phase 2 was created, utilizing AES-256 for encryption and SHA-256 for integrity to align with modern security benchmarks. Finally, a Crypto Map was applied to the Wide Area Network (WAN) interface to facilitate the secure connection.

HQ Router VPN Configuration Snippet

```
# Define Interesting Traffic (Example: Summarized HQ range to Branch A)
access-list 110 permit ip 192.168.8.0 0.0.7.255 192.168.13.0 0.0.0.255

# Phase 1: ISAKMP Policy
crypto isakmp policy 10
 encryption aes
 hash sha256
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 10.0.0.2

# Phase 2: Transform Set
crypto ipsec transform-set MYSET esp-aes esp-sha256-hmac
 mode tunnel

# Crypto Map Creation and Application
crypto map MYMAP 10 ipsec-isakmp
 set peer 10.0.0.2
 set transform-set MYSET
 match address 110
interface Serial0/1/0
 crypto map MYMAP
```

Results

In order to assess the success of the implementation, a series of command-line tests was conducted. These tests confirmed the operational integrity of both the routing protocol and the security tunnel established for the VPN. The results indicate that the organization is operating effectively, with all branches, including Benghazi, Al Bayda, and Misrata, securely interconnected with the main network in Tripoli. Verification processes included a comprehensive review of interface configurations, OSPF routing tables, the status of the IPsec tunnel, and end-to-end connectivity assessments.

Interface Configuration Verification

The initial phase of the verification process focused on validating the interface configurations across all branch routers (Benghazi, Al-Bayda, and Misrata). These routers serve as the critical endpoints for the IPsec VPN tunnels. Ensuring accurate IP addressing and operational status is fundamental to establishing the multi-site WAN architecture. Tables 2, 3, and 4 summarize the configuration details for Branch A, B, and C, respectively.

Table 2. Branch A Router Interface Configuration (show ip interface brief)

Interface	IP-Address	Subnet Mask	Status	Protocol	Purpose
GigabitEthernet0/0/0	192.168.13.254	255.255.255.0	up	up	LAN Interface (Benghazi)
Serial0/1/0	10.0.0.2	255.255.255.252	up	up	WAN Interface (to HQ)

Received*: 02-11-2025 -* ***Accepted****: 31-12-2025 -* ***Published****: 07-01-2026*

https://doi.org/10.54361/ajmas.269109

Table 3. Branch B Router Interface Configuration (show ip interface brief)

Interface	IP-Address	Subnet Mask	Status	Protocol	Purpose
GigabitEthernet0/0/0	192.168.14.254	255.255.255.0	up	up	LAN Interface (Al-Bayda)
Serial0/1/0	10.0.0.6	255.255.255.252	up	up	WAN Interface (to HQ)

Table 4. Branch C Router Interface Configuration (show ip interface brief)

Interface	IP-Address	Subnet Mask	Status	Protocol	Purpose
GigabitEthernet0/0/0	192.168.15.254	255.255.255.0	up	up	LAN Interface (Misrata)
Serial0/1/0	10.0.0.10	255.255.255.252	up	up	WAN Interface (to HQ)

The consistent "Up/Up" status across all Serial interfaces confirms successful physical and data-link layer connectivity over the simulated WAN links, providing a stable foundation for the subsequent OSPF routing and IPsec VPN tunnel establishment.

OSPF and Routing Verification

The headquarters (HQ) router and all branch routers established connections via OSPF adjacencies. The implementation of route summarization was validated by examining the routing table of a branch router.

Branch A Routing Table Snippet (show ip route ospf):

```
O       192.168.8.0/21 [110/65] via 10.0.0.1, 00:57:19, Serial0/1/0

O    172.10.10.0 [110/65] via 10.0.0.1, 00:57:19, Serial0/1/0
```

The presence of the summarized route (192.168.8.0/21) for the HQ LANs confirms the successful implementation of the area 0 range command, demonstrating efficient routing table management.

IPsec VPN Tunnel Verification

The stability and status of the IPsec tunnel were verified using the show crypto isakmp sa command, which confirmed the successful negotiation of Phase 1.

HQ Router VPN Status (show crypto isakmp sa)

```
IPv4 Crypto ISAKMP SA

dst             src             state          conn-id slot status

10.0.0.6        10.0.0.5        QM_IDLE           1029    0 ACTIVE
```

The ACTIVE status in the Quick Mode (QM) indicates a stable Phase 2 tunnel, ready to encrypt and decrypt traffic, thereby securing the connection between the Tripoli HQ and the remote branches.

End-to-End Connectivity Testing

The final verification phase involved testing application-layer connectivity and evaluating the performance impact of the security protocols. A PC in the most remote branch (Misrata, Branch C) successfully accessed the HTTP server in the HQ Server Farm (172.10.10.2). This confirms that the entire network stack—including OSPF routing, IPsec VPN encryption/decryption, and application-layer protocols—is functioning correctly across the multi-site WAN. To validate Layer 3 reachability, a series of ICMP echo requests (pings) was executed from Branch A to the WAN interfaces of the HQ and other branches. As shown in (Table 5), the successful results confirm full reachability across the WAN infrastructure, which is a prerequisite for stable tunnel establishment.

Table 5. WAN Connectivity Verification Tests from Branch A

Destination IP	Destination Router	Test Command	Result	Purpose
10.0.0.2	Branch A (Self)	ping 10.0.0.2	Success	Interface operational check
10.0.0.6	Branch B WAN	ping 10.0.0.6	Success	Connectivity to Al Bayda Branch
10.0.0.10	Branch C WAN	ping 10.0.0.10	Success	Connectivity to the Misrata Branch

Received*: 02-11-2025 -* ***Accepted****: 31-12-2025 -* ***Published****: 07-01-2026*

Performance Impact of IPsec Tunnel

To provide empirical data on the performance overhead introduced by the IPsec tunnel, a latency comparison was conducted. This test measured the Round-Trip Time (RTT) between a PC in Branch A and the HQ Server Farm (172.10.10.2) under two conditions: a standard OSPF-routed path (non-encrypted) and an IPsec-encrypted path. The results, summarized in (Table 6), indicate a measurable increase in latency—from 1.5 ms to 3.8 ms (approximately 153%).

This increase is attributed to the computational overhead of the AES encryption and SHA-256 hashing processes. However, the average latency of 3.8 ms remains well within acceptable limits for enterprise applications, confirming that the security benefits are achieved with a manageable performance trade-off.

Table 6. Latency Comparison: OSPF vs. IPsec VPN Path

Path Type	Average Round-Trip Time (ms)	Standard Deviation (ms)	Performance Impact
Standard OSPF Path	1.5	0.2	Baseline
IPsec VPN Encrypted Path	3.8	0.5	153% Increase

Discussion

Comparative Analysis: IPsec VPN vs. MPLS

The decision to implement IPsec VPN over MPLS was based on a comparative evaluation of key factors, primarily cost and security. The comparison is summarized in (Table 7).

Table 7. Comparative Analysis of IPsec VPN and MPLS for Enterprise WAN

Feature	IPsec VPN	MPLS	Justification for VPN Selection
Cost	Low. Utilizes existing public internet infrastructure [3].	High. Requires dedicated, leased circuits and service provider contracts.	Cost-Effectiveness: Studies indicate MPLS costs can be 10-50 times higher than VPNs [3].
Security	High. Data is encrypted end-to-end [8].	Moderate. Relies on the provider's private network for security; no default encryption [3].	Data Confidentiality: IPsec provides a superior security posture through mandatory encryption.
Performance	Variable. Dependent on public internet congestion and latency.	High. Guaranteed performance and low latency via Service Level Agreements (SLAs).	Acceptable Trade-off: The cost savings outweigh the variable performance, which is often sufficient for non-critical traffic.
Scalability	High. New sites can be added quickly by configuring a new tunnel over the Internet.	Moderate. Requires physical circuit installation and service provider provisioning.	Deployment Flexibility: VPN allows for rapid, on-demand scaling of the network.

Justification for VPN Selection

The analysis clearly indicates that for an enterprise prioritizing cost-effectiveness and end-to-end security, IPsec VPN is the superior choice. While MPLS offers performance guarantees, the high cost associated with dedicated circuits and the lack of inherent encryption make it less appealing for many organizations. The IPsec VPN successfully addresses the security requirement by encrypting all traffic, ensuring that sensitive corporate data remains protected even while traversing the public internet [3] [8].

Conclusion

This technical implementation study has successfully designed, deployed, and validated a secure multi-site Wide Area Network (WAN) utilizing Open Shortest Path First (OSPF) and Internet Protocol Security (IPsec) Virtual Private Network (VPN) protocols. The comparative analysis indicates that IPsec VPN presents a compelling, cost-effective, and highly secure alternative to conventional Multiprotocol Label Switching (MPLS) for enterprise WAN connectivity. The implementation of route summarization, coupled with end-to-end application traffic verification, effectively demonstrated the viability of the proposed solution, ensuring a secure connection between the Tripoli headquarters and its remote branches in Benghazi, Al Bayda, and Misrata. Future endeavors should focus on the integration of Quality of Service (QoS) mechanisms to mitigate performance variability associated with public internet transport. Additionally, exploring advanced VPN architectures, such as Dynamic Multipoint VPN (DMVPN), may enhance the scalability of the project.

Conflict of interest. Nil

Received: *02-11-2025* - ***Accepted***: *31-12-2025* - ***Published***: *07-01-2026*

https://doi.org/10.54361/ajmas.269109

References

1. Dudczyk J. Analysis of SD-WAN architectures and techniques for modern enterprise networks. J Netw Syst Manage. 2025;33(2):45.
2. Troia S, Alvizu R, Hernández JA, Rodríguez S, Maier G. A comprehensive survey on software-defined wide area networks (SD-WAN). IEEE Commun Surv Tutor. 2025;27(1):350-89.
3. Sharma S, Singh AK, Gupta R. VPN: a boon or trap?: a comparative study of MPLS, IPSec, and SSL virtual private networks. In: 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN). IEEE; 2018. p. 760-5.
4. Fu C, Wang Z, Huang M, Cheng G. Software-defined wide area networks (SD-WANs): a survey. Electronics. 2024;13(15):3011.
5. Moy J. OSPF: anatomy of an Internet routing protocol. Boston (MA): Addison-Wesley; 1998.
6. Jain S. Extensive reviews of OSPF and EIGRP routing protocols based on route summarization and route redistribution. Int J Eng Res Gen Sci. 2014;2(6):1144-51.
7. Dong Y, Li Z, Li G. Network topology monitoring method of large scale OSPF network based on hierarchical modeling. In: Journal of Physics: Conference Series. IOP Publishing; 2020. p. 012021.
8. Frankel S, Hoffman P, Orebaugh A, Park R. Guide to IPsec VPNs. Gaithersburg (MD): National Institute of Standards and Technology; 2020. (NIST Special Publication; 800-77r1).
9. Hallqvist N. Implementing Internet Key Exchange (IKE). New York: Columbia University; 2001.
10. Felsch D, Grothe M, Schwenk J, Czubak A, Szymanek M. The dangers of key reuse: practical attacks on IPsec IKE. In: Proceedings of the 27th USENIX Security Symposium. USENIX Association; 2018. p. 567-83.

Received*: 02-11-2025 -* ***Accepted****: 31-12-2025 -* ***Published****: 07-01-2026*