Comprehensive Journal of Science
Volume (10), Issue (38), (Dec, 2025)
ISSN: 3014-6266

مجلة العلوم الشاملة
المجلد (10) ملحق العدد 38 ديسمبر 2025
ردمد: 3014-6266

Design and Implementation of a Secure DMVPN Architecture for Enterprise Networks

Ahmad Said Chahine [1], Abrar Haytham Ahmed[2], Sokaina Mawlood Ibraibish[2]

[1]College of Computer Technology-AlZawia

[2]University of Tripoli Al'Ahlia

Email: chahine.ahmad@gmail.com

تاريخ الاستلام:2025/12/16 –تاريخ المراجعة: 2025/12/19– تاريخ القبول: 2025/12/23– تاريخ للنشر : 26/1/ 2026

Abstract

This paper presents the design and implementation of a secure Dynamic Multipoint Virtual Private Network (DMVPN) architecture for enterprise networks with geographically distributed branches. Traditional site-to-site VPN solutions often suffer from scalability and management limitations as the number of branches increases [1], [2]. DMVPN addresses these challenges by enabling dynamic, scalable, and efficient connectivity between multiple sites over public networks [3].

The proposed architecture integrates Multipoint Generic Routing Encapsulation (mGRE), the Next Hop Resolution Protocol (NHRP), and the Open Shortest Path First (OSPF) routing protocol to provide dynamic routing and direct spoke-to-spoke communication [4], [5]. To ensure secure data transmission, IPsec encrypts tunnel traffic and protects network communications against potential threats [6], [7].

The solution is implemented and evaluated using the GNS3 network simulation environment [8]. Performance evaluation focuses on latency, throughput, and routing convergence time under normal operation and link failure conditions. Experimental results demonstrate that the proposed DMVPN architecture provides secure, flexible, and scalable connectivity while maintaining acceptable performance for enterprise requirements [7], [9].

Findings confirm that DMVPN, when combined with dynamic routing and robust security mechanisms, is an effective solution for modern enterprise wide-area networks [2], [5].

Keywords: DMVPN, IPsec, OSPF, Network Simulation (GNS3), Enterprise VPN, Performance Evaluation

I. Introduction

Enterprise networks increasingly rely on wide-area connectivity to support distributed branches, remote offices, and centralized services. Ensuring secure, reliable, and scalable communication between geographically dispersed sites has therefore become critical [1], [2].

Traditional site-to-site VPN solutions, while effective for small deployments, face scalability and management challenges as the number of branches grows due to static tunnel configurations and complex routing [3]. DMVPN addresses these limitations by enabling dynamic tunnel establishment and reducing configuration overhead [4], [5].

By combining mGRE and NHRP, DMVPN allows multiple branch routers (spokes) to form secure connections through a central hub, with the option of direct spoke-to-spoke communication [5], [6]. When integrated with dynamic routing protocols such as OSPF, DMVPN enhances network adaptability and simplifies route management in large-scale enterprises [4], [7].

Security is a fundamental concern, particularly over public networks. DMVPN deployments typically secure communications using IPsec, providing encryption, authentication, and data integrity [6], [7]. This combination ensures a balance between scalability, performance, and security [7], [9].

Despite widespread adoption, there is a need for implementation-focused studies that analyze DMVPN performance under realistic enterprise conditions, including routing convergence, tunnel stability, and latency under normal and failure scenarios [8], [10].

Contributions:

- Design of a secure enterprise DMVPN architecture integrating mGRE, NHRP, OSPF, and IPsec for scalable inter-branch connectivity [4] [6].
- Practical implementation and validation using GNS3 to emulate real-world enterprise conditions [8].
- Performance evaluation based on latency, throughput, and routing convergence during link failures [9], [10].
- Analytical discussion highlighting DMVPN advantages over traditional site-to-site VPN solutions [1] [3].

The remainder of the paper is organized as follows: Section II presents background and related work. Section III describes the proposed DMVPN architecture and security design. Section IV details implementation and experimental setup. Section V discusses performance evaluation and results. Section VI concludes and outlines future work [2], [5].

II. Background and Related Work

A. Background

Enterprise WANs interconnect geographically distributed sites such as headquarters, branch offices, and remote locations [1], [2]. Traditionally, such networks relied on leased lines or static site-to-site VPNs, which involve high operational costs and limited flexibility [3], [9]. The increasing use of the public Internet necessitates VPNs for secure communication [2], [6].

DMVPN is a scalable VPN solution enabling dynamic tunnel creation. It integrates mGRE, NHRP, and dynamic routing protocols [4], [5]. mGRE allows a single tunnel interface to support multiple peers, while NHRP dynamically maps private tunnel addresses to public IPs [5].

A hub-and-spoke model is commonly used, where the hub manages registration and control, and spokes establish secure tunnels dynamically. Phase 3 DMVPN supports direct spoke-to-spoke communication, reducing latency and offloading traffic from the hub [4], [5].

IPsec secures GRE tunnels with encryption, authentication, and integrity, meeting scalability and security requirements simultaneously [6], [7], [10].

B. Related Work

Research on VPN technologies has evolved from traditional site-to-site VPNs, which face scalability challenges [1], [2], [9], to dynamic solutions like DMVPN [4], [5]. Studies have explored DMVPN components, branch connectivity, and performance improvements over traditional VPNs [7], [8].

Dynamic routing protocols (OSPF, EIGRP) integrated with DMVPN enhance resilience and reduce recovery time after failures [10]. IPsec trade-offs between security and performance are widely discussed [6], [7].

Despite these efforts, implementation-focused analyses under realistic conditions remain limited. This study addresses this gap by designing, implementing, and evaluating a secure DMVPN architecture using OSPF and IPsec [4], [6], [7].

III. Proposed Secure DMVPN Architecture

A. Architectural Overview

The architecture uses a hub-and-spoke model with a central hub at headquarters and multiple branch spokes. All sites are interconnected over a simulated public IP network [8]. The hub acts as the registration point, while spokes dynamically establish secure tunnels [5].

A single mGRE tunnel interface on the hub supports multiple spokes without individual tunnel definitions [4], [5]. Each spoke registers dynamically via NHRP [5], [6]. This design reduces configuration complexity and enhances scalability [4], [5].

B. DMVPN Components and Operation

- **mGRE:** Single interface supports multiple endpoints for dynamic tunnel establishment [4].
- **NHRP:** Maps private tunnel IPs to public IPs and facilitates direct spoke-to-spoke tunnels [5], [6].
- **DMVPN Phase Configuration:** Supports dynamic spoke-to-spoke communication, optimizing latency and bandwidth [5], [7].

C. Routing with OSPF

OSPF is deployed across DMVPN tunnels within a single backbone area (Area 0), providing automatic route discovery, fast convergence, and simplified network expansion [7], [10].

D. Security with IPsec

IPsec in tunnel mode secures all GRE tunnels. IKE negotiates security associations, ensuring only authorized routers participate. Strong cryptographic algorithms balance security and performance [6], [7], [11].

E. Design Considerations and Scalability

Considerations include tunnel addressing, MTU/MSS optimization, and coordination of routing and security configurations. The architecture allows seamless addition of new spokes with minimal configuration [4], [5], [8].

IV. Implementation and Experimental Setup

A. Environment

The proposed DMVPN architecture was implemented using the GNS3 network simulation platform with Cisco IOS virtual routers. GNS3 enables realistic emulation of enterprise network environments and supports advanced routing and security configurations. [8], [12].

B. Topology and Addressing

A hub-and-spoke topology was adopted, consisting of one central hub located at the headquarters and multiple branch routers acting as spokes. All sites were interconnected through a simulated public IP network. [4], [5].

Private IP addressing was applied inside the GRE tunnels to separate the overlay network from the underlay infrastructure. Each tunnel interface was assigned an IP address from the 172.16.1.0/24 network.

C. DMVPN and Routing Configuration

Multipoint GRE tunnels were configured at the hub to support multiple spokes using a single logical interface. NHRP was enabled to allow dynamic registration of spoke addresses and facilitate direct spoke-to-spoke communication. [5], [6], [7], [10].

OSPF was deployed over the tunnel interfaces in Area 0 to provide automatic route discovery and fast convergence. All internal LAN networks were advertised through OSPF to ensure full inter-site connectivity.

D. IPsec Implementation

IPsec tunnel mode provides confidentiality, authentication, and integrity. IKE establishes security associations dynamically [6], [7], [11]. IPsec was implemented in tunnel mode to secure GRE traffic. Internet Key Exchange (IKE) Phase 1 and Phase 2 policies were configured using AES encryption and pre-shared key authentication. Security associations were dynamically established between the hub and spokes.

An IPsec profile was created and applied directly to tunnel interfaces to ensure seamless integration between routing and security mechanisms.

E. Practical Configuration Parameters

To optimize tunnel performance and reduce packet fragmentation caused by GRE and IPsec encapsulation, the Maximum Transmission Unit (MTU) and Maximum Segment Size (MSS) values were adjusted on all tunnel interfaces.

Specifically, the MTU was set to 1400 bytes and the TCP MSS was configured to 1360 bytes. These values ensured that transmitted packets remained within acceptable limits after encapsulation, preventing fragmentation and retransmissions.

Furthermore, verification commands such as *show crypto isakmp sa*, *show crypto ipsec sa*, and *show dmvpn* were used to validate tunnel establishment, routing stability, and security associations.

F. Experimental Methodology and Metrics

Experimental evaluation focused on tunnel stability, routing convergence, secure communication, latency, packet delivery rate, and system reliability.

Measurements were collected during normal operation and under simulated link failure conditions. ICMP-based tests, IPsec counters, and routing protocol states were used to assess overall network performance.

V. Results and Performance Evaluation

A. Tunnel Stability

All spoke routers successfully registered with the hub using NHRP. The mGRE tunnels remained operational throughout the experiments, and dynamic spoke-to-spoke tunnels were established when required.

No tunnel disconnections or registration failures were observed during normal operation.

B. Routing Convergence

OSPF adjacencies reached the FULL state between the hub and all spokes. When tunnel interfaces were administratively disabled, OSPF neighbors transitioned to the DOWN state and automatically reconverged after reactivation.

The average routing convergence time was below five seconds, indicating rapid recovery after failures.

C. Security Verification

IPsec security associations were successfully established in QM_IDLE state, confirming the completion of IKE Phase 1 and Phase 2 negotiations.

Packet counters showed consistent encryption and decryption without transmission errors, validating the effectiveness of the security configuration.

D. Connectivity and Latency

Connectivity tests were conducted using ICMP echo requests with specified source addresses. All tests achieved full packet delivery between enterprise sites.

MTU and MSS optimization eliminated packet fragmentation, contributing to stable latency and efficient packet transmission.

E. Reliability and Scalability

Additional spokes were dynamically integrated into the network without requiring changes to existing configurations. The registration process and routing updates occurred automatically, demonstrating high scalability.

The hub successfully maintained simultaneous tunnels with multiple spokes while preserving stable performance.

F. Performance Summary

Table I summarizes the main performance indicators obtained during the experiments.

Table I: **Performance Evaluation Results**

Parameter	Measured Value
Tunnel MTU	1400 bytes
TCP MSS	1360 bytes
Ping Success Rate	100%
Average RTT	32 ms
Encrypted Packets	137
Decrypted Packets	81
Packet Loss	0%
DMVPN Recovery Time	≈ 43 s

G. Discussion

The results presented in Table I demonstrate stable tunnel operation and reliable secure communication between enterprise branches. The optimized MTU and MSS values contributed significantly to eliminating packet fragmentation, resulting in zero packet loss and consistent latency.

IPsec packet counters confirm successful encryption and decryption processes without errors, validating the security configuration. The difference between encrypted and decrypted packets is due to asymmetric traffic patterns and control messages.

Furthermore, rapid OSPF reconvergence ensured minimal service disruption during link failures.

After tunnel reactivation, the complete recovery process including IPsec negotiation and OSPF adjacency establishment required approximately 43 seconds. This duration reflects the full DMVPN recovery time rather than pure routing convergence.

Compared to traditional site-to-site VPNs, the proposed DMVPN architecture provides superior scalability, simplified management, and efficient utilization of network resources while maintaining strong security guarantees.

VI. Conclusion and Future Work

The proposed secure DMVPN architecture integrating OSPF and IPsec provides scalable, reliable, and secure connectivity for enterprise networks [4]–[8], [10].

Future work includes testing on physical devices, implementing IKEv2 and certificate-based authentication, and exploring advanced routing and SD-WAN enhancements [11].

References

[1] Cisco Systems, *Dynamic Multipoint VPN (DMVPN) Overview*, Cisco Technical Documentation, 2020.

[2] Cisco Systems, *Dynamic Multipoint VPN: Design Guide*, Cisco Press, 2019.

[3] Cisco Systems, *Configuring DMVPN Phase 3 Using IKEv2*, Cisco Documentation, 2023.

[4] D. L. Meyer, “Next Hop Resolution Protocol (NHRP),” RFC 2332, IETF, Apr. 1998.
[5] S. Kent and K. Seo, “Security Architecture for the Internet Protocol,” RFC 4301, IETF, Dec. 2005.
[6] J. Moy, “OSPF Version 2,” RFC 2328, IETF, Apr. 1998.
[7] M. Hasan et al., “DMVPN Network Performance Based on Dynamic Routing Protocols and Basic IPsec Encryption,” Proc. ICECCE, Kuala Lumpur, Malaysia, 2021.
[8] M. A. Said et al., “Analysis of IPsec Implementation on DMVPN Using Dynamic Routing Protocols,” Building of Informatics, Technology and Science, vol. 4, no. 2, pp. 112–120, 2022.
[9] A. Bahnasse and N. El Kamoun, “Scalability Analysis of Dynamic Routing Protocols over DMVPN,” Int. J. Computer Applications, vol. 123, no. 2, 2015.
[10] R. Khelf and N. Ghoualmi-Zine, “A Survey on Dynamic Multipoint Virtual Private Networks,” CEUR Workshop Proc., vol. 2379, 2017.
[11] I. M. Abushawer, “Performance Evaluation of DMVPN over Secure WAN Networks,” Engineering and Info. Management Journal, 2025.
[12] GNS3 Technologies, *GNS3 Documentation*, Version 2.x, 2023.

Appendix A: Sample Configuration and Verification Outputs

This appendix presents representative configuration samples and verification outputs used in the implementation and evaluation of the proposed secure DMVPN architecture.

A.1 DMVPN Tunnel and NHRP Configuration

The following configuration illustrates the main tunnel and NHRP settings applied on the hub router.

```
interface Tunnel1
 ip address 172.16.1.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip tcp adjust-mss 1360
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 100
 ip nhrp authentication dmvpn
 ip nhrp network-id 1
 ip nhrp map multicast dynamic
 ip nhrp redirect
 ip nhrp shortcut
 tunnel protection ipsec profile DMVPN
```

This configuration enables multipoint GRE tunneling, dynamic spoke registration using NHRP, and secure tunnel protection using IPsec.

A.2 OSPF Routing Configuration

Dynamic routing was implemented using OSPF to ensure automatic route discovery and fast convergence.

```
router ospf 100
 network 172.16.1.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.255 area 0
```

OSPF was deployed within Area 0 to simplify routing management and support scalability.

A.3 IPsec and IKE Security Configuration

IPsec was configured in tunnel mode to secure all GRE traffic.

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 15

crypto isakmp key cisco address 0.0.0.0

crypto ipsec transform-set TS esp-aes esp-sha-hmac
 mode tunnel

crypto ipsec profile DMVPN
 set transform-set TS
```

This configuration ensures encrypted communication, peer authentication, and data integrity.

A.4 Security Association Verification

The following command was used to verify the successful establishment of IKE and IPsec sessions:

```
show crypto isakmp sa
show crypto ipsec sa
```

Sample output indicated that Security Associations reached the **QM_IDLE** and **ACTIVE** states, confirming successful Phase 1 and Phase 2 negotiations.

A.5 Tunnel Status and NHRP Registration

Tunnel and peer status were verified using:

```
show dmvpn
```

The output confirmed that all spokes were registered dynamically with the hub and maintained active tunnel connections.

A.6 Connectivity and Performance Testing

Connectivity and performance were evaluated using ICMP echo requests with a specified source address.

```
ping 192.168.3.1 source 192.168.1.1
```

Test results showed a 100% success rate with acceptable round-trip delays, indicating stable and reliable communication.

Packet encryption and decryption statistics were obtained using:

```
show crypto ipsec sa
```

The counters demonstrated successful packet encapsulation and decapsulation without transmission errors.

A.7 MTU and MSS Optimization

To reduce packet fragmentation caused by GRE and IPsec encapsulation, MTU and MSS values were optimized as follows:

```
ip mtu 1400
ip tcp adjust-mss 1360
```

These settings improved throughput and reduced retransmissions, contributing to stable tunnel performance.

A.8 Summary

The presented configurations and verification outputs confirm the correct deployment of DMVPN, dynamic routing, and IPsec security mechanisms. The results demonstrate reliable tunnel establishment, secure data transmission, and efficient routing under both normal and failure conditions.