DMVPN WAN Design

1. Overview

This document describes the design and implementation of a secure WAN using DMVPN (Dynamic Multipoint VPN) built on mGRE, NHRP, IPsec, and EIGRP. The solution provides encrypted, scalable connectivity between remote sites which are health facilities(spokes) and a centralized data center at DHA(hub). All this being implemented using Layer2 and Layer3 connections sourced from multiple ISPs without requiring internet connectivity just a logic Wide Area Network for the need managed internally.

2. Architecture Components

2.1 Core Technologies

- mGRE (Multipoint GRE): Enables a single tunnel interface to support multiple endpoints
- NHRP (Next Hop Resolution Protocol): Maps public IPs to tunnel addresses for dynamic spoke discovery with protection
- IPsec: Provides encryption and data integrity
- EIGRP: Handles dynamic routing between hub and spokes

2.2 Topology

- 1 Hub (Data Center)
- Multiple Spokes (Remote Sites – Health Facilities, DROs)
- Spoke-to-spoke communication via NHRP

3. Underlay Network

- ISPs provide Layer 2 or Layer 3 private connectivity only
- No native internet access on WAN links (except Starlink connections that internet is disabled on configuration)
- WAN functions as a private transport network

4. Routing Design

- EIGRP advertises only internal site routes
- The hub acts as the default route (0.0.0.0/0)
- All traffic from spokes is forwarded to the hub
- In cases where the end point is on the IP server and network, LAN segmentation and routing is implemented. This is done even introducing static routes on the server. For example in many cases with LIMS/EID/VL Traffic Flow

5. Internet Access Control

5.1 Default Policy

- Internet access is blocked by default at the data center firewall

5.2 Exception Handling

- Specific hosts/services may be temporarily whitelisted
- Approved traffic exits through the central hub (CHSU)

5.3 Security Benefits

- Centralized policy implementation

- Centralized inspection, monitoring and logging
- Reduced attack surface
- Controlled outbound access

6. Starlink Integration

Starlink provides direct internet access and is treated as a special case.

Controls Implemented

- ACLs to restrict inbound and outbound traffic – explicit blocking of internet access for the LAN
- Routing policies to prevent bypassing DMVPN
- SSH port hardening (non-standard port) Access control Lists to deny access from the internet.
- Starlink router is bypassed to the site gateway – IP address

Objective

Prevent Starlink from acting as an uncontrolled internet breakout path.

7. Remote Access VPN

This is remote access when one is not on the Wide Area Network or site.

- Implemented using Sophos SSL VPN
- Fully isolated from DMVPN site-to-site network

Benefits

- No additional load on WAN tunnels
- Segmented access control
- Improved performance for site traffic

8. Security Design

- End-to-end encryption using IPsec
- Centralized firewall enforcement
- Access control via ACLs and route filtering
- Segmentation between:

o Site-to-site traffic

o Internet-bound traffic

o Remote access users

9. Advantages

- DMVPN architecture is highly scalable
- Strong centralized security posture
- Efficient routing (no unnecessary prefixes)
- Controlled internet exposure

10. Limitations

- Hub is a single point of failure for internet breakout
- Increased latency due to centralized routing
- Manual effort required when whitelisting a remote server to access internet when a need arises during updates and upgrades

11. High-Level Diagram

12. Configuration Samples (Cisco)

12.1 Hub Configuration (Simplified)

```
interface Tunnel0
 description TNM-WAN-LINK
 ip address 10.0.0.1 255.255.255.0
 no ip redirects
```

```
 ip nhrp authentication <authenticator>
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile <security profile>
router eigrp 100
 network 10.0.0.0 0.0.0.255
 passive-interface default
 no passive-interface Tunnel0
```

12.2 Spoke Configuration (Simplified)

```
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 no ip redirects
 ip nhrp authentication <authenticator>
 ip nhrp map 10.0.0.1 <HUB_PUBLIC_IP>
 ip nhrp map multicast <HUB_PUBLIC_IP>
 ip nhrp network-id 1
 ip nhrp nhs 10.0.0.1
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile <security profile>
router eigrp 100
 network 10.0.0.0 0.0.0.255
 network <LAN_SUBNET>
 passive-interface default
 no passive-interface Tunnel0
```

14. Monitoring and Logging

- SNMP monitoring for tunnel/interface status
- NetFlow for traffic visibility
- IP SLA for tunnel health tracking

Summary

This DMVPN design delivers a secure, scalable WAN with centralized control over routing and internet access. By leveraging private underlay connectivity and strict policy enforcement, the solution minimizes exposure while maintaining operational flexibilit

---

Revision #1
Created 24 April 2026 10:04:17 by Martin Suleman
Updated 24 April 2026 10:05:47 by Martin Suleman