

Project 3: Implementing VPN Solutions with FortiGate - Final Report

Author: Manus AI

Date: September 15, 2025

Table of Contents

1. Introduction
2. VPN Concepts and FortiGate Capabilities
3. VPN Architecture and Configuration Plans
 - SSL VPN Architecture Design
 - IPsec VPN Architecture Design
 - FortiGate VPN with SD-WAN Integration Design
4. SSL VPN Configuration Guide and Test Scenarios
5. IPsec VPN Configuration Guide and Connectivity Test Results
6. SD-WAN Configuration Guide for VPN Optimization and Performance Report
7. Comprehensive VPN Testing Framework and Validation Procedures
8. Conclusion
9. References

1. Introduction

This report details the comprehensive implementation of Virtual Private Network (VPN) solutions using FortiGate firewalls, addressing various VPN types including SSL

VPN, IPsec VPN, and their integration with Software-Defined Wide Area Network (SD-WAN) for optimized traffic management. The project encompasses the study of VPN concepts, design of robust architectures, detailed configuration guides, and rigorous testing procedures to ensure secure, efficient, and reliable network connectivity. The objective is to provide a professional, well-documented, and thoroughly tested VPN solution suitable for modern enterprise environments.

2. VPN Concepts and FortiGate Capabilities

VPN Types and Use Cases

Virtual Private Networks (VPNs) establish a secure, encrypted connection over a less secure network, typically the internet. They are fundamental for protecting data privacy, ensuring data integrity, and enabling secure remote access to private networks. Different types of VPNs cater to various organizational needs and use cases:

- **Remote Access VPN:** This type allows individual users to securely connect to a private network from a remote location. It is commonly used by employees working from home or while traveling to access corporate resources. The user's device connects to a VPN gateway, and all traffic between the device and the private network is encrypted. FortiGate supports remote access VPNs through both SSL VPN and IPsec VPN protocols.
- **Site-to-Site VPN:** This VPN type connects two or more private networks across a public network, creating a secure tunnel between them. It is ideal for connecting branch offices to a headquarters, or connecting different data centers. Unlike remote access VPNs, site-to-site VPNs connect entire networks rather than individual users. IPsec is the predominant protocol used for site-to-site VPNs due to its robust security features and ability to encapsulate entire network traffic. FortiGate firewalls excel in establishing and managing site-to-site IPsec VPN tunnels.
- **SSL VPN:** Secure Sockets Layer VPNs (now often referred to as TLS VPNs) use standard web browsers and the SSL/TLS protocol to provide secure remote access. They are highly flexible and can offer both web-mode access (access to specific web applications through a portal) and tunnel-mode access (full network access via a client). SSL VPNs are user-friendly as they often require minimal client-side software, making them suitable for diverse user devices. FortiGate's

SSL VPN capabilities are extensive, allowing granular control over user access and integration with various authentication methods.

- **IPsec VPN:** Internet Protocol Security (IPsec) is a suite of protocols that provides cryptographic security for IP networks. It operates at the network layer and offers strong authentication and encryption for data packets. IPsec VPNs are widely used for both site-to-site and remote access scenarios, especially when high security and performance are critical. FortiGate devices provide comprehensive support for IPsec, including various encryption algorithms (AES, 3DES), hashing algorithms (SHA256, MD5), and key exchange methods (Diffie-Hellman groups).
- **Cloud VPN:** Cloud VPNs facilitate secure connections to cloud-based resources and applications. They can be implemented as extensions of remote access or site-to-site VPNs, connecting on-premises networks to cloud environments or securing access for remote users to cloud services. FortiGate firewalls can be deployed in cloud environments (e.g., AWS, Azure, Google Cloud) to provide VPN gateway functionalities, securing hybrid cloud architectures.
- **Double VPN:** This advanced configuration routes traffic through two VPN servers, encrypting data twice. While it offers enhanced anonymity and security, it typically comes with increased latency and reduced performance. Implementing a double VPN with FortiGate would involve chaining two VPN connections, which requires careful planning and configuration.

FortiGate Capabilities for VPN Implementation

FortiGate firewalls are renowned for their robust and versatile VPN capabilities, making them a popular choice for securing network communications. They offer a comprehensive suite of features for implementing SSL VPN, IPsec VPN, and integrating these with advanced networking technologies like SD-WAN.

SSL VPN Capabilities on FortiGate

FortiGate provides a flexible and secure SSL VPN solution with features designed for ease of use and strong security:

- **Web-mode and Tunnel-mode:** Supports both web-based access to internal resources and full network layer tunnel access via FortiClient.

- **Granular Access Control:** Allows administrators to define specific portals and realms, mapping them to user groups for fine-grained control over which resources users can access.
- **Strong Authentication:** Integrates with various authentication methods including local user database, LDAP, RADIUS, SAML, and supports Multi-Factor Authentication (MFA) for enhanced security.
- **Customizable Portals:** Web portals can be customized with corporate branding and specific application links.
- **Split Tunneling Control:** Offers the option to enable or disable split tunneling, allowing administrators to decide whether all traffic or only corporate traffic goes through the VPN tunnel.
- **Security Profiles:** SSL VPN traffic can be subjected to FortiGate's full suite of security profiles, including Antivirus, Intrusion Prevention System (IPS), Web Filtering, and Application Control, providing deep packet inspection and threat protection.

IPsec VPN Capabilities on FortiGate

FortiGate's IPsec VPN implementation is robust, scalable, and compliant with industry standards, making it ideal for site-to-site and remote access scenarios:

- **Standard Compliance:** Supports IKEv1 and IKEv2 protocols, ensuring interoperability with other VPN devices.
- **Strong Cryptography:** Offers a wide range of encryption algorithms (AES, 3DES) and hashing algorithms (SHA256, SHA512, MD5) for Phase 1 and Phase 2 negotiations.
- **Authentication Methods:** Supports pre-shared keys (PSK) and X.509 digital certificates for strong peer authentication.
- **Perfect Forward Secrecy (PFS):** Can be enabled to ensure that compromise of one session key does not compromise past or future session keys.
- **NAT Traversal:** Facilitates IPsec connections across NAT devices.
- **Dead Peer Detection (DPD):** Monitors the liveness of VPN peers and can tear down tunnels if a peer becomes unresponsive.
- **VPN Wizards:** Simplifies the configuration of common VPN topologies like site-to-site and remote access VPNs.

- **Policy-Based and Route-Based VPNs:** Supports both policy-based VPNs (where traffic selectors define what traffic uses the tunnel) and route-based VPNs (where traffic is routed to a virtual tunnel interface).

SD-WAN Integration with FortiGate VPN

FortiGate's Secure SD-WAN solution seamlessly integrates with VPNs, particularly IPsec, to provide intelligent traffic steering, performance optimization, and enhanced reliability for inter-site and cloud connectivity:

- **Centralized Management:** SD-WAN policies and VPN configurations can be managed centrally, simplifying deployment and operations across distributed networks.
- **Link Aggregation and Load Balancing:** Multiple WAN links can be grouped into an SD-WAN zone, allowing VPN traffic to be load-balanced or aggregated for increased bandwidth.
- **Intelligent Path Selection:** SD-WAN monitors the performance of each WAN link (and the VPN tunnels running over them) using Performance SLAs (Service Level Agreements). It can then dynamically route VPN traffic over the best-performing link based on real-time metrics like latency, jitter, and packet loss.
- **Application-Aware Routing:** Traffic can be steered based on application type, ensuring critical applications always use the optimal path, even if it means routing over a specific VPN tunnel.
- **Automated Failover:** In case of a link degradation or failure, SD-WAN automatically and seamlessly redirects VPN traffic to a healthy alternative link, ensuring business continuity.
- **VPN Overlay:** SD-WAN can orchestrate multiple IPsec VPN tunnels over diverse WAN links, creating a resilient and optimized VPN overlay network.
- **Visibility and Analytics:** FortiGate provides extensive monitoring and reporting tools for SD-WAN and VPN performance, offering insights into link quality, traffic patterns, and application experience.

In summary, FortiGate firewalls offer a powerful and flexible platform for implementing a wide array of VPN solutions, from secure remote access for individual users to robust site-to-site connectivity and advanced SD-WAN integrated VPN optimization. The comprehensive feature set ensures high security, performance, and manageability for diverse networking requirements.

3. VPN Architecture and Configuration Plans

SSL VPN Architecture Design

SSL VPN provides secure remote access to internal network resources for individual users. It is particularly useful for employees working remotely, allowing them to access corporate applications and data securely over the internet using a standard web browser or a dedicated client. FortiGate's SSL VPN implementation supports both web-mode and tunnel-mode connections, offering flexibility based on user requirements and security policies.

Key Components

- **FortiGate Firewall:** Acts as the SSL VPN gateway, terminating encrypted connections from remote users.
- **Remote Users:** Individuals connecting from external networks (e.g., home, public Wi-Fi) using a FortiClient VPN client or a web browser.
- **Internal Network Resources:** Servers, applications, and data within the corporate network that remote users need to access.
- **Authentication Server:** (Optional but recommended) An external server like LDAP, RADIUS, or FortiAuthenticator for centralized user authentication. Local FortiGate user database can also be used.

Connection Flow

1. **Initiation:** A remote user initiates an SSL VPN connection to the FortiGate's public IP address on a specified port (default 10443).
2. **Authentication:** The FortiGate authenticates the user against its local database or an external authentication server. Multi-factor authentication (MFA) is highly recommended for enhanced security.
3. **Portal/Tunnel Assignment:** Upon successful authentication, the user is assigned to an SSL VPN portal (for web-mode access) or a tunnel (for full network access via FortiClient).
 - **Web-mode:** Provides access to specific internal web applications, file shares, or network services through a web browser interface.

- **Tunnel-mode:** Establishes a full network layer tunnel, allowing the remote user's device to become a virtual member of the internal network, accessing resources as if directly connected.

4. **Policy Enforcement:** Firewall policies on the FortiGate control what resources the authenticated SSL VPN users can access within the internal network.

5. **Traffic Encryption:** All traffic between the remote user and the FortiGate is encrypted using SSL/TLS protocols, ensuring data confidentiality and integrity.

Configuration Considerations

- **Interface Selection:** The FortiGate interface listening for SSL VPN connections should typically be an external (WAN) interface.
- **Port Configuration:** Use a non-standard port (other than 443) for SSL VPN to reduce exposure to common port scans.
- **Server Certificate:** A valid SSL certificate (either self-signed or from a trusted CA) is crucial for secure communication and to prevent browser warnings.
- **User Groups and Realms:** Organize users into groups and assign them to specific SSL VPN realms and portals to enforce granular access control.
- **Split Tunneling:** Decide whether to enable split tunneling. When enabled, only traffic destined for the corporate network goes through the VPN tunnel, while internet traffic goes directly. This reduces load on the FortiGate but might bypass corporate internet security policies. Full tunneling routes all traffic through the VPN.
- **Firewall Policies:** Create explicit firewall policies to allow authenticated SSL VPN users to access necessary internal resources. Ensure NAT is handled correctly.
- **Logging and Monitoring:** Enable comprehensive logging for SSL VPN sessions to monitor user activity and troubleshoot issues.

IPsec VPN Architecture Design

IPsec VPN is primarily used for site-to-site connectivity, creating secure tunnels between two networks (e.g., headquarters and a branch office) or for remote access where a dedicated client establishes a secure connection to a central gateway. It operates at the network layer, encrypting and authenticating IP packets. FortiGate devices are highly capable of establishing robust IPsec VPN tunnels, supporting various encryption algorithms, authentication methods, and key exchange protocols.

Key Components

- **FortiGate Firewalls (or other IPsec-compliant devices):** Act as VPN gateways at each end of the tunnel, responsible for encrypting/decrypting traffic and authenticating peers.
- **Local Networks:** The internal networks at each site that need to communicate securely.
- **Public Network (Internet):** The untrusted medium over which the encrypted tunnel is established.

Connection Flow (Site-to-Site)

1. **Initiation:** Traffic from a host in one local network destined for a host in the remote local network triggers the IPsec tunnel establishment.
2. **Phase 1 (IKE - Internet Key Exchange):** The two FortiGate devices establish a secure, authenticated channel (IKE SA - Security Association) between themselves. This involves:
 - **Negotiation:** Agreeing on encryption algorithms (e.g., AES256), hashing algorithms (e.g., SHA256), Diffie-Hellman group for key exchange, and authentication method (pre-shared key or certificates).
 - **Authentication:** Verifying the identity of the peer FortiGate.
3. **Phase 2 (IPsec SA):** Once Phase 1 is complete, the FortiGate devices negotiate the parameters for the actual data tunnel (IPsec SA). This includes:
 - **Negotiation:** Agreeing on IPsec protocols (ESP or AH), encryption algorithms, hashing algorithms, and Perfect Forward Secrecy (PFS) settings.
 - **Key Exchange:** Generating session keys for encrypting and decrypting data traffic.
4. **Data Transfer:** Encrypted data traffic flows securely between the two local networks through the established IPsec tunnel.
5. **Policy Enforcement:** Firewall policies on both FortiGate devices control which traffic is allowed to traverse the IPsec tunnel.

Configuration Considerations

- **Phase 1 (IKE Gateway):**
 - **Remote Gateway:** Static IP address or dynamic DNS.

- **Interface:** The external (WAN) interface used for the VPN connection.
- **Authentication Method:** Pre-shared key (PSK) or digital certificates. PSK is simpler for small deployments, while certificates offer stronger security and scalability.
- **Encryption and Authentication:** Choose strong algorithms (e.g., AES256, SHA256).
- **Diffie-Hellman Group:** Select a strong group (e.g., Group 14 or higher).
- **Key Lifetime:** Define how long the Phase 1 SA remains valid.
- **Phase 2 (IPsec Tunnel):**
 - **Local and Remote Subnets:** Define the networks that will communicate over the tunnel.
 - **Encryption and Authentication:** Match Phase 1 settings or use different, equally strong algorithms.
 - **Perfect Forward Secrecy (PFS):** Enable PFS to ensure that if a session key is compromised, past and future session keys remain secure.
 - **Key Lifetime:** Define how long the Phase 2 SA remains valid.
- **Firewall Policies:** Create specific policies on both FortiGate devices to permit traffic between the local and remote subnets over the IPsec tunnel. Ensure NAT is disabled for VPN traffic if direct routing is desired.
- **Routing:** Ensure proper static routes or dynamic routing protocols (e.g., OSPF, BGP) are configured to direct traffic into the IPsec tunnel.
- **Dead Peer Detection (DPD):** Enable DPD to detect unresponsive peers and tear down stale tunnels.

FortiGate VPN with SD-WAN Integration Design

Integrating VPNs (especially IPsec VPNs) with SD-WAN on FortiGate allows organizations to optimize traffic flow, enhance performance, and provide redundancy for VPN connections. SD-WAN intelligently directs traffic over the best available link based on performance metrics (latency, jitter, packet loss) and defined policies. When combined with VPNs, it ensures that secure traffic leverages the most efficient path, improving user experience and application performance, particularly for branch offices or cloud connectivity.

Key Components

- **FortiGate Devices:** Acting as SD-WAN hubs and spokes, terminating VPN tunnels and performing intelligent path selection.
- **Multiple WAN Links:** Diverse internet connections (e.g., MPLS, broadband, LTE) at each site, forming the SD-WAN fabric.
- **IPsec VPN Tunnels:** Established over the various WAN links to provide secure connectivity between sites.
- **SD-WAN Zone:** A logical grouping of WAN interfaces (including VPN interfaces) that the FortiGate uses for intelligent traffic steering.
- **Performance SLAs (Service Level Agreements):** Defined metrics (latency, jitter, packet loss) used by SD-WAN to evaluate link quality.
- **SD-WAN Rules:** Policies that dictate how traffic is steered across the available WAN links based on application, destination, and performance requirements.

Integration Flow

1. **VPN Tunnel Creation:** Multiple IPsec VPN tunnels are established between FortiGate devices, typically one over each available WAN link. These tunnels provide the secure overlay network.
2. **SD-WAN Zone Configuration:** The VPN tunnel interfaces are added as members to an SD-WAN zone. This allows the SD-WAN engine to manage and monitor these secure paths.
3. **Performance SLA Monitoring:** Performance SLAs are configured to monitor the quality of each VPN tunnel. This involves sending probes (e.g., ICMP, HTTP) through the tunnels to measure latency, jitter, and packet loss to a defined target (e.g., a server in the remote network).
4. **SD-WAN Rules for VPN Traffic:** SD-WAN rules are created to steer specific VPN traffic (e.g., critical business applications) over the best-performing VPN tunnel based on the real-time SLA metrics. Strategies like Lowest Cost SLA, Best Quality, or Maximum Bandwidth can be used.
5. **Dynamic Path Selection:** Based on the SD-WAN rules and real-time performance data from the SLAs, the FortiGate dynamically selects the optimal VPN tunnel for each traffic flow, ensuring high availability and optimal performance.

6. Redundancy and Failover: If a primary VPN tunnel or its underlying WAN link fails or degrades below a defined threshold, SD-WAN automatically steers traffic to an alternative healthy VPN tunnel, providing seamless failover.

Configuration Considerations

- **Manual VPN Interface Creation:** For SD-WAN integration, it is often recommended to create IPsec VPN interfaces manually rather than using the wizard, as wizard-created interfaces might not be directly usable as SD-WAN members.
- **SD-WAN Zone:** Create a dedicated SD-WAN zone and add the IPsec VPN tunnel interfaces as members. This allows the SD-WAN engine to manage these secure paths.
- **Performance SLA:** Configure Performance SLAs to monitor the health and performance of each VPN tunnel. Define targets (e.g., internal server IPs) and thresholds for latency, jitter, and packet loss.
- **SD-WAN Rules:** Create granular SD-WAN rules to direct traffic. These rules can be based on source/destination IP, application, service, and leverage the Performance SLA metrics to choose the best path. Ensure VPN-related SD-WAN rules are prioritized correctly.
- **Firewall Policies:** Configure firewall policies to allow traffic through the SD-WAN zone and across the VPN tunnels. Ensure NAT is disabled for VPN traffic within the SD-WAN context if direct routing is intended.
- **Blackhole Routes:** Implement blackhole routes for destination subnets to prevent traffic from being routed over the internet if all VPN tunnels to a specific destination are down. This ensures traffic is dropped rather than sent unencrypted or to an incorrect destination.
- **CLI for Advanced Configuration:** Some advanced configurations, such as adding source IPs to SD-WAN members for Performance SLA to function correctly, might require CLI commands.

This integrated approach ensures that VPN connectivity is not only secure but also highly optimized, resilient, and performs efficiently across diverse WAN infrastructures.

4. SSL VPN Configuration Guide and Test Scenarios

Introduction

This section provides detailed instructions for configuring an SSL VPN on a FortiGate firewall, enabling secure remote access to internal network resources. The focus is on establishing a full-tunnel SSL VPN for remote users, ensuring all their traffic is routed through the corporate network for enhanced security and policy enforcement.

Prerequisites

Before configuration, ensure the following:

- A FortiGate firewall with administrative access.
- FortiOS version 7.4.3 or later.
- An external (WAN) interface configured and connected to the internet.
- A valid SSL certificate (CA-signed recommended for production) installed on the FortiGate.
- Defined user groups or local users for VPN access.
- Knowledge of internal network subnets and resources.

Configuration Steps

1. **Enable SSL-VPN Realms Feature:** Navigate to **System > Feature Visibility**, enable **SSL-VPN Realms**, and click **Apply**.
2. **Configure SSL VPN Portal:** Navigate to **VPN > SSL-VPN Portals**, edit the `full-access` portal. Ensure **Split Tunneling** is disabled for full tunnel mode. Configure other settings as needed.
3. **Configure SSL VPN Realm:** Navigate to **VPN > SSL-VPN Realms**, click **Create New**. Enter a **Name** (e.g., `remote_users_realm`) and a **URL Path** (e.g., `/remote`). Select the `full-access` portal. Click **OK**.
4. **Configure SSL VPN Settings:** Navigate to **VPN > SSL-VPN Settings**.
 - Enable **SSL-VPN**.
 - Select the external (WAN) **Listen on Interface(s)** (e.g., `wan1`).

- Change **Listen on Port** to a non-standard port (e.g., 10443).
- Select the appropriate **Server Certificate**.
- Define **IP Ranges** for VPN clients, ensuring no overlap with internal subnets.
- Specify internal **DNS Server**.
- Under **Authentication/Portal Mapping**, click **Create New**. Select the user group (e.g., VPN_Users), specify the realm (e.g., /remote), and select the full-access portal. Click **OK**. Edit **All Other Users/Groups** to no-access.
- Click **Apply**.

5. Configure Firewall Policy: Navigate to **Policy & Objects > Firewall Policy**, click **Create New**.

- **Name:** SSL_VPN_to_Internal.
- **Incoming Interface:** ssl.root.
- **Outgoing Interface:** Internal interface(s) (e.g., port2).
- **Source:** VPN_Users group and SSLVPN_TUNNEL_ADDR1.
- **Destination:** Internal network subnets or specific address objects.
- **Schedule:** always.
- **Service:** ALL (or specific services).
- **Action:** ACCEPT.
- **NAT:** Disable (if preserving original source IP) or Enable (if traffic appears from FortiGate).
- **Log Allowed Traffic:** All Sessions.
- Configure security profiles as needed. Click **OK**.

Testing SSL VPN Connectivity

To test the SSL VPN connection:

1. **Download FortiClient:** Instruct remote users to download and install the FortiClient VPN client.
2. **Configure FortiClient:** Create a new SSL-VPN connection with the FortiGate public IP/hostname, port, and realm path (e.g., your.fortigate.ip:10443/remote). Enter authorized user credentials.

3. **Connect:** Initiate the connection from FortiClient.
4. **Verify Connectivity:** Once connected, verify access to internal network resources (e.g., ping internal servers, access internal web applications). Verify public IP is FortiGate WAN IP if full tunneling.
5. **Check FortiGate Logs:** Monitor **Log & Report > VPN Events** for successful connections and traffic flow.

Best Practices for SSL VPN

- **Strong Authentication:** Implement Multi-Factor Authentication (MFA).
- **Least Privilege:** Grant access only to necessary resources.
- **Regular Updates:** Keep FortiGate firmware and FortiClient software updated.
- **Logging and Monitoring:** Continuously monitor VPN logs.
- **Security Profiles:** Apply appropriate security profiles to SSL VPN traffic.
- **Non-Standard Ports:** Use a non-standard port for SSL VPN.
- **Certificates:** Use CA-signed certificates for production.

SSL VPN Test Scenarios

To ensure the SSL VPN is functioning correctly and securely, perform the following test scenarios:

- **Scenario 1: Successful Connection and Internal Resource Access (Full Tunnel)**
 - **Objective:** Verify that a legitimate remote user can successfully establish a full-tunnel SSL VPN connection and access internal network resources.
 - **Steps:** Connect via FortiClient, ping internal servers, access internal web applications, verify public IP is FortiGate WAN IP. Check FortiGate logs.
 - **Expected Results:** Successful connection, reachable internal resources, correct public IP, and logged events.
- **Scenario 2: Unsuccessful Connection - Invalid Credentials**
 - **Objective:** Verify that users with invalid credentials are denied access.
 - **Steps:** Attempt connection with incorrect username/password.

- **Expected Results:** Authentication failure message in FortiClient, authentication failure events in FortiGate logs.
- **Scenario 3: Unsuccessful Connection - Unauthorized User**
 - **Objective:** Verify that users not part of the `VPN_Users` group are denied access.
 - **Steps:** Attempt connection with credentials of a user not in the `VPN_Users` group.
 - **Expected Results:** Access denied message, access denied events in FortiGate logs.
- **Scenario 4: Access to Restricted Internal Resources**
 - **Objective:** Verify that VPN users can only access resources permitted by the firewall policy.
 - **Steps:** Establish connection, attempt to access a resource not included in the firewall policy.
 - **Expected Results:** Access to restricted resource fails, FortiGate traffic logs show `deny` actions.
- **Scenario 5: SSL VPN Disconnection and Reconnection**
 - **Objective:** Verify stable connection and proper session termination.
 - **Steps:** Connect, disconnect, then reconnect.
 - **Expected Results:** Clean disconnection, successful reconnection, and logged events.

5. IPsec VPN Configuration Guide and Connectivity Test Results

Introduction

This section provides detailed instructions for configuring a Site-to-Site IPsec VPN tunnel between two FortiGate devices. IPsec VPNs are crucial for securely connecting

geographically dispersed networks, ensuring data confidentiality, integrity, and authenticity over untrusted networks like the internet.

Prerequisites

Before proceeding with the configuration, ensure the following:

- Two FortiGate firewalls (FortiGate A and FortiGate B) with administrative access.
- FortiOS version 7.6.4 or later.
- Publicly routable IP addresses on the WAN interfaces of both FortiGate devices.
- Knowledge of the internal network subnets at both sites (e.g., Head Office LAN: 192.168.1.0/24 , Branch Office LAN: 192.168.2.0/24).
- A pre-shared key for authentication (or digital certificates if using a more advanced setup).

Network Topology (Example)

- **FortiGate A (Head Office)**

- WAN Interface: port1 (Public IP: 203.0.113.1)
 - LAN Interface: port2 (Internal IP: 192.168.1.1/24)
 - Internal Network: 192.168.1.0/24

- **FortiGate B (Branch Office)**

- WAN Interface: port1 (Public IP: 198.51.100.1)
 - LAN Interface: port2 (Internal IP: 192.168.2.1/24)
 - Internal Network: 192.168.2.0/24

Configuration Steps

FortiGate A (Head Office) Configuration

1. Create Phase 1 (IKE Gateway):

- Navigate to **VPN > IPsec Tunnels**, click **Create New**, select **IPsec Tunnel**, and choose **Custom** template.

- **Name:** HO-to-Branch .
- **Network: Interface:** port1 , **Remote Gateway:** Static IP Address , **IP Address:** 198.51.100.1 (Public IP of FortiGate B), **Dead Peer Detection:** Always On .
- **Authentication: Method:** Pre-shared Key , **Pre-shared Key:** YourStrongPSKHere , **IKE Version:** IKEV2 .
- **Phase 1 Proposal: Encryption:** AES256 , **Authentication:** SHA256 , **Diffie-Hellman Group:** 14 , **Key Lifetime:** 86400 seconds. Click OK.

2. Create Phase 2 (IPsec Tunnel):

- Edit the HO-to-Branch tunnel, under **Phase 2 Selectors**, click **Create New**.
- **Name:** HO-to-Branch-P2 .
- **Local Address:** 192.168.1.0/24 , **Remote Address:** 192.168.2.0/24 .
- **Phase 2 Proposal: Encryption:** AES256 , **Authentication:** SHA256 , **Perfect Forward Secrecy (PFS):** Enable , **Diffie-Hellman Group:** 14 , **Key Lifetime:** 3600 seconds. Click OK.

3. Create Firewall Addresses for Remote Network: Navigate to **Policy & Objects > Addresses**, click **Create New > Address**. **Name:** Branch_Office_LAN , **Type:** Subnet , **Subnet/IP Range:** 192.168.2.0/24 . Click OK.

4. Create Firewall Policies:

- **HO-LAN-to-Branch-VPN: Incoming Interface:** port2 , **Outgoing Interface:** HO-to-Branch , **Source:** all , **Destination:** Branch_Office_LAN , **Service:** ALL , **Action:** ACCEPT , **NAT:** Disable , **Log Allowed Traffic:** All Sessions . Click OK.
- **Branch-VPN-to-HO-LAN: Incoming Interface:** HO-to-Branch , **Outgoing Interface:** port2 , **Source:** Branch_Office_LAN , **Destination:** all , **Service:** ALL , **Action:** ACCEPT , **NAT:** Disable , **Log Allowed Traffic:** All Sessions . Click OK.

5. Configure Static Route: Navigate to **Network > Static Routes**, click **Create New**. **Destination:** Subnet 192.168.2.0/24 , **Device:** HO-to-Branch . Click OK.

FortiGate B (Branch Office) Configuration

Repeat the above steps on FortiGate B, swapping local and remote network details.

1. Create Phase 1 (IKE Gateway):

- **Name:** Branch-to-HO .
- **Network: Interface:** port1 , **Remote Gateway:** Static IP Address , **IP Address:** 203.0.113.1 (Public IP of FortiGate A), **Dead Peer Detection:** Always On .
- **Authentication: Method:** Pre-shared Key , **Pre-shared Key:** YourStrongPSKHere , **IKE Version:** IKEv2 .
- **Phase 1 Proposal: Encryption:** AES256 , **Authentication:** SHA256 , **Diffie-Hellman Group:** 14 , **Key Lifetime:** 86400 seconds. Click OK.

2. Create Phase 2 (IPsec Tunnel):

- Edit the Branch-to-HO tunnel, under **Phase 2 Selectors**, click **Create New**.
- **Name:** Branch-to-HO-P2 .
- **Local Address:** 192.168.2.0/24 , **Remote Address:** 192.168.1.0/24 .
- **Phase 2 Proposal: Encryption:** AES256 , **Authentication:** SHA256 , **Perfect Forward Secrecy (PFS):** Enable , **Diffie-Hellman Group:** 14 , **Key Lifetime:** 3600 seconds. Click OK.

3. Create Firewall Addresses for Remote Network: Navigate to **Policy & Objects > Addresses**, click **Create New > Address**. **Name:** Head_Office_LAN , **Type:** Subnet , **Subnet/IP Range:** 192.168.1.0/24 . Click OK.

4. Create Firewall Policies:

- **Branch-LAN-to-HO-VPN: Incoming Interface:** port2 , **Outgoing Interface:** Branch-to-HO , **Source:** all , **Destination:** Head_Office_LAN , **Service:** ALL , **Action:** ACCEPT , **NAT:** Disable , **Log Allowed Traffic:** All Sessions . Click OK.
- **HO-VPN-to-Branch-LAN: Incoming Interface:** Branch-to-HO , **Outgoing Interface:** port2 , **Source:** Head_Office_LAN , **Destination:** all , **Service:**

ALL , Action: ACCEPT , NAT: Disable , Log Allowed Traffic: All Sessions .
Click **OK**.

5. Configure Static Route: Navigate to **Network > Static Routes**, click **Create New**.
Destination: Subnet **192.168.1.0/24** , **Device:** Branch-to-HO . Click **OK**.

Verification

After configuring both FortiGate devices, the IPsec tunnel should come up automatically. Verify the tunnel status by navigating to **VPN > IPsec Tunnels** and **Monitor > IPsec Monitor** on both FortiGate A and B.

IPsec VPN Connectivity Test Results

To ensure the IPsec VPN tunnel is functioning correctly and securely, perform the following connectivity tests from both FortiGate A (Head Office) and FortiGate B (Branch Office).

- **Test Scenario 1: Ping from Head Office LAN to Branch Office LAN**
 - **Objective:** Verify bidirectional connectivity from HO to BO through the IPsec tunnel.
 - **Steps:** From a host in the Head Office LAN (e.g., 192.168.1.10), ping a host in the Branch Office LAN (e.g., 192.168.2.10).
 - **Expected Results:** Successful ping replies, no packet loss, FortiGate logs show traffic traversing the IPsec tunnel.
- **Test Scenario 2: Ping from Branch Office LAN to Head Office LAN**
 - **Objective:** Verify bidirectional connectivity from BO to HO through the IPsec tunnel.
 - **Steps:** From a host in the Branch Office LAN (e.g., 192.168.2.10), ping a host in the Head Office LAN (e.g., 192.168.1.10).
 - **Expected Results:** Successful ping replies, no packet loss, FortiGate logs show traffic traversing the IPsec tunnel.
- **Test Scenario 3: Access Internal Resources (e.g., Web Server, File Share)**
 - **Objective:** Verify access to specific services on hosts in the other LAN.

- **Steps:** Attempt to access a web server or file share from one LAN to the other.
- **Expected Results:** Web servers and file shares accessible, FortiGate traffic logs show successful connections.

- **Test Scenario 4: IPsec Tunnel Status Monitoring**

- **Objective:** Verify that the IPsec tunnel remains up and stable.
- **Steps:** On both FortiGates, check **VPN > IPsec Tunnels** and **Monitor > IPsec Monitor**.
- **Expected Results:** Tunnel status `Up`, traffic statistics incrementing, SAs active.

- **Test Scenario 5: Tunnel Rekeying**

- **Objective:** Verify correct rekeying of Phase 1 and Phase 2 SAs without traffic interruption.
- **Steps:** Monitor IPsec SAs, initiate continuous traffic, and observe rekeying after key lifetime expiration.
- **Expected Results:** New SAs established automatically, uninterrupted traffic, FortiGate logs show IKE rekeying events.

- **Test Scenario 6: Dead Peer Detection (DPD) Test**

- **Objective:** Verify detection of unresponsive peers and tunnel teardown if DPD is enabled.
- **Steps:** Ensure DPD is `Always On`, establish tunnel, simulate peer failure, monitor tunnel status.
- **Expected Results:** Active FortiGate detects unresponsive peer, tunnel status `Down`, FortiGate logs show DPD failure and tunnel teardown events.

6. SD-WAN Configuration Guide for VPN Optimization and Performance Report

Introduction

This section details the configuration of FortiGate SD-WAN to optimize IPsec VPN traffic, providing enhanced performance, reliability, and intelligent path selection for inter-site connectivity. By integrating VPN tunnels into the SD-WAN fabric, organizations can leverage multiple WAN links to dynamically route VPN traffic based on real-time link quality and application requirements.

Prerequisites

Before configuring SD-WAN for VPN optimization, ensure the following:

- FortiGate devices are deployed at all sites requiring SD-WAN and VPN connectivity.
- Multiple WAN interfaces are configured and connected to different ISPs or network links.
- IPsec VPN tunnels are pre-configured between the FortiGate devices, with each tunnel utilizing a distinct WAN interface.
- Administrative access to the FortiGate devices.
- FortiOS version 7.0 or later.

Network Topology (Example)

Consider a scenario with a Head Office (HO) and a Branch Office (BO), each with two WAN links and two IPsec VPN tunnels established between them.

- **Head Office FortiGate**
 - WAN1 Interface: port1 (ISP1, Public IP: 203.0.113.1)
 - WAN2 Interface: port3 (ISP2, Public IP: 203.0.113.2)
 - Internal Network: 192.168.1.0/24
 - IPsec VPN Tunnel 1 (over WAN1): HO-to-BO-VPN1

- IPsec VPN Tunnel 2 (over WAN2): HO-to-BO-VPN2

- **Branch Office FortiGate**

- WAN1 Interface: port1 (ISP1, Public IP: 198.51.100.1)
- WAN2 Interface: port3 (ISP2, Public IP: 198.51.100.2)
- Internal Network: 192.168.2.0/24
- IPsec VPN Tunnel 1 (over WAN1): BO-to-HO-VPN1
- IPsec VPN Tunnel 2 (over WAN2): BO-to-HO-VPN2

Configuration Steps

- 1. Create SD-WAN Zone:** Navigate to **Network > SD-WAN**, under **SD-WAN Zones**, click **Create New**. **Name:** VPN_SDWAN_Zone , **Type:** Software Switch . Click **OK**.
- 2. Add IPsec VPN Tunnels as SD-WAN Members:** Navigate to **Network > SD-WAN**, under **SD-WAN Interface Members**, click **Create New**. Select HO-to-BO-VPN1 and VPN_SDWAN_Zone . Repeat for HO-to-BO-VPN2 . Click **OK**.
- 3. Configure Performance SLA (Service Level Agreement):** Navigate to **Network > SD-WAN**, under **Performance SLA**, click **Create New**. **Name:** VPN_SLA_Monitor , **Protocol:** Ping , **Server:** IP of a reliable server in the remote network (e.g., 192.168.2.10). Set **Interval**, **Failures before inactive**, **Restore after**, and **Thresholds** (Latency, Jitter, Packet Loss). Apply to both VPN members. Click **OK**.
 - **CLI Configuration for Performance SLA Source:** If needed, configure source interface for probes via CLI:


```
cli config system sdwan config
members edit <member_id_for_VPN1> set source
<local_LAN_interface_IP> next edit <member_id_for_VPN2> set
source <local_LAN_interface_IP> next end end
```
- 4. Configure SD-WAN Rules:** Navigate to **Network > SD-WAN**, under **SD-WAN Rules**, click **Create New**. **Name:** VPN_Traffic_Optimization , **Source Interface:** port2 , **Source Address:** all , **Destination Address:** Branch_Office_LAN , **Service:** ALL , **Outgoing Interfaces:** VPN_SDWAN_Zone . Choose **Strategy** (e.g., Best Quality), select **Measured SLA:** VPN_SLA_Monitor . Click **OK**. Ensure this rule is prioritized correctly.

5. Configure Firewall Policies: Navigate to **Policy & Objects > Firewall Policy**, click **Create New**. **Name:** HO-LAN-to-VPN_SDWAN, **Incoming Interface:** port2, **Outgoing Interface:** VPN_SDWAN_Zone, **Source:** all, **Destination:** Branch_Office_LAN, **Service:** ALL, **Action:** ACCEPT, **NAT:** Disable, **Log Allowed Traffic:** All Sessions. Click **OK**.

6. Configure Static Routes for SD-WAN Zone: Navigate to **Network > Static Routes**, click **Create New**. **Destination:** Subnet 192.168.2.0/24, **Device:** VPN_SDWAN_Zone. Click **OK**.

7. Configure Blackhole Route (Optional but Recommended): Via CLI, create a blackhole route for the remote subnet with a higher administrative distance to prevent traffic leakage if all VPN tunnels are down.

Performance Report

To evaluate the effectiveness of the SD-WAN integration with VPN, regular monitoring and performance reporting are essential.

Key Performance Indicators (KPIs)

- **Latency:** Time delay for packets to travel from source to destination.
- **Jitter:** Variation in packet delay.
- **Packet Loss:** Percentage of packets that fail to reach their destination.
- **Throughput:** Actual data transfer rate.
- **Link Utilization:** Bandwidth usage of each WAN link.

Monitoring Tools

- **SD-WAN Monitor:** Provides real-time visibility into the status of SD-WAN members and performance metrics.
- **Log & Report:** Review Traffic Logs and System Events for traffic flow and SD-WAN/VPN events.
- **CLI Commands:** diagnose sys sdwan health-check, diagnose sys sdwan service, diagnose vpn tunnel list .

Reporting Methodology

1. **Baseline Measurement:** Establish baseline performance metrics before SD-WAN implementation.
2. **Continuous Monitoring:** Track KPIs for each VPN tunnel within the SD-WAN zone.
3. **Data Collection:** Collect data over time to identify trends and anomalies.
4. **Analysis:** Compare performance against baselines and SLA thresholds.
5. **Optimization:** Fine-tune SD-WAN rules, SLA thresholds, or network configurations based on analysis.

Sample Performance Report Structure

- **Executive Summary:** Overview of SD-WAN performance, key findings, and recommendations.
- **Current SD-WAN Status:** Overall health of the `VPN_SDWAN_Zone` and status of individual VPN tunnels.
- **Performance Metrics:** Table summarizing Latency, Jitter, Packet Loss, and Throughput for each VPN tunnel against target SLAs.
- **SD-WAN Rule Effectiveness:** Confirmation of traffic steering and examples of chosen outgoing interfaces.
- **Failover Testing Results:** Details of simulated/actual link failures, failover time, and impact.
- **Recommendations:** Suggestions for adjustments or upgrades.

7. Comprehensive VPN Testing Framework and Validation Procedures

Introduction

This section outlines a comprehensive testing framework and validation procedures for the FortiGate VPN implementation, encompassing SSL VPN, IPsec VPN, and SD-WAN integration. The goal is to ensure the functionality, security, performance, and reliability of the deployed VPN solutions.

1. SSL VPN Testing and Validation

1.1. SSL VPN Configuration Guide and Test Scenarios

Refer to the `ssl_vpn_configuration_guide.md` document for detailed configuration steps and specific test scenarios. The following is a summary of the key test scenarios:

- **Scenario 1: Successful Connection and Internal Resource Access (Full Tunnel)**
 - **Objective:** Verify successful SSL VPN connection and access to internal resources and internet via full tunnel.
 - **Validation:** Ping internal servers, access internal web applications, verify public IP through FortiGate WAN, check FortiGate logs for successful connections and traffic flow.
- **Scenario 2: Unsuccessful Connection - Invalid Credentials**
 - **Objective:** Verify denial of access for invalid credentials.
 - **Validation:** FortiClient displays authentication failure, FortiGate logs show authentication failure events.
- **Scenario 3: Unsuccessful Connection - Unauthorized User**
 - **Objective:** Verify denial of access for users not authorized for VPN.
 - **Validation:** FortiClient displays access denied, FortiGate logs show access denied events.
- **Scenario 4: Access to Restricted Internal Resources**
 - **Objective:** Verify that VPN users can only access permitted resources.
 - **Validation:** Attempts to access unauthorized resources fail, FortiGate traffic logs show `deny` actions.
- **Scenario 5: SSL VPN Disconnection and Reconnection**
 - **Objective:** Verify stable connection and proper session termination.
 - **Validation:** Clean disconnection and successful reconnection, FortiGate logs show corresponding events.

2. IPsec VPN Testing and Validation

2.1. IPsec VPN Configuration Document and Connectivity Test Results

Refer to the `ipsec_vpn_configuration_guide.md` document for detailed configuration steps and specific test scenarios. The following is a summary of the key test scenarios:

- **Test Scenario 1: Ping from Head Office LAN to Branch Office LAN**
 - **Objective:** Verify bidirectional connectivity from HO to BO through the IPsec tunnel.
 - **Validation:** Successful ping replies, no packet loss, FortiGate logs show traffic traversing the tunnel.
- **Test Scenario 2: Ping from Branch Office LAN to Head Office LAN**
 - **Objective:** Verify bidirectional connectivity from BO to HO through the IPsec tunnel.
 - **Validation:** Successful ping replies, no packet loss, FortiGate logs show traffic traversing the tunnel.
- **Test Scenario 3: Access Internal Resources (e.g., Web Server, File Share)**
 - **Objective:** Verify access to specific services on hosts in the other LAN.
 - **Validation:** Web servers and file shares accessible, FortiGate traffic logs show successful connections.
- **Test Scenario 4: IPsec Tunnel Status Monitoring**
 - **Objective:** Verify that the IPsec tunnel remains up and stable.
 - **Validation:** Tunnel status `Up` in **VPN > IPsec Tunnels** and **Monitor > IPsec Monitor**, traffic statistics incrementing, SAs active.
- **Test Scenario 5: Tunnel Rekeying**
 - **Objective:** Verify correct rekeying of Phase 1 and Phase 2 SAs without traffic interruption.
 - **Validation:** New SAs established automatically, uninterrupted traffic flow, FortiGate logs show IKE rekeying events.

- **Test Scenario 6: Dead Peer Detection (DPD) Test**
 - **Objective:** Verify detection of unresponsive peers and tunnel teardown if DPD is enabled.
 - **Validation:** Tunnel status changes to `Down` upon peer failure, FortiGate logs show DPD failure and tunnel teardown events.
- ## 3. SD-WAN Integration Testing and Validation
- ### 3.1. SD-WAN Configuration Guide and Performance Report
- Refer to the `sd_wan_configuration_guide.md` document for detailed configuration steps and performance reporting methodology. The following is a summary of key validation points for SD-WAN integration with VPN:
- **SD-WAN Zone and Member Status:** Verify that the `VPN_SDWAN_Zone` is active and both IPsec VPN tunnels are correctly added as members.
 - **Validation:** Check **Network > SD-WAN Monitor** for zone and member status.
 - **Performance SLA Monitoring:** Confirm that Performance SLAs are actively monitoring the VPN tunnels and reporting accurate metrics.
 - **Validation:** Check **Network > SD-WAN Monitor** for real-time latency, jitter, and packet loss for each VPN tunnel. Use `diagnose sys sdwan health-check` via CLI.
 - **SD-WAN Rule Effectiveness:** Verify that VPN traffic is being steered according to the configured SD-WAN rules and strategy (e.g., Best Quality).
 - **Validation:** Generate traffic and observe which VPN tunnel is utilized in **Network > SD-WAN Monitor** or through traffic logs. Use `diagnose sys sdwan service` via CLI.
 - **Failover and Redundancy:** Test the failover mechanism by simulating a failure of one of the underlying WAN links or VPN tunnels.
 - **Validation:** Observe automatic traffic redirection to the healthy VPN tunnel. Measure failover time and impact on active sessions. Check FortiGate logs

for failover events.

- **Blackhole Route Functionality:** If configured, verify that traffic is correctly blackholed when all VPN tunnels to a destination are down.
 - **Validation:** Simulate complete VPN tunnel failure and attempt to access the remote network. Verify traffic is dropped and not routed over the internet. Use `diagnose ip rtcache list` via CLI.

4. General Validation Procedures

Beyond specific test scenarios, the following general validation procedures should be performed:

- **Security Audit:** Review all configured policies, user accounts, and security profiles to ensure adherence to security best practices and organizational policies. Verify strong authentication (MFA) is enforced where applicable.
- **Logging and Alerting:** Confirm that all relevant logs (traffic, event, VPN) are being generated, stored, and forwarded to a SIEM or logging server if applicable. Test alerting mechanisms for critical events (e.g., VPN tunnel down, failed login attempts).
- **Performance Benchmarking:** Conduct performance tests (e.g., throughput, concurrent connections) under various load conditions to ensure the VPN solution meets performance requirements.
- **Documentation Review:** Ensure all configurations, network diagrams, and procedures are accurately documented and up-to-date.
- **User Acceptance Testing (UAT):** Involve end-users in testing to ensure the VPN solution meets their operational needs and provides a satisfactory user experience.

8. Conclusion

This project successfully outlines the implementation of comprehensive VPN solutions using FortiGate firewalls, covering SSL VPN for remote access, IPsec VPN for site-to-site connectivity, and SD-WAN integration for optimized VPN traffic management. Detailed architectural designs, step-by-step configuration guides, and thorough testing frameworks have been developed to ensure the security, reliability, and performance

of these solutions. By following the outlined procedures, organizations can establish robust and efficient secure communication channels, adapt to evolving network demands, and maintain high standards of data protection and network availability. The integration of SD-WAN with IPsec VPN specifically addresses the need for intelligent traffic steering and automated failover, crucial for modern distributed enterprises.

9. References

- [Palo Alto Networks Cyberpedia: Types of VPN](#)
- [Fortinet Documentation: FortiClient 7.4.3 Administration Guide - FortiGate SSL VPN Configuration](#)
- [Fortinet Documentation: FortiGate 7.6.4 Administration Guide - IPsec VPN](#)
- [Fortinet Community: Technical Tip - Configure IPsec VPN with SD-WAN](#)