

fortinet sd wan deployment guide

Fortinet SD-WAN Deployment Guide

In today's increasingly interconnected world, businesses are relying heavily on cloud-based applications and services. This reliance has made traditional WAN architectures insufficient, leading to a growing interest in Software-Defined Wide Area Network (SD-WAN) solutions. Fortinet, a leader in cybersecurity, offers a robust SD-WAN solution that combines networking and security capabilities. This guide provides a comprehensive overview of the Fortinet SD-WAN deployment process, helping organizations take full advantage of its features.

Understanding Fortinet SD-WAN

Fortinet's SD-WAN solution integrates advanced security features with WAN management, offering several advantages over conventional WAN architectures:

- Improved Performance: Using multiple WAN connections, Fortinet SD-WAN optimizes application performance by routing traffic based on real-time conditions.
- Enhanced Security: Built-in security features such as firewalls, intrusion prevention, and secure web gateways protect against various cyber threats.
- Cost Efficiency: By leveraging broadband and other cost-effective connections, organizations can reduce their reliance on expensive MPLS circuits.
- Centralized Management: A single management interface allows for simplified configuration, monitoring, and troubleshooting.

Prerequisites for Deployment

Before deploying Fortinet SD-WAN, organizations should prepare in the following areas:

1. Network Assessment

Conduct a thorough assessment of your existing network infrastructure to identify:

- Current bandwidth utilization and performance metrics
- Existing WAN technologies (MPLS, Ethernet, broadband, etc.)
- Applications in use and their bandwidth requirements
- Locations of branch offices and remote sites

2. Hardware and Licensing Requirements

Ensure you have the required hardware, which may include FortiGate devices or FortiWiFi appliances.

Additionally, verify that you have the appropriate licensing for Fortinet SD-WAN features:

- FortiGate appliances (model selection based on throughput and feature needs)
- FortiOS version that supports SD-WAN capabilities
- Additional licenses for advanced features (if needed)

3. Connectivity Options

Identify the types of internet connections available at each branch site:

- MPLS
- Broadband (DSL, cable, fiber)
- LTE/4G/5G

A balanced approach using multiple connection types can enhance redundancy and performance.

Deployment Steps

Deploying Fortinet SD-WAN involves several steps, from initial configuration to ongoing management. Below is a structured approach:

Step 1: Initial Configuration

1. Access the FortiGate Interface:

- Connect to the FortiGate device using a web browser. The default IP address is usually `192.168.1.99`.

2. Log In:

- Enter the default credentials (username: admin, password: no password).

3. Run the Setup Wizard:

- Follow the prompts to configure initial settings such as the admin password, time zone, and network interfaces.

Step 2: Configure WAN Interfaces

1. Identify and Configure WAN Links:

- Navigate to Network > Interfaces.
- Select each WAN interface and configure settings like IP addresses, DHCP, and other relevant parameters.

2. Set Link Health Monitoring:

- Ensure that each WAN link is monitored using ping or other protocols to detect link failures.

Step 3: Enable SD-WAN Features

1. Access SD-WAN Settings:

- Go to Network > SD-WAN and enable SD-WAN features.

2. Create SD-WAN Rules:

- Define rules to prioritize certain applications over others. For instance, prioritize VoIP traffic over standard web browsing.

3. Configure Performance SLAs:

- Set up Service Level Agreements (SLAs) to monitor performance parameters like latency, jitter, and packet loss.

Step 4: Security Configuration

1. Implement Security Policies:

- Create firewall rules that permit or block traffic based on your organization's security requirements.

2. Enable Security Features:

- Activate additional security features such as intrusion prevention, web filtering, and anti-malware scanning.

Step 5: Centralized Management

Utilize FortiManager for centralized management of multiple FortiGate devices. Key features include:

- Configuration Management: Push configurations across multiple devices.
- Monitoring and Reporting: Gain insights into network performance and security events.

Step 6: Testing and Validation

1. Test Connectivity:

- Validate that all links are operational and that traffic is being routed according to your SD-WAN rules.

2. Monitor Application Performance:

- Use Fortinet's reporting tools to analyze application performance and make any necessary adjustments.

3. Conduct Failover Tests:

- Simulate link failures to ensure that traffic is rerouted appropriately without disrupting services.

Best Practices for Fortinet SD-WAN

To maximize the benefits of your Fortinet SD-WAN deployment, consider the following best practices:

- **Regularly Update Firmware:** Ensure all FortiGate devices run the latest firmware for optimal performance and security.
- **Monitor Traffic Patterns:** Use Fortinet's analytics to understand traffic patterns and adjust SD-WAN configurations accordingly.
- **Implement Change Management:** Document all changes to configurations and maintain backups to facilitate recovery in case of issues.
- **Train IT Staff:** Provide training for your IT staff on Fortinet products to enhance troubleshooting and configuration skills.

Troubleshooting Common Issues

Even with a well-configured Fortinet SD-WAN, issues may arise. Here are some common problems and their solutions:

1. Link Failover Not Working

- Check Link Health Monitoring Settings: Ensure that the monitoring protocols are correctly configured.
- Validate SD-WAN Rules: Confirm that the rules allowing traffic to flow over secondary links are properly set.

2. Performance Issues with Applications

- Review Traffic Prioritization: Ensure critical applications are prioritized in the SD-WAN rules.
- Analyze Bandwidth Usage: Use Fortinet's analytics tools to identify bandwidth hogs and take necessary actions.

3. Security Alerts and Incidents

- Examine Security Logs: Check Fortinet logs to identify potential threats and take appropriate action.
- Adjust Security Policies: Update security policies based on the type of traffic and threats observed.

Conclusion

Deploying Fortinet SD-WAN can significantly enhance your organization's network performance and security posture. By following this comprehensive guide, you can effectively implement and manage your SD-WAN solution, ensuring a robust and reliable network that meets the demands of modern business operations. Whether you are a small business or a large enterprise, Fortinet's SD-WAN offers scalable solutions that can adapt to your needs while providing the security and performance essential in today's digital landscape.

Frequently Asked Questions

What is Fortinet SD-WAN and how does it work?

Fortinet SD-WAN is a software-defined wide area networking solution that enhances network performance and security by intelligently managing network traffic across multiple WAN links. It works by dynamically routing traffic based on real-time conditions and application needs.

What are the key benefits of deploying Fortinet SD-WAN?

The key benefits include improved application performance, reduced WAN costs, enhanced security features, simplified management, and better visibility into network traffic.

What are the prerequisites for deploying Fortinet SD-WAN?

Prerequisites include having FortiGate devices, a valid Fortinet license, network architecture planning, and ensuring that WAN links are in place.

How do you configure Fortinet SD-WAN for the first time?

Configuration involves accessing the FortiGate interface, enabling SD-WAN, defining WAN interfaces, creating SD-WAN rules, and configuring policies to manage traffic flows.

What is the role of FortiManager in SD-WAN deployment?

FortiManager provides centralized management for configuring, monitoring, and maintaining multiple FortiGate devices in an SD-WAN environment, simplifying policy management and reporting.

How can I monitor the performance of my Fortinet SD-WAN?

Performance can be monitored using FortiGate's built-in logging and reporting features, as well as FortiAnalyzer for more advanced analytics and insights into traffic patterns and application performance.

What security features are included in Fortinet SD-WAN?

Fortinet SD-WAN includes integrated security features such as next-generation firewall capabilities,

intrusion prevention systems (IPS), web filtering, and secure VPN functionalities.

How does Fortinet SD-WAN handle failover?

Fortinet SD-WAN uses dynamic path selection to automatically reroute traffic to the next best WAN link in case of a failure, ensuring continuous connectivity and minimal disruption.

Can Fortinet SD-WAN be integrated with existing network infrastructure?

Yes, Fortinet SD-WAN can be integrated with existing network infrastructure, allowing organizations to leverage current setups while enhancing performance and security with SD-WAN capabilities.

What kind of support does Fortinet provide for SD-WAN deployments?

Fortinet offers extensive support, including documentation, technical support, community forums, and professional services for deployment and optimization of SD-WAN solutions.

[Fortinet Sd Wan Deployment Guide](#)

Fortinet Sd Wan Deployment Guide

Related Articles

- [functional writing skills for students with autism](#)
- [free printable geography worksheets](#)
- [foundations of it service management based on itil](#)

[Back to Home](#)