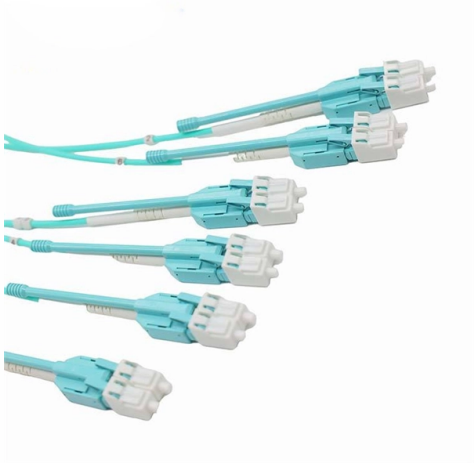
EML Selection Guide for Surveillance-Grade SD-WAN Devices



Overview

The Secure SD-WAN Ordering Guide is a complete reference for choosing and ordering Fortinet SD-WAN solutions.

Key Takeaways

Selecting the right EML for surveillance-grade SD-WAN devices requires evaluating device performance, security capabilities, centralized management, and deployment scale.

Key Considerations for EM

L Selection1. Device Performance and Throughput Surveillance-grade SD-WAN devices must handle high-bandwidth video streams and low-latency traffic. Evaluate devices based on: IPsec VPN throughput and SSL inspection capacity (Fortinet branch and hub devices provide detailed metrics for these)Concurrent session handling for multiple video feedsQoS and traffic prioritization to ensure real-time video delivery 2.

Security Features Surveillance networks require robust security to protect sensitive video data: Next-Generation Firewall (NGFW) with intrusion prevention, malware protection, and URL filtering (Cisco Security Cloud Control integration supports these features)WAN interface protection and end-to-end zone-based firewalls (HPE Aruba EdgeConnect)TLS/SSL decryption and inspection for encrypted video streamsCentralized threat analytics via Security Cloud Control or FortiAnalyzer for monitoring and logging 3.

© 2026 CGWEB NETWORK INFRASTRUCTURE - All rights reserved

Centralized Management and Orchestration Efficient EM

L deployment relies on centralized management platforms: Cisco SD-WAN Manager integrated with Security Cloud Control for policy orchestration and analyticsFortiManager and FortiAnalyzer for device provisioning, configuration, and monitoringHPE Aruba SD-WAN Orchestrator for consistent security policy deployment across multiple sites 4. Deployment Flexibility Consider the network topology and connectivity options: Branch vs. hub devices: select based on site size and traffic loadConnectivity options: DSL, PoE, WiFi, cellular (3G/4G/5G) for remote surveillance sitesVirtual and cloud support: AWS, Azure, VMware compatibility for hybrid deployments 5.

Licensing and EML Tiers

Choose EM

L tiers that match throughput, security, and analytics requirementsEnsure licenses cover advanced inspection, malware protection, and intrusion preventionFor Fortinet, the FortiAI Assistant Subscription and FortiCare Elite contracts may be required for full functionality 6.

Flow and Qo

S Management Surveillance traffic requires predictable performance: Devices like Prisma SD-WAN ION classify flows, apply QoS policies, and re-queue traffic based on application typeEnsure the EML supports dynamic path selection and policy-based routing to optimize video delivery 7.

Professional Services and Training

Consider vendor-provided deployment guides, QuickStart services, and training for SD-WAN administratorsMSSP-focused deployment workflows (Fortinet) recommend using Model Devices for consistent configuration and ZTP/LTP support Summary RecommendationFor surveillance-grade SD-WAN deployments: Select devices with high throughput, robust NGFW capabilities, and advanced QoS supportUse centralized management platforms (Cisco Security Cloud Control, FortiManager, or Aruba Orchestrator) for policy orchestration and analyticsChoose EML tiers that include advanced security, inspection, and logging featuresEnsure deployment flexibility for branch, hub, and cloud integrationLeverage professional services and training to optimize configuration and monitoring By aligning device performance, security, and centralized management with the EML tier, organizations can ensure reliable, secure, and high-performance SD-WAN for surveillance applications.

© 2026 CGWEB NETWORK INFRASTRUCTURE - All rights reserved

Article Content

16 Best SD-WAN Solutions Reviewed in 2026

The Secure SD-WAN Ordering Guide is a complete reference for choosing and ordering Fortinet SD-WAN solutions. It is designed to support a wide range of deployment needs—from small branch

Cisco Catalyst SD-WAN Security Configuration Guide, Cisco IOS XE ...

Cisco Catalyst SD-WAN edge devices support SD-WAN, routing, security, and other LAN access features that can be managed centrally. On high-end devices, you can enable all these

Secure SD-WAN Portfolio Solution Overview

Deploy the AR SD-WAN network for basic security, deploy the USG SD-WAN network for advanced security, and deploy two independent silo networks for different tenants, as shown in Figure 1-5.

BRKSEC-3058

Enable SD-WAN Application Monitoring from Health Policy User can enable/disable SD-WAN Monitoring feature from Settings -> Health -> Edit FTD Policy page By default, SD-WAN Monitoring is enabled

Managed SD-WAN Selection Guide 2026: Expert Comparison ...

In-depth Managed SD-WAN selection guide comparing 11 tools. Feature matrices, pricing analysis, use-case recommendations — free, no sign-in required.

Cisco Catalyst SD-WAN Design Guide

It discusses the architecture and components of the solution, including control plane, data plane, routing, authentication, and onboarding of SD-WAN devices. It covers redundancy of SD

BRKSEC-2708

In this session, we will explore Cisco''s robust secure SDWAN capabilities in the Catalyst, Meraki MX and Secure Firewall branch platforms. The most common deployment use cases of each will be

Secure SD-WAN Buyer''s Gui

Integrating digital experience monitoring (DEM) with SD-WAN is important to help identify issues on LAN and WAN and optimize the experience of users and organizations.

© 2026 CGWEB NETWORK INFRASTRUCTURE - All rights reserved

Secure SD-WAN Ordering Guide

SD-WAN Hub, Branches, and Management available in: Appliance Virtual Machine Cloud BRANCH BUNDLES

Cisco Catalyst SD-WAN Security Configuration Guide, Cisco IOS XE ...

For information about using a device template, see Device Configuration-Based CLI Templates for Cisco IOS XE Catalyst SD-WAN devices. To configure Interface Based Zones and

Required Capabilities for Effective and Secure SD-WAN: The

Centralized visibility of all deployed secure SD-WAN devices across the distributed organization is key. A simplified workflow to deploy and update policies with few easy clicks/steps should be included.

The Complete Guide to SD-WAN Architecture: Edge, Overlay

This guide breaks down SD-WAN architecture into five key components, explores design best practices, and provides real-world insights for deployment, procurement, and operations.

Analysis of SD-WAN Architectures and Techniques for Efficient Traffic ...

Analysis of solutions indicates that SD-WAN improves performance, reduces latency, and lowers operating costs compared to traditional WAN architectures. The paper concludes with guidelines and

10 Best SD-WAN Vendors & System Solutions

SD-WANs offer an easy, cost-effective way to unify the networks of a multi-site business. Learn which SD-WANs will get your LANs merged into a WAN easily.

Cisco Catalyst Software-Defined WAN (SD-WAN) FAQ

Cisco SD-WAN is a cloud-delivered overlay WAN architecture connecting branches to data center and multicloud environments through a single fabric. This FAQ answers questions about

BRKSEC-2708

SD-WAN Basics Traditional WAN Architecture Traditional WAN topology backhauls all internet traffic to the enterprise Data center, resulting in poor application experience, Packet Latency, drops and Jitter.

Cisco SD-WAN for Critical Networks Infrastructure

When the use of a dedicated cryptographic device is required, Cisco SD-WAN offers a transformational overlay architecture that overcomes the

© 2026 CGWEB NETWORK INFRASTRUCTURE - All rights reserved

Cisco Secure Firewall Threat Defense SD-WAN Design and Deployment Guide

SD-WAN allows for dynamic, policy-based application path selection over multiple WAN connections and facilitates integration with additional services such as WAN optimization and

Contact Us

Continue your research online:

Website: https://cgweb.co.za
Technical inquiry: https://cgweb.co.za/project-enquiry.html

This document is for preliminary research. Verify specifications against current standards, product documentation and project requirements.

© 2026 CGWEB NETWORK INFRASTRUCTURE - All rights reserved