SD-WAN: A Comprehensive Guide to Network Transformation (A Deep Dive into Cisco and Fortinet SD-WAN Solutions)

Hesham Naser Elzentani

………………………………………………………………………

Abstract

Software-Defined Wide Area Network (SD-WAN) has revolutionized the way organizations manage their WAN infrastructure. By centralizing control, providing intelligent path selection, and integrating advanced security features, SD-WAN offers significant benefits in terms of agility, cost-effectiveness, and performance. This paper delves into the fundamental concepts of SD-WAN, its key components, and its operational mechanisms. It then conducts a comparative analysis of two leading SD-WAN solutions: Cisco SD-WAN and Fortinet SD-WAN, highlighting their strengths, weaknesses, and suitability for different organizational needs.

Keywords: Network Transformation,SD-WAN, Cisco, Fortinet.

Introduction

In today's digital age, organizations are increasingly reliant on network connectivity to support remote workforces, cloud applications, and critical business operations. Traditional WAN architectures, however, often struggle to meet the demands of modern networks, characterized by increasing complexity, rising costs, and stringent security requirements. To address these challenges, organizations are turning to Software-Defined Wide Area Network (SD-WAN) technology.

SD-WAN offers a flexible and cost-effective approach to managing WAN connections by abstracting the underlying physical infrastructure and providing intelligent traffic routing. By leveraging advanced networking technologies and software-defined principles, SD-WAN enables organizations to optimize network performance, enhance security, and reduce operational costs.

SD-WAN: A Primer

Key Components of SD-WAN

1. SD-WAN Controller: The central brain of the SD-WAN network, responsible for policy enforcement, monitoring, and orchestration.

2. SD-WAN Edge Devices: Deployed at branch offices or remote sites, these devices encapsulate and decrypt traffic and select the optimal path for transmission.

SD-WAN Operation

1. Traffic Ingress: Traffic enters the SD-WAN edge device.
2. Traffic Classification: The edge device classifies traffic based on application type, priority, and other parameters.
3. Path Selection: The SD-WAN controller determines the optimal path based on network conditions and policy rules.
4. Traffic Encapsulation: The edge device encapsulates traffic for secure transmission.
5. Traffic Forwarding: Encapsulated traffic is forwarded to the destination.
6. Traffic Decapsulation: The destination edge device decapsulates the traffic and delivers it to the recipient.

SD-WAN Benefits

- Improved Application Performance: Prioritizes critical applications.
- Enhanced Network Security: Integrates advanced security features.
- Reduced Costs: Leverages lower-cost broadband internet connections.
- Simplified Network Management: Centralized management console.
- Increased Agility: Rapid deployment of new sites and services.

SD-WAN Market Growth

The SD-WAN market has experienced significant growth in recent years, driven by the increasing adoption of cloud-based applications, remote workforces, and the need for improved network performance and security. According to a report by MarketsandMarkets, the global SD-WAN market is expected to grow from USD 3.4 billion in 2021 to USD 13.7 billion by 2026, with a compound annual growth rate (CAGR) of 31.9% [1].

SD-WAN vs MPLS

There are a handful of factors to consider before shifting an organization to an SD-WAN solution from a traditional MPLS configuration.

Feature	SD-WAN	MPLS
Complexity	If security is not automatically built-in, teams need add-on options	Internet traffic backhauled to the data center
Visibility	Broad application visibility	Packet routing limits visibility
Cost	Consolidated services greatly reduce TCO	Expensive to build and maintain
Performance & Availability	Enables MPLS, broadband, LTE for high-speed	MPLS offers limited bandwidth and single point of failure

Related Work

Several studies and research papers have explored the benefits and challenges of SD-WAN. Here are some notable examples:

1. Gartner Magic Quadrant for WAN Edge Infrastructure [2].
2. Forrester Total Economic Impact™ of SD-WAN [3].
3. IDC White Paper: SD-WAN: A Catalyst for Digital Transformation [4].
4. Cisco SD-WAN Solution Briefs [5].
5. Fortinet SD-WAN Solution Briefs [6].
6. Software Defined Wide Area Network SD-WAN: Principles and Architecture [7].
7. SD-WAN: Hybrid Edge Cloud Network between Multi-site SDDC [8].
8. Software-Defined Wide Area Networks (SD-WANs): A Survey [9].
9. A survey on Software-defined Wide Area Network (SD-WAN) architectures[10].

In addition to these formal studies, numerous industry publications, blogs, and forums discuss the latest trends and best practices in SD-WAN. By staying informed about the latest developments, organizations can make informed decisions about their SD-WAN deployments.

SD-WAN: A Comparative Analysis of Cisco and Fortinet

Cisco SD-WAN

Cisco SD-WAN is a comprehensive solution that offers a wide range of features and capabilities. It leverages Cisco's extensive experience in networking to provide a robust and reliable SD-WAN platform.

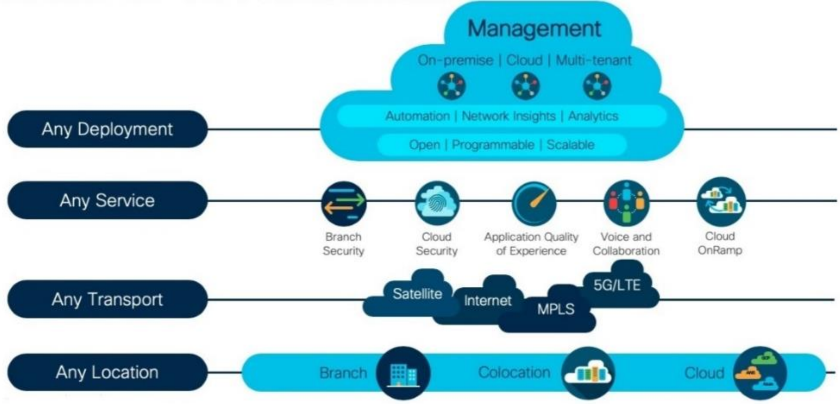

Figure 1: Cisco SD-WAN Architecture.

Cisco SD-WAN Components

Cisco SD-WAN solution is made up of four segregated planes - **Orchestration plane**, **Management Plane**, **Control Plane**, and **Data Plane**. Each plane has its own functions and responsibilities and is abstracted away from the other planes. For example, if you replace a device in the data plane, that does not affect the control/management or orchestration plane. The same applies if you replace a controller in the Control plane or the Management Plane.

1. **Cisco vManage:** Cisco vMange is the **Management Plane** of the SD-WAN system. It runs the user interface of the system and is the dashboard network administrators interact with daily. It is responsible for collecting network telemetry data, running analytics, and alert on events in the SD-WAN fabric. It is also the tool that admins use to create device templates, push configurations, and perform overlay traffic engineering.Cisco vManage can be deployed on-prem, in the public cloud, or in the Cisco cloud-hosted environment. It is significantly resource-intensive, and most customers go with the cloud options.
2. **Cisco vBond:** Cisco vBond is the **Orchestration Plane** of the SD-WAN system. Its job is to orchestrate the process of onboarding new unconfigured devices to the SD-WAN fabric. It

is responsible for the authentication and whitelisting of vEdge routers and control/management information distribution.

3. **Cisco vSmart:** Cisco vSmart is the **Control Plane** of the SD-WAN system. vSmart controllers are the brain of the overlay fabric. They advertise routing, policies, and security. They are positioned as hub routers in the control plane topology and all vEdge routers peer with all vSmart controllers. For experienced network engineers, vSmart controllers are like BGP Route-reflectors or DMVPN NHRP routers. However, it is important to understand these appliances are not part of the Data Plane and do not participate in packet forwarding.
4. **Cisco vEdge:** Cisco vEdge devices represent **the Data Plane** of the SD-WAN system. They sit at the WAN edge and establish the network fabric and join the SD-WAN overlay. If you look at the architecture shown in figure 1, everything southbound of the vEdge routers is typically traditional networking - offices, data centers, and branches. Everything northbound of the vEdge routers is the SD-WAN system itself. vEdge routers exchange routing information with the vSmart controllers over the **Overlay Management Protocol (OMP)**. If for example, we have a campus network running OSPF. At the vEdge devices, the OSPF routes are redistributed into the SD-WAN fabric to the vSmart controllers via OMP and then the vSmart controllers populate this routing information to other vEdge devices if it is required by the WAN topology.

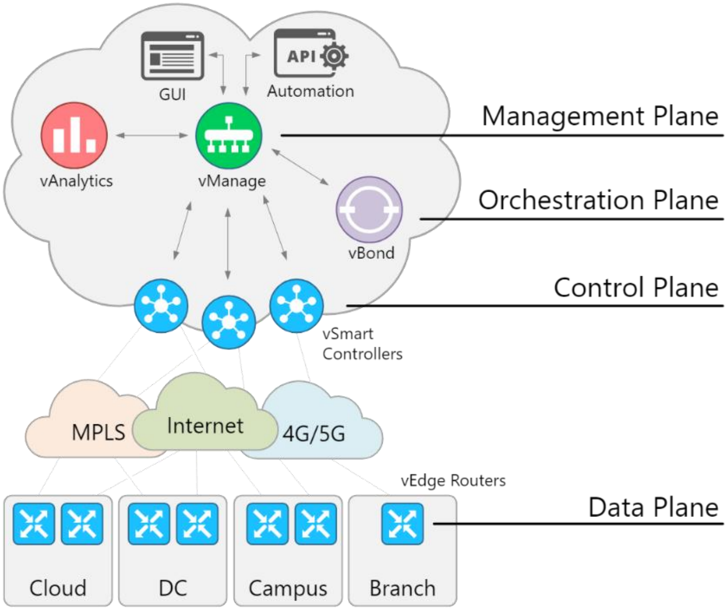

Figure 2: Cisco SD-WAN Components.

Advantages

- Advanced Routing Protocols: Supports BGP, OSPF, and EIGRP.
- Integrated Security: Provides built-in security features.
- Cloud Integration: Seamlessly integrates with cloud-based applications.
- Scalability: Easily scales to accommodate growing network needs.
- Strong Vendor Support: Offers extensive support and resources.

Disadvantages

- Higher Cost: Can be more expensive than other solutions.
- Complex Configuration: Can be complex to configure for large-scale deployments.

Fortinet SD-WAN

Fortinet SD-WAN is a powerful solution that combines SD-WAN with security features from Fortinet's FortiGate security platform.

Fortinet SD-WAN solution manages a hybrid architecture inclusive of both private WAN (MPLS) and broadband internet connectivity, The following figure illustrates theFortinet SD-WAN solution:

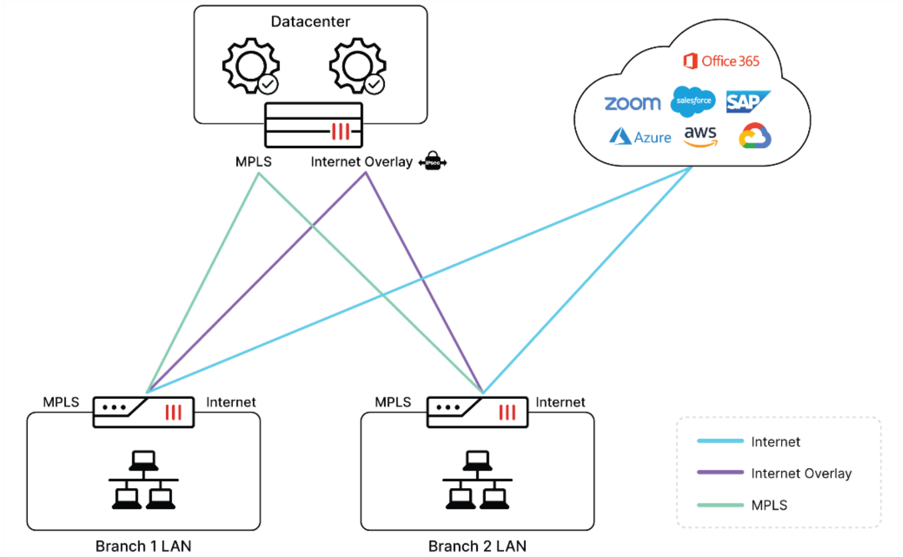

Figure 3: Fortinet SD-WAN solution.

In this example, the brancheshave multiple transports, or connectivity options, the corporate WAN MPLS network remains, but this organization has introduced a single broadband connection to provide direct internet access (DIA) from the branch. In addition, the organization has established an overlay network using Internet Protocol security (IPsec) tunnels between branches and the datacenter over the broadband internet transport. The result is that multiple paths are possible from the branch to both the datacenter and a multi-cloud environment.

The DIA inherently provides for a redundant connectivity architecture, the overlay network (IPsec tunnel) delivers an alternative path for critical applications that would normally traverse the MPLS. In the same way, the private WAN path will continue to provide its path to the internet but is now superseded by the DIA connection.

Fortinet SD-WAN Components

SD-WAN can be broken down into three layers:

1. Management and orchestration
2. Control, data plane, and security
3. Network access

The control, data plane, and security layer can only be deployed on a FortiGate firewall. The other two layers can help to scale and enhance the solution. For large deployments, FortiManager and FortiAnalyzer provide the management and orchestration capabilities FortiSwitch and FortiAP provide the components to deploy an SD-Branch.

Advantages

- Unified Security Platform: Integrates SD-WAN with advanced security features.
- Simplified Deployment: Offers a streamlined deployment process.
- Performance Optimization: Utilizes advanced techniques like WAN optimization and application acceleration.
- Cloud-Ready Architecture: Supports hybrid and multi-cloud environments.
- Competitive Pricing: Often more cost-effective than Cisco SD-WAN.

Disadvantages

- Limited Routing Capabilities: May not support advanced routing protocols as extensively as Cisco.
- Security Feature Complexity: Can be complex to configure and manage security features.

Comparison

The following table summarizes the main differences:

Feature	Cisco SD-WAN	Fortinet SD-WAN
Routing Protocols	Advanced support for BGP, OSPF, EIGRP	Limited support for routing protocols
Security	Integrated security features, but requires additional licensing	Unified security platform with advanced features
Deployment	More complex deployment	Simplified deployment with pre-configured templates
Management	Centralized management console	User-friendly management interface

Feature	Cisco SD-WAN	Fortinet SD-WAN
Cloud Integration	Strong cloud integration capabilities	Good cloud integration capabilities

Conclusion

SD-WAN has emerged as a critical technology for organizations seeking to optimize their WAN infrastructure, improve application performance, enhance security, and reduce costs. By understanding the core concepts and mechanisms of SD-WAN, organizations can leverage its benefits to drive digital transformation and achieve business objectives.

Both Cisco SD-WAN and Fortinet SD-WAN are powerful solutions that can help organizations transform their WAN infrastructure. The choice between the two depends on specific requirements and priorities. Cisco SD-WAN offers advanced routing capabilities and a strong focus on network performance, while Fortinet SD-WAN provides a unified security platform with simplified deployment.

References

1. MarketsandMarkets. SD-WAN Market by Component, Organization Size, Deployment Mode, Vertical, and Region. (2021).
2. Gartner. Magic Quadrant for WAN Edge Infrastructure. (2023).
3. Forrester. The Total Economic Impact™ Of SD-WAN. (2022).
4. IDC. (2020). SD-WAN: A Catalyst for Digital Transformation.
5. Cisco. Cisco SD-WAN Solution Briefs. (2023).
6. Fortinet. Fortinet SD-WAN Solution Briefs. (2023).
7. Fatma AL Deeb, Abdussalam Ali Ahmed. Software Defined Wide Area Network SD-WAN: Principles and Architecture. 4th International African Conference on Current Studies. (2021).
8. Junjie Wang , Michael Bewong , Lihong Zheng. SD-WAN: Hybrid Edge Cloud Network between Multi-site SDDC. Computer Networks 250. (2024).
9. Chunle Fu, Bailing Wang, Wei Wang. Software-Defined Wide Area Networks (SD-WANs): A Survey. Electronics. (2024).
10. Khirota Gorgees Yalda, Diyar Jamal Hamad, Nicolae Ţăpuş. A survey on Software-defined Wide Area Network (SD-WAN) architectures. IEEE. (2022).