Cyber Hub (/cyber-hub/) / Secure The Network (/cyber-hub/network-security/)

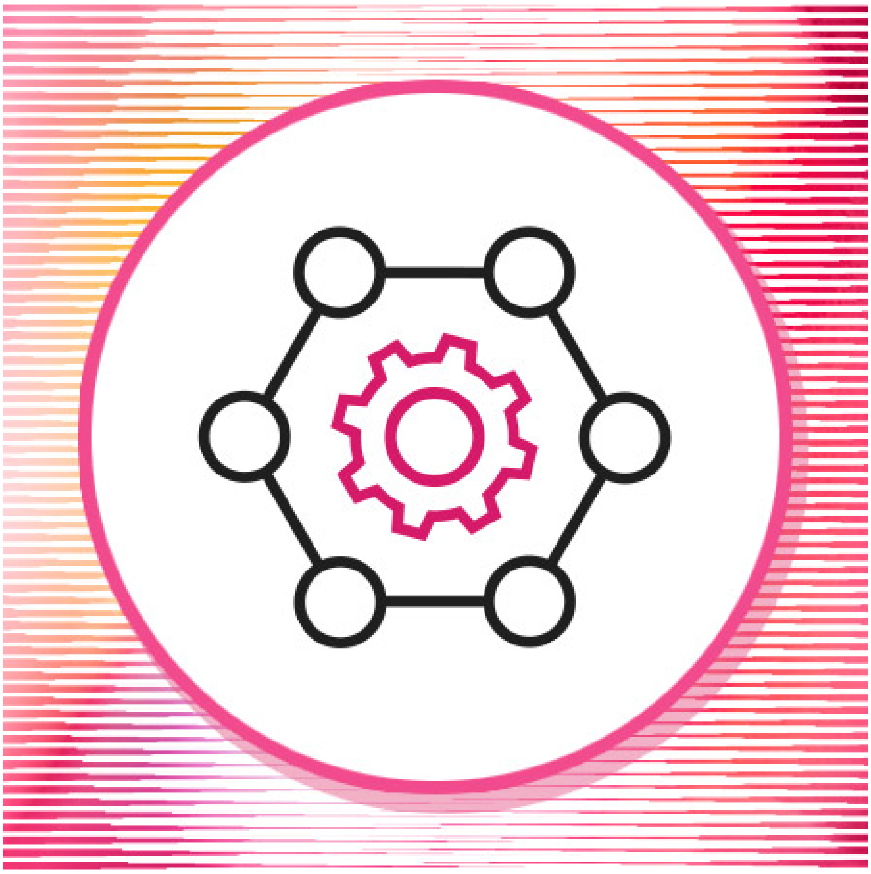
/ SD-WAN | What is Software-Defined WAN?

SD-WAN - What is Software-Defined WAN?

Software-defined WAN (SD-WAN) technology applies software-defined networking (SDN) concepts for the purpose of distributing network traffic throughout a wide area network (WAN). SD-WANs work automatically, using predefined policies to identify the most effective route for application traffic passing from branch offices to headquarters, the cloud, and the Internet. There is rarely any need to configure your routers manually in branch locations. A centralized controller manages the SD-WAN, sending policy information to all connected devices. Information technology (IT) teams can program network edge devices remotely, using low-touch or zero-touch provisioning.

Download the ESG Guide (https://resources.checkpoint.com/cyber-security-resources/esg-guide-to-optimizing-sd-wan-performance-and-security-for-any-size-business?utm_term=cyber-hub)

Learn More (https://resources.checkpoint.com/cyber-security-resources/how-to-implement-sd-wan-for-your-organization-a-simple-technical-intro?utm_term=cyber-hub)



SD-WAN Use Cases

SD-WAN technology typically creates a transport-agnostic virtual overlay. This is achieved by abstracting underlying public or private WAN connections, such as Internet broadband, fiber, long-term evolution (LTE), wireless, or multiprotocol label switching (MPLS (/cyber-hub/network-security/what-is-mpls/)). An SD-WAN overlay helps organizations to continue using their own existing WAN links. SD-WAN technology centralizes control of the network, reducing costs and providing real-time application traffic management over existing links.

The most common SD-WAN use cases fall into the following categories:

- **Geographic expansion**—when a company expands into a new geographical region, or executes a merger or acquisition, it can use the existing network services at the new location, leveraging SD-WAN to manage new and old locations using one unified policy and control interface.
- **Making better use of WAN capacity**—using a dual connectivity strategy combining public and private network services. SD-WAN can use public Internet services to offload some

private network traffic, reserving private network capacity for applications that are business critical or need low latency.

- **Improving WAN resilience**—creating a hybrid network environment with multiple network connections to the same site, operating in an active/active configuration. Under normal circumstances, traffic can be balanced between services, but if one connection is lost, traffic can fail over to another service.
- **Cloud migration**—enabling digital transformation, by migrating various applications to the cloud. SD-WAN supports application-based routing, so each application can use the wide area service that best suits its needs, whether it is deployed in the cloud or on-premises.

SD-WAN Architecture and Components

SD-WAN uses an abstracted network architecture composed of two separate parts:

- **A control plane**—operated from a central location, meaning that IT staff can manage WAN resources remotely without being on-premises
- **A forwarding plane**—manages traffic flows, dynamically configuring network resources according to policies set by the control plane

An SD-WAN architecture consists of the following components:

- **Edge**—this consists of network equipment deployed in the cloud, in on-premises data centers, or in branch offices.
- **Controller**—provides centralized management and enables operators to visualize and monitor the network and set policies.
- **Orchestrator**—a virtualized network administration component, which monitors traffic and enforces policies and protocols as defined by the controller.

SD-WAN Concepts

SD-WAN implementations leverage a wide range of technologies, including:

Controller

A centralized controller that manages SD-WAN deployments. The controller enforces security and routing policies, as well as monitors the virtual overlay, any software updates, and provides reports and alerts.

Software-defined networking (SDN)

Enables key components in the architecture, including the virtual overlay, the centralized controller, and link abstraction.

Wide area network (WAN)

Responsible for connecting geographically separated facilities or multiple LANs, using either wireless or wired connections.

Virtual network functions (VNFs)

First-party or third-party network functions, such as caching tasks and firewalls. VNFs are typically used for the purpose of reducing the amount of physical appliances or to increase flexibility and interoperability.

Commodity bandwidth

SD-WAN technology can leverage multiple bandwidth connections and assign traffic to any specific link. This provides users with more control and enables cost savings, by moving traffic from traditional costly MPLS lines to low cost commodity bandwidth connections.

Last-mile technology

SD-WAN technology can improve existing last-mile connections through the use of more than one transport link or by simultaneously using multiple links.

What is the Difference Between WAN and SD-WAN?

Let’s look at the key differences between traditional WAN and SD-WAN solutions.

WAN	SD-WAN
Load balancing and disaster recovery available, but can be complex to deploy	Load balancing and disaster recovery built in with fast or zero-touch deployment

Configuration changes take time and require manual configuration work, which is error prone	Real-time configuration changes, automated to prevent human error
Requires edge devices to be configured one by one, does not allow blanket application of policies	Uses virtual overlays—can replicate policies instantly across large numbers of edge devices
Limited to one connectivity option—legacy MPLS lines	Can make optimal use of multiple connectivity options—MPLS and SDN-managed broadband lines
Relies on VPNs, which work well with a single IP backbone, but cannot coexist with high throughput workloads like voice and video	Able to steer traffic for different types of applications, conserving bandwidth for the applications that need it most
Requires manual tuning	Detects network conditions automatically and can dynamically optimize the WAN

SD-WAN Best Practices

Use Public Internet Selectively

SD-WAN can use public Internet connections for all middle mile transmissions, and while this can be extremely cost effective, it is not advised. There is no way to know which links traffic will go through, raising security and performance concerns.

Whenever possible, especially for sensitive or mission critical communication, prefer to transmit SD-WAN traffic over private networks. Some SD-WAN providers let you use their own secure global network. Reserve public Internet capacity for non-critical and non-sensitive workloads, or failover scenarios when the private network is down.

Communicate the Deployment Process to Stakeholders

When embarking on an SD-WAN project, educate stakeholders about the deployment process and explain that SD-WAN is an addition to existing network infrastructure. Executives should not view SD-WAN as a simple drop-in replacement for traditional network technology.

Make it clear that you need to keep the existing technology and integrate it with new SD-WAN investments. A better understanding of the technical background and deployment methods will give you better leadership support.

Test the SD-WAN Service

SD-WAN solutions may offer automation and zero touch deployment, but you need to verify that it works as expected. Testing is often overlooked, but it is a critical part of an SD-WAN project. Ensure you test extensively before, during, and after implementation. A typical SD-WAN project involves testing over 3-6 months, focusing on quality of service (QoS) (/cyber-hub/network-security/what-is-quality-of-service-qos/), scalability, availability and failover, and reliability of management tools.

SD-WAN Security and SASE

The SD-WAN model operates using a distributed network fabric, which typically does not include the security and access controls needed to protect enterprise networks in the cloud.

To address this problem, Gartner proposed a new network security model called secure access service edge (SASE) (/cyber-hub/network-security/what-is-secure-access-service-edge-sase/). SASE combines WAN functionality with security features such as:

- Firewall as a Service (FWaaS) (/cyber-hub/network-security/firewall-as-a-service-fwaas/)
- Secure web gateway (SWG) (/cyber-hub/network-security/what-is-secure-web-gateway/)
- Cloud access security broker (CASB) (/cyber-hub/cloud-security/what-is-casb/)
- Zero trust network access (ZTNA) (/cyber-hub/network-security/what-is-zero-trust-network-access-ztna/)

The combination of these security capabilities, built for a cloud environment, makes it possible to ensure SD-WAN networks are secure.

SASE solutions provide mobile users and branch offices with secure connectivity and consistent security. They provide a centralized view of the entire network, allowing administrators and security teams to identify users, devices and endpoints across a globallydistributed SD-WAN, enforce access and security policies, and provide consistent security capabilities across multiple geographical locations and multiple cloud providers.

SD-WAN with Check Point

Prior to SD-WAN remote office connections were backhauled to the corporate data center where they were protected using the corporate network security stack. With the advent of SD-WAN, cloud and Internet connections connected directly to the Internet expose WAN users to sophisticated attacks.

Firewall as a Service (/cyber-hub/network-security/firewall-as-a-service-fwaas/) and Secure Access Service Edge (SASE (/cyber-hub/network-security/what-is-secure-access-service-edge-sase/)) solutions protect SD-WAN connections to cloud applications and the Internet. To learn more about Check Point's SASE solutions and how they can improve your organization's WAN security, contact us (/about-us/contact-us/). You're also welcome to request a demonstration (https://pages.checkpoint.com/cloudguard-connect-demo.html) to see Check Point's SASE solution in action.

SD-WAN Articles

Benefits of SD-WAN (/cyber-hub/network-security/what-is-sd-wan/benefits-of-sd-wan/)

MPLS Alternatives (/cyber-hub/network-security/what-is-sd-wan/mpls-alternatives/)

SD-WAN Solutions (/cyber-hub/network-security/what-is-sd-wan/what-are-sd-wan-solutions/)

SD-WAN vs MPLS (/cyber-hub/network-security/what-is-sd-wan/sd-wan-vs-mpls/)

SD-WAN vs VPN (/cyber-hub/network-security/what-is-sd-wan/sd-wan-vs-vpn/)

Get Started

Must-Haves of an SD-WAN Solution – eBook (https://resources.checkpoint.com/network-security/must-haves-of-an-sd-wan-solution-ebook?utm_term=cyber-hub)

Personal Demo of Quantum SD-WAN (https://pages.checkpoint.com/quantum-sd-wan-demo-request.html?utm_term=cyber-hub)

SD-WAN Security (/solutions/sd-wan-security/)

Secure Access Service Edge (SASE) (/products/cloudguard-connect-sase/)

Secure Corporate Access (/odo/platform-overview/)

Related Topics

What is Secure Access Service Edge (SASE)? (/cyber-hub/network-security/what-is-secure-access-service-edge-sase/)

What is Zero Trust Network Access (ZTNA)? (/cyber-hub/network-security/what-is-zero-trust-network-access-ztna/)

What is Firewall-as-a-Service (FWaaS)? (/cyber-hub/network-security/firewall-as-a-service-fwaas/)

What is MPLS? (/cyber-hub/network-security/what-is-mpls/)

Recommended Resources

Check Point a Leader in the Forrester Wave™ for Enterprise Firewall Report

(https://pages.checkpoint.com/forrester-wave-for-enterprise-firewalls-2022.html?utm_term=cyber-hub&utm_content=td)

Check Point Firewall Company of the Year by Frost & Sullivan

(https://resources.checkpoint.com/cyber-security-resources/frost-sullivan-check-point-company-of-the-year?utm_term=cyber-hub&utm_content=td)

Combat Against Sophisticated Cyber Attacks with Check Point's Next...

(https://pages.checkpoint.com/nex
generation-firewall-buyers-guide.html?utm_term=cyber-hub&utm_content=td)