JUNIPER NETWORKS | Engineering Simplicity

eGuide

Avoiding SD-WAN Buyer's Remorse

Key Considerations to Ensure SD-WAN Success

February 2020

SD-WAN: An Introduction

SD-WAN largely exists to support two key enterprise transformations: multicloud and the software-defined branch (SD-Branch).

Multicloud has changed the enterprise applications landscape, and with that, traffic patterns.

Traffic no longer needs to flow to enterprise data center sites or central internet peering points and breakouts. Most user and device traffic from inside enterprise campuses and branches go to cloud-based applications scattered across a host of different clouds.

This is neither economical nor efficient.

To optimize multicloud-bound traffic cost and performance, modern WAN edge routers, or customer premises equipment (CPE), are now equipped with hybrid WAN links and routing. Hybrid WAN interfaces may include WAN provider-dedicated links such as MPLS, as well as direct internet links over xDSL, broadband and 4G/LTE wireless.

However, these will impact your security. The move to cloud has effectively multiplied the attack surface and introduced new sources of risk. To protect your users, data and business, your SD-WAN must include effective security at all touchpoints.

So where does SD-WAN come into this?

SD-WAN involves the ability to route application traffic over hybrid WAN connections dynamically, based on policy constraints, the variable state of the network links, and the end-to-end experience of reaching applications.

With the shift to SD-WAN, CPE devices are now remotely managed with abstract control and automated workflows across all sites. SD-Branch provides an expanded view of the branch's entire network, including security, LAN switching, Wi-Fi and other branch-based infrastructure.

> **"Some SD-WANs give you security, others simply provide a connection. With Juniper, get the best of both with NG Firewalls, Universal Threat Management, and Advanced Threat Protection."**

WAN Edge Devices

Not all branch CPE devices are created equal:

- Some may solve your routing or security challenges but are not SD-WAN.
- Some may secure your SD-WAN but force you to use a specific security solution despite your preferences.
- Some CPE lock you into an SD-WAN vendor or a service provider.
- Some may work for your branch, but not for larger campuses or your public cloud sites.

Major types of WAN edge CPE devices suitable:

- SD-WAN dedicated appliances
- Legacy branch routers with SD-WAN and security bolted on
- Next-generation firewalls that support SD-WAN
- Universal CPE devices supporting SD-WAN
- Virtual CPE devices primarily used for a WAN edge

> **“Give your branch users a sense of relief when working with customers by giving them the best application performance.”**

SD-WAN networking and management

Managing a software-defined network should be simpler than a legacy network. However, many won't combine secure connectivity and security threat management. Some don't even provide granular visibility of users, traffic, applications, threats and automatic network changes.

In some solutions, management is restricted by its design and how it controls vendor-specific gateways and proprietary that won't integrate efficiently with traditional WAN and data centers.

The networking and management aspects of SD-WAN solutions are highly variable. Choosing the right solution is a challenge. You must prepare for tomorrow, so you need to consider how to keep your architecture and operations flexible and evolvable.

Start your SD-WAN journey by asking these questions about your branch WAN edge devices:

CPE device range

"Are your branch and campus performance needs covered? Are there any networking interface-type constraints?"

Internet-facing connections

"How do you mitigate risk?"

CPE reliability

"Can they be clustered together to increase performance and availability?"

Legacy routing devices

"Can SD-WAN and security be supported without affecting performance and evolvability?"

Virtual CPE

"Are equivalent virtual form factors available for public and private clouds?"

Legacy CPEs

"Outfit branches with SD-WAN in front or replace and simplify sites?"

uCPEs

"Can you integrate with your own branch security, WAN optimization or applications?"

Integrated management

"How is the rest of the branch and campus security, LAN and WLAN managed?"

Management organization

"Can you go multi-tenant/ multi-department for ease of control and security?"

Observability

"Can service-level indicators be used for user and application experience?"

Simplicity

"Can you scale operations with abstract routing and security automation?"

Remote management

"Can you use zero-touch-provision devices?"

Gateways and topologies

"Are you locked into specific gateways? Can you design your own? Does it support dynamic links to optimize paths?"

Choice of vendors

"Is the solution offered by multiple trusted providers? Is there freedom to do it yourself?"

Futureproofing

"Can you interoperate/federate with another SD-WAN and open standards-based routing?"

Security and SD-WAN routing

"Is it tightly coupled, integrated, or loosely coupled for future flexibility?"

Management options

"Are on-premise and cloud-managed options available?"

Internet breakouts

"Are they supported only at site spokes, or hubs? What about waypoints to cloud-based security like Zscaler?"

Juniper SD-WAN: Get better, simplified SD-WAN

Your network is expanding. It's happening, so an evolvable architecture is crucial to be able to successfully manage your brand, WAN, LAN, Wi-Fi, and security. Juniper Contrail SD-WAN enables that growth in a simple, consistent and effective way that doesn't compromise security.

Contrail SD-WAN features include:

SD-WAN, LAN, Wi-Fi and security:
See, secure and deliver any or all of these across your branch and campus sites in a single place.

Operations simplicity:
Experience SDN without the need to run any software or choose on-premise software for control on your own terms. Both options come with smart default policies that manage thousands of enterprise applications.

Optimize application experience and performance:
Quality-of-experience sensors and management combined with fine-grained dynamic path selection offer best controls to improve application performance, resiliency and ultimately user experience.

Optimize WAN costs:
Rule all your WAN edge interfaces like MPLS, broadband, xDSL, TI/EI, T3/E3 and 4G LTE wireless links through one system. Design policies to maximize best performance and economics.

No need for local IT expertise:
Simply ship our secure CPE or universal CPE to your site and experience zero-touch provisioning (ZTP) for instant access.

Deep integral security:
In addition to strong routing, Juniper SRX & NFX Series, and vSRX WAN edge devices all offer next-generation firewalling, universal threat management, and the option to add more advanced threat protection.

Software-define your WAN, LAN and your entire branch:
Don't stop with SD-WAN. Manage all aspects of your branch using the very same software. Enjoy simpler operations in all aspects of your branch network.

> **"Set up a zero-touch branch in minutes without leaving your desk."**

Further reading

If you'd like to take a more detailed look at SD-WAN technology from an enterprise perspective, take a look at these two executive briefings from STL Partners:

Enterprise Networking Challenges: How Can SD-WAN Help?

Flavors Of SD-WAN: What's On Offer, And Which Work?

Head to juniper.net/sdwan to explore demo playlists on SD-WAN and SD-LAN features in action

Experience Juniper cloud-managed SD-WAN first-hand today

Sign up now for your free product tour

Corporate and Sales Headquarters

Juniper Networks, Inc.

1133 Innovation Way
Sunnyvale, CA 94089 USA

Phone: 888-JUNIPER
(888-586-4737) or +1.408.745.2000

Fax: +1.408.745.2100

APAC and EMEA Headquarters

Juniper Networks International B.V.

Boeing Avenue 240
119 PZ Schipol-Rijk
Amsterdam, The Netherlands

Phone: +31.0.207.125.700

Fax: +31.0.207.125.701

PN 7400108-003-EN

Please Note:

This guide contains general information about legal matters.
The legal information is not advice, and should not be treated as such.

Any legal information in this guide is provided “as is” without any representations or warranties, express or implied. Juniper Networks makes no representations or warranties in relation to the information in this guide.

You must not rely on the information in this guide as an alternative to legal advice from your attorney or other professional legal services provider. You should never delay seeking legal advice, disregard legal advice, or commence or discontinue any legal action because of information in this guide.

Information correct at time of publication (February 2020).

JUNIPER NETWORKS | Engineering Simplicity