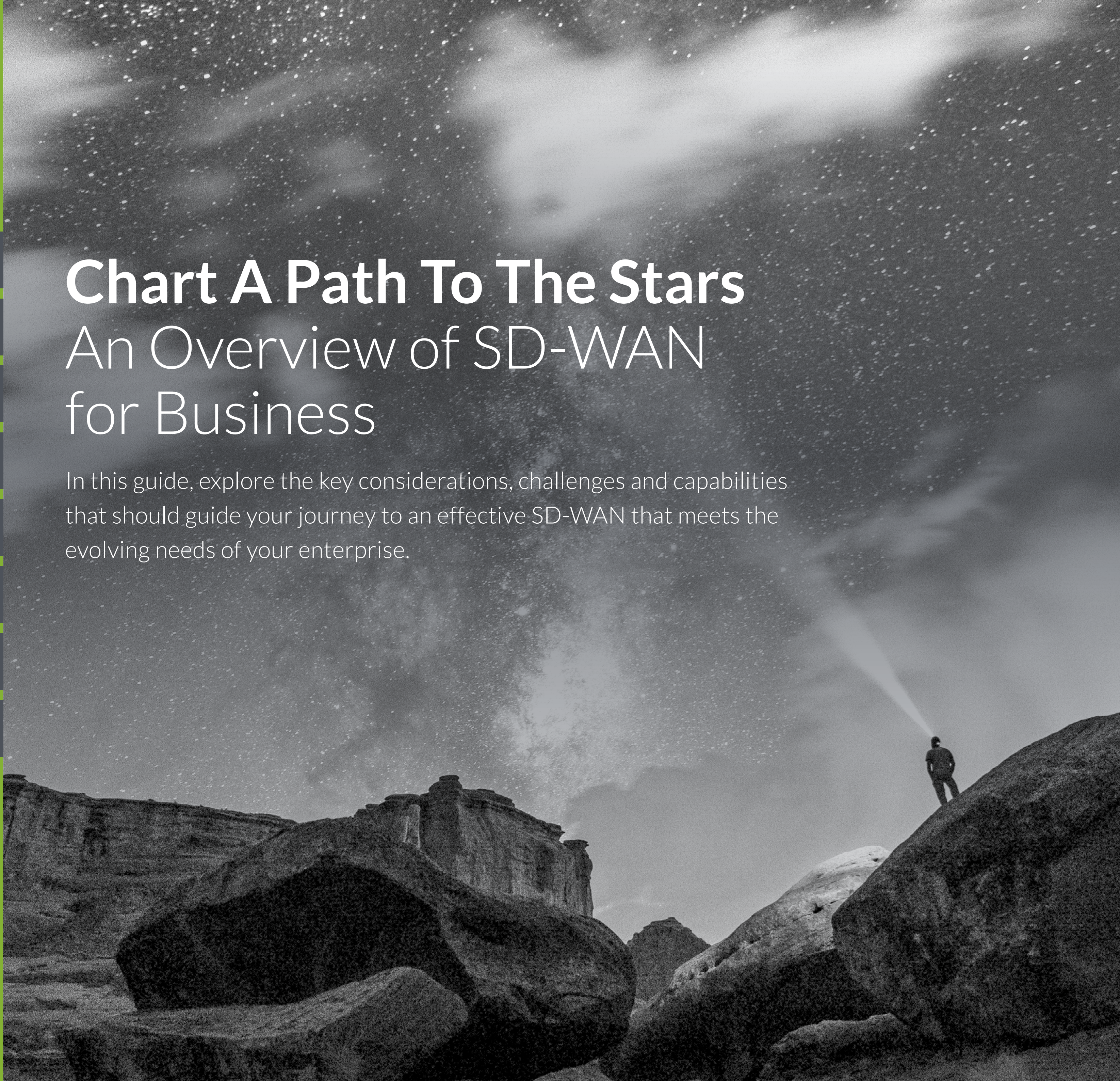


Chart A Path To The Stars An Overview of SD-WAN for Business

In this guide, explore the key considerations, challenges and capabilities that should guide your journey to an effective SD-WAN that meets the evolving needs of your enterprise.

Introduction

Seven Major Challenges

CPE

Networks

Topologies

Security

Extension

Juniper's Solution

PARTNERS

Introduction

Enterprises throughout the world are rapidly digitizing their operations and adopting a multicloud environment. Unfortunately, legacy WAN architecture models often do not provide the scale, flexibility or agility required to support this transition. Enter SD-WAN.

No single platform will be able to deliver every piece in the jigsaw for every type of enterprise and every application-specific set of requirements. The key is to select vendor partners whose platforms are sufficiently open, modular and comprehensive in their functionality and components that they will be able to adapt to enterprises' increasingly varied, flexible and exacting networking and compute requirements going forward.

Only by doing so will they secure the ability to stay ahead in a multicloud future.

To read more on this topic, click here to read the full executive briefing: Predicting The Future: Where Next For SD-WAN Services?

Introduction

Seven Major Challenges

CPE

Networks

Topologies

Security

Extension

Juniper's Solution

The Seven Major Challenges

Any decision made about SD-WAN aspects or management must be taken not just in context of enterprises' current networking challenges, but also in the context of how these challenges, as well as networking technology, are likely to evolve.

There are seven major enterprise networking challenges for which SD-WAN can be a major part of the solution. These are:

- Managing the costs of WAN links
- Improving control of hybrid WAN and multicloud environments
- Assuring service and prioritizing business-critical traffic
- Introducing new sites and capabilities
- Preventing attacks and mitigating security risks
- Managing different network domains and services across the whole enterprise
- Future-proofing enterprises' advancing requirements while reducing complexity

To read more on this topic, click here to read the full executive briefing: Enterprise Networking Challenges: How Can SD-WAN Help?

Introduction
Seven Major Challenges
CPE
Dedicated Appliances
uCPE
Cloud
Networks
Topologies
Security
Extension
Juniper's Solution

Consideration 1: CPE Deployment

Dedicated Appliances

Installed at each enterprise site, these host a closed and pre-integrated set of virtual network functions (VNFs), such as firewall, routing, WAN optimization, policy management, VPN, etc. Dedicated SD-WAN appliances are typically installed and managed by the enterprise itself, with support from the vendor, and the WAN services are delivered as an SDN overlay across multiple, physical service provider networks.

What to know:

- Dedicated, vendor-supplied CPE offers little flexibility for enterprises to upgrade, add or change VNFs and features.
- A fully software overlay-based service entails less ability to guarantee service levels, security, redundancy etc.
- The need to replace existing networking CPE and services with the SD-WAN appliance and service can bring disruption and unexpected upfront costs to the business.

Read the Full Executive Briefing

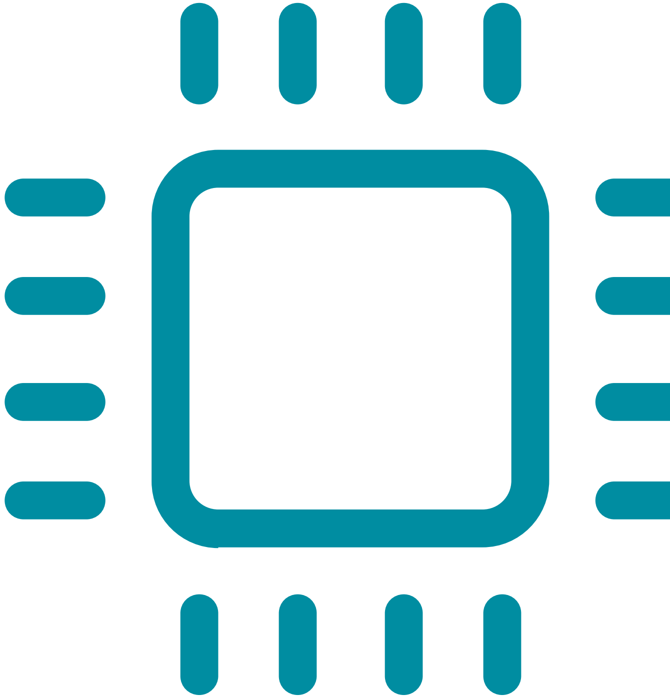
Consideration 1: CPE Deployment

Universal CPE (uCPE)

Here, the SD-WAN VNFs are hosted on a vendor-neutral, 'universal CPE' (uCPE) appliance – typically but not always based on an Intel x86 chipset – that can run additional SD-WAN, VNFs and other software (including security) from the same or other vendors. It provides more flexibility to make device configuration changes, carry out VNF software upgrades, and bring new sites into service without needing to dispatch engineers across an increasingly sprawling network footprint.

What to know:

- Enterprises purchasing uCPE appliances should not be pressured into also using the vendor's SD-WAN solutions too.
- Many enterprises will choose not to run SD-WAN on their uCPE appliances. You may like the flexibility to deploy arbitrary virtual machines (VMs) on the uCPE alongside VNFs, which is an increasingly popular option.
- If enterprises are looking for the dynamic, policy-driven routing capabilities of SD-WAN, they are better off turning to a combined SD-WAN and uCPE management solution from a service provider or single vendor. However, if they do not need all of these capabilities but are still set on a uCPE, they need to look for products offering simple network management with VNF and chaining abilities.



Read the Full Executive Briefing

Introduction
Seven Major Challenges
CPE
Dedicated Appliances
uCPE
Cloud
Networks
Topologies
Security
Extension
Juniper’s Solution

Consideration 1: CPE Deployment

Cloud CPE, or ‘vCPE’

The SD-WAN appliance can be offered as a VM hosted in the enterprise, public or service provider cloud, rather than as an on-premises device. Cloud CPE is relevant to any enterprise with applications in the public cloud that need to be on the enterprise network. This mode of SD-WAN presents minimal upfront equipment or integration costs and offers enterprises the ability to consume WAN services on a pay-per-use basis like any other cloud service.

What to know:

- Cloud CPE-based SD-WAN is also often combined in a hybrid form with dedicated CPE- or uCPE-based SD-WAN, depending on a range of factors. These include the preference of many enterprises to retain on-premises networking facilities alongside cloud-based solutions for reasons of security, redundancy and desire to maximise existing infrastructure investments.
- Cloud CPE-based SD-WAN is relevant for rapidly growing or changing businesses whose networking requirements are expanding and evolving fast, and who need to manage the complexity and costs involved while ensuring enough connectivity and bandwidth for mission-critical applications.
- Assess carefully whether an overlay-based, cloud CPE-delivered SD-WAN can ensure compliance with service level, security and redundancy requirements to the same extent as a managed SD-WAN.
- Consider too whether cloud CPE can offer sufficiently granular, application-specific routing and performance management compared with SD-WAN supported by on-premises appliances.

Read the Full Executive Briefing

Consideration 2: Networks

Overlay

Under the model of SD-WAN based on dedicated CPE, the WAN services are delivered as an SDN overlay across multiple, physical service provider networks. This mode of delivery is also used for some SD-WAN services supported by uCPE or cloud CPE, although a higher proportion of uCPE-based services are provided over hybrid or dedicated infrastructure. The overlay mode of SD-WAN can be an effective means for enterprises to manage the costs of WAN links, by enabling the routing of WAN traffic across broadband access connections and the public internet as a low-cost alternative to IP-MPLS and dedicated Internet lines.

What to know:

- Ripping out networking kit and replacing a managed IP-MPLS WAN service with SD-WAN equipment and overlay-based networking is not a pain-free option with some vendors.
- Depending on which vendors you engage, overlay-based SDN offers fewer guarantees in the areas of service levels, security and redundancy.

Read the Full Executive Briefing

Consideration 2: Networks

Hybrid

In hybrid delivery mode, SD-WAN connectivity is generally provided over a hybrid combination of a service provider's networks and services (e.g. Ethernet, IP-MPLS) and overlays on the public internet. Sourcing the SD-WAN from a hybrid combination of dedicated network platforms, public internet and broadband access links supports policy-driven, dynamic switching and prioritization of network traffic across different network domains, and also enables tighter integration between the SDN overlay and the network underlay.

What to know:

- Service provider networks tend nowadays to support dedicated, direct internet breakout connections to leading public cloud providers, such as AWS or Microsoft Azure. SD-WAN providers can therefore manage network performance and traffic prioritization end-to-end across the WAN and the hybrid (private and public) clouds to which it is connected.
- Enterprises should consider vendor or service provider partners that can offer sufficient scale or depth of network coverage, skills and support to ensure trouble-free integration, implementation and operation.
- Similarly, enterprises should seek assurance that a SD-WAN platform is sufficiently open and interoperable with other vendors' VNFs and SD-WAN products.
- Larger enterprise customers typically have specialized network management personnel that can manage SD-WAN services themselves. However, enterprises can also opt to outsource management, monitoring and configuration tasks to a SD-WAN vendor or service provider.

Read the Full Executive Briefing

Consideration 2: Networks

Dedicated

A less common mode of SD-WAN delivery is when the service is provided end-to-end across a dedicated SD-WAN software and hardware platform: either across a single service provider's infrastructure or across a federated SD-WAN platform connecting multiple service provider networks. There is no single management model for this and providers vary in the degree to which they place management in the hands of the enterprise user via a centralized portal or carry out all configuration and administration tasks themselves on behalf of their enterprise clients.

What to know:

- Enterprises are able to obtain strict guarantees around network security, data sovereignty, redundancy, SLAs, etc. But this may come at the expense of lock-in to a service provider's network and SD-WAN platform, and reduced ability to take charge of the process of evolving the virtualized networking services deployed across the network.

Read the Full Executive Briefing

Consideration 3:

Network Topologies

Consider the degree to which a SD-WAN solution supports different WAN topologies, such as:

Hub and Spoke

A single site acts as the "hub" through which other branches connect. This mirrors the traditional, simple approach to designing a WAN, in which functions such as security and traffic inspection take place at a central point.

Full Mesh

All branches of the network are interconnected, and traffic can pass between them freely. This enables more efficient peer-to-peer apps (such as conference calling) but is complex to design and provision.

Partial Mesh

A hybrid approach, where sites are divided into logical groups (such as geographic regions), each of which has its own central hub. This may give a "best of both" balance of performance benefits while keeping design and provision as simple as possible.

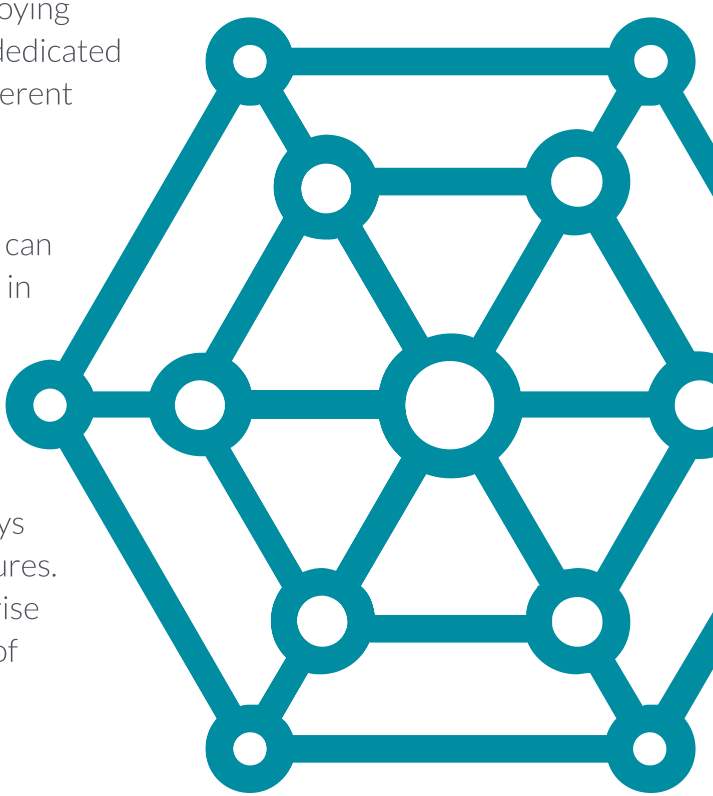
Read the Full Executive Briefing

Consideration 3:

Network Topologies

What to know:

- Not all SD-WAN platforms and appliances (physical and virtual) support all of these modes. Consequently, enterprises need to plan SD-WAN deployments carefully to ensure their chosen platforms and services will support the evolution of their network topology, and so help them deal with the challenge of managing different domains and services across the enterprise and its burgeoning hybrid network footprint.
- Enterprises need to consider the respective benefits of deploying physical or virtual hub gateways instead of – or alongside – dedicated SD-WAN CPE or uCPE-hosted SD-WAN, along with the different hub form factors (i.e. physical router, physical firewall, virtual router or virtual firewall).
- Deploying SD-WAN capabilities in public cloud-hosted hubs can help with the challenge of introducing new sites, particularly in cases where it is important to control 'traffic sovereignty' (i.e. where data is physically flowing and processed) alongside data sovereignty (where data is stored).
- SD-WAN hubs can be strategically placed at co-location sites, making them physically close to the multicloud highways used by many SaaS applications and public cloud infrastructures. This makes them a low-cost, flexible way to optimize enterprise WANs to enhance the performance and reduce the latency of mission-critical application data flows.



Read the Full Executive Briefing

Introduction
Seven Major Challenges
CPE
Networks
Topologies
Security
What to know
Extension
Juniper's Solution

Consideration 4:

Security

The SD-WAN proposition centers on integration of threat and traffic visibility in the analytics view. Enterprises no longer need separate firewall appliances or VMs — and the associated management burden – as the firewall functionality can be handled by the same CPE and platform as the routing.

This sort of offer is an obvious response to the inherent security risks of SD-WAN, which involves carrying more WAN traffic over the public Internet, where the multiplication of endpoints and internet gateways expands the attack surface. When deep security measures, such as next-generation firewalling and unified threat management (UTM) are provided as an integral part of an SD-WAN solution, this potentially eliminates the complexity, network load, and risks of adding a separate security layer on top of SD-WAN networking.

Enterprises need to plan carefully how to build enhanced security in to their SD-WAN services, or how to add networking to their existing firewall and security appliances and platforms. For example, when it comes to CPE, the options are similar to those for SD-WAN CPE:

1. Dedicated appliances —routers, secure routers or firewall — to which further security software or SD-WAN VNFs respectively can be added by the vendor or service provider: enterprise self-management option.
2. uCPE hosting SD-WAN VNFs alongside other networking and security functions: installation, implementation and lifecycle management generally outsourced; day-to-day operational management/configuration changes etc. by the enterprise.
3. Cloud-hosted, -delivered and -managed security, e.g. firewall, UTM, DPI etc. hosted at the WAN edge/edge cloud, internet breakout points or WAN/cloud hubs and gateways: outsourced, on-demand business model, with vendor or service provider taking responsibility for management, upgrades, etc.

Read the Full Executive Briefing

Consideration 4:

Security

What to know:

- Choosing integrated security is not always a no-brainer decision. There are further aspects to consider, such as whether a security-focused vendor is able to provide a comprehensive networking feature set, and how well the integrated security measures perform. In many cases, the decision not to use an SD-WAN solution with integrated security will be influenced by an organisation's existing WAN deployment model.
- An option that is increasingly popular for enterprises is installing SD-WAN VNFs on existing branch routers and branch secure routers. However, enterprises should be aware of the potentially detrimental impact on throughput of running SD-WAN over legacy routers.

Read the Full Executive Briefing

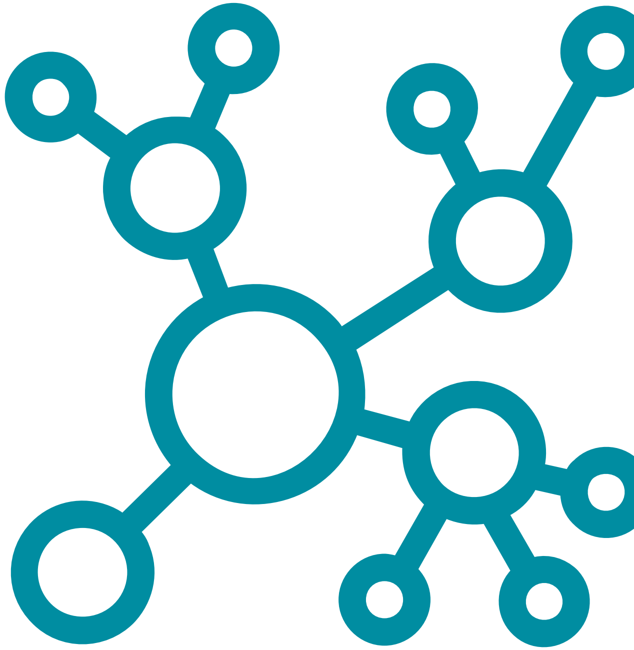
Consideration 5: Extension across geographies and domains

Implementation of Multiple SD-WANs Throughout the Enterprise

Increasingly, many larger enterprises are deploying multiple SD-WAN platforms from different vendors. These can be used to support different geographies, applications, legacy network environments and departments within the enterprise. In addition, there may be a need to assure data sovereignty (where data is stored) and traffic sovereignty (where it flows) so that retaining an existing SD-WAN platform and separating it from platforms and clouds used elsewhere in the enterprise can be an effective means to achieve this goal.

What to know:

- The multi-SD-WAN approach could be seen as a driver of growing ICT complexity across the enterprise as much as it is a means to resolve or manage that complexity.
- From a technological standpoint, the solution to multi-SD-WAN interoperability is likely to be the open standards-based Border Gateway Protocol (BGP), which has been used effectively for traditional enterprise or carrier WAN routing. However, in cases where service providers are already contending with multiple platforms, other less-proven protocols are sometimes being used.



Read the Full Executive Briefing

Consideration 5: Extension across geographies and domains

The Software-Defined Enterprise (SD-Enterprise)

One of the means by which SD-WAN does have the potential to help manage ICT complexity is by expanding into other areas of enterprise networking, such as the branch, LAN and Wi-Fi. Various terms are used to describe this expansion, e.g. 'SD-Branch', 'SD-LAN' and 'SD-Enterprise.'

What to know:

- The benefit to enterprises is if it genuinely helps to simplify networking services, and to consolidate the management of networking and application environments and domains.
- From the LAN and campus perspective, this also helps incorporate management of individual users and connected IoT devices into the overall software-defined networking and management framework.
- Potential limitations to this approach include whether the 'SD-Enterprise' platform has a sufficiently mature, full feature set to manage a diverse set of network domains and services in a consolidated manner.
- This option is also dependent on the enterprise's experience of SD-WAN and cloud-based networking being sufficiently deep and broad for the organization to have the confidence and capabilities to consolidate its ICT management and systems in this way, in partnership with the vendor or service provider, or indeed with a third-party integrator.

Read the Full Executive Briefing

Juniper Contrail SD-WAN: Launch your SD-Branch rocketship

Your network will expand over private and public cloud boundaries, so an evolvable architecture is needed to make that happen. Juniper Contrail SD-WAN enables that growth, free from the barriers of complexity, with:

SD-WAN, LAN, Wi-Fi and security:

See, secure and deliver any or all of these from one place across your branch and campus sites.

Operations simplicity:

Experience SDN without the need to run any software by using cloud-managed Contrail SD-WAN, or choose on-premises software for control on your own terms. Both options come with smart default policies to 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 available in improving 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 and 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 Series, NFX Series and vSRX WAN edge devices all offer next-generation firewalling, universal threat management, and the option to add a subscription to advanced threat protection services.

Find out more about how Juniper Contrail SD-WAN can help your multicloud take off **here.**

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 7400109-001-EN

JUNIPER NETWORKS | **Engineering** Simplicity

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 (July 2019).