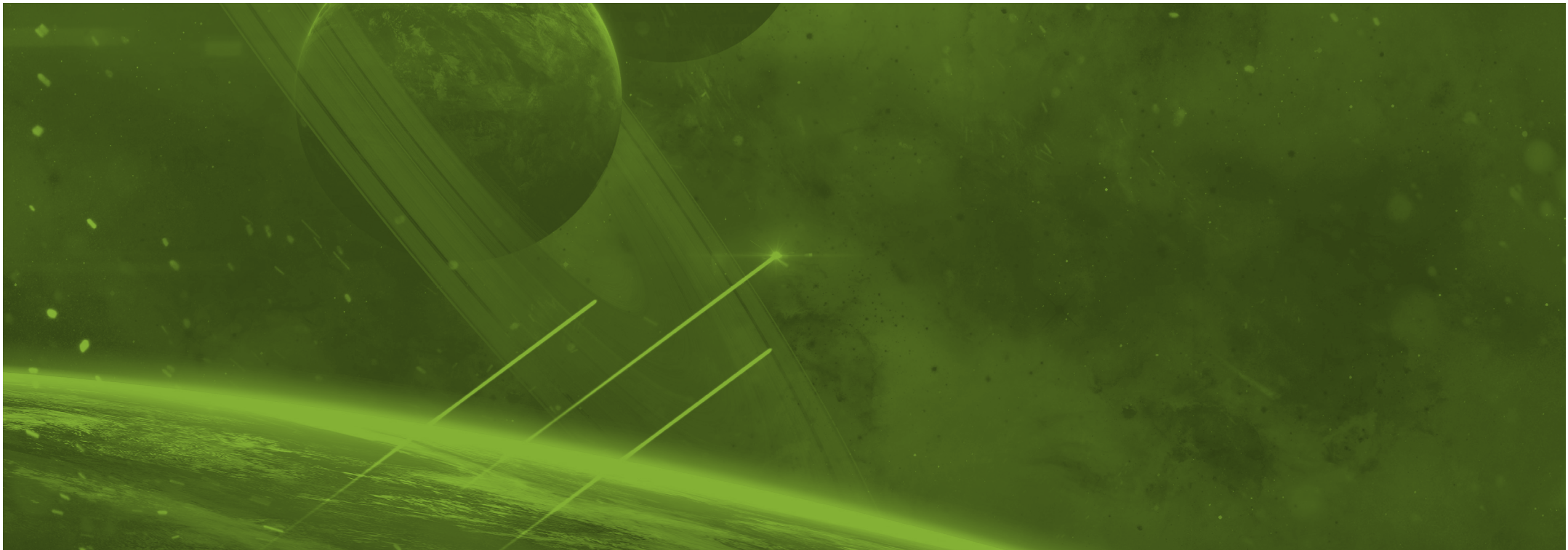


Comparing SD-WAN, LAN and SD-Branch Solutions

Software-defined networking solutions are not equal. Many SD-WAN's focus on a few traits, when in fact there is a bigger operational picture to consider across SD-WAN, LAN, Wi-Fi and security that span across all campus and cloud endpoints. All of this must optimize the WAN design that ties the enterprise together.

Let's compare* solutions in their breadth and depth of features



Feature



Solution Versatility

Cloud-managed option	● ● ● ● ● Cloud-managed CSO	● ● ● ● ●	● ● ● ● ●	○ ○ ○ ○ ○ No in-Cloud management and Control option	● ● ● ● ●
On-premises management option	● ● ● ● ● CSO on premises	● ● ● ● ●	● ● ● ● ●	● ● ● ● ●	● ● ● ● ●
Free tour and trial option	● ● ● ● ● juniper.net/try guided tour demo of global WAN topology with Wi-Fi and LAN. Private evaluation environment with select free SRX giveaways	● ● ○ ○ ○ Gated simple demo environment only	● ● ○ ○ ○ Gated simple demo environment only	○ ○ ○ ○ ○ Sales-led demo	● ● ● ○ ○ On-demand demo environment of a single site, but not guided nor any offer
Device upgrade path from CLI to SDN operations	● ● ● ● ● Evolvable SRX, NFX, EX Series	○ ○ ○ ○ ○ No traditional CLI device management	● ● ○ ○ ○ Split product lines with different management	○ ○ ○ ○ ○ No traditional CLI device management	● ● ● ● ●
SD-WAN edge device range of performance	● ● ● ● ● vSRX, SRX and NFX Series from 100Mbps to 95Gbps Secure SD-WAN	● ● ○ ○ ○ Largest WAN edge device offers 10G throughput with limited routing capabilities	● ● ● ● ○ Large product range, but split product lines with different management solutions	● ● ○ ○ ○ The largest branch CSG700 offers up to 4Gbps throughput. White box options with 10G ports	● ● ● ● ○ Portfolio of 12 Fortigate models support SD-WAN with NGFW up to 9.5Gbps
LAN and Wi-Fi device range of performance	● ● ● ● ● Large range of EX and QFX Series switches and Mist wireless	○ ○ ○ ○ ○ No LAN or wireless portfolio	● ● ● ● ● Large range of LAN and wireless	● ○ ○ ○ ○ No LAN switching portfolio. Limited Wi-Fi integrated into WAN edge devices	● ● ● ○ ○ Limited routing and switching performance options
Native security beyond encryption (e.g. NGFW, IPS, Advanced Threat Prevention)	● ● ● ● ● vSRX, SRX and NFX Series include NGFW and IPS features with option for additional advanced threat prevention and enforcement in WAN, LAN and Wi-Fi	○ ○ ○ ○ ○ Requires another vendor's firewall	● ● ● ○ ○ Split product lines with different management. Unlike the ISR line, the primary ASA security line is not integrated with SD-WAN management. Cisco maintains a matrix to determine which branch devices support which security functions.	● ● ● ○ ○ Includes essentials for NGFW, but not an established security innovator with a threat lab team. Doesn't protect against advanced threats	● ● ● ● ●
Integrates SaaS waypoint services/security	● ● ● ● ● Customizable security services as a waypoint	● ● ● ● ●	● ● ● ● ●	● ● ● ● ●	○ ○ ○ ○ ○ No ZScaler integration
Universal CPE WAN edge embedding third-party apps	● ● ● ● ● Juniper NFX Series	○ ○ ○ ○ ○ No universal CPE portfolio	● ● ● ● ● Cisco 5000 ENCS	● ● ● ● ○ Certified White Boxes	○ ○ ○ ○ ○ No universal CPE portfolio

Feature



SDN Operations

<p>Intuitive operator experience with abstracted control and automated workflows</p>	<p>● ● ● ● ●</p> <p>Guided tour and guided workflows with inline help and links to documentation with animations</p> <p>Control groups across sites, applications, users, etc. Simple customize aggregate views and to drill down across statistics, threats, jobs and logs data</p>	<p>● ● ○ ○ ○</p> <p>No tour. Workflows of large form filling for configuration are overwhelming</p>	<p>● ● ● ○ ○</p> <p>Form filling and wizards in a fairly austere and unguided web interface</p>	<p>● ● ● ○ ○</p> <p>Form filling and wizards. Some features are present but not working</p>	<p>● ● ● ○ ○</p> <p>Large menu-driven options for configuration and operations. Some basic branch level abstraction and overviews of aggregate statistics</p>
<p>AI-driven insights and assisted actions</p>	<p>● ● ● ● ○</p> <p>Integration with Mist Marvis for wired, wireless and WAN assurance</p>	<p>● ○ ○ ○ ○</p> <p>2020 acquisition of Nyansa signals that VMware is thinking of this, but has yet to deliver on it</p>	<p>○ ○ ○ ○ ○</p> <p>No public information on AI for SD-Branch or enterprise networking</p>	<p>○ ○ ○ ○ ○</p> <p>No public information on AI for SD-Branch or enterprise networking</p>	<p>○ ○ ○ ○ ○</p> <p>No public information on AI for SD-Branch or enterprise networking</p>
<p>Automatable and extensible with APIs and templates</p>	<p>● ● ● ● ●</p> <p>API and Config templates. EngNet community and app exchange</p>	<p>● ● ● ○ ○</p> <p>API available</p>	<p>● ● ● ● ●</p> <p>API and DevNet community and code exchange</p>	<p>● ● ● ○ ○</p> <p>API available</p>	<p>● ● ● ○ ○</p> <p>API available</p>
<p>Multi-tenancy</p>	<p>● ● ● ● ●</p> <p>Hierarchical for multiple providers, enterprises and departments, all from one controller or cloud-managed account with configurable RBAC. One user login can switch between environments. Mist Wi-Fi and assurance services are also multitenant from a single login</p>	<p>● ● ● ○ ○</p> <p>Multitenant cloud gateways and orchestrators. See "Scale" rating, where accommodating many tenants requires many on-premises software instances. LAN n/a</p>	<p>● ● ● ○ ○</p> <p>One vSmart per customer and limited number of customers per v/Bond per vManage. With alternative option, Meraki, multitenancy is not possible</p>	<p>● ● ● ● ○</p> <p>Built for service provider multitenancy. No hierarchy. LAN n/a</p>	<p>● ● ● ○ ○</p> <p>One level of provider and customer multitenancy, but switching between these views requires separate logins</p>
<p>Scale to support many tenants, sites and devices</p>	<p>● ● ● ● ●</p> <p>EANTC verified at more than 10,000 sites and devices from a single controller instance. Juniper claims it can support much more than this, depending on the network topology and desired multitenancy</p>	<p>● ● ○ ○ ○</p> <p>Multitenant and multi-site scale requires adding many orchestrators and gateways</p>	<p>● ● ● ○ ○</p> <p>Scaling is complex and requires managing vManage, vBond and vSmart components in the management and control plane. Cisco recommends Meraki for Lean IT, meaning there is a forklift software and hardware upgrade to its full featured SD-WAN</p>	<p>● ● ● ○ ○</p> <p>Currently claims to support 5,000 CPEs</p>	<p>● ● ● ● ○</p> <p>Claims of FortiManager supporting 100,000 sites. This has not been publicly tested and substantiated, and this pertains to only the management plane of the solution</p>
<p>SLAs visibility and assurance</p>	<p>● ● ● ● ●</p>	<p>● ● ● ● ●</p>	<p>● ● ● ● ●</p>	<p>● ● ● ● ●</p>	<p>● ● ● ● ●</p>

Feature



SDN Operations

<p>Operator-defined SLAs</p>	<p>● ● ● ● ●</p> <p>Create service-level agreement (SLA) profiles and map them to SD-WAN policies for traffic management</p>	<p>● ○ ○ ○ ○</p> <p>No operator-defined SLAs. Operator has limited control to change a few predefined values</p>	<p>● ● ● ● ●</p>	<p>● ● ● ● ●</p>	<p>● ● ● ● ●</p>
<p>Operator-defined applications</p>	<p>● ● ● ● ●</p> <p>Application identification supports custom application signatures to detect applications as they pass through the device</p>	<p>○ ○ ○ ○ ○</p> <p>No operator-defined applications capability</p>	<p>○ ○ ○ ○ ○</p> <p>No operator-defined applications capability</p>	<p>● ● ● ● ●</p>	<p>● ● ● ● ●</p>
<p>Application-traffic performance monitoring</p>	<p>● ● ● ● ●</p> <p>Monitor SLA performance per application, per site, per tenant, or across multiple tenants</p>	<p>● ● ● ● ●</p>	<p>● ● ● ○ ○</p> <p>vQoE monitors application performance per pre-defined scale and not per operator-defined SLAs</p>	<p>● ● ● ● ●</p>	<p>○ ○ ○ ○ ○</p> <p>No application traffic performance monitoring per defined SLA</p>
<p>End-user identity and visibility</p>	<p>● ● ● ● ●</p> <p>Juniper Identity Management Service (JIMS) provides a robust and scalable user identification and IP address mapping implementation that includes endpoint context and machine ID. It can integrate with Active Directory</p>	<p>● ● ○ ○ ○</p> <p>Basic RBAC functionality. For advanced features and IP mapping, VMWare UEM console/integration is required</p>	<p>● ● ○ ○ ○</p> <p>Basic RBAC functionality with whitelisting of IP using ACLs</p>	<p>● ● ● ● ●</p>	<p>● ● ● ● ●</p>
<p>Centralized security policy control</p>	<p>● ● ● ● ●</p> <p>Integrated into Juniper management portal</p>	<p>○ ○ ○ ○ ○</p> <p>Security relies on adding technology and devices from partners that are increasingly competing with VMware. Security policy is not controlled with VMware software</p>	<p>● ● ● ○ ○</p> <p>vEdge is a DNS forwarder to Cisco Umbrella Cloud. Security features depend heavily on the branch platforms being used</p>	<p>● ● ● ● ●</p>	<p>● ● ● ● ●</p>
<p>Centralized security visibility, threat map and pervasive enforcement</p>	<p>● ● ● ● ●</p> <p>Integrated into the management portal. ATP and SecIntel enforcement in SD-WAN edge, LAN and Wi-Fi</p>	<p>○ ○ ○ ○ ○</p> <p>See above. No integrated security</p>	<p>● ● ● ○ ○</p> <p>Limited zero-day advanced threat learning and prevention and security features integrated with LAN. Recent NSS Labs report did not recommend Cisco security</p>	<p>● ● ● ○ ○</p> <p>Limited zero-day advanced threat learning and prevention</p>	<p>● ● ● ● ●</p>

Feature



LAN and Wi-Fi Features

<p>LAN switch, fabric (e.g. MC-LAG) management</p>	● ● ● ● ●	○ ○ ○ ○ ○ No LAN management	● ● ● ● ○ SDA only	○ ○ ○ ○ ○ No LAN management	● ● ● ● ●
<p>Integrated Wi-Fi management See mist.com/compare-wlan-solutions/ for more detailed wireless comparison beyond integration</p>	● ● ● ● ● AI-driven wireless networking and visibility and integrated pass through into Mist portal	○ ○ ○ ○ ○ No LAN or wireless management	● ● ● ● ○ Split between Meraki and DNA	○ ○ ○ ○ ○ No LAN or wireless management	● ● ● ● ● Fully integrated Wi-Fi management, though not a strong wireless networking contender
<p>VLAN management and virtual network segmentation</p>	● ● ● ● ●	○ ○ ○ ○ ○ No LAN	● ● ● ● ●	○ ○ ○ ○ ○ No LAN	● ● ● ● ●
<p>Integrated network access control</p>	● ● ● ● ● Integrated with Forescout, Clearpass, ISE	○ ○ ○ ○ ○ No LAN management	● ● ● ● ● Integrated with ISE	○ ○ ○ ○ ○ No LAN management	● ● ● ● ● Integrated with FortiNAC
<p>Integrated advanced threat intelligence and prevention at the switch or Wi-Fi AP</p>	● ● ● ● ●	○ ○ ○ ○ ○ No LAN management nor security	● ● ● ● ●	○ ○ ○ ○ ○ No LAN management nor security	● ● ● ● ●



Engineering
Simplicity

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

www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands

Phone: +31.0.207.125.700

Fax: +31.0.207.125.701

Copyright 2020 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.