Cisco SD-WAN with Secure Access Service Edge (SASE) Competitive Independent Solution Assessment

May 2021

DR210419C

Contents

1.0 Executive Summary ... 3

2.0 Product Overview ... 6

2.1 Cisco ISR vs Prisma SD-WAN ION Series ... 7

2.2 Cisco vManage vs. Prisma SD-WAN Controller ... 7

2.3 Cisco Umbrella vs. Prisma Access ... 7

3.0 How We Did It ... 8

4.0 Day 0 SD-WAN with SASE Comparison ... 9

4.1 Required Touch Points and Setup Complexity ... 9

4.2 Controllers & Edge Device Administration - Deployment Flexibility ... 16

4.3 Browser Support ... 19

4.4 Troubleshooting ... 20

5.0 Application Visibility SD-WAN Comparison ... 23

5.1 Number of Applications ... 23

5.3 Easy Application UI ... 25

6.0 High Availability and Best Path Optimization ... 27

6.1 High Availability ... 27

6.2 Setup Complexity ... 33

6.3 Application Awareness ... 34

6.4 Application Metrics Visibility ... 36

7.0 Performance and Feature SD-WAN Comparison ... 40

7.1 Performance ... 40

7.2 On-Box Security ... 44

7.3 Full Stack Features ... 45

7.4 Cost ... 46

About Miercom ... 47

Use of This Report ... 47

1.0 Executive Summary

Miercom was engaged by Cisco to independently validate and compare the functionality, performance and Total Cost of Ownership (TCO) of its SD-WAN with Secure Access Service Edge (SASE) solution. Cisco SASE connects cloud applications with users and devices anywhere in the network. We compared Cisco's SD-WAN with SASE solution to Palo Alto's Prisma SD-WAN (formerly known as CloudGenix SD-WAN) with Prisma Access.

Miercom considered four areas of analysis in this review including:

- Day 0 setup simplicity
- Remote Worker
- Secure SD-WAN
- Branch and Full Stack deployment

When comparing Cisco and Palo Alto's Prisma SD-WAN solutions, Miercom found that Cisco offered significant benefits for the modern branch network and remote worker solution. This was seen in terms of ease of deployment, architecture that is simple to operate and manage, scalability, and the latest built-in security features – making it the perfect choice for customers.

Key Findings and Observations:

- **Cisco's SD-WAN with SASE Day 0 setup is easy to deploy and configure.** Cisco's setup is simple, intuitive and a true zero-touch SD-WAN solution that is easier to deploy and configure than the complex, multi-touchpoint Prisma SD-WAN setup – which requires manual intervention with no automated process, lacks template-based guided workflows and is more confusing to navigate. Cisco's SD-WAN integration with Cisco Umbrella via Cisco Smart Account licensing allows for template-based configuration workflows and automated secure tunnel deployment between SD-WAN routers and the nearest Cisco Umbrella data center. Prisma SD-WAN offers complex integration between SD-WAN and SASE components, is not automated, and requires support intervention at multiple steps during setup.
- **Cisco's unified management is designed for the everyday customer.** Cisco proved more efficient in unified management mostly from a single platform (vManage), making it simple for even beginner engineers to manage via preloaded templates and troubleshooting features. Cisco provides multiple browser options (i.e. Google Chrome, Safari, Firefox), providing flexibility to customers for accessing the vManage dashboard. Cisco also provides a network topology with guided workflows for troubleshooting to make it easy for customers to remediate issues. Prisma SD-WAN had more steps for integration, requiring customer support, that is more complex to understand for customers setting up the network on their own. Troubleshooting was proven to be basic and ineffective. Prisma SD-WAN is browser dependent and limited to Google Chrome.

- **Cisco's Cloud OnRamp for SaaS and IaaS offers seamless deployment with intuitive dashboard configurations.** Cisco delivers cost-effective, scalable SaaS services for cloud applications, with lower latency and loss than traditional backhaul technologies. Its automated, real-time path optimization yields the highest efficiency, security and quality. For IaaS, Cisco provides template-based configuration workflows within Cisco vManage that, once complete, integrates with AWS to automatically deploy virtual instances of Cisco SD-WAN routers within defined AWS data centers. These routers are deployed with redundancy and dynamic routing services. Cloud OnRamp for SaaS has a manual configuration process, with no templates or intuitive dashboard for viewing application performance metrics. For IaaS, the process is the same. It also requires multiple manual configurations on the AWS platform and Prisma SD-WAN controller dashboard which increases complexity.
- **Cisco's SD-WAN solution provides granular application visibility and intuitive application dashboard.** Cisco recognizes 1400+ application signatures with granular visibility of cloud application performance. As a key differentiator, Cisco's partnership and integration with Microsoft Office365 for enhanced telemetry, allowing customers to easily remediate sub-optimal performance. Informed routing lets customers improve end user experience. Cisco's new URL categorization feature provides significant improvement for customers using Cloud OnRamp with Microsoft365. Conversely, Prisma SD-WAN offers only 533 applications, including cloud applications in the Prisma SD-WAN controller dashboard. It doesn't offer an intuitive dashboard and partnership with Microsoft for enhanced telemetry showcasing advanced application performance metric analysis.
- **Cisco SD-WAN offers faster link failover leading to a more Highly Available and resilient network.** Cisco offers faster link convergence during link failure with near-zero downtime. Cisco uses a single port for controller and Internet connectivity to simplify port configuration and seamless traffic flow despite dropped control plane sessions. Prisma SD-WAN ION devices have separate ports for controller connection that adds complexity and dependency for data plane traffic.
- **Cisco offers enhanced Application Awareness.** While both Cisco and Palo Alto successfully performed failover path optimization for applications, Cisco had no interruptions. Prisma SD-WAN showed significant delays between failover path selection. Customers with high-traffic enterprises or data centers will find this delay troublesome for their business.
- **Cisco SD-WAN offers better performance with all SD-WAN features enabled.** Cisco SD-WAN performed consistently better by offering more than 50 percent higher performance in terms of on-box throughput than Prisma SD-WAN with key features like IPSec, Zone-Based Firewall, QoS and NAT.
- **Cisco SD-WAN provides robust on-box security when compared to Prisma SD-WAN.** Cisco offers advanced on-box features to enhance SD-WAN performance and security while Prisma SD-WAN only provides a basic firewall capability.

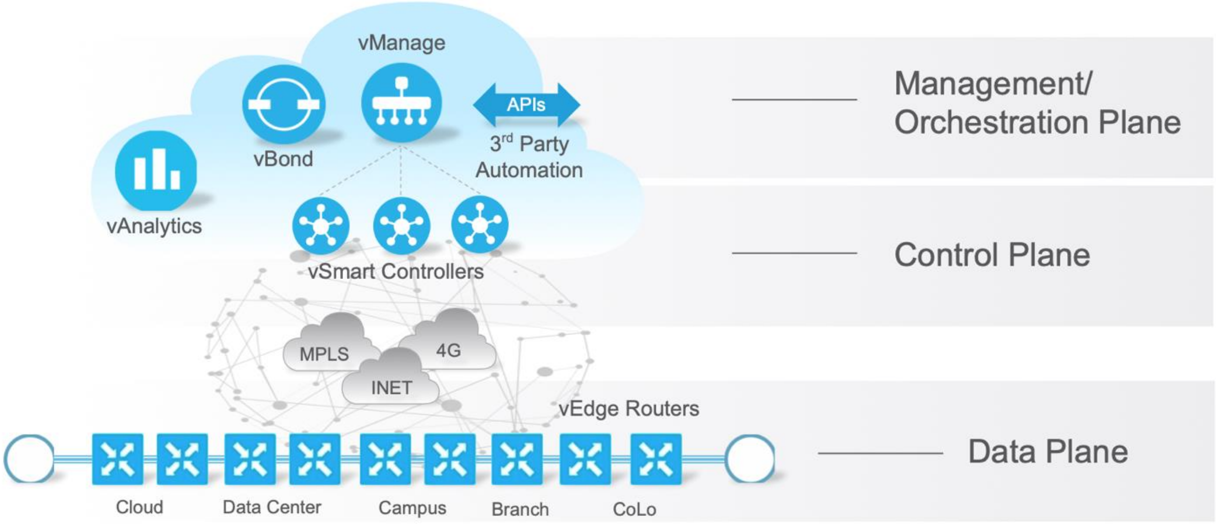
- **Cisco SD-WAN provides full stack capabilities with different feature sets.** Cisco offered full stack capabilities, including wireless. Cisco can scale wireless management for up to 50 access points. The Cisco ISR's built-in Mobility Express feature allows routers to act as a virtual wireless controller, whereas Prisma SD-WAN lacked this feature – relying on third-party vendors for this capability. Cisco's on-box LTE capabilities provide on-box SIM card slots; Prisma SD-WAN, again, must rely on third-party vendors. Customers have a broader range of choice and management with Cisco's additional wireless features that reduce cost, complexity and setup. Additionally, Cisco offers Stealthwatch for visibility, threat analysis and network compliance using machine-learning detection. Prisma SD-WAN does not offer such advanced capabilities.
- **Cisco SD-WAN offers a resourceful licensing model.** Cisco's simplified licensing structure eliminates the need for numerous add-on licenses and support contracts to activate features. Its tiered model reduces time, complexity, and cost for customers. Prisma SD-WAN's a-la-carte approach requires the complex, costly enablement of individual add-on features. It also does not provide the option for both consumption-based and subscription licensing, like Cisco.
- **Return On Investment (ROI).** Cisco guarantees investment protection for its customers – offering consistently improved tools for migration and services (e.g., voice) to be used on existing routing/edge platforms with SD-WAN. Combined with Cisco's extensive partner network, with focused product line expertise, Cisco delivers a more cost-effective solution than Prisma SD-WAN – which is 51 percent more expensive.

Based on our observations, Cisco's SD-WAN Secure Access Service Edge (SASE) solution provides lower TCO, better return on investment, for both CAPEX and OPEX. Miercom verified Cisco's outstanding, competitively superior security and performance, and we proudly award the Cisco SASE solution the ***Miercom Performance Verified*** certification.

Rob Smithers, CEO
Miercom

2.0 Product Overview

Cisco SD-WAN is a true software defined networking solution with separate layers for the orchestration, management, control and data planes.



- **Orchestration Plane** – the first point of authentication, where the vBond Orchestration creates any device introduced to the network to form an initial connection between the vSmart Controller, and vManage, to all vEdge routers.
- **Data Plane** – performs entry forwarding, where zero-touch provisioning establishes the secure fabric and implements data plane policies.
- **Control Plane** – managed by the vSmart Controllers and responsible for maintenance and control of edge device connections. It distributes policies for either edge-to-edge communication (through the Control Plane, or "brain" of the solution) or vManage (part of the Management Plane). Acting as a single pane-of-glass for Day0/Day1 operations, it supports both multi-tenant and single tenant dashboards.

2.1 Cisco ISR vs Prisma SD-WAN ION Series

Cisco ISR

Cisco Integrated Services Routers (ISRs) are highly secure and high-performance routers, offering routing and switching in one platform. These ISRs additionally feature high-availability and simplified management.

Cisco 1000 Series ISRs

Prisma SD-WAN

Prisma SD-WAN Instant-On Network (ION) devices provide integration of the cloud and WAN links with the local branch network devices with performance and visibility.

Prisma SD-WAN ION 3000

Prisma SD-WAN ION 2000

2.2 Cisco vManage vs. Prisma SD-WAN Controller

Cisco vManage is a Graphical User Interface (GUI) where administrators and operators can configure, provision, troubleshoot and monitor activity centrally in the whole network including multiple clouds. vManage offers two dashboards: single-tenant and multi-tenant. Cisco's vManage can be deployed on-premises, cloud hosted (Cloud Ops Service) and also Public Cloud (via AWS, Microsoft Azure).

Palo Alto Prisma SD-WAN Controller is a cloud hosted service (SaaS) that provides a secure SD-WAN solution for offices, campuses, and large enterprises.

2.3 Cisco Umbrella vs. Prisma Access

Cisco Umbrella is a cloud native security service that simplifies network security by helping organizations secure internet access and control cloud app usage across the network, branch offices, and roaming users. Umbrella unifies DNS-layer protection, secure web gateway, firewall and cloud access security broker (CASB) functionality, to easily help protect remote and roaming users, secure SD-WAN and embrace direct internet access.

Prisma Access is a cloud security platform which has two management options, Prisma Access SaaS and Panorama managed which have significant differences in their respective features and capabilities. Prisma Access offers a SASE solution as well as analytics and machine learning for threat prevention and further DNS security. Customers can store and manage logs through Cortex Data Lake which is an additional component for application traffic analysis and reporting.

3.0 How We Did It

Using a realistic network environment, we tested the capabilities of Cisco ISR 1100 and Prisma SD-WAN ION 2000 and 3000, the intuitiveness of the GUI for Cisco vManage and Prisma SD-WAN cloud controller, and the aptitude and feature difference between Cisco Umbrella and Prima Access. We used Prisma Access for remote networks with Panorama VM for management to make sure Prisma Access is enabled with all the features.

Test Tools

The following tools are a representative list of software tools and exploits we used to carry out our analysis.

Spirent Test Center (version 4.91)

Offers end-to-end performance testing for network verification and QoE measurement. Controlled parameter customization allows for customizable testing with real-time feedback. Customers are able to troubleshoot issues and view device behavior in specific conditions.

4.0 Day 0 SD-WAN with SASE Comparison

4.1 Required Touch Points and Setup Complexity

4.1.1 Cisco (SD-WAN with SASE)

The Cisco vManage acts as the single management plane for Day 0/Day 1 operations. All provisioning, configuration, monitoring, troubleshooting, is managed through the vManage.

Cisco vManage provides customizable templates for customers to quickly set up Day 0 configurations. Templates simplify the process of configuring automatically and include both security and policies.

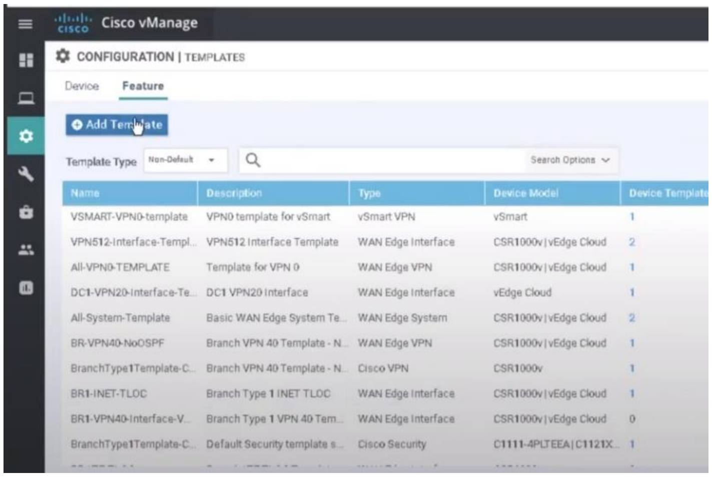
Cisco Day 0 Setup is network planning, first deploying and tuning of SD-WAN controllers. The authorized list of serial numbers was received when the devices were ordered. This list was uploaded with the controllers, and once added, the edge devices were added to the network.

This setup was simpler than Prisma SD-WAN for the following reasons:

- Simplified configuration from vManage to Umbrella
- Automated user account registration between vManage and Umbrella
- Automated tunnel provisioning between remote sites and nearest Umbrella data centers
- No extra equipment or settings needed
- Cisco Zero Touch Provisioning feature offers ease of organization and management
- Simple and intuitive Day 0 configuration
- Faster to deploy, with least number of touchpoints

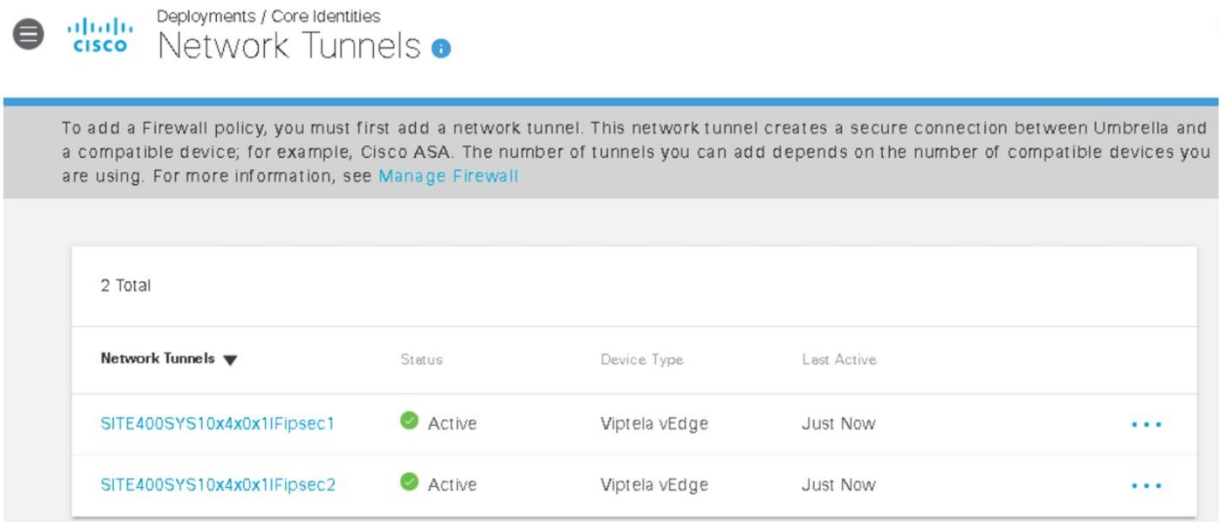
Cisco had an automated account registration between SD-WAN and Umbrella dashboards, via Cisco Smart Account licensing. Once registered for both services, Cisco SD-WAN provides intuitive template-based configuration workflows.

Integrations between Cisco SD-WAN and Cisco Umbrella automate secure tunnel deployment between SD-WAN routers and the nearest Cisco Umbrella data center.



Name	Description	Type	Device Model	Device Template
VSMART-VPN0-template	VPN0 template for vSmart	vSmart VPN	vSmart	1
VPN512-Interface-Templ...	VPN512 Interface Template	WAN Edge Interface	CSR1000v | vEdge Cloud	2
All-VPN0-TEMPLATE	Template for VPN 0	WAN Edge VPN	CSR1000v | vEdge Cloud	1
DC1-VPN20-Interface-Te...	DC1 VPN20 Interface	WAN Edge Interface	vEdge Cloud	1
All-System-Template	Basic WAN Edge System Te...	WAN Edge System	CSR1000v | vEdge Cloud	2
BR-VPN40-NoOSPF	Branch VPN 40 Template - N...	WAN Edge VPN	CSR1000v | vEdge Cloud	1
BranchType1Template-C...	Branch VPN 40 Template - N...	Cisco VPN	CSR1000v	1
BR1-INET-TLOC	Branch Type 1 INET TLOC	WAN Edge Interface	CSR1000v | vEdge Cloud	1
BR1-VPN40-Interface-V...	Branch Type 1 VPN 40 Tem...	WAN Edge Interface	CSR1000v | vEdge Cloud	0
BranchType1Template-C...	Default Security template s...	Cisco Security	C1111-4PLTEEA | C1121X...	1

Customers have the option of selecting configuration templates provided in Cisco vManage, creating their own configurations, or uploading a template. This simplifies the process of configuring automatically. These templates include security, policy, and routing rules.



Deployments / Core Identities

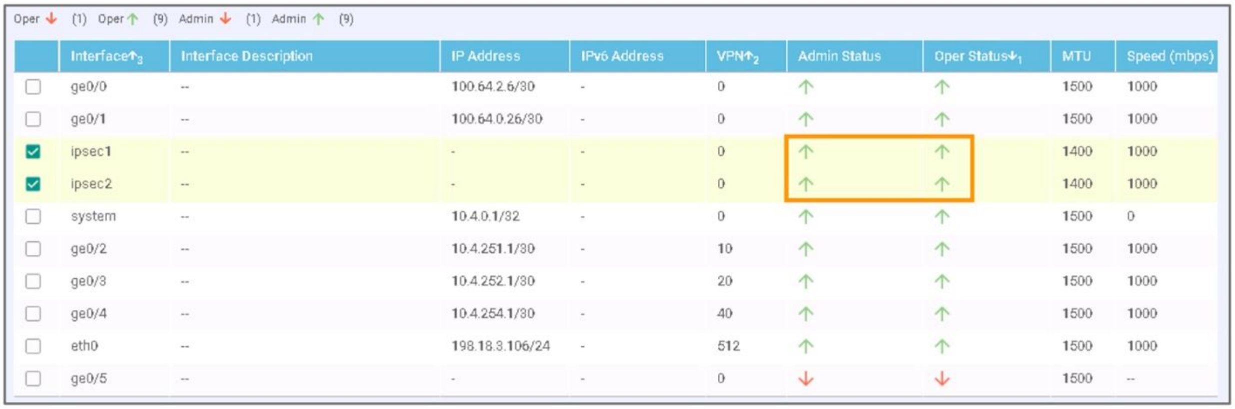
Network Tunnels

To add a Firewall policy, you must first add a network tunnel. This network tunnel creates a secure connection between Umbrella and a compatible device; for example, Cisco ASA. The number of tunnels you can add depends on the number of compatible devices you are using. For more information, see Manage Firewall

2 Total

Network Tunnels ▼	Status	Device Type	Last Active	
SITE400SYS10x4x0x1IFipsec1	● Active	Viptela vEdge	Just Now	•••
SITE400SYS10x4x0x1IFipsec2	● Active	Viptela vEdge	Just Now	•••

Umbrella Dashboard



Oper ↓ (1) Oper ↑ (9) Admin ↓ (1) Admin ↑ (9)

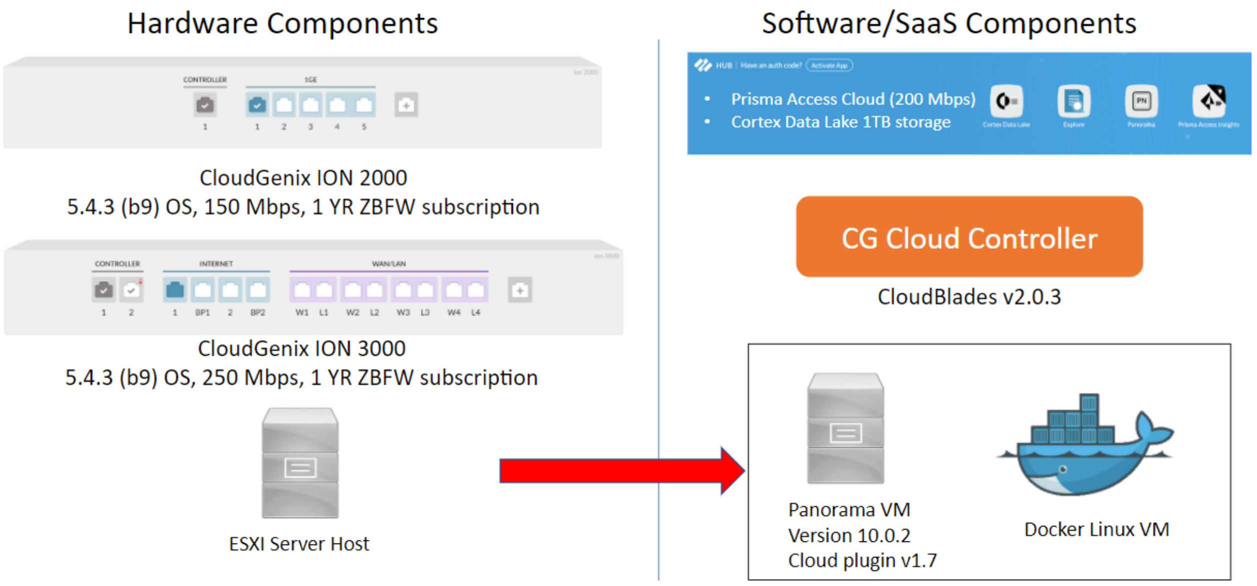
	Interface↑3	Interface Description	IP Address	IPv6 Address	VPN↑2	Admin Status	Oper Status↓1	MTU	Speed (mbps)
☐	ge0/0	--	100.64.2.6/30	-	0	↑	↑	1500	1000
☐	ge0/1	--	100.64.0.26/30	-	0	↑	↑	1500	1000
☑	ipsec1	--	-	-	0	↑	↑	1400	1000
☑	ipsec2	--	-	-	0	↑	↑	1400	1000
☐	system	--	10.4.0.1/32	-	0	↑	↑	1500	0
☐	ge0/2	--	10.4.251.1/30	-	10	↑	↑	1500	1000
☐	ge0/3	--	10.4.252.1/30	-	20	↑	↑	1500	1000
☐	ge0/4	--	10.4.254.1/30	-	40	↑	↑	1500	1000
☐	eth0	--	198.18.3.106/24	-	512	↑	↑	1500	1000
☐	ge0/5	--	-	-	0	↓	↓	1500	--

vManage Dashboard

Customers have the option of viewing the status of the IPSEC tunnels from both Umbrella and vManage dashboard.

4.1.2 Palo Alto (Prisma SD-WAN with SASE)

Palo Alto was not truly zero touch. Prisma SD-WAN with SASE Day 0 is complex to setup with multiple touchpoints. It required several steps where customer support services were necessary. Additionally, manual claiming of devices, datacenter identification, and software upgrades were required.

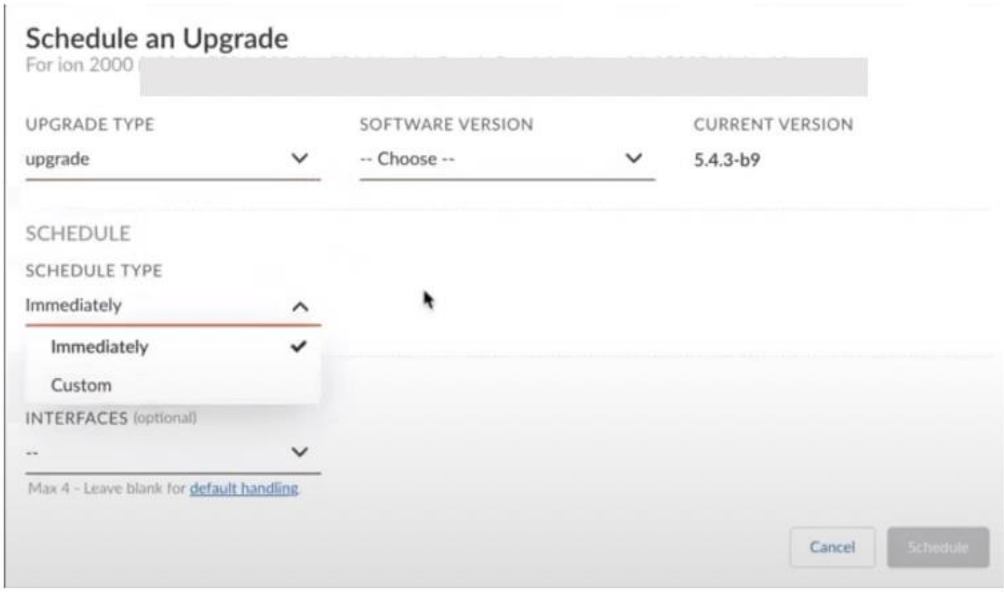


Above is an example of necessary components for setting up the Prisma SD-WAN with SASE solution. Prisma SD-WAN needed Panorama VM and Docker to integrate the following APIs: CloudBlades, Prisma Access and Panorama.

The Prisma SD-WAN Cloud Controller was used to access the Prisma SD-WAN ION 2000/3000 for software upgrades, claiming of devices, and cloud configuration.

Additionally, Prisma SD-WAN support required claiming the ION edge devices. Deploying, claiming and configuring the WAN and ION devices was necessary for completion of the SD-WAN solution. Customers must then purchase the Prisma SD-WAN License and connect the ION devices to the Internet via Internet and controller ports.

The Prisma SD-WAN dashboard displayed the devices under the unclaimed device section. After purchasing the licenses, the serial numbers were uploaded and visible via Customer Support. Upgrading firmware, to the current version 5.4.3 used at the time of testing, was not automatic and required upgrades for each individual device.



Schedule an Upgrade

For ion 2000 [redacted]

UPGRADE TYPE: upgrade

SOFTWARE VERSION: -- Choose --

CURRENT VERSION: 5.4.3-b9

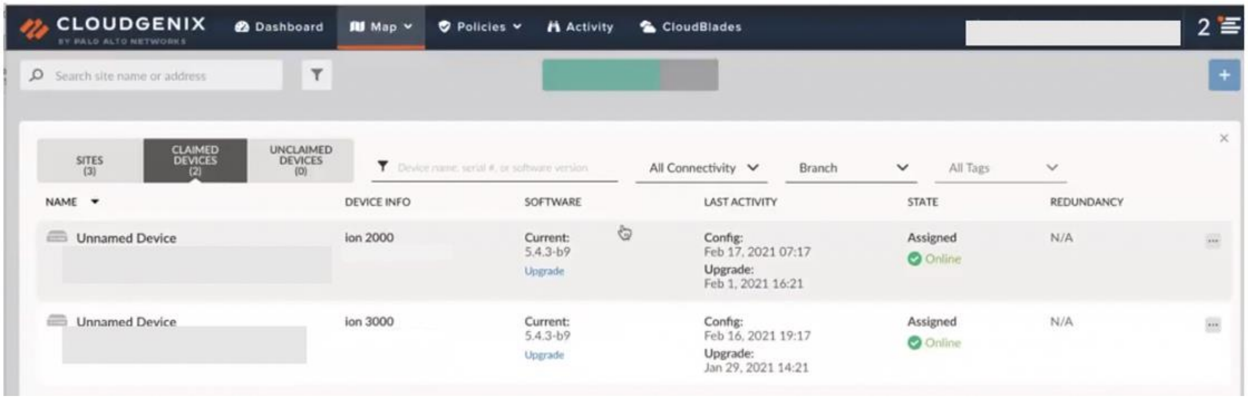
SCHEDULE

SCHEDULE TYPE: Immediately

INTERFACES (optional): --

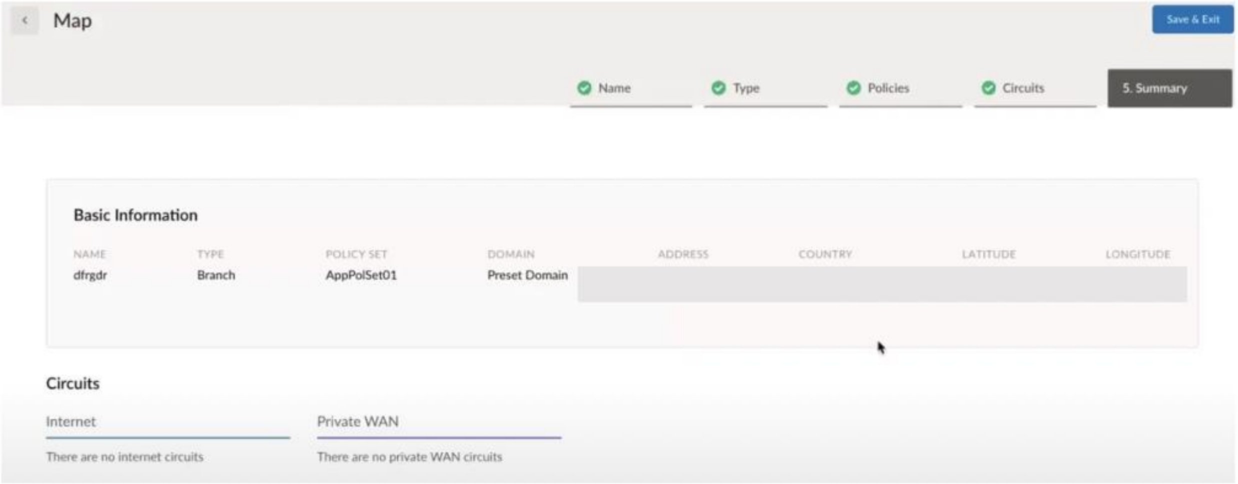
Max 4 - Leave blank for default handling

After upgrading, you must manually claim the device. This requires cloud connection. And once claimed, you will view unclaimed devices under claimed devices section.



NAME	DEVICE INFO	SOFTWARE	LAST ACTIVITY	STATE	REDUNDANCY
Unnamed Device [redacted]	ion 2000	Current: 5.4.3-b9 Upgrade	Config: Feb 17, 2021 07:17 Upgrade: Feb 1, 2021 16:21	Assigned Online	N/A
Unnamed Device [redacted]	ion 3000	Current: 5.4.3-b9 Upgrade	Config: Feb 16, 2021 19:17 Upgrade: Jan 29, 2021 14:21	Assigned Online	N/A

Customers must assign the ION devices to specific sites, which are created manually. There are no templates for automatic site creation. Customers can choose categories (e.g., address, type, domain, policy, circuit).



Basic Information

NAME	TYPE	POLICY SET	DOMAIN	ADDRESS	COUNTRY	LATITUDE	LONGITUDE
dfrgdr	Branch	AppPolSet01	Preset Domain				

Circuits

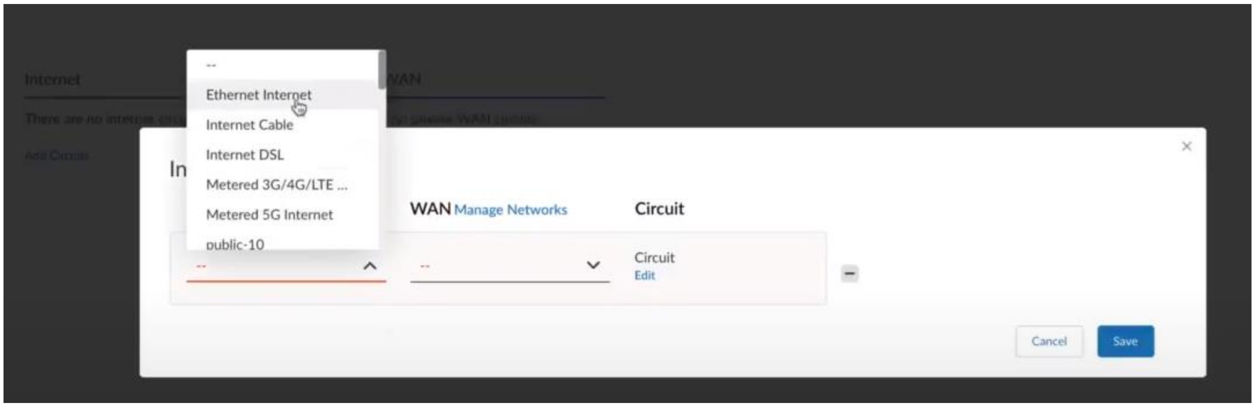
Internet

There are no internet circuits

Private WAN

There are no private WAN circuits

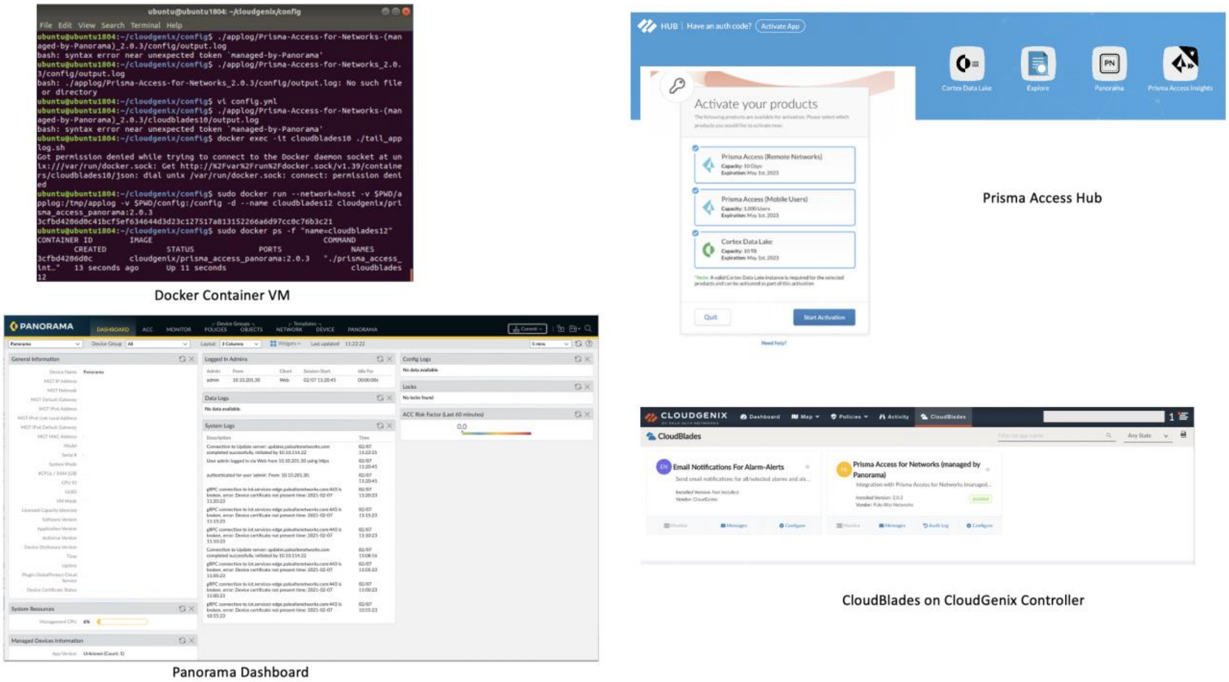
Customers configure Internet ports individually, with port names and circuit labels; predefined labels are available. Additionally, the customer must configure DHCP or static IPs, external NAT and ports to manually establish a secure overlay connection.



The Secure Fabric overlay was established between devices in 7 steps.

The Prisma SD-WAN dashboard provided CloudBlades for API integration with Prisma Access SASE solution through the docker container. Support Intervention requirement was observed during this step to enable CloudBlades on the Prisma SD-WAN controller dashboard which was time consuming. Besides the support intervention, there were additional touchpoints like the following to complete the integration process:

- On-Prem Docker Container for key management and integration,
- Activate Prisma Access and Cortex Data lake on the Palo Alto Hub and generate the One-time-password to use in the Panorama GUI to activate cloud services
- Install Cloud plugin by Logging into the Panorama GUI. Retrieve the Prisma Access Licenses from license server. Verify the OTP and activate cloud services on Panorama GUI



```
ubuntu@ubuntu1804: ~/cloudgenix/config
File  Edit  View  Search  Terminal  Help
ubuntu@ubuntu1804:~/cloudgenix/config$ ./applog/Prisma-Access-for-Networks-(man
aged-by-Panorama)_2.0.3/config/output.log
bash: syntax error near unexpected token `managed-by-Panorama'
ubuntu@ubuntu1804:~/cloudgenix/config$ ./applog/Prisma-Access-for-Networks_2.0.
3/config/output.log
bash: ./applog/Prisma-Access-for-Networks_2.0.3/config/output.log: No such file
 or directory
ubuntu@ubuntu1804:~/cloudgenix/config$ vi config.yml
ubuntu@ubuntu1804:~/cloudgenix/config$ ./applog/Prisma-Access-for-Networks-(man
aged-by-Panorama)_2.0.3/cloudblades10/output.log
bash: syntax error near unexpected token `managed-by-Panorama'
ubuntu@ubuntu1804:~/cloudgenix/config$ docker exec -it cloudblades10 ./tail_app
log.sh
Got permission denied while trying to connect to the Docker daemon socket at un
ix:///var/run/docker.sock: Get http://%2Fvar%2Frun%2Fdocker.sock/v1.39/containe
rs/cloudblades10/json: dial unix /var/run/docker.sock: connect: permission deni
ed
ubuntu@ubuntu1804:~/cloudgenix/config$ sudo docker run --network=host -v $PWD/a
pplog:/tmp/applog -v $PWD/config:/config -d --name cloudblades12 cloudgenix/pri
sma_access_panorama:2.0.3
3cfbd4206d0c41bcf5ef634644d3d23c127517a813152266a6d97cc0c76b3c21
ubuntu@ubuntu1804:~/cloudgenix/config$ sudo docker ps -f "name=cloudblades12"
CONTAINER ID        IMAGE                                     COMMAND
        CREATED             STATUS              PORTS               NAMES
3cfbd4206d0c        cloudgenix/prisma_access_panorama:2.0.3   "./prisma_access_
int…"   13 seconds ago      Up 11 seconds                           cloudblades
12
```

Docker Container VM

Prisma Access Hub

Panorama Dashboard

CLOUDGENIX
Dashboard
Map
Policies
Activity
CloudBlades
CloudBlades
Email Notifications For Alarm-Alerts
Prisma Access for Networks (managed by Panorama)

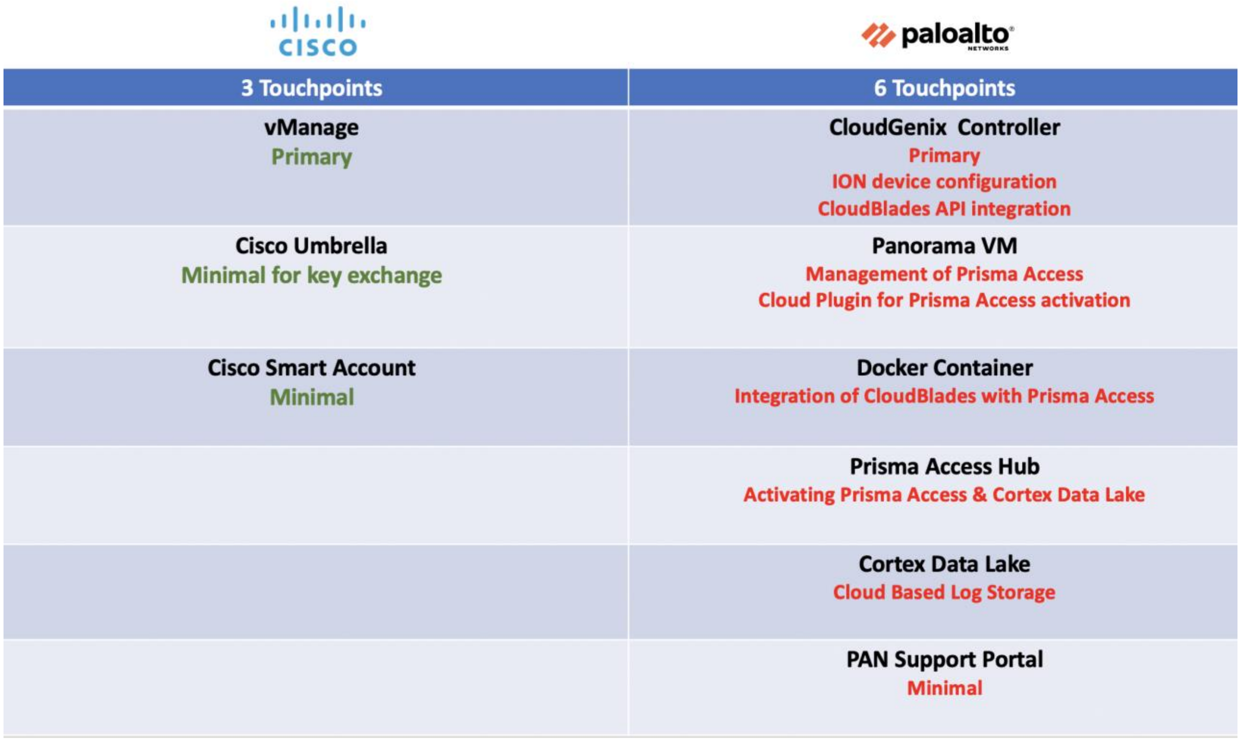
CloudBlades on CloudGenix Controller

Palo Alto needs multiple touchpoints to integrate Prisma SD-WAN with Prisma Access SASE solution

Prisma SD-WAN Cloud OnRamp for SaaS configuration was a manual process that did not offer template-based configurations, had less intuitive dashboard for viewing performance metrics of different SaaS applications and involved manual intervention. Therefore, we find this solution does not truly offer zero-touch provisioning. Similarly, Prisma SD-WAN Cloud OnRamp for IaaS configuration requires manual process unlike Cisco's intuitive and template based automated approach with guided workflows.

Test Case Summary

Unlike Prisma SD-WAN, Cisco offers a less complex, truly zero-touch SD-WAN solution through its vManage platform. Its short learning curve, template gallery and intuitive process is smoother and more efficient than Prisma SD-WAN. The Prisma SD-WAN procedure is more time-consuming, involves multiple touchpoints, requires customer support intervention, lacks templates, and is more confusing to navigate its interface.



cisco	paloalto NETWORKS
3 Touchpoints	**6 Touchpoints**
vManage Primary	**CloudGenix Controller** Primary ION device configuration CloudBlades API integration
Cisco Umbrella Minimal for key exchange	**Panorama VM** Management of Prisma Access Cloud Plugin for Prisma Access activation
Cisco Smart Account Minimal	**Docker Container** Integration of CloudBlades with Prisma Access
	Prisma Access Hub Activating Prisma Access & Cortex Data Lake
	Cortex Data Lake Cloud Based Log Storage
	PAN Support Portal Minimal

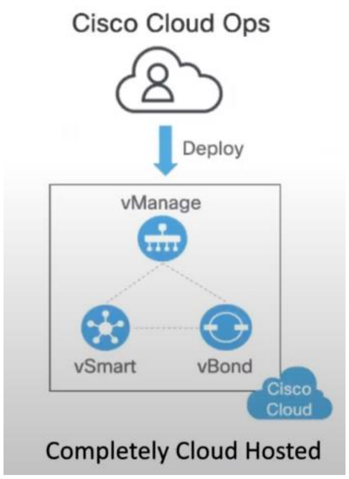
Comparison table showcasing twice the number of touchpoints required by Palo Alto to integrate Prisma SD-WAN with Prisma Access SASE solution when compared to Cisco's solution

4.2 Controllers & Edge Device Administration - Deployment Flexibility

4.2.1 Cisco

For Day 0 Controller deployment, Cisco provides the three options below.

Cloud Ops Deployment



Cisco utilized the Cloud Ops deployment – a completely cloud-hosted solution where every component of the control plane is deployed transparently by Cisco and with Cisco management for controller access.

Customers are not required to manually configure the control plane and adding these devices – a true zero-touch deployment. Cisco takes care of everything in the cloud. Management is then given to customers. This process can also be done through the managed service providers, public or private, or on premise. And enterprise customers can do it manually on their own by either deploying the physical device on premise or cloud via AWS or Azure.

Subscription-based Virtual Controllers

Cisco's subscription-based portfolio of vManage, vBond, and vSmart controllers were deployed on Azure or AWS cloud platforms and the administrative access was given. By default, Cisco provided a single vManage, vBond, and vSmart controller in the primary region and gave a backup of the vBond Orchestrator and vSmart Controller in the secondary region to ensure redundancy. This process was managed by a single portal called the "Plug-and-Play Portal".

(As opposed to Prisma SD-WAN that needs manager navigation, requires multiple devices and touchpoints, no support for enabling is need in case of Cisco).

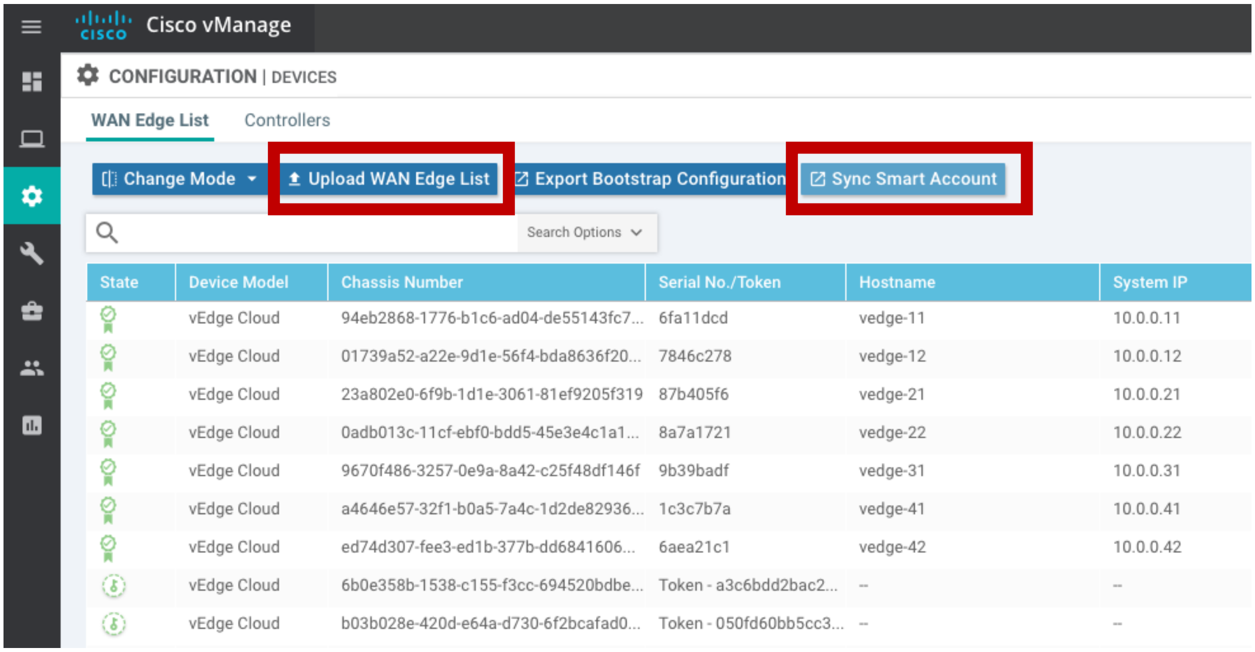
Using Cisco's Smart Account, customers can purchase the Plug-and-Play (PnP) service that integrates with the Zero Touch Provisioning (ZTP) Server – a true zero-touch experience with added devices. After defining the vBond controller in the PnP service, obtaining the license and viewing of devices capable of associating with the controller comes next. Once vBond was selected, we were able to add devices, use the PnP service to push configurations, and successfully redirect ISRs to vManage. We then had the option to automatically sync with devices available in the PnP service account.

On-Prem Controller deployment

The last option is deployment of on-prem controllers with ESXI VM options.

Manual WAN Edge List

For WAN Edge devices, Cisco gives an option to manually upload the WAN edge device list.

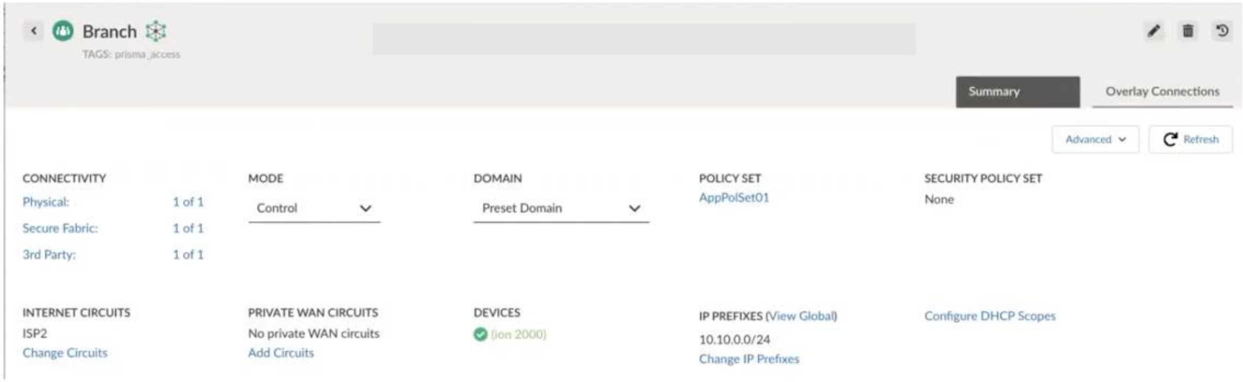


State	Device Model	Chassis Number	Serial No./Token	Hostname	System IP
✓	vEdge Cloud	94eb2868-1776-b1c6-ad04-de55143fc7...	6fa11dcd	vedge-11	10.0.0.11
✓	vEdge Cloud	01739a52-a22e-9d1e-56f4-bda8636f20...	7846c278	vedge-12	10.0.0.12
✓	vEdge Cloud	23a802e0-6f9b-1d1e-3061-81ef9205f319	87b405f6	vedge-21	10.0.0.21
✓	vEdge Cloud	0adb013c-11cf-ebf0-bdd5-45e3e4c1a1...	8a7a1721	vedge-22	10.0.0.22
✓	vEdge Cloud	9670f486-3257-0e9a-8a42-c25f48df146f	9b39badf	vedge-31	10.0.0.31
✓	vEdge Cloud	a4646e57-32f1-b0a5-7a4c-1d2de82936...	1c3c7b7a	vedge-41	10.0.0.41
✓	vEdge Cloud	ed74d307-fee3-ed1b-377b-dd6841606...	6aea21c1	vedge-42	10.0.0.42
○	vEdge Cloud	6b0e358b-1538-c155-f3cc-694520bdbe...	Token - a3c6bdd2bac2...	--	--
○	vEdge Cloud	b03b028e-420d-e64a-d730-6f2bcafad0...	Token - 050fd60bb5cc3...	--	--

vManage offers two options for customers, to automatically sync with what devices are in the Plug-and-Play account, or to manually upload the WAN edge list.

4.2.2 Palo Alto

Palo Alto Prisma SD-WAN only provides Cloud based SaaS option to customers. Palo Alto required support intervention to activate the device licenses and claim the edge routers on the dashboard. . The Prisma SD-WAN Controller was used to access the Prisma SD-WAN ION 2000/3000 to perform software upgrades, claim, and configure on the cloud.



TAGS: prisma_access

CONNECTIVITY
Physical: 1 of 1
Secure Fabric: 1 of 1
3rd Party: 1 of 1

MODE: Control

DOMAIN: Preset Domain

POLICY SET: AppPolSet01

SECURITY POLICY SET: None

INTERNET CIRCUITS: ISP2

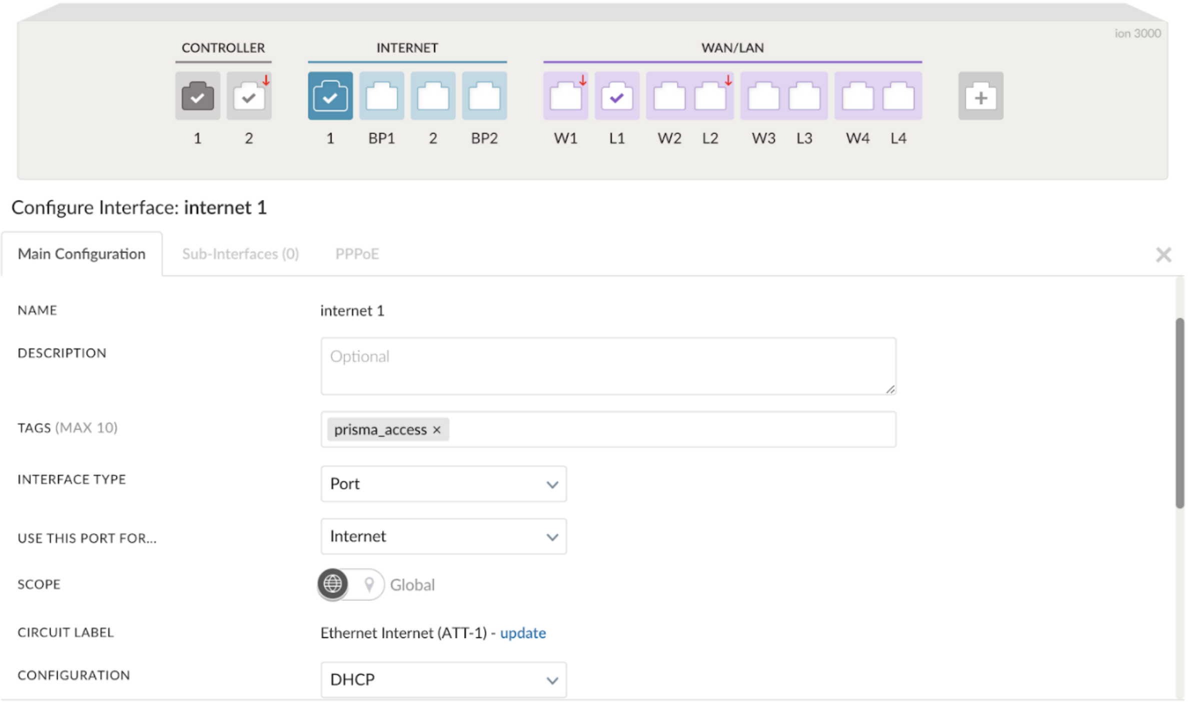
PRIVATE WAN CIRCUITS: No private WAN circuits

DEVICES: (ion 2000)

IP PREFIXES (View Global): 10.10.0.0/24

Palo Alto shows site status. . Devices can be deployed in either of two modes: analytics mode or controller mode. The analytics mode inspects the application traffic passing through the device. The control mode inspects the application traffic and applies the policy, end-to-end, for complete management of traffic.

To bring ION devices online and form the secure fabric connection, customers need to navigate to the devices individually and claim, then assign each to a site with a policy. Once the devices are claimed, we navigated the interface to set the configuration.



Configure Interface: internet 1

Main Configuration | Sub-Interfaces (0) | PPPoE

NAME: internet 1

DESCRIPTION: Optional

TAGS (MAX 10): prisma_access ×

INTERFACE TYPE: Port

USE THIS PORT FOR...: Internet

SCOPE: Global

CIRCUIT LABEL: Ethernet Internet (ATT-1) - update

CONFIGURATION: DHCP

Customers must manually set the device configuration. After claiming and assigning to a site, designating ports and port types, circuit levels, and scope depending on the customer needs. These steps can be found on the “Prisma SD-WAN Getting Started Guide”.

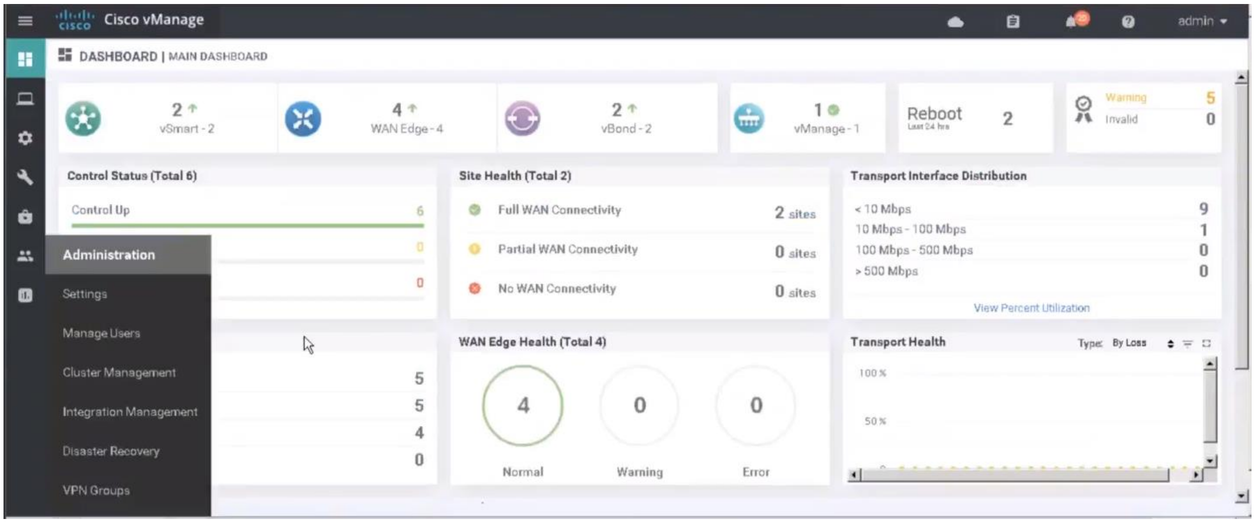
Test Case Summary

Cisco Day 0 deployment offers 3 options: Cloud Ops, a cloud-hosted solution for controller access; zero-touch provisioning via a subscription-based portfolio of vManage, vBond and vSmart controller on Azure or AWS with administrative access and On-Prem controller deployment . Cisco offers manual upload of the WAN edge device list. Prisma SD-WAN offers the option of cloud-based SaaS controller and has only one approach for upload of WAN edge devices – manual and individual activation of ION devices for upgrades, claims and configurations – which requires customer support intervention to accomplish.

4.3 Browser Support

4.3.1 Cisco

Cisco vManage had no browser dependency and supported multiple browsers (e.g. Chrome, Safari, Firefox).



2 vSmart - 2

4 WAN Edge - 4

2 vBond - 2

1 vManage - 1

Reboot Last 24 hrs 2

Warning 5

Invalid 0

Control Status (Total 6)

Control Up 6

Site Health (Total 2)

Full WAN Connectivity	2 sites
Partial WAN Connectivity	0 sites
No WAN Connectivity	0 sites

Transport Interface Distribution

< 10 Mbps	9
10 Mbps - 100 Mbps	1
100 Mbps - 500 Mbps	0
> 500 Mbps	0

View Percent Utilization

WAN Edge Health (Total 4)

Normal	Warning	Error
4	0	0

Transport Health

Type: By Loss

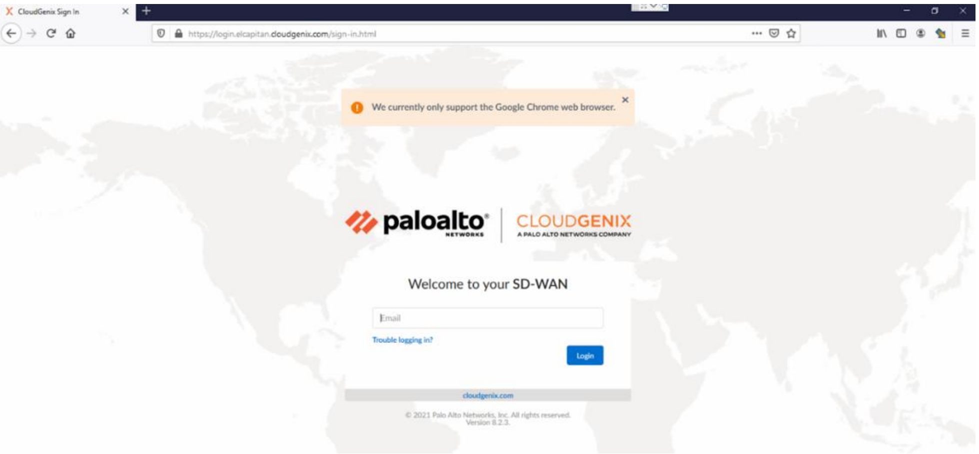
100 %

50 %

Cisco vManage is not limited to a type of browser, unlike Palo Alto which only works on Google Chrome, as demonstrated above.

4.3.2 Palo Alto

Prisma SD-WAN showed support through Google Browser only. This may pose a security risk.


CloudGenix Sign In
https://login.elcapitan.cloudgenix.com/sign-in.html
paloalto NETWORKS
CLOUDGENIX A PALO ALTO NETWORKS COMPANY
Email
Trouble logging in?
Login
cloudgenix.com

We currently only support the Google Chrome web browser.

Welcome to your SD-WAN

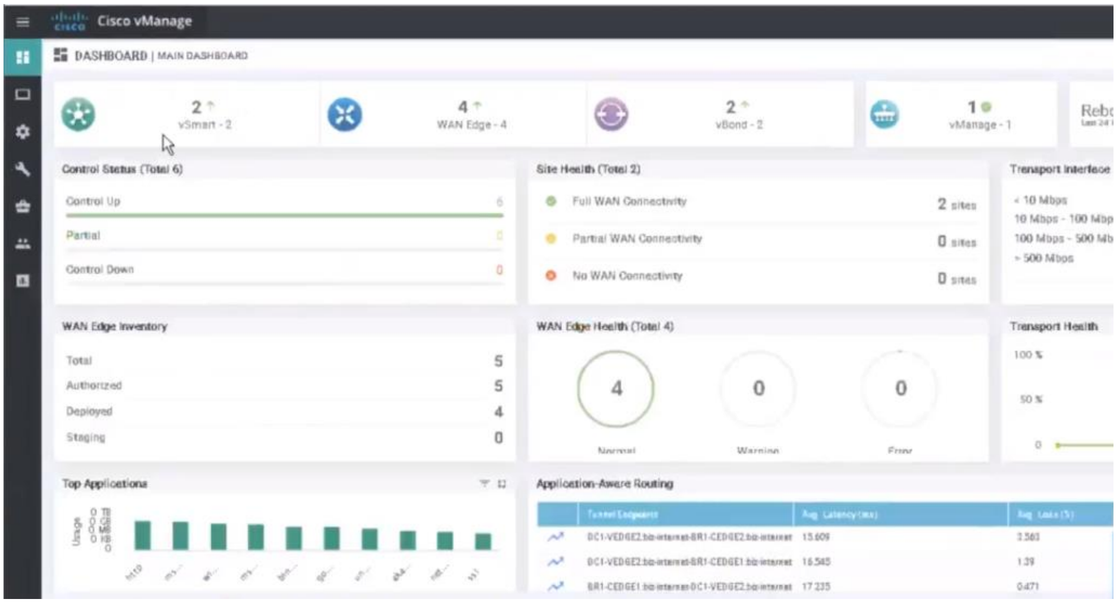
© 2021 Palo Alto Networks, Inc. All rights reserved.
Version 8.2.3.

We observed Prisma SD-WAN’s browser dependency

4.4 Troubleshooting

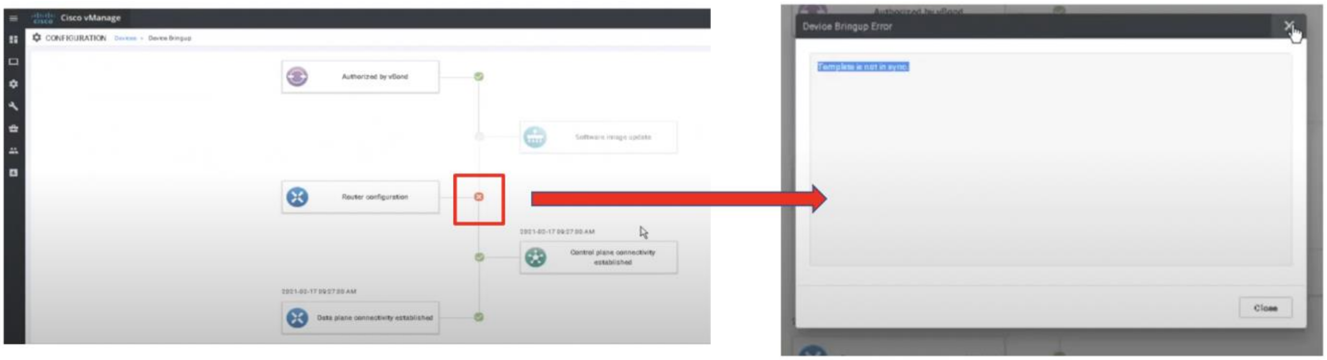
4.4.1 Cisco

Cisco offers dedicated troubleshooting section in vManage dashboard with guided workflows which makes it easy for customers to identify, troubleshoot and rectify a problem in their network.



	Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)
	DC1-VEDGE2:biz-internet-BR1-CEDGE2:biz-internet	15.609	2.563
	DC1-VEDGE2:biz-internet-BR1-CEDGE1:biz-internet	16.545	1.39
	BR1-CEDGE1:biz-internet-DC1-VEDGE2:biz-internet	17.235	0.471

To ease customer setup, Cisco vManage provides a visual step-by-step visual topology map for Day 0 configuration under the “Device Bringup” pane. Any issues or errors are displayed for easy identification.



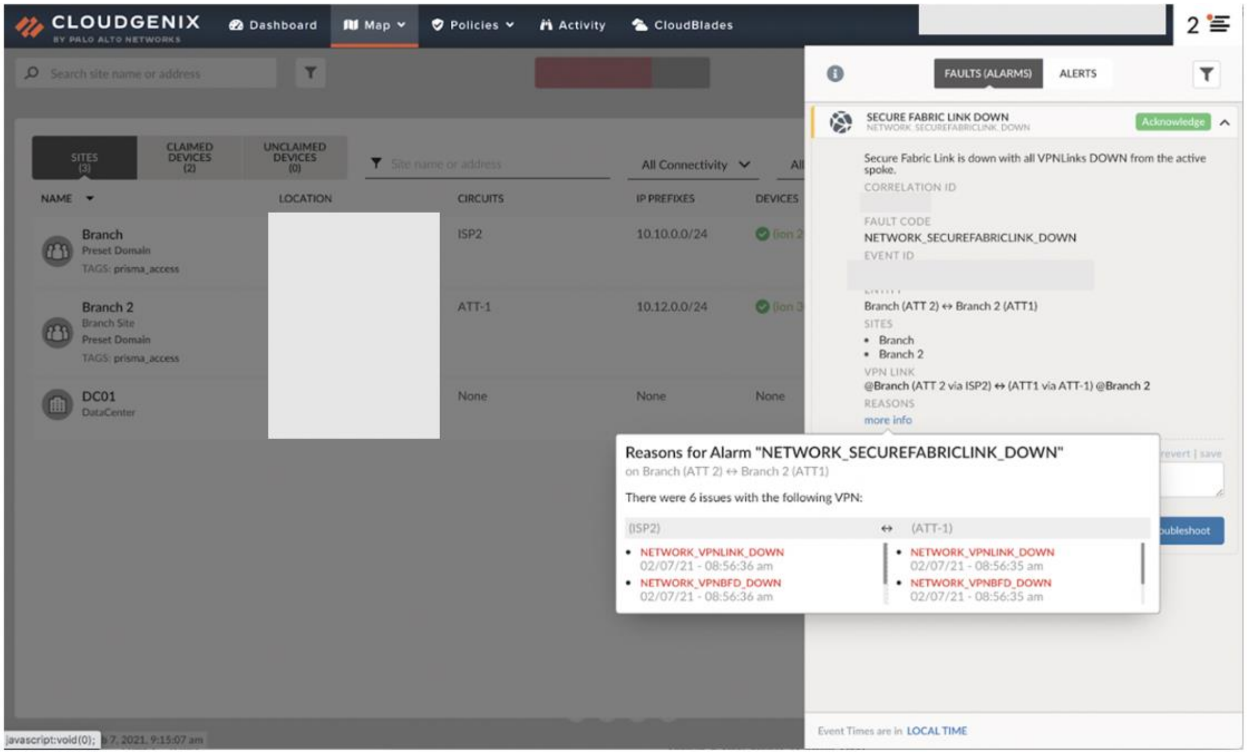
Template is not in sync.

“Device Bringup” is available for customers to view troubleshooting features and steps for getting the device ready. Clicking on the issue area brings up the following error and issue.

4.4.2 Palo Alto

The Prisma SD-WAN dashboard offers basic troubleshooting not providing much in terms of notification and alerts. While providing support tickets, Prisma SD-WAN does not have immediate troubleshooting solutions for the client.

The Prisma SD-WAN Dashboard contained basic troubleshooting with alarms and alerts that provided reasonings for failure. Although this Dashboard provided support ticket generation, there were no troubleshooting steps available. Contacting and waiting for support was time consuming and frustrating.



NAME	LOCATION	CIRCUITS	IP PREFIXES	DEVICES
Branch Preset Domain TAGS: prisma_access		ISP2	10.10.0.0/24	(ion 2
Branch 2 Branch Site Preset Domain TAGS: prisma_access		ATT-1	10.12.0.0/24	(ion 3
DC01 DataCenter		None	None	None

SECURE FABRIC LINK DOWN
NETWORK_SECUREFABRICLINK_DOWN

Secure Fabric Link is down with all VPNLinks DOWN from the active spoke.

CORRELATION ID

FAULT CODE
NETWORK_SECUREFABRICLINK_DOWN

EVENT ID

ENTITY
Branch (ATT 2) ↔ Branch 2 (ATT1)

SITES
- Branch
- Branch 2

VPN LINK
@Branch (ATT 2 via ISP2) ↔ (ATT1 via ATT-1) @Branch 2

REASONS
more info

Reasons for Alarm "NETWORK_SECUREFABRICLINK_DOWN"
on Branch (ATT 2) ↔ Branch 2 (ATT1)

There were 6 issues with the following VPN:

(ISP2)	↔ (ATT-1)
NETWORK_VPNLINK_DOWN 02/07/21 - 08:56:36 am	NETWORK_VPNLINK_DOWN 02/07/21 - 08:56:35 am
NETWORK_VPNBFD_DOWN 02/07/21 - 08:56:36 am	NETWORK_VPNBFD_DOWN 02/07/21 - 08:56:35 am

Event Times are in LOCAL TIME

Prisma SD-WAN troubleshooting capabilities are too simple, with no visible solutions for networking issues.

Test Case Summary

The Cisco solution proved more efficient, containing all customer management needs in one platform. Customer support was not needed for setup, demonstrating true zero-touch provisioning. Customers who wish to self-manage, and beginner engineers may find Cisco to be easier to manage because of preloaded templates and helpful troubleshooting features that are provided. Cisco additionally has little to no browser dependency which acts as an extra security measure for customers.

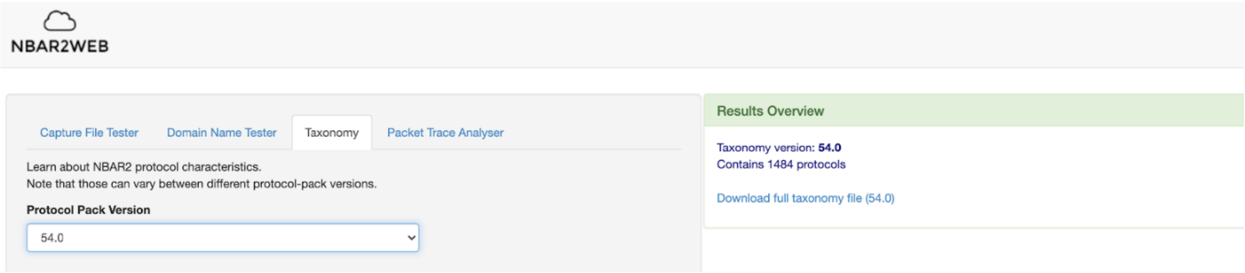
Palo Alto required more touchpoints, manual intervention, and more time to be able to create a successful network. There were more steps involved with Palo Alto integration and some required customer support for device activation to proceed. Navigating through the WebUI and configuring devices with Prisma SD-WAN was more time consuming and complex any may prove to be more difficult for beginner engineers or customers that wish to manage the network on their own. Troubleshooting was shown to be basic and unsupportive. Prisma SD-WAN was limited to Google Chrome - a possible security concern.

5.0 Application Visibility SD-WAN Comparison

5.1 Number of Applications

5.1.1 Cisco

Cisco recognizes over 1400 application signatures, including cloud applications with granular visibility into each application and its performance.



Learn about NBAR2 protocol characteristics.
Note that those can vary between different protocol-pack versions.

Protocol Pack Version: 54.0

Results Overview

Taxonomy version: **54.0**
Contains 1484 protocols

Cisco SDWAN supports 1400 + apps including cloud apps and has partnership with vendors like Microsoft to provide a better app experience when it comes to applications.

Cisco uses deep packet inspection to classify more than 1400 applications including cloud applications. Using Quality of Service capabilities, Cisco can reprioritize applications using statistics such as traffic and business relevance in real-time. This allows for optimal bandwidth utilization.

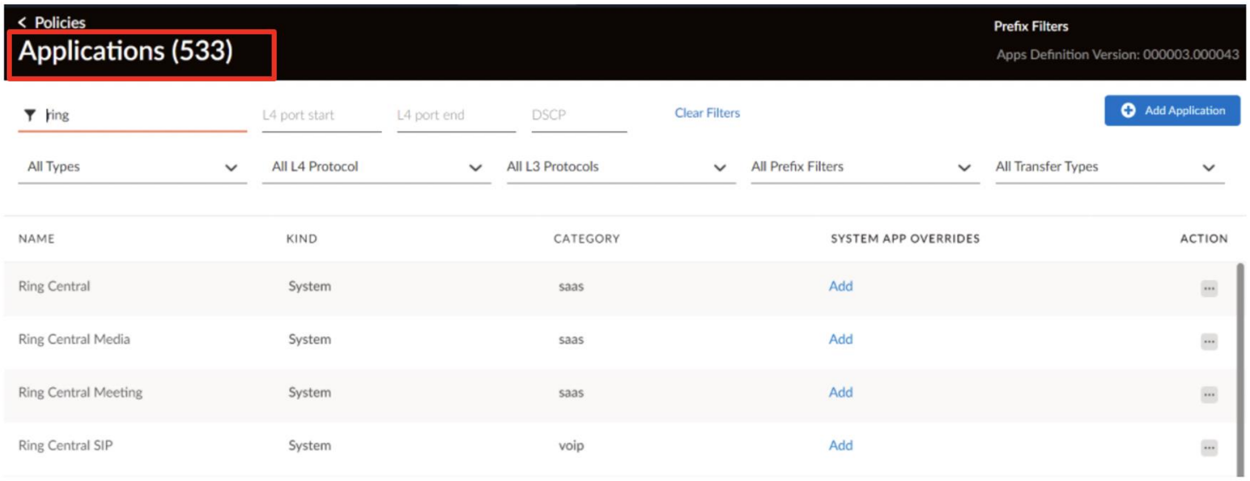
Cisco's partnership with Microsoft offers integration with Office365 for enhanced telemetry – a key Cisco SD-WAN differentiator. Cisco SD-WAN and Office365 integration allows customers to easily remediate sub-optimal application performance. With informed network routing, customers can improve their end user experience via monitoring and automatic intervention whenever performance is deficient relative to Office 365's specific expectations for applications (e.g. Microsoft SharePoint, Outlook, Teams).

Cisco's new URL Categorization feature provides significant improvement in this area for those who use Cloud OnRamp with Microsoft Office365.

5.1.2 Palo Alto

Prisma SD-WAN offers only 533 applications, including the cloud applications in the Prisma SD-WAN controller dashboard. It does not offer an intuitive application dashboard and is missing key elements, like top application dashboard.

Unlike Cisco, it does not have a partnership and therefore enhanced Office365 telemetry for intuitive application performance metrics.



Applications (533)

ring

NAME	KIND	CATEGORY	SYSTEM APP OVERRIDES	ACTION
Ring Central	System	saas	Add	···
Ring Central Media	System	saas	Add	···
Ring Central Meeting	System	saas	Add	···
Ring Central SIP	System	voip	Add	···

Prisma SD-WAN displaying support for 533 applications, including cloud applications.

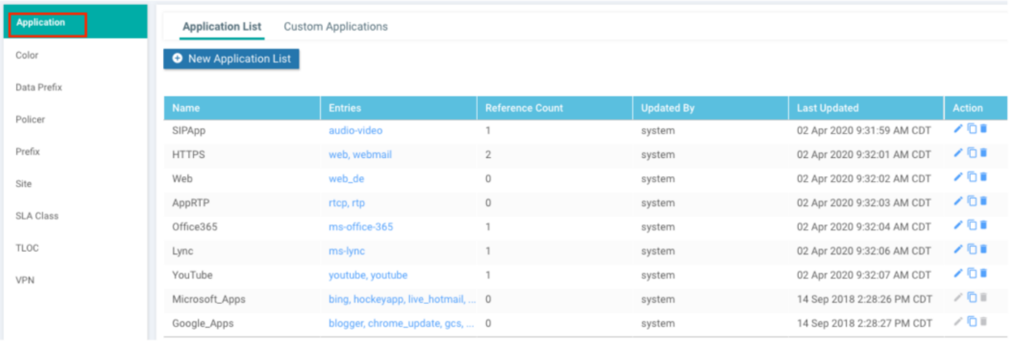
Test Case Summary

Cisco offers almost 1000 more application signatures than Palo Alto, as well as a more intuitive dashboard and granular application visibility. Cisco's partnership with Microsoft Office365 for enhanced telemetry to remediate sub-optimal application performance that Palo Alto cannot provide.

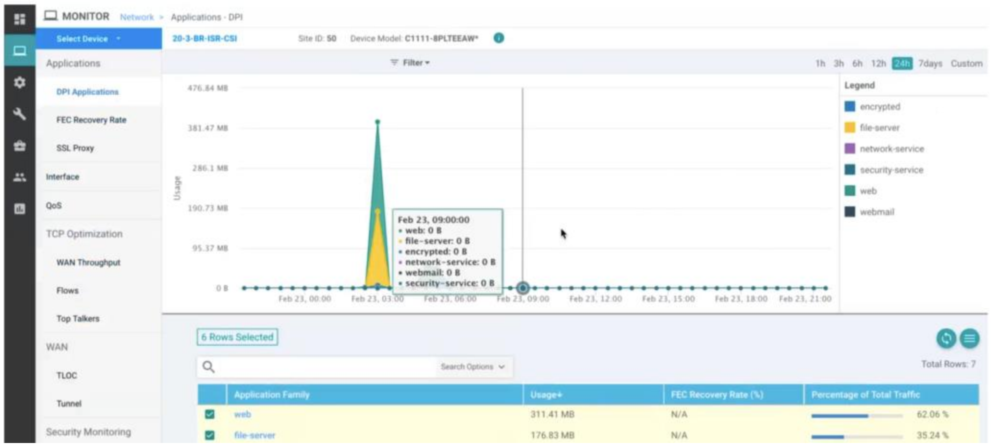
5.3 Easy Application UI

5.3.1 Cisco

Cisco vManage offered multiple features, including top applications used, and displayed them using an easy-to-read chart with details.



Name	Entries	Reference Count	Updated By	Last Updated	Action
SIPApp	audio-video	1	system	02 Apr 2020 9:31:59 AM CDT	
HTTPS	web, webmail	2	system	02 Apr 2020 9:32:01 AM CDT	
Web	web_de	0	system	02 Apr 2020 9:32:02 AM CDT	
AppRTP	rtcp, rtp	0	system	02 Apr 2020 9:32:03 AM CDT	
Office365	ms-office-365	1	system	02 Apr 2020 9:32:04 AM CDT	
Lync	ms-lync	1	system	02 Apr 2020 9:32:06 AM CDT	
YouTube	youtube, youtube	1	system	02 Apr 2020 9:32:07 AM CDT	
Microsoft_Apps	bing, hockeyapp, live_hotmail, ...	0	system	14 Sep 2018 2:28:26 PM CDT	
Google_Apps	blogger, chrome_update, gcs, ...	0	system	14 Sep 2018 2:28:27 PM CDT	



Feb 23, 09:00:00
- web: 0 B
- file-server: 0 B
- encrypted: 0 B
- network-service: 0 B
- webmail: 0 B
- security-service: 0 B

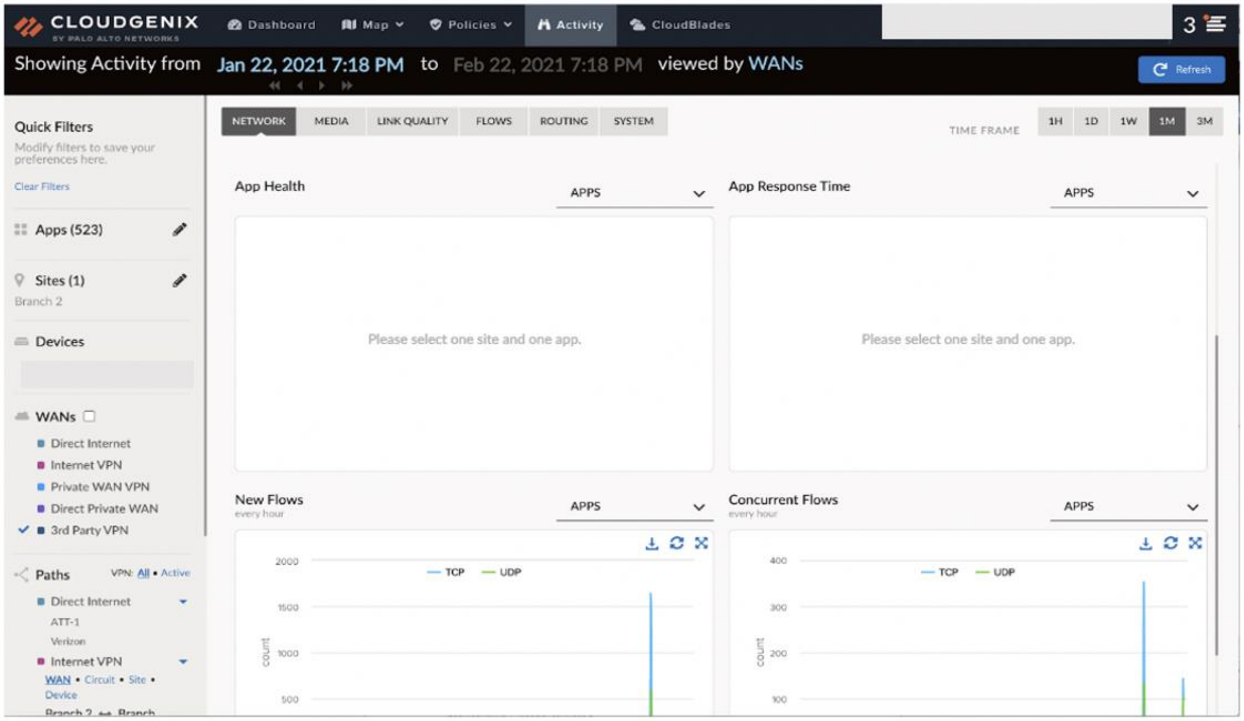
	Application Family	Usage	FEC Recovery Rate (%)	Percentage of Total Traffic
☑	web	311.41 MB	N/A	62.06 %
☑	file-server	176.83 MB	N/A	35.24 %

Cisco vManage dashboard provides detailed view of application traffic, including bandwidth usage, application family, traffic type, duration etc.

5.3.2 Palo Alto

Prisma SD-WAN identified applications, however it required us to go to the Flow section to view this path or the applications being utilized.

The Prisma SD-WAN Application Dashboard showed the entire flow, successful count, application health, and response time. Applications had to be individually selected to view their statistics. This limitation did not allow for viewing of all or selected applications for comparison.



Showing Activity from Jan 22, 2021 7:18 PM to Feb 22, 2021 7:18 PM viewed by WANs

Please select one site and one app.

Please select one site and one app.

One application must be selected in order to view individual statistics rather than having the option for comparison.

To retain and access up to 90 days of statistics, customers need to obtain an additional Network DVR license, per device.

Test Case Summary

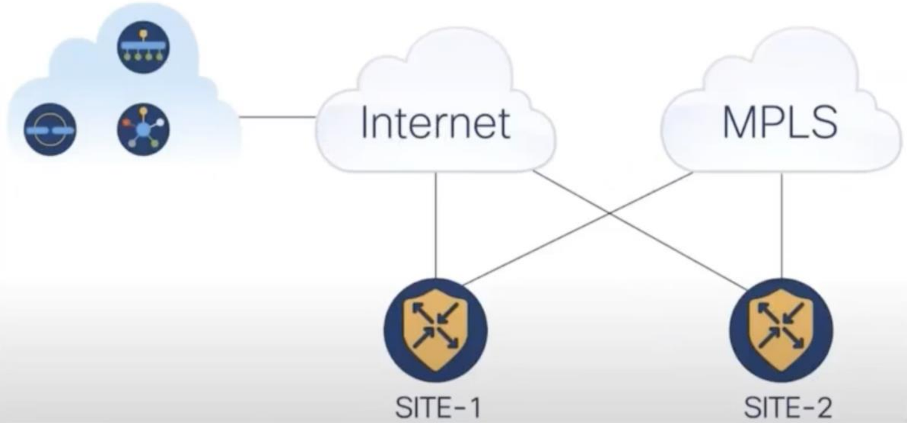
Cisco and Palo Alto had similar ways of identifying applications. But Palo Alto lacked the ability to view and compare statistics for all or selected applications, requiring individual selections to view. The application UI limitations of Prisma SD-WAN may pose a minor nuisance for customers; however, this may be a preference.

6.0 High Availability and Best Path Optimization

6.1 High Availability

6.1.1 Cisco

Cisco demonstrated through two different use cases that they can operate seamlessly without any disruption, even if the control connection goes down. When Cisco devices formed a tunnel, they were not dependent on the control plane connections in order to pass traffic. Cisco demonstrated this by displaying traffic continuously flowing even with a control link shut down.



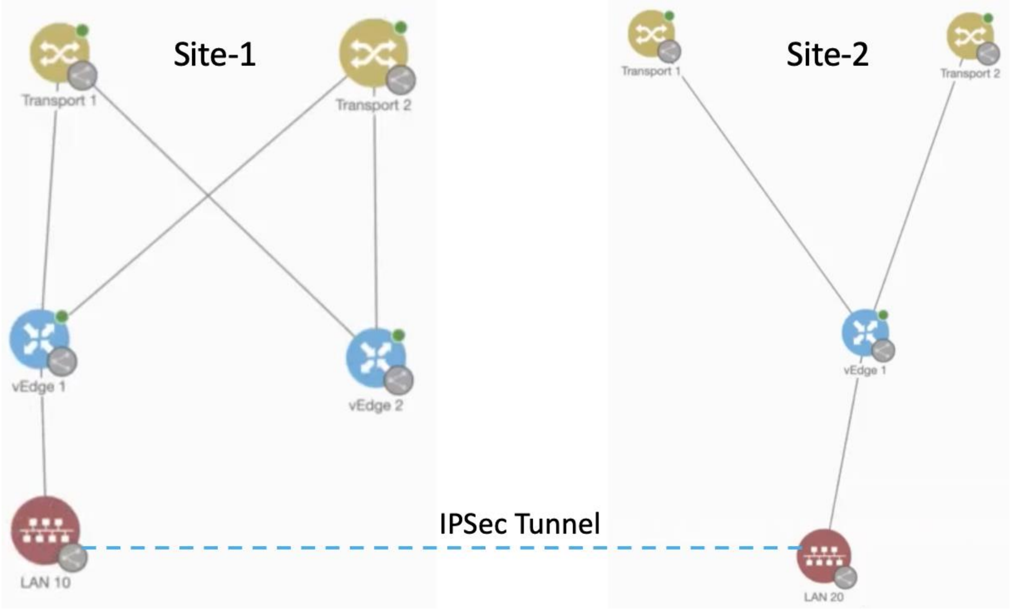
We observed that Cisco was able to maintain the IPSec tunnel and traffic flow between Site-1 and Site-2 without any interruptions. We viewed the control connection status on the dashboard along with other components of the control plane.

There were 2 Use cases demonstrated:

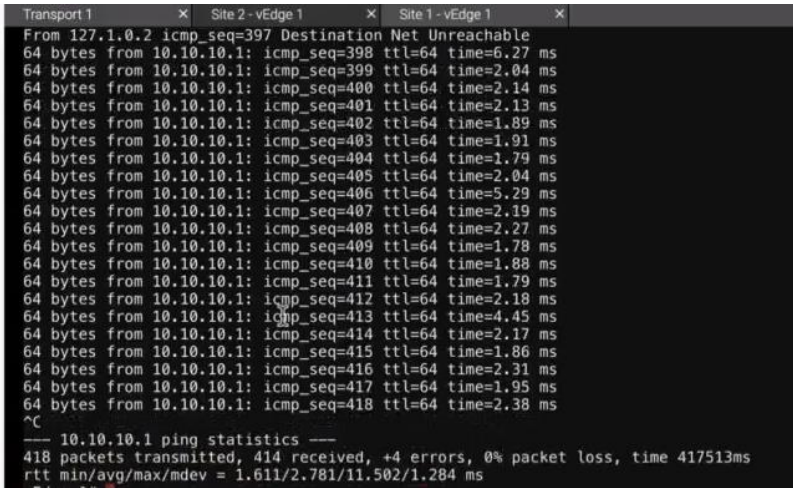
1. Use Case-1: Internet link from Site-2 toward control plane was shut down, disconnecting it from controllers.
2. Use Case-2: Internet link toward control plane was shut down, disconnecting both the sites from the controllers.

During the live demonstration, we observed no disruption or packet loss during Use Case 1 and Use Case 2.

USE CASE 1



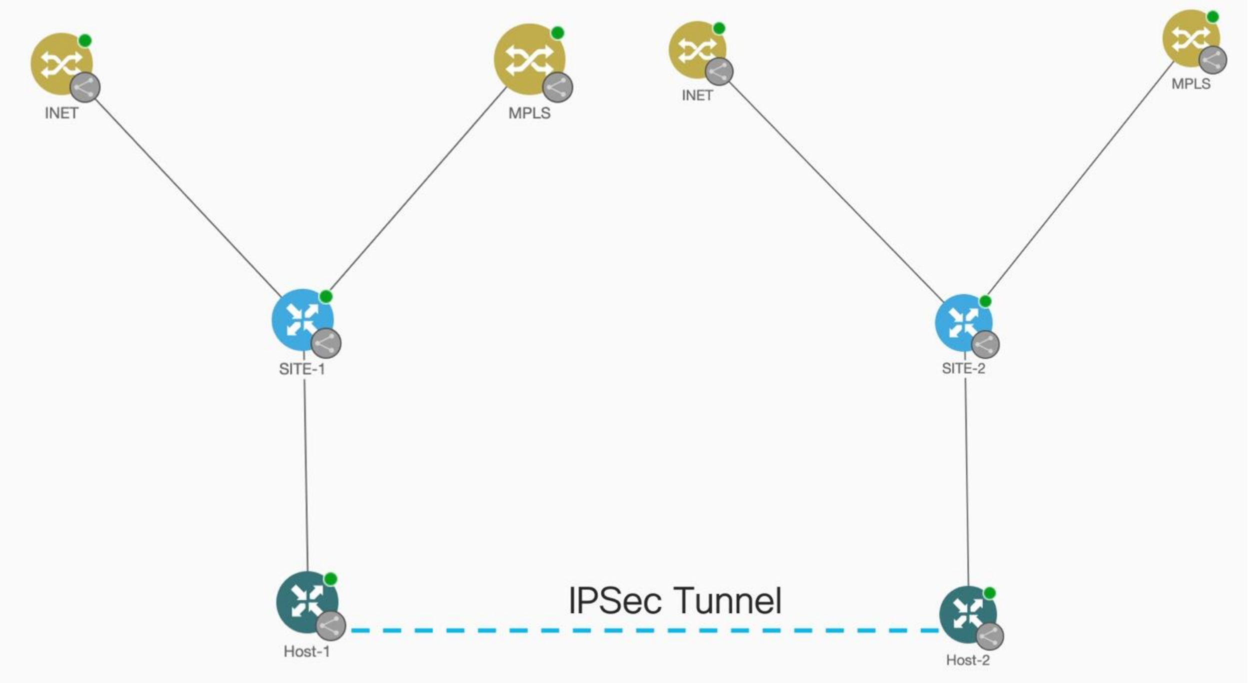
In Use Case 1, we generated traffic through LAN 20 located on Site 2 going through vEdge1, going through either transport paths to Site 1 to LAN 10. The control connection link going from Transport 1 was shut down, and we observed all control connections down. Traffic flow continued without any loss.

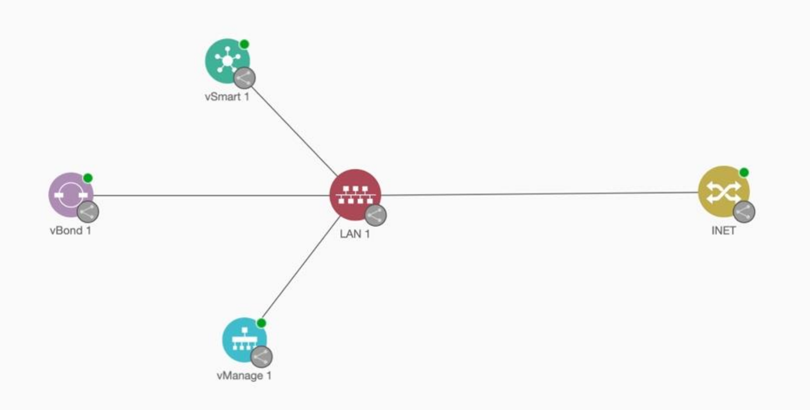


```
From 127.1.0.2 icmp_seq=397 Destination Net Unreachable
64 bytes from 10.10.10.1: icmp_seq=398 ttl=64 time=6.27 ms
64 bytes from 10.10.10.1: icmp_seq=399 ttl=64 time=2.04 ms
64 bytes from 10.10.10.1: icmp_seq=400 ttl=64 time=2.14 ms
64 bytes from 10.10.10.1: icmp_seq=401 ttl=64 time=2.13 ms
64 bytes from 10.10.10.1: icmp_seq=402 ttl=64 time=1.89 ms
64 bytes from 10.10.10.1: icmp_seq=403 ttl=64 time=1.91 ms
64 bytes from 10.10.10.1: icmp_seq=404 ttl=64 time=1.79 ms
64 bytes from 10.10.10.1: icmp_seq=405 ttl=64 time=2.04 ms
64 bytes from 10.10.10.1: icmp_seq=406 ttl=64 time=5.29 ms
64 bytes from 10.10.10.1: icmp_seq=407 ttl=64 time=2.19 ms
64 bytes from 10.10.10.1: icmp_seq=408 ttl=64 time=2.27 ms
64 bytes from 10.10.10.1: icmp_seq=409 ttl=64 time=1.78 ms
64 bytes from 10.10.10.1: icmp_seq=410 ttl=64 time=1.88 ms
64 bytes from 10.10.10.1: icmp_seq=411 ttl=64 time=1.79 ms
64 bytes from 10.10.10.1: icmp_seq=412 ttl=64 time=2.18 ms
64 bytes from 10.10.10.1: icmp_seq=413 ttl=64 time=4.45 ms
64 bytes from 10.10.10.1: icmp_seq=414 ttl=64 time=2.17 ms
64 bytes from 10.10.10.1: icmp_seq=415 ttl=64 time=1.86 ms
64 bytes from 10.10.10.1: icmp_seq=416 ttl=64 time=2.31 ms
64 bytes from 10.10.10.1: icmp_seq=417 ttl=64 time=1.95 ms
64 bytes from 10.10.10.1: icmp_seq=418 ttl=64 time=2.38 ms
^C
--- 10.10.10.1 ping statistics ---
418 packets transmitted, 414 received, +4 errors, 0% packet loss, time 417513ms
rtt min/avg/max/mdev = 1.611/2.781/11.502/1.284 ms
```

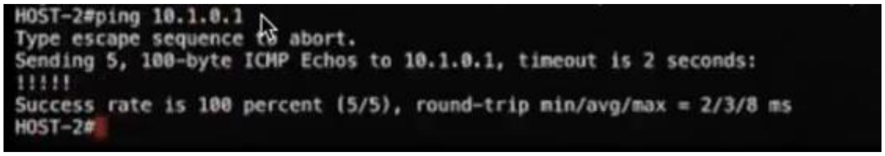
Test Case 1 showed no traffic interruption.

USE CASE 2





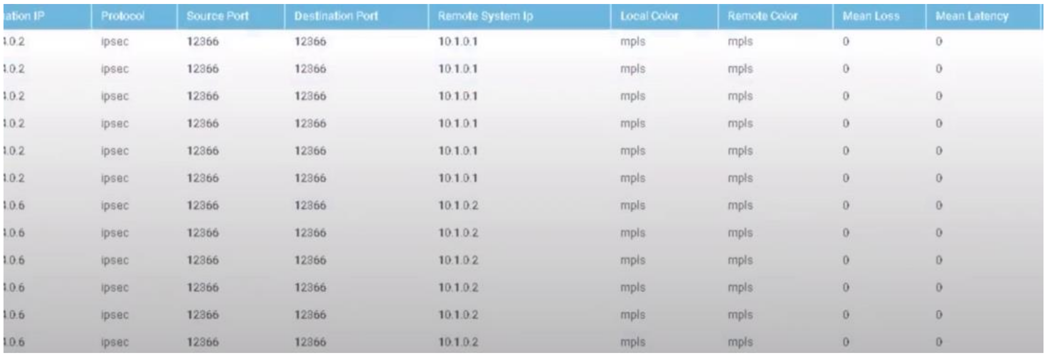
Use Case 2 had a similar topology with an INET connection and a MPLS connection. INET was connected to the controller, but the MPLS was not. The IPSec tunnel between Site 1 and Site 2 was successfully formed. Traffic was generated from Site 2 toward Site 1 and the INET link to the control plane was brought down. Similar to Use Case 1, we observed that even though the control connections went down for both the sites, there was no interruption in data plane traffic flow.



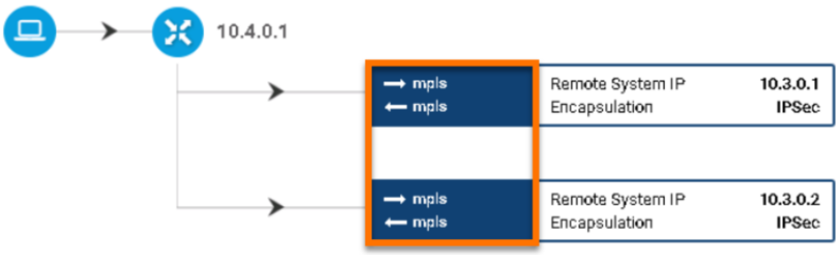
```
HOST-2#ping 10.1.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/8 ms
HOST-2#
```

Test Case 2 showed no traffic interruption.

Cisco additionally demonstrated application path optimization. We created application routing polices to map specific application to specific transport types, Internet links for example. Some of our applications were directed to use MPLS if there was any latency or jitter exceeding what was defined; the traffic was expected to automatically shift to the backup link.



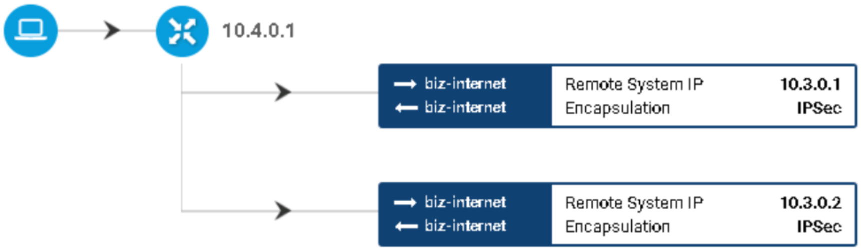
ation IP	Protocol	Source Port	Destination Port	Remote System Ip	Local Color	Remote Color	Mean Loss	Mean Latency
1.0.2	ipsec	12366	12366	10.1.0.1	mpls	mpls	0	0
1.0.2	ipsec	12366	12366	10.1.0.1	mpls	mpls	0	0
1.0.2	ipsec	12366	12366	10.1.0.1	mpls	mpls	0	0
1.0.2	ipsec	12366	12366	10.1.0.1	mpls	mpls	0	0
1.0.2	ipsec	12366	12366	10.1.0.1	mpls	mpls	0	0
1.0.2	ipsec	12366	12366	10.1.0.1	mpls	mpls	0	0
1.0.6	ipsec	12366	12366	10.1.0.2	mpls	mpls	0	0
1.0.6	ipsec	12366	12366	10.1.0.2	mpls	mpls	0	0
1.0.6	ipsec	12366	12366	10.1.0.2	mpls	mpls	0	0
1.0.6	ipsec	12366	12366	10.1.0.2	mpls	mpls	0	0
1.0.6	ipsec	12366	12366	10.1.0.2	mpls	mpls	0	0
1.0.6	ipsec	12366	12366	10.1.0.2	mpls	mpls	0	0



Remote System IP 10.3.0.1
Encapsulation IPSec

Remote System IP 10.3.0.2
Encapsulation IPSec

When we increased the latency on specific transports, we observed no interruption in traffic and no manual intervention was required to failover the application traffic toward secondary WAN link defined in the SLA policy.



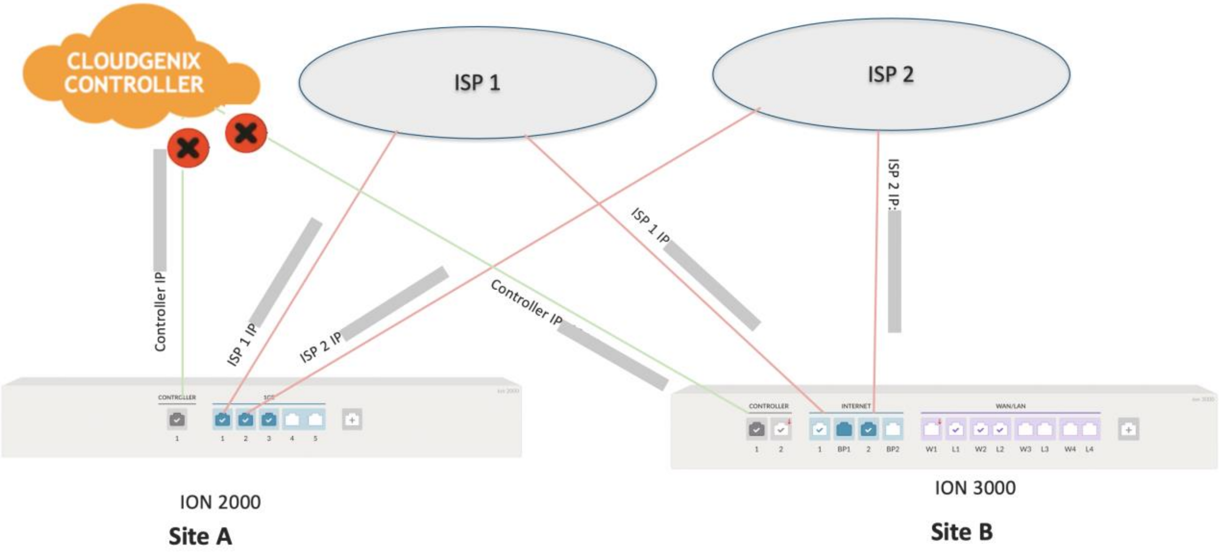
Remote System IP 10.3.0.1
Encapsulation IPSec

Remote System IP 10.3.0.2
Encapsulation IPSec

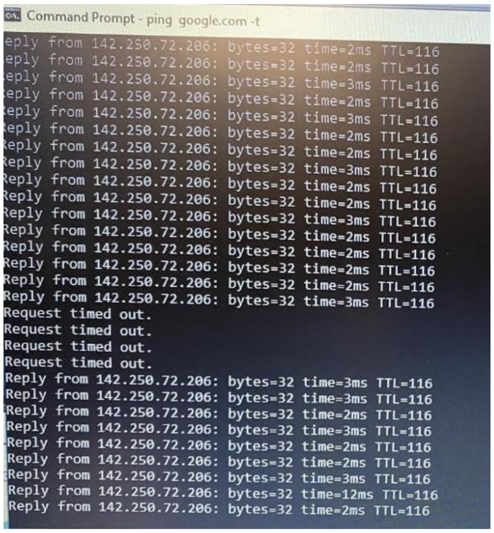
6.1.2 Palo Alto

Prisma SD-WAN ION devices had specific ports for Controller communication and Internet/WAN for data traffic. If the Controller port is taken down, the controller traffic is managed by the Internet/WAN port.

Through a video demonstration, we observed Prisma SD-WAN perform path optimization using the following topology.



In the topology scenario, the ION 2000 and ION 3000, are connected to both ISP 1, ISP 2, and the Prisma SD-WAN controller. The links to the controller were taken down during this use case as marked by the "x" on the top left. Once the controller connection is down, controller connection is made through the ISP ports. Once the ISP 1 port is taken down, the traffic flow is not seamless. We can see significant ping drops for approximately 10 seconds before the traffic switches to ISP 2.



Command Prompt - ping google.com -t

```
eply from 142.250.72.206: bytes=32 time=2ms TTL=116
eply from 142.250.72.206: bytes=32 time=2ms TTL=116
eply from 142.250.72.206: bytes=32 time=3ms TTL=116
eply from 142.250.72.206: bytes=32 time=2ms TTL=116
Reply from 142.250.72.206: bytes=32 time=3ms TTL=116
Reply from 142.250.72.206: bytes=32 time=2ms TTL=116
Reply from 142.250.72.206: bytes=32 time=2ms TTL=116
Reply from 142.250.72.206: bytes=32 time=3ms TTL=116
Reply from 142.250.72.206: bytes=32 time=2ms TTL=116
Reply from 142.250.72.206: bytes=32 time=2ms TTL=116
Reply from 142.250.72.206: bytes=32 time=3ms TTL=116
Reply from 142.250.72.206: bytes=32 time=2ms TTL=116
Reply from 142.250.72.206: bytes=32 time=2ms TTL=116
Reply from 142.250.72.206: bytes=32 time=2ms TTL=116
Reply from 142.250.72.206: bytes=32 time=2ms TTL=116
Reply from 142.250.72.206: bytes=32 time=3ms TTL=116
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 142.250.72.206: bytes=32 time=3ms TTL=116
Reply from 142.250.72.206: bytes=32 time=3ms TTL=116
Reply from 142.250.72.206: bytes=32 time=2ms TTL=116
Reply from 142.250.72.206: bytes=32 time=3ms TTL=116
Reply from 142.250.72.206: bytes=32 time=2ms TTL=116
Reply from 142.250.72.206: bytes=32 time=2ms TTL=116
Reply from 142.250.72.206: bytes=32 time=3ms TTL=116
Reply from 142.250.72.206: bytes=32 time=12ms TTL=116
Reply from 142.250.72.206: bytes=32 time=2ms TTL=116
```

The video demonstrated the Prisma SD-WAN high availability capabilities during traffic disruption.

Following the disruption of the controller links, we observed an approximate 10 second disruption in traffic during the failover testing. This means that during path optimization and failover, clients would experience a brief disruption in work. This is problematic for high traffic enterprises such as those in the financial district. Also, if the ISP ports are taken down for disconnecting the controller communication, as it is a Cloud based SaaS offering, the dependency is more on the cloud controller. Hence the ION devices will also go offline disrupting the whole network.

Test Case Summary

We observed Cisco providing data plane resiliency even during control plane down events, without any interruption in data traffic forwarding, as opposed to Prisma SD-WAN which demonstrated an approximate 10 second delay. For mission critical applications, this may pose a problem. It is important to note that the Prisma SD-WAN dashboard did not display to the customer that the controller port is down. Customers must navigate into the device via Map > Sites > Device > Interface Config > Interface Status. Cisco displays this clearly on the vManage Dashboard.

6.2 Setup Complexity

6.2.1 Cisco

Cisco edge devices can establish control plane sessions over any available transport interface. In cases where control plane sessions were lost for any reason, data traffic continued to flow seamlessly without any issues and no manual intervention required to keep the traffic flowing. Cisco SD-WAN solution do not require any separate and dedicated physical interface just for control plane sessions for enabling Data Plane connection.

6.2.2 Palo Alto

Palo Alto Prisma SD-WAN ION devices have a dedicated physical port just for control plane connectivity. This extra port is necessary for the Prisma SD-WAN ION boxes to connect to the controller. When the controller port went down, the controller traffic automatically switched to port 1 with Internet connection. This controller connection port required an additional public IP increasing complexity and dependency on the controller connection during the device bring up process.

Test Case Summary

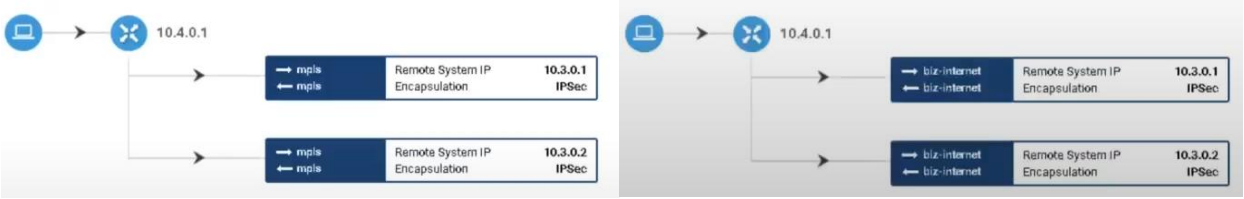
Cisco edge devices can use any transport Interface for communication with the vSmart controllers. By default each Cisco edge device will establish two control sessions to each vSmart. Palo Alto by default utilizes a dedicated physical port for control plane communication and required an additional IP address and configurations for a secondary control session to be established over other transport interfaces. This adds complexity and cost.

6.3 Application Awareness

6.3.1 Cisco

Any applications with defined SLAs were pinned to a specific link. We were directing these applications to use only MPLS, and if there was any latency or jitter exceeding what we defined, the traffic automatically shifted or seamlessly failed over to the backup link.

No manual intervention was required. This was easily viewed, and no delay was noticed during testing.



10.4.0.1

→ mpls ← mpls | Remote System IP 10.3.0.1 | Encapsulation IPSec

→ mpls ← mpls | Remote System IP 10.3.0.2 | Encapsulation IPSec

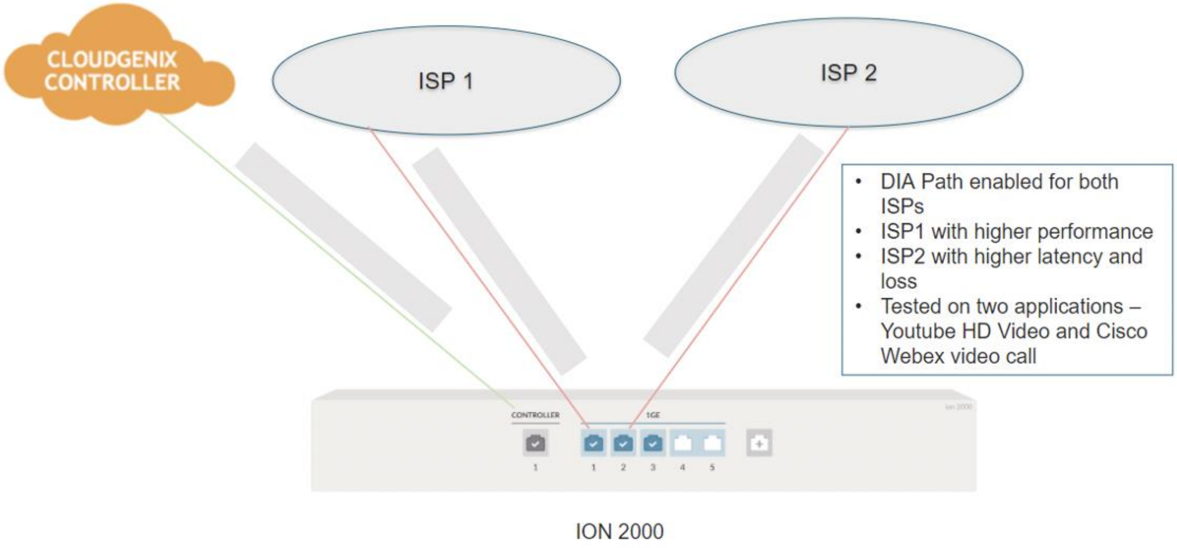
10.4.0.1

→ biz-internet ← biz-internet | Remote System IP 10.3.0.1 | Encapsulation IPSec

→ biz-internet ← biz-internet | Remote System IP 10.3.0.2 | Encapsulation IPSec

We observed the original traffic pathway (left), where traffic took the MPLS pathway. The application failover path was viewed after introducing latency which exceeded what was defined. We observed traffic now flowing through the Internet link (right).

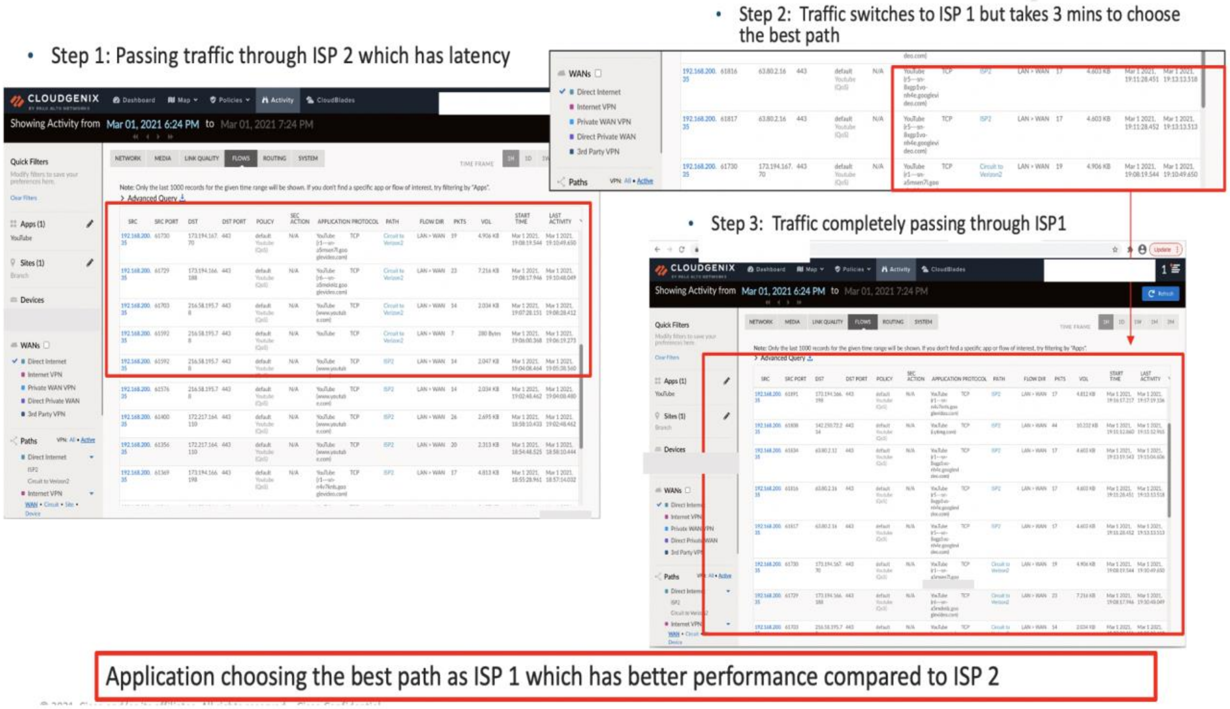
6.3.2 Palo Alto



- DIA Path enabled for both ISPs
- ISP1 with higher performance
- ISP2 with higher latency and loss
- Tested on two applications – Youtube HD Video and Cisco Webex video call

Above is the topology used to demonstrate application awareness. Prisma SD-WAN controller was connected through the controller port to the ION 2000. ISP 1 and ISP 2 were both connected to the Prisma SD-WAN device WAN ports. Both ISPs have a direct internet access path that was defined. ISP2 is the link where latency was introduced. YouTube (HD 1080p quality) and Webex were the used applications.

Miercom observed that for any latency produced, the application would choose the path with better performance. Although this process successfully occurred, there was a significant 3-minute delay between failover path optimizations.



- Step 1: Passing traffic through ISP 2 which has latency
- Step 2: Traffic switches to ISP 1 but takes 3 mins to choose the best path
- Step 3: Traffic completely passing through ISP1

Application choosing the best path as ISP 1 which has better performance compared to ISP 2

Palo Alto showed successful application path optimization. Viewing the timestamps show there was a 3-minute delay during the switch to path optimization.

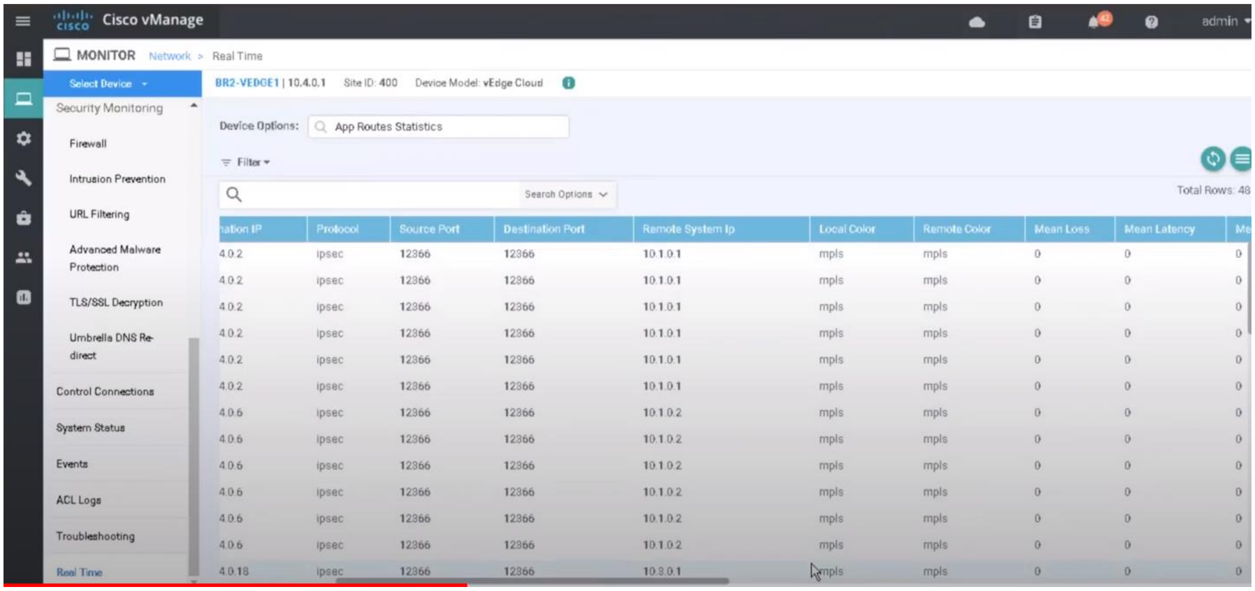
Test Case Summary

While both Cisco and Palo Alto successfully performed failover path optimization for applications, Cisco had no interruptions. Prisma SD-WAN showed significant delays between failover path selection, wherein customers with high-traffic enterprises or data centers will find this delay troublesome for their business.

6.4 Application Metrics Visibility

6.4.1 Cisco

Cisco showed the quality of experience metric. Link quality showed all parameters: packet loss, latency, jitter within the vManage Dashboard. We viewed the overall statistics of applications.



BR2-VEDGE1 | 10.4.0.1 Site ID: 400 Device Model: vEdge Cloud

Device Options: App Routes Statistics

Total Rows: 48

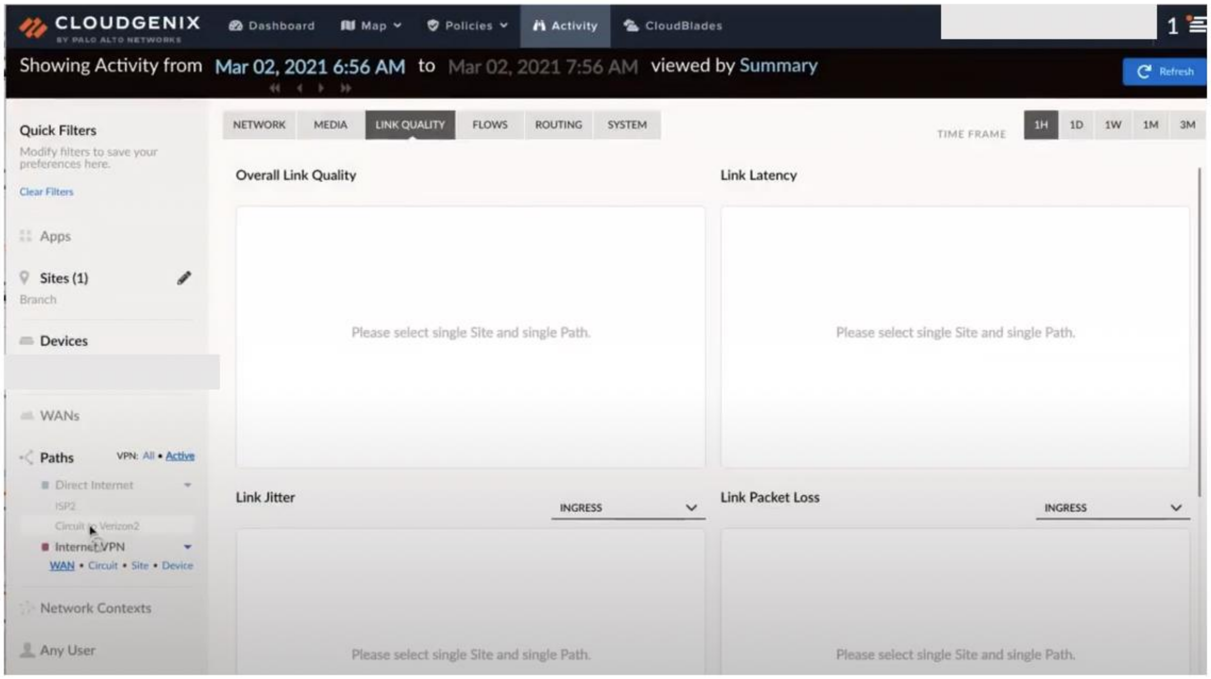
ation IP	Protocol	Source Port	Destination Port	Remote System Ip	Local Color	Remote Color	Mean Loss	Mean Latency	Me
4.0.2	ipsec	12366	12366	10.1.0.1	mpls	mpls	0	0	0
4.0.2	ipsec	12366	12366	10.1.0.1	mpls	mpls	0	0	0
4.0.2	ipsec	12366	12366	10.1.0.1	mpls	mpls	0	0	0
4.0.2	ipsec	12366	12366	10.1.0.1	mpls	mpls	0	0	0
4.0.2	ipsec	12366	12366	10.1.0.1	mpls	mpls	0	0	0
4.0.2	ipsec	12366	12366	10.1.0.1	mpls	mpls	0	0	0
4.0.6	ipsec	12366	12366	10.1.0.2	mpls	mpls	0	0	0
4.0.6	ipsec	12366	12366	10.1.0.2	mpls	mpls	0	0	0
4.0.6	ipsec	12366	12366	10.1.0.2	mpls	mpls	0	0	0
4.0.6	ipsec	12366	12366	10.1.0.2	mpls	mpls	0	0	0
4.0.6	ipsec	12366	12366	10.1.0.2	mpls	mpls	0	0	0
4.0.6	ipsec	12366	12366	10.1.0.2	mpls	mpls	0	0	0
4.0.18	ipsec	12366	12366	10.8.0.1	mpls	mpls	0	0	0

By navigating to Network > Real Time > App Route Statistics (via Device Options), users are able to view overall statistics to applications including Loss and Latency.

6.4.2 Palo Alto

Users were unable to view link quality metrics in detail in the Prisma SD-WAN dashboard. We observed direct Internet connection to Prisma SD-WAN, which failed to showcase Link Quality metrics of latency, jitter, and packet loss. For application path optimization and link quality metrics, we only saw parameters via Internet VPN and were unable to see metrics such as jitter and packet loss.

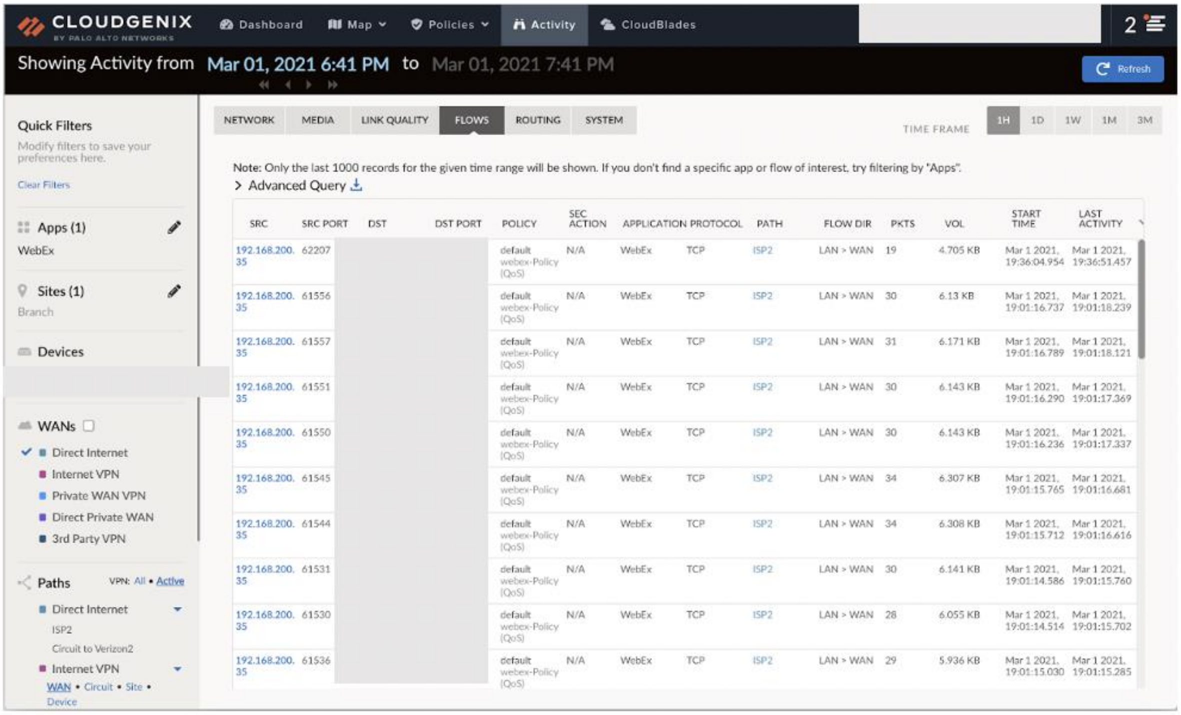
There was no overall application display; users must specifically choose the application to see basic application health or response time. This was a similar process for viewing packet flow statistics.



Showing Activity from Mar 02, 2021 6:56 AM to Mar 02, 2021 7:56 AM viewed by Summary

We observed parameters by navigating to Activity > Link Quality. Although connected to the Direct Internet, the option to view the parameter was greyed out as shown in the bottom left.

Prisma SD-WAN failed to provide real-time reporting. Although flows were viewed to demonstrate traffic flow, Prisma SD-WAN did not show any metrics for this application, even when selected. Activity parameters were still not displayed after one day of wait time.



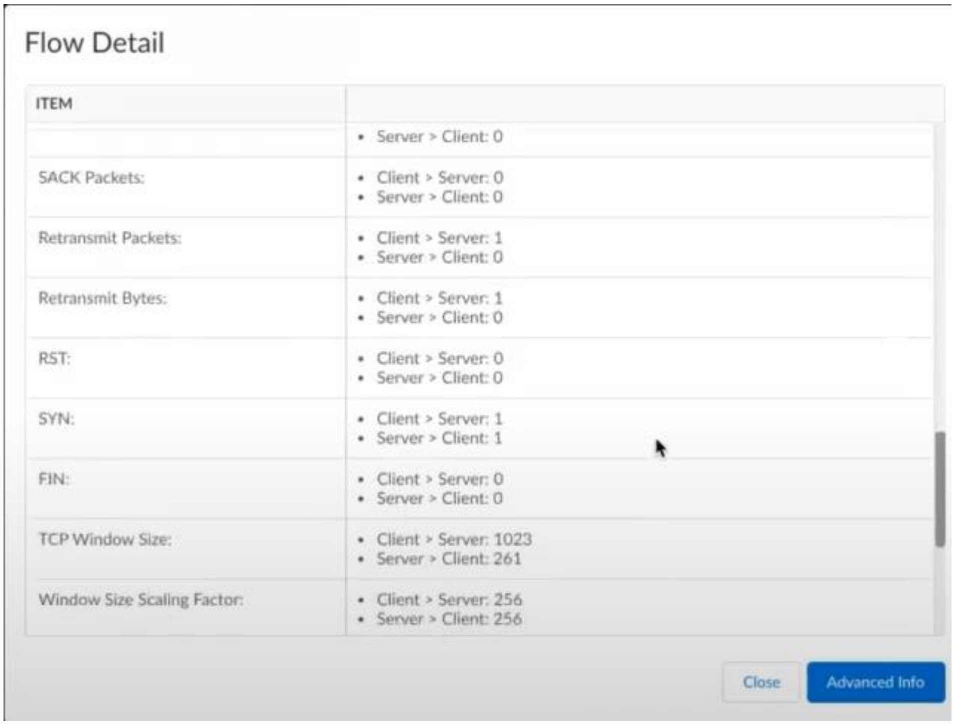
Showing Activity from Mar 01, 2021 6:41 PM to Mar 01, 2021 7:41 PM

Note: Only the last 1000 records for the given time range will be shown. If you don't find a specific app or flow of interest, try filtering by "Apps".

> Advanced Query

SRC	SRC PORT	DST	DST PORT	POLICY	SEC ACTION	APPLICATION	PROTOCOL	PATH	FLOW DIR	PKTS	VOL	START TIME	LAST ACTIVITY
192.168.200.35	62207	[redacted]	[redacted]	default webex-Policy (QoS)	N/A	WebEx	TCP	ISP2	LAN > WAN	19	4.705 KB	Mar 1 2021, 19:36:04.954	Mar 1 2021, 19:36:51.457
192.168.200.35	61556	[redacted]	[redacted]	default webex-Policy (QoS)	N/A	WebEx	TCP	ISP2	LAN > WAN	30	6.13 KB	Mar 1 2021, 19:01:16.737	Mar 1 2021, 19:01:18.239
192.168.200.35	61557	[redacted]	[redacted]	default webex-Policy (QoS)	N/A	WebEx	TCP	ISP2	LAN > WAN	31	6.171 KB	Mar 1 2021, 19:01:16.789	Mar 1 2021, 19:01:18.121
192.168.200.35	61551	[redacted]	[redacted]	default webex-Policy (QoS)	N/A	WebEx	TCP	ISP2	LAN > WAN	30	6.143 KB	Mar 1 2021, 19:01:16.290	Mar 1 2021, 19:01:17.369
192.168.200.35	61550	[redacted]	[redacted]	default webex-Policy (QoS)	N/A	WebEx	TCP	ISP2	LAN > WAN	30	6.143 KB	Mar 1 2021, 19:01:16.236	Mar 1 2021, 19:01:17.337
192.168.200.35	61545	[redacted]	[redacted]	default webex-Policy (QoS)	N/A	WebEx	TCP	ISP2	LAN > WAN	34	6.307 KB	Mar 1 2021, 19:01:15.765	Mar 1 2021, 19:01:16.681
192.168.200.35	61544	[redacted]	[redacted]	default webex-Policy (QoS)	N/A	WebEx	TCP	ISP2	LAN > WAN	34	6.308 KB	Mar 1 2021, 19:01:15.712	Mar 1 2021, 19:01:16.616
192.168.200.35	61531	[redacted]	[redacted]	default webex-Policy (QoS)	N/A	WebEx	TCP	ISP2	LAN > WAN	30	6.141 KB	Mar 1 2021, 19:01:14.586	Mar 1 2021, 19:01:15.760
192.168.200.35	61530	[redacted]	[redacted]	default webex-Policy (QoS)	N/A	WebEx	TCP	ISP2	LAN > WAN	28	6.055 KB	Mar 1 2021, 19:01:14.514	Mar 1 2021, 19:01:15.702
192.168.200.35	61536	[redacted]	[redacted]	default webex-Policy (QoS)	N/A	WebEx	TCP	ISP2	LAN > WAN	29	5.936 KB	Mar 1 2021, 19:01:15.030	Mar 1 2021, 19:01:15.285

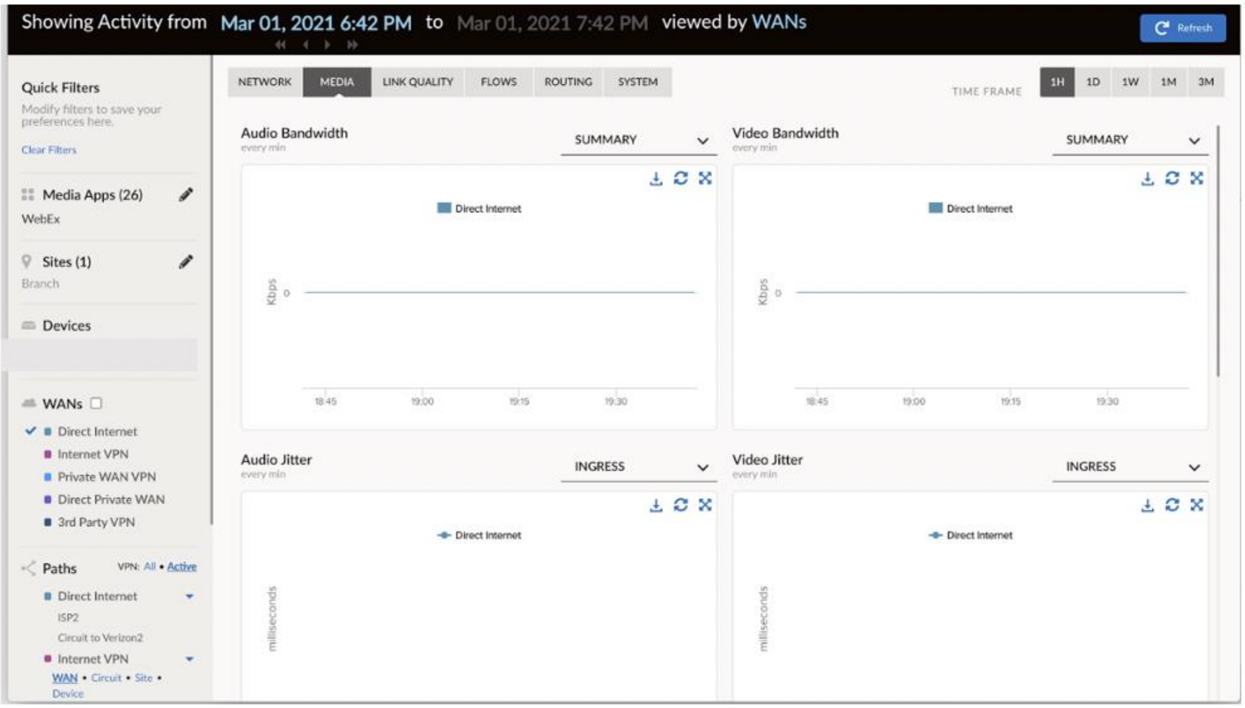
Real traffic flows were displayed and showed that traffic was successfully generated.



Flow Detail

ITEM	
	• Server > Client: 0
SACK Packets:	• Client > Server: 0 • Server > Client: 0
Retransmit Packets:	• Client > Server: 1 • Server > Client: 0
Retransmit Bytes:	• Client > Server: 1 • Server > Client: 0
RST:	• Client > Server: 0 • Server > Client: 0
SYN:	• Client > Server: 1 • Server > Client: 1
FIN:	• Client > Server: 0 • Server > Client: 0
TCP Window Size:	• Client > Server: 1023 • Server > Client: 261
Window Size Scaling Factor:	• Client > Server: 256 • Server > Client: 256

Prisma SD-WAN Application Flow details can only be viewed by clicking each packet individually.



Showing Activity from Mar 01, 2021 6:42 PM to Mar 01, 2021 7:42 PM viewed by WANs

Quick Filters
Modify filters to save your preferences here.

Media Apps (26)
WebEx

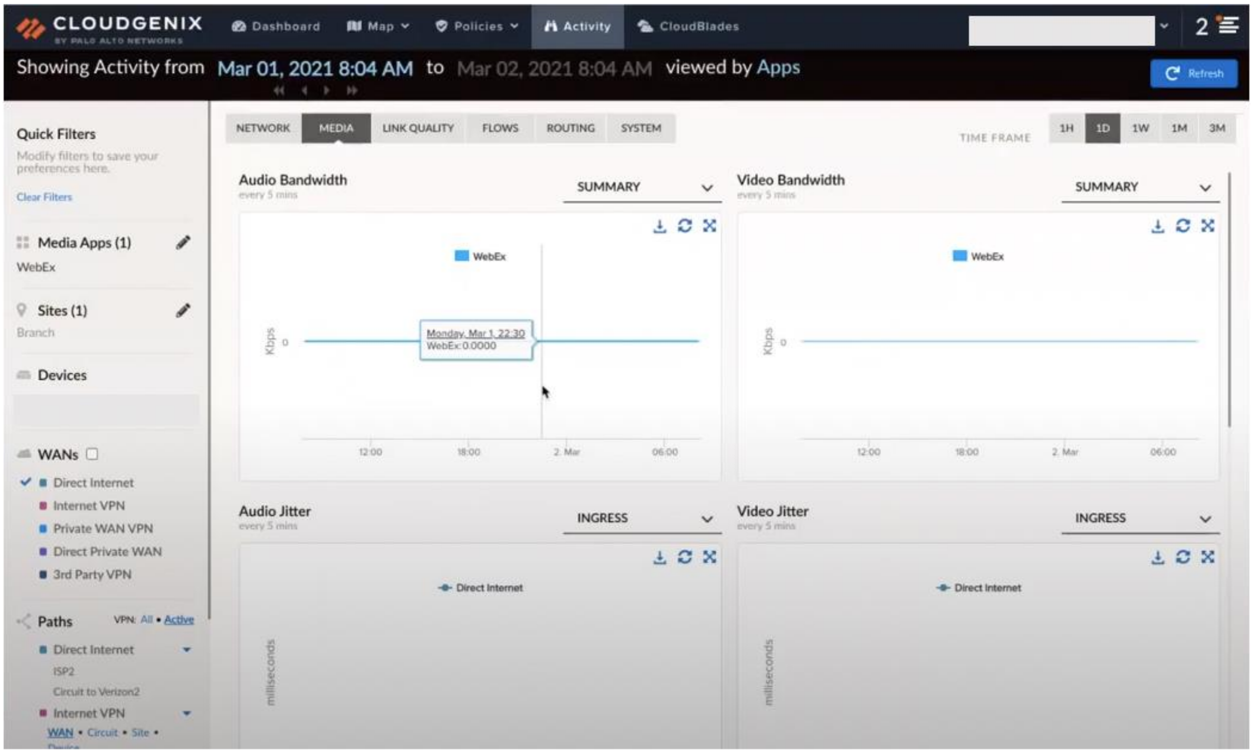
Sites (1)
Branch

Devices

WANs
✓ Direct Internet
Internet VPN
Private WAN VPN
Direct Private WAN
3rd Party VPN

Paths VPN: All • Active
Direct Internet
ISP2
Circuit to Verizon2
Internet VPN
WAN • Circuit • Site • Device

No live metrics were shown after application selection.


Showing Activity from Mar 01, 2021 8:04 AM to Mar 02, 2021 8:04 AM viewed by Apps

Prisma SD-WAN media parameters did not appear after 24 hours of wait time.

It is important to note that this testing only utilized Cisco WebEx media. Although this application was part of the Prisma SD-WAN Media application collection, no other media applications such as Zoom, AdobeConnect, or FaceTime were tested.

Test Case Summary

Cisco vManage had more efficient viewing parameters than Prisma SD-WAN. vManage provided parameters for all flows, in one screen – making it easier for users to observe and compare, rather than view individually. Prisma SD-WAN displays link quality parameters under specific requirements. However, Prisma SD-WAN requires users to individually navigate through each packet for application statistics.

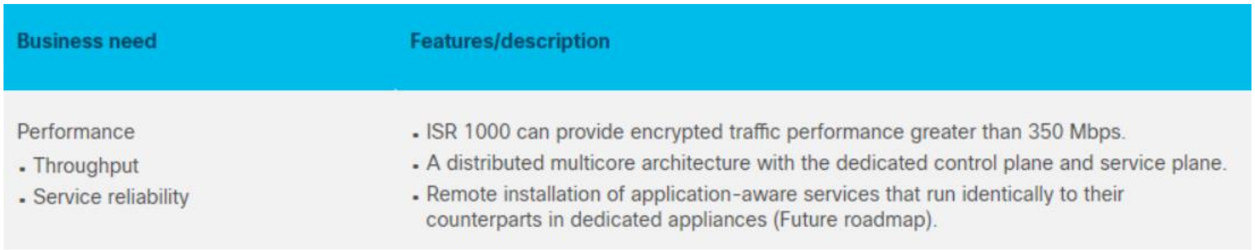
7.0 Performance and Feature SD-WAN Comparison

7.1 Performance

Features taken into consideration for performance evaluation include IPSec, Zone Based Firewall (ZBFW), Quality of Service (QoS), Network Address Translation (NAT). The tests were done on Cisco ISR 1000 Series routers and Prisma SD-WAN ION devices by enabling/disabling the above-mentioned features for each test case.

7.1.1 Cisco

A live demonstration for performance testing was provided using Spirent Test Center. The most updated device specifications for both Cisco and Palo Alto were provided for comparison.

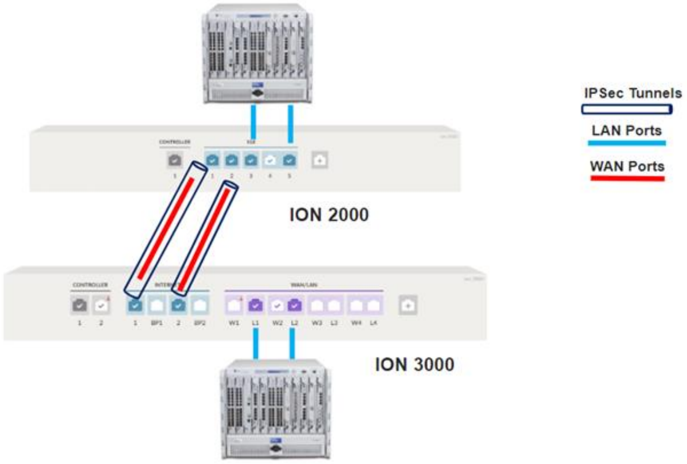


Business need	Features/description
Performance - Throughput - Service reliability	- ISR 1000 can provide encrypted traffic performance greater than 350 Mbps. - A distributed multicore architecture with the dedicated control plane and service plane. - Remote installation of application-aware services that run identically to their counterparts in dedicated appliances (Future roadmap).

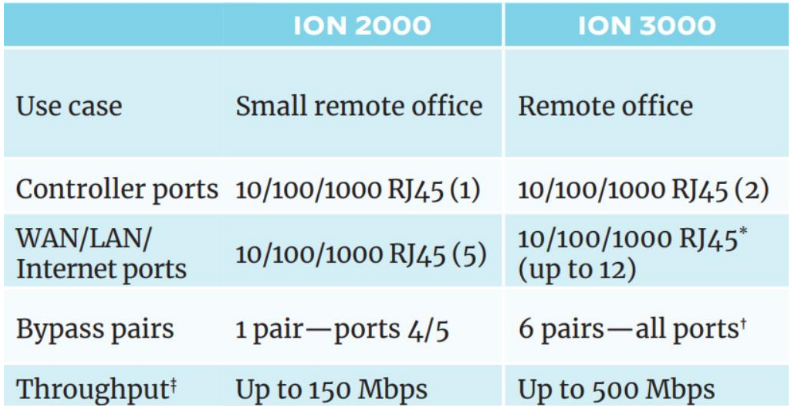
Cisco 1000 Series ISR hardware model specifications were taken from the 2019 Cisco 1000 Series Integrated Services Routers Data Sheet.

7.1.2 Palo Alto

A live demonstration for performance testing was provided using Spirent Test Center.



The topology above was used for performance testing of the Prisma SD-WAN solution.

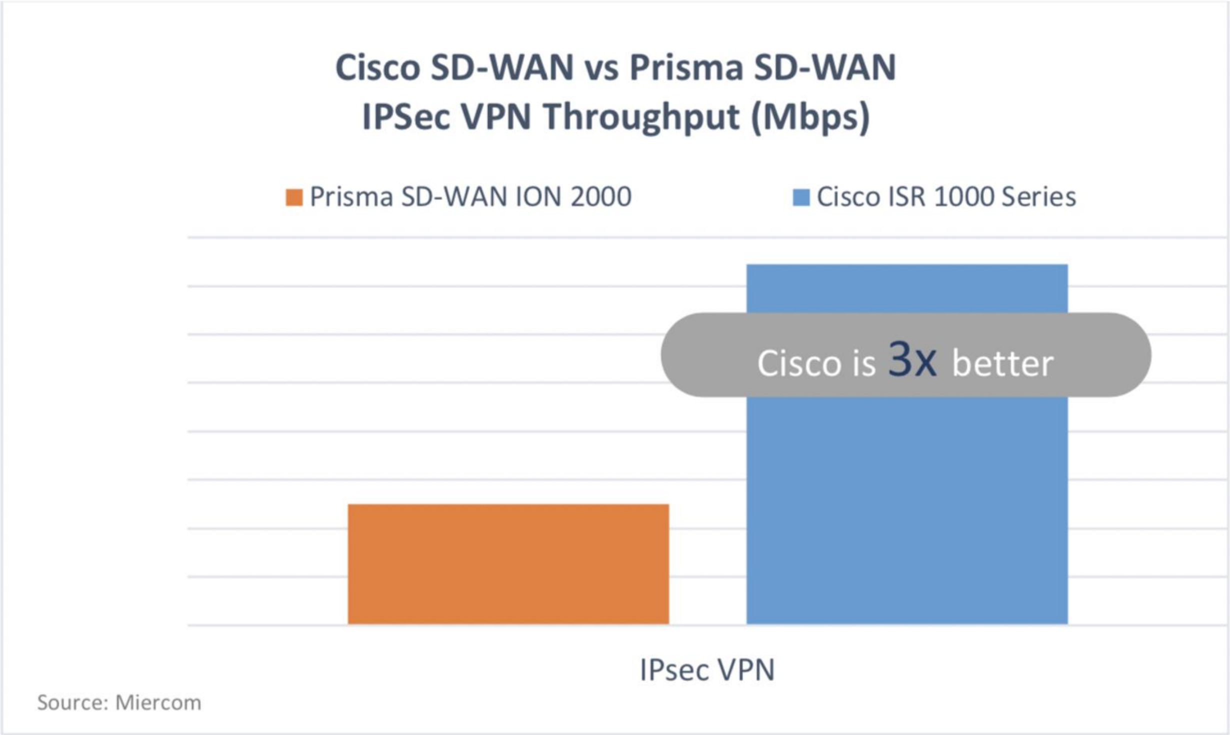


	ION 2000	ION 3000
Use case	Small remote office	Remote office
Controller ports	10/100/1000 RJ45 (1)	10/100/1000 RJ45 (2)
WAN/LAN/ Internet ports	10/100/1000 RJ45 (5)	10/100/1000 RJ45* (up to 12)
Bypass pairs	1 pair—ports 4/5	6 pairs—all ports†
Throughput‡	Up to 150 Mbps	Up to 500 Mbps

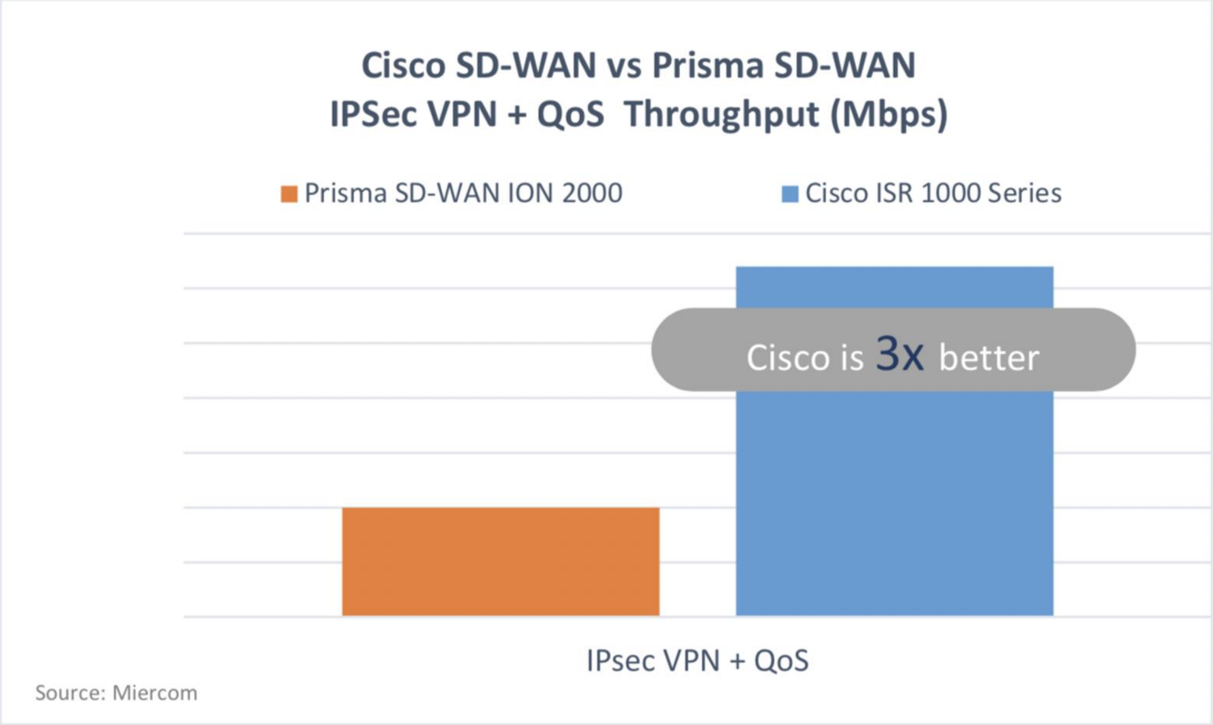
The Prisma SD-WAN ION 2000 and ION 3000 hardware model specifications were taken from the 2021 Prisma SD-WAN Instant-On Network (ION) Device Specifications.

Test Case Summary

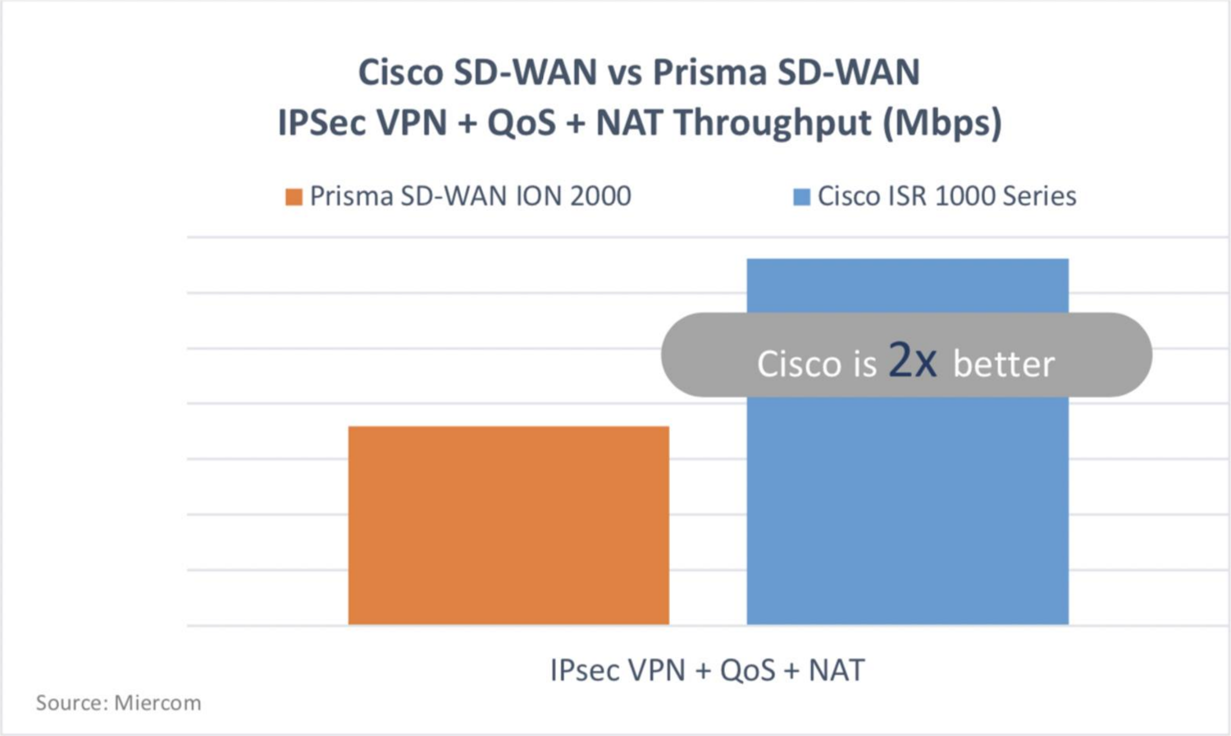
Cisco SD-WAN performed consistently better than Prisma SD-WAN- offering more than 50 percent higher average on-box throughput performance for key features.



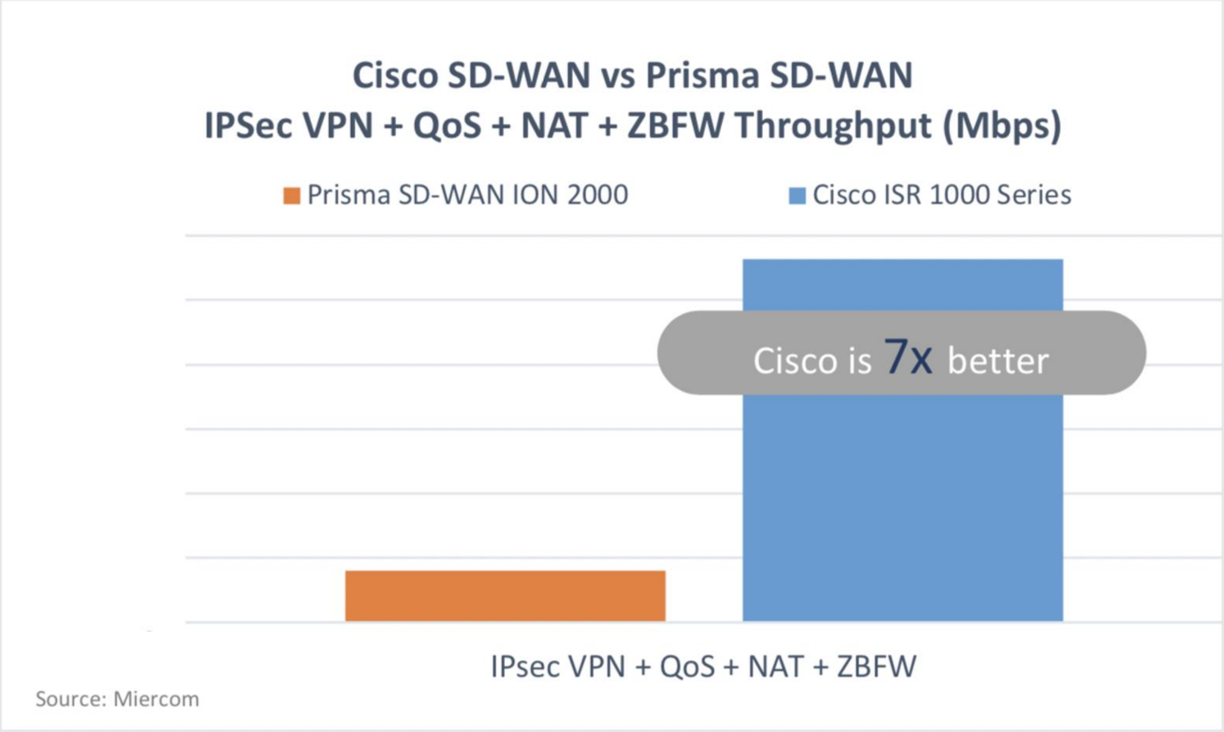
Throughput comparison of Cisco and Prisma, with IPSec VPN enabled, showed Cisco performed nearly three times better than Prisma SD-WAN.



Throughput comparison of Cisco and Prisma, with IPSec VPN and QOS features enabled, showed Cisco performed nearly three times better than Prisma SD-WAN.



Throughput comparison of Cisco and Prisma, with IPSec VPN, QOS and NAT features enabled, showed Cisco performed nearly two times better than Prisma SD-WAN.



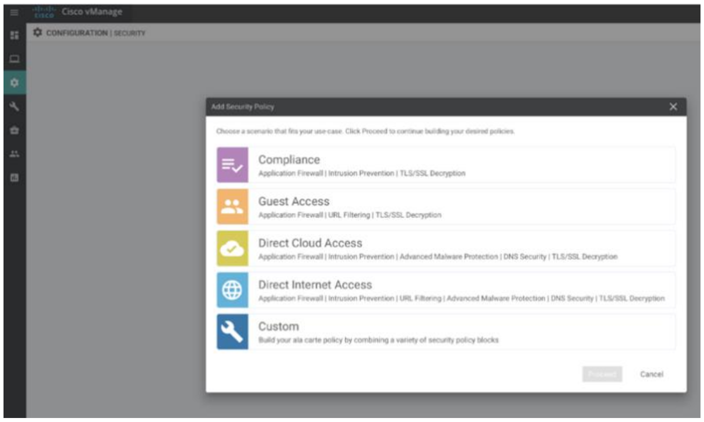
Source: Miercom

Throughput comparison of Cisco and Prisma, with IPSec VPN, QOS, NAT and ZBFW features enabled, showed Cisco performed nearly seven times better than Prisma SD-WAN.

7.2 On-Box Security

7.2.1 Cisco

Cisco offered advanced on-box SD-WAN security capabilities (e.g. ZBFW, Advanced Malware Protection – also known as AMP, URL Filtering, IPS etc.). Cisco SD-WAN also offered other on-box features like Full routing capabilities (e.g. BGP, OSPF), Multicast support, Application and SLA based policy, Full Mesh/ Partial Mesh, and more.



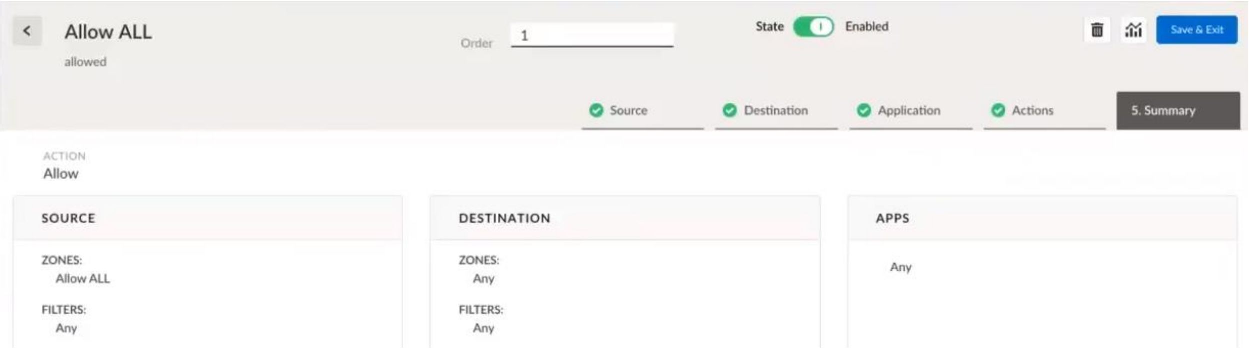
Choose a scenario that fits your use case. Click Proceed to continue building your desired policies.

- Compliance
  Application Firewall | Intrusion Prevention | TLS/SSL Decryption
- Guest Access
  Application Firewall | URL Filtering | TLS/SSL Decryption
- Direct Cloud Access
  Application Firewall | Intrusion Prevention | Advanced Malware Protection | DNS Security | TLS/SSL Decryption
- Direct Internet Access
  Application Firewall | Intrusion Prevention | URL Filtering | Advanced Malware Protection | DNS Security | TLS/SSL Decryption
- Custom
  Build your ala carte policy by combining a variety of security policy blocks

Cisco vManage depicted different security options provided for users. Apart from the ZBFW, multiple advance options were offered.

7.2.2 Palo Alto

Prisma SD-WAN offered a basic ZBFW with primitive allow/ deny rules defined for different security zones. Advanced capabilities were not offered.



Allow ALL
allowed

Order: 1

State: Enabled

ACTION: Allow

SOURCE	DESTINATION	APPS
ZONES: Allow ALL FILTERS: Any	ZONES: Any FILTERS: Any	Any

The Summary of On-Box security with Prisma SD-WAN depicted different customizable firewall features.

Test Case Summary

Cisco offers advanced on-box features to enhance SD-WAN performance and security while Prisma SD-WAN only provides a basic firewall capability.

7.3 Full Stack Features

7.3.1 Cisco

Cisco SD-WAN offered features, like a built-in Wi-Fi capability, with a management scale of up to 50 access points. Cisco's ISR routers had the built-in Mobility Express functionality where the ISR can act as a virtual wireless controller providing Wi-Fi capabilities to customers. Cisco ISR Routers also provided on-box LTE capabilities, with on-box SIM card slots, and offered Stealthwatch – giving visibility, threat identification and network compliance using machine-learning detection. Also, Cisco SD-WAN supports native unified communications integration which includes support for FXO/FXS, T1/E1 Voice PRI, DSPFarm Services for SD-WAN voice, Fax/Modem Support etc.

7.3.2 Palo Alto

Palo Alto did not offer a wireless solution. Prisma SD-WAN relies on third-party vendors to provide wireless and LTE capabilities to customers – adding more cost, complexity, and touchpoints. Also, Prisma SD-WAN fails to offer native unified communications integration unlike Cisco and has dependency on third party services.

Test Case Summary

Cisco offered full stack capabilities, including wireless. Prisma SD-WAN lacked this feature. Customers have a broader range of choice and management with Cisco's additional wireless feature.

7.4 Cost

7.4.1 Cisco

The Cisco SD-WAN with SASE solution offers a simplified licensing structure where the customer does not need to worry about numerous add-on licenses and support contracts to activate features. Its tiered model was easy to activate, consume and renew – reducing cost and complexity for customers.

Cisco offers both consumption-based and subscription-based licensing options.

From a Return On Investment (ROI) perspective, Cisco focuses on existing customer investments to guarantee investment protection. For example, the existing Cisco ISR 1000 and ISR 4000 Series routers can be converted/migrated from IOS-XE to SD-WAN IOS-XE, with zero capital outlay – taking advantage of the simplified licensing model. Other examples are the free and available SD-WAN Conversion Tool (convert2sdwan.cisco.com) and SASTRE (CX tool available for purchase) that make migration easier for partners and customers. Cisco continues to develop and improve tools for simpler migration.

Cisco is the only SD-WAN provider to offer voice services. Existing ISR 1000 and ISR 4000 Series customers can use their existing routers/edge platforms that are being used for voice and migrate to SD-WAN to use those same platforms for voice services. The Cisco "brownfield" migration program incentivizes customers to migrate to SD-WAN.

Customers can benefit from Cisco's extensive partner network for expert assistance with migration in any area they may need. This includes training, architecture, deployment, support, and managed services to meet business needs.

7.4.2 Palo Alto

Prisma SD-WAN has an a-la-carte approach to enabling add-on features which quickly increases cost and complexity. Prisma SD-WAN does not support both consumption-based and subscription-based licensing options.

Test Case Summary

Cisco offers a more cost-effective solution than Prisma SD-WAN, which is 51 percent more expensive. Its simplified licensing options yield lower TCO, greater ROI and consistently developed tools for easier migration to SD-WAN with existing Cisco products. Prisma SD-WAN has a more costly a-la-carte model for adding features.

About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable™, Certified Reliable™, Certified Secure™ and Certified Green™. Products may also be evaluated under the Performance Verified™ program, the industry's most thorough and trusted assessment for product usability and performance.

Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report, but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in part or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

By downloading, circulating or using this report this report in any way you agree to Miercom's Terms of Use. For full disclosure of Miercom's terms, visit: https://miercom.com/tou.