Palo Alto Networks and Citrix SD-WAN

Multi-Layer Security for Branch and Cloud
Introduction

As the pace of adoption towards digital transformation accelerates, enterprises are realizing that the old architectural paradigm based on MPLS, data center backhaul, and traditional perimeter security, designed before the cloud, is no longer adequate.

Forrester Research reported that in 2018, 56% of companies were in the middle of a digital transformation (The Sorry State of Digital Transformation In 2018, April 2018), but the success rate tends to be small. Consulting firm McKinsey & Company reported that 70% of transformations fall short of achieving their goals (Changing Change Management, McKinsey Digital July 2015).

Network and security operations teams are in a pivotal position to help their enterprises succeed in this new era of digital transformation. This requires a sweeping architectural change across several technology vectors: the WAN or branch edge, the cloud, and security.

- Once siloed functions in the branch – routing, path control, WAN Optimization, security – they are all converging into a new WAN Edge.
- Applications and workloads are migrating out of data centers to multiple public clouds which essentially means that the enterprise network must be extended.
- Security also now needs to extend across the cloud and protect this larger enterprise environment that includes distributed branch offices, data centers, and multiple public clouds.

SD-WAN represents a big-leap forward in enterprise networking. This new technology is designed to deliver a better branch user experience regardless where the applications reside. SD-WAN also treats both private and public
networks as a single unified WAN for higher efficiency and lower cost, so enterprises have the freedom to establish a branch presence anywhere and anytime with the last mile of their choosing.

However, being part of a vast public network and public clouds also directly exposes branch users and applications to ever-increasing cyber threats. A security breach can proliferate quickly, thus infecting users, crippling services, and worst of all, damaging company brand value. This fact is so well-known that according to a recent Gartner report (Address Security and Digital Concerns to Maintain Rapid SD-WAN Growth, November, 2018), 72% of the respondents said that security is their top concern when it comes to WAN and cloud services.

**The Synergy of Palo Alto Networks and Citrix**

The partnership between Palo Alto Networks and Citrix is aimed to address those concerns. The combination of the Palo Alto Networks Next-Gen Firewall on Citrix SD-WAN offers a best-of-breed networking and security solution that provides flexible choices for distributed enterprises.

As a next-generation WAN edge solution, Citrix SD-WAN provides an unparalleled experience for mission- and business-critical applications delivered from any location with comprehensive security that protects users, applications, and data across the branch, network, and cloud.

Citrix SD-WAN leads the industry with the native capability to identify 4,500 applications using deep packet inspection technology for real-time discovery and classification of applications. It uses this application knowledge to intelligently steer traffic from the branch to the Internet, private data center, or public clouds. This is particularly beneficial to customers using Citrix Virtual Apps & Desktops as Citrix SD-WAN can granularly parse and optimize HDX traffic.

Take the most widely adopted cloud-based enterprise productivity suite, such as Microsoft Office 365, as an example. By supporting Office 365’s Network Connectivity Principles, Citrix SD-WAN can accelerate latency-sensitive Skype or Teams applications. This is accomplished through an automated exchange of the published Office 365’s endpoint URLs and IP addresses, that in essence provides direct connection of branches to the local Office 365 front door.

Citrix SD-WAN then adds a security protection layer from Palo Alto Networks, with flexible deployment models:

1. As an on-premises service with the virtualized VM-50/100 next-gen firewall (VNF) hosted in the new Citrix SD-WAN 1100.
2. As-a-service whereby a Citrix SD-WAN appliance provides an automated and secure connection to the nearest Palo Alto Networks Prisma Access (aka GlobalProtect cloud service) point-of-presence (PoP).

Citrix has also invested significant effort in tightly integrating these solutions onto its management platform, and optimizing them for fast branch onboarding, seamless deployment and easy service delivery. Citrix achieves these goals by building Palo Alto Networks VM-50/100 and Prisma Access service provisioning right into its SD-WAN Orchestrator, as shown in the figure below.

With Citrix SD-WAN Orchestrator, customers can easily onboard WAN edge capabilities using Zero-Touch-Deployment (ZTD) and automate multi-cloud connectivity while spinning up the Palo Alto Networks firewall instances.
The control will then be handed off to Palo Alto Networks Panorama, which will control the customer’s security policies, and provide policy consistency for both physical or virtualized or cloud-based next-generation firewalls.

**Palo Alto Networks VM-50/100 on Citrix SD-WAN 1100 for On-Premises Security**

Before we look at the Palo Alto Networks VM-50/100 running as a virtualized network function (VNF), we must first look at the new Citrix SD-WAN 1100 as the host platform.

The new Citrix SD-WAN 1100 is a purpose-built, high-performance appliance in a compact 1RU form factor. Under the hood, it’s an SDN/NFV-ready platform powered by eight-core CPUs and designed to host various virtualized network functions (VNFs) from select partners.

The first hosted virtualized network function is the Palo Alto Networks VM-50 and VM-100 NG-FWs. Both are full-featured next-generation firewalls (NG-FWs) known for their advanced security capabilities.

The combination of Citrix SD-WAN 1100 and Palo Alto Networks VM-Series NG-FWs represents an advanced WAN edge and security solution in a single appliance.
Deploy Palo Alto Networks VM-Series from Citrix SD-WAN Orchestrator

Citrix SD-WAN customers can activate a pre-defined workflow designed to automate the spin-up of the Palo Alto Networks VM-Series (Virtual Machine, or VM) directly from within Citrix SD-WAN Orchestrator. Behind the scenes, the SD-WAN Orchestrator uploads the VM image from a Palo Alto Networks server and deploys the VM to all SD-WAN 1100 platforms as a VNF service. As a final step, every Palo Alto Networks VM will in turn contact Palo Alto Networks Panorama for service entitlement and license validation.

Citrix SD-WAN Orchestrator also allows the integrated firewall traffic to be redirected directly to the Palo Alto Networks VM. There are several benefits in doing so:

1. The Palo Alto Networks VM will inspect all LAN-to-LAN traffic before forwarding. When an infected user or device or application is detected, the infected host will be quarantined first until the threat source is neutralized.

2. Direct internet-bound traffic is scrubbed clean by the Palo Alto Network's VM. Because the Palo Alto Networks VM is locally hosted in the WAN edge, users will benefit from minimal latency, higher security efficacy, and enhanced quality of experience overall.

3. Data-center-bound traffic can be steered for local inspection or handled by the central full-stack firewall.

Palo Alto Networks Prisma Access

By using Palo Alto Networks Prisma Access to complement Citrix SD-WAN, branch customers can benefit from a cloud-based, cost-effective Secure Web Gateway service (SWG) for centralizing and simplifying policy management. A SWG service is typically the most basic set of security services and can be expanded to the full-suite of next-gen firewall services, such as protection against data exfiltration and high-scale SSL offload. Premium zero-day subscription services, such as the Advanced Threat Protection (ATP) and Global Threat Intelligence Services, are also available.

Simple Connectivity Setup to Palo Alto Networks Prisma Access from Citrix SD-WAN Orchestrator

Through the SD-WAN Orchestrator, Citrix relies on a set of APIs to automate the setup of IPsec tunnels from customer branches and redirect their Internet traffic to nearest Prisma Access points of presence (PoPs). This allows Prisma Access to
inspect application content in real-time for data theft and malware protection. It can also enable intrusion detection to look for malicious activity in the network and provide URL filtering to identify and control access to web traffic.

Additionally, security policies can be applied towards branch-to-internet and branch-to-branch traffic with the SD-WAN for both active-active or active-passive IPsec connections.

As a cloud service, Palo Alto Networks Prisma Access provides cloud-based firewall capabilities to reduce the overhead of having to manage full-stack firewalls distributed at each branch. As a result, enterprises can lower in-house resource overhead and increase operational agility.

**Key Benefits Summary**

- These joint solutions replace the need to install multiple costly full-stack firewalls at each branch with a more cost-effective and straightforward model.
- Citrix SD-WAN ensures that branch users have reliable and secure connectivity, with exceptional application experience delivered from data centers and public clouds to boost productivity.
- Citrix SD-WAN provides a more efficient WAN edge to connect users to the cloud over the internet at a cost that is much less compared to the legacy WAN router.

![Figure 4: Automated connectivity to Palo Alto Networks Prisma Access Cloud Security](image)

- Citrix SD-WAN Orchestrator serves as the starting point to automate the setup of a secure IPsec tunnel to Palo Alto Networks Prisma Access points of presence (PoPs).
- Citrix SD-WAN Orchestrator simplifies the provisioning of the Palo Alto Networks VM-50/100 when running as a VNF in the SD-WAN 1100 through easy deployment steps and traffic redirect policies.
- Using deep packet inspection, Palo Alto Networks VM-50/100 and Prisma Access identifies all applications, across all ports, irrespective of protocol, SSL encryption, or evasive tactic. The application identification is the basis for applying all security policies.
• Palo Alto Networks VM-50/100 and Prisma Access inspect content in real-time. Intrusion prevention technology provides identification of attacks and malware embedded in application traffic in the network (at low-latency, high throughput speeds) and then determines what action needs to be taken for the protection of the network.

• Palo Alto Networks Prisma Access service leverages a cloud-based infrastructure, allowing customers to avoid the challenges of sizing firewalls and compute resource allocation. This can minimize coverage gaps or inconsistencies associated with distributed organizations.

• Palo Alto Networks Panorama can be used with Palo Alto Networks Cortex logging services for analysis and report generation or incident forensics.

Learn more at https://www.citrix.com/networking/sd-wan-security.html