

PALO ALTO NETWORKS AND VIPTELA

Securing the Hybrid WAN for the Enterprise and Service Provider

Highlights

- Reduce WAN costs typically by 50% with software-defined WAN
- Threat protection for the branch, cloud and data center with Palo Alto Networks Next-Generation Security Platform
- Security with high performance in virtual or physical form factors
- Best path selection for security inspection points

Enterprise connectivity has changed, and organizations are increasingly replacing traditional routing (MPLS) with software-defined wide area networks (SD-WANs). SD-WAN technology allows global companies to build scalable, carrier-agnostic and policy-controlled infrastructure to meet the needs of modern applications like cloud, video, IoT and social. With the integrated solution from Viptela and Palo Alto Networks, customers can seamlessly migrate to hybrid WANs and achieve comprehensive protection against sophisticated attacks.

Viptela Secure Extensible Network

The Viptela Secure Extensible Network (SEN) solution enables enterprises to migrate from MPLS to a hybrid overlay WAN infrastructure. Enterprises get full integration of routing, security, centralized policy and orchestration. The end result is a network that is operationally easy to manage and eliminates disconnects between business and IT teams. With Viptela SEN, enterprises typically drop their WAN costs by 50%, reduce network downtime, and achieve optimized cloud performance.

Palo Alto Networks Next-Generation Security Platform

Palo Alto Networks Next-Generation Security Platform, comprised of the Next-Generation Firewall (NGFW), Threat Intelligence Cloud and Advanced Endpoint Protection, uses an innovative traffic-classification engine that provides full context by identifying all traffic by application, use and content. By combining network, cloud and endpoint security with advanced threat intelligence in a natively integrated security platform, Palo Alto Networks safely enables all applications and delivers highly automated, preventive protection against cyberthreats at all stages in the attack lifecycle without compromising performance.

Palo Alto Networks and Viptela Secure Extensible Network

Palo Alto Networks and Viptela seamlessly integrate to deliver a joint solution of enterprise-grade security with an SD-WAN infrastructure. Protection is achieved in real time with increased visibility to effectively combat today's advanced threats. Viptela SEN provides the key infrastructure elements to enable an overlay WAN infrastructure, and customers can benefit from the Palo Alto Networks platform to prevent threats. Viptela inserts traffic into the Palo Alto Networks platform with centralized policy configuration, enabling the seamless insertion of security into the WAN.

USE CASE #1

SD-WAN and Distributed Enterprise Security

Challenge: Enterprises are increasingly leveraging direct internet breakouts at remote locations to provide optimal and scalable connectivity for the purposes of guest Wi-Fi or SaaS applications, such as Office 365®, Salesforce® and Google®. This approach provides the best overall user experience, but it also creates challenges when securing an increased number of internet access points and maintaining compliance with the organization's security teams.

Solution: Viptela SD-WAN and the Palo Alto Networks NGFW can be deployed at enterprise remote locations, provisioned with direct internet access to ensure compliance and symmetry with security policies, regardless of internet access point.

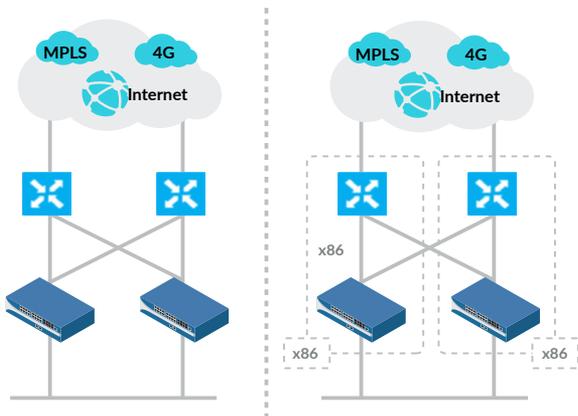


Figure 1: Distributed enterprise security

USE CASE #2

SD-WAN and Regional Secure Perimeter

Challenge: Traditional centralized deployments at the data center lack agility and waste WAN bandwidth. Organizations must have the flexibility to select local, regional or data center inspection points to enforce security policies.

Solution: Viptela SD-WAN policy allows insertion of Palo Alto Networks NGFW into the user traffic data path by steering the traffic of interest to the regional inspection and policy enforcement points. Regional deployment of the Palo Alto Networks NGFW with the Viptela SD-WAN fabric, as an alternative to traditional centralized deployments at the data center, provides the ability to rapidly mitigate security incidents without the unnecessary waste of WAN bandwidth that results from centralized traffic backhaul.

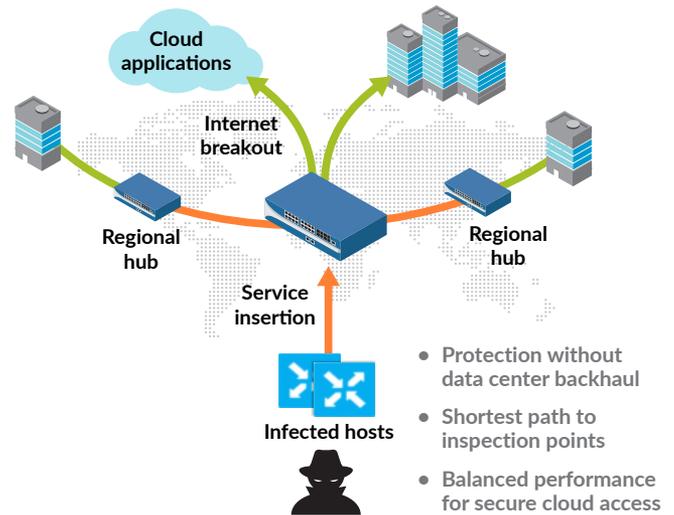


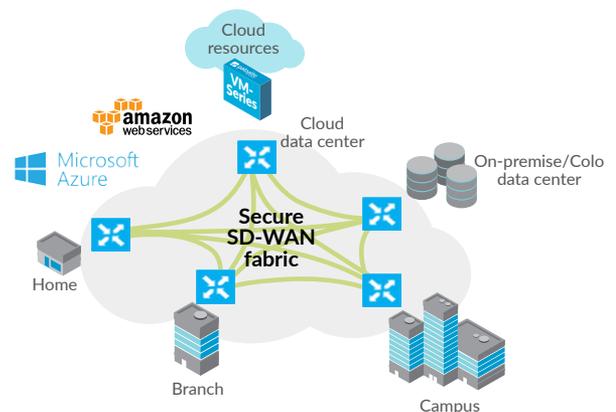
Figure 2: Regional secure perimeter

USE CASE #3

SD-WAN and Hybrid Cloud Security

Challenge: Many enterprises are looking to shift their compute resources from on-premise data centers to the public cloud to achieve higher levels of reliability and to accommodate increased demand for compute power. Securing access to cloud computing resources and creating security zones for resource segregation creates significant challenges hindering adoption.

Solution: The Viptela SD-WAN solution offers a scalable and secure fabric that can be seamlessly extended to infrastructure-as-a-service (IaaS) cloud platforms, such as Amazon® Web Services and Microsoft® Azure®, by leveraging Viptela vEdge Cloud software routers. Palo Alto Networks VM-Series virtualized NGFW, positioned on the service side of Viptela vEdge Cloud software routers, provides perimeter security and zoning for cloud workloads.



Extend WAN to IaaS	Segment workload resources	High availability for cloud connectivity
<ul style="list-style-type: none"> • AWS • Azure 	<ul style="list-style-type: none"> • On-Prem DC • Colo DC • IaaS DC 	<ul style="list-style-type: none"> • Active/Active • Active/Passive

Figure 3: Securing the hybrid cloud data center

About Viptela

Viptela provides Software-Defined Wide Area Network (SD-WAN) technology that allows global companies to build carrier agnostic, policy-controlled and cost-effective WANs. Viptela has been deployed at thousands of sites, mostly by Fortune-500 enterprises; and major carriers including Verizon and Singtel are using Viptela to deliver managed SD-WAN services. Viptela cuts existing operating costs in the WAN by more than 50%, increases bandwidth 10x, and, significantly improves security and uptime. The company was named a Gartner Cool Vendor and a Next Billion Dollar Startup by Forbes in 2015. Viptela is backed by Sequoia Capital and headquartered in San Jose, CA. Follow us on Twitter @viptela or LinkedIn.

Find out more at www.viptela.com.

About Palo Alto Networks

Palo Alto Networks is the next-generation security company, leading a new era in cybersecurity by safely enabling applications and preventing cyber breaches for tens of thousands of organizations worldwide. Built with an innovative approach and highly differentiated cyberthreat prevention capabilities, our game-changing security platform delivers security far superior to legacy or point products, safely enables daily business operations, and protects an organization's most valuable assets.

Find out more at www.paloaltonetworks.com.



4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000

Sales: +1.866.320.4788

Support: +1.866.898.9087

www.paloaltonetworks.com

© 2016 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <http://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies. viptela-tpsb-120516