velocloud | paloalto NETWORKS®

PALO ALTO NETWORKS AND VELOCLOUD

Technology Segment: Secure Cloud-Delivered SD-WAN

Benefits

- Eliminate expensive backhaul and deliver application assurance and security for enterprise and cloud applications over internet and hybrid-WAN.

- Enable VNF deployments in the cloud or on-premises with simple service insertion, thus dramatically simplifying deployments and reducing costs.

Customers are challenged to adopt distributed firewalls due to deployment complexity and the difficulty of forwarding traffic to these firewalls. Today, cloud traffic is backhauled across the private wide area network (WAN) to centralized firewalls to simplify configurations. This results in backhaul penalties. Additionally, traditional WAN solutions rely on expensive private circuits for application performance. Backhaul of cloud traffic, guest Wi-Fi, and more bandwidth-intensive applications, such as video and virtual desktop integration (VDI), cause further pressure on private WAN bandwidth.

With SD-WAN the trend is to include inexpensive internet as a transport mechanism to support bandwidth-intensive applications. Public internet links are "best efforts" and susceptible to attacks. A secure, cloud-delivered SD-WAN solution delivers ubiquitous security and enterprise-grade application performance for cloud or on-premises applications.

VeloCloud Networks

VeloCloud Cloud-Delivered SD-WAN™ is an overlay solution between VeloCloud Edges in distributed sites and data centers, as well as cloud-hosted VeloCloud Gateways. The overlay is independent of physical transport and providers, enabling unified control and visibility, business-level abstraction and incremental migration.

This overlay provides key benefits:

- **Assured application performance:** VeloCloud Dynamic Multipath Optimization (DMPO) with application-aware, per-packet steering and on-demand remediation assures transport-independent performance for demanding, real-time applications.

- **Simplified WAN via business policy automation:** VeloCloud can be deployed as zero-touch appliances, virtual appliances, or hosted as multi-tenant services platforms. Business-level policies enable one-click, policy-based service chaining of traffic (e.g., inserting Palo Alto Networks® firewall) to enterprise service hubs on the branch edge or in the cloud.

- **Managed cloud on-ramp:** VeloCloud's system of cloud gateways uniquely provides a managed cloud onramp. Unlike "best effort" direct branch-to-cloud alternatives, VeloCloud's full SD-WAN capabilities are deployed at the doorstep of cloud applications and provide optimized and secure connectivity to SaaS/IaaS and network/cloud security services.

Result 1: Voice Improvements using VeloCloud Cloud-Delivered SD-WAN
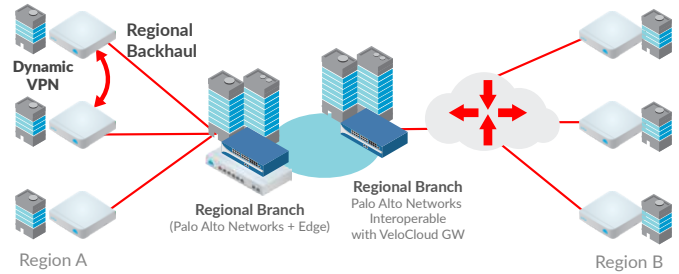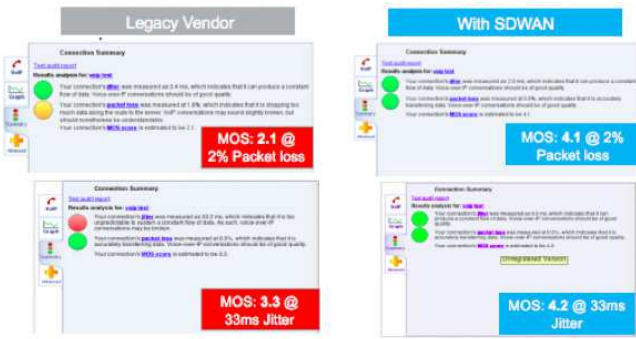
Result 2: Transactional Application Improvement Using VeloCloud Cloud-Delivered SD-WAN

Deliver 20 times better performance.

1% packet loss:

- Throughput without SD-WAN = 6 Mbps
- Throughput with SD-WAN (Single Link) = 25 Mbps (NACK in action)
- Throughput with SD-WAN (Dual Link) = 42 Mbps (NACK + Aggregation in action)

Palo Alto Networks + VeloCloud Networks

VeloCloud and Palo Alto Networks jointly assure the performance and security of enterprise and cloud applications over the internet and hybrid-WAN while dramatically simplifying deployments and reducing costs.

Use Case #1: Secure SD-WAN With Distributed Regionalized Firewall Services

Challenge: To service chain – that is to say, forward traffic to multiple, distributed firewalls across the WAN at enterprise regional data centers – is a complex and time-consuming process with hundreds of lines of policy-based routing (PBR) rules on WAN routers.
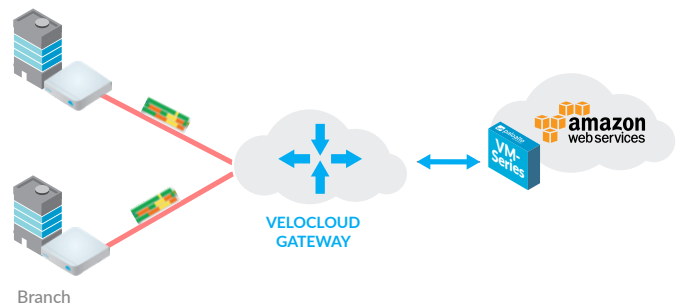
Solution:

- VeloCloud business policy framework enables one-click services insertion, eliminating complex configurations. These business policies can be based on applications and business objectives.
- Can easily forward traffic from many branches to the selected regional data center with a VeloCloud Edge and Palo Alto Networks firewall installed.
- Forwarding traffic to a regional data center for Palo Alto Networks security service insertion can also be accomplished without the need to install SD-WAN hardware in the data center. The Palo Alto Networks firewall can simply connect via VPN to a cloud-hosted VeloCloud Gateway to provide connectivity to multiple branches – ideal for quick onboarding in mergers and acquisitions situations.

- Example:
  - **All internet traffic:** Insert Palo Alto Networks firewall in the regional branch.
  - **All corporate traffic:** Dynamic VPN with the push of a button to enable optimized voice/video directly between branches.

Use Case #2: Secure SD-WAN for Optimized Access to IaaS Services

Challenge: Organizations are moving data center workloads to IaaS (e.g., Amazon Web Services). To access "N" VPC instances from "N" branches, customers would often need to manually configure "NxN" secure overlay tunnel, which is operationally complex. Further, customers would like to enable private WAN, like security and performance, as they redirect traffic to IaaS services.

Solution:

- Branches automatically build a secure and optimized overlay with VeloCloud Gateway using VeloCloud Dynamic Multipath Optimization.
- VeloCloud Gateway service chains AWS VPC instance, via either a private connection or IPsec tunnel to AWS VPC. Thus, only "N" tunnels are needed instead of the previously needed "NxN" tunnels. Insertion of the Gateway also guarantees high-performance access to IaaS resources.
- Once the secure overlay with Dynamic Multipath Optimization is established, Palo Alto Networks VM-Series for AWS can be deployed on-demand for inserting firewall services, thus providing the same level of security and performance as workloads in the customer data center.

Use Case #3: Virtual CPE and SD-WAN

Challenge: Deploying a distributed firewall with the click of a button with SD-WAN CPE to avoid the truck rolls, costs and inflexibility associated with a stack of appliances.

Solution:

- Many customers prefer local internet breakout from the remote branch offices and prefer to keep security functions highly distributed.

- Service providers and large enterprise customers can easily deploy VM-Series virtualized firewalls on the VeloCloud Edge and program and manage them from remote locations. They can be inserted on the VeloCloud Branch Edge with the click of a button, thus delivering a cost-effective and secure SD-WAN solution.

Edge + VM-Series

Use Case #4: Secure SD-WAN for Service Providers

Challenge: Service providers are looking to expand beyond connectivity services and want to drive demand for revenue-generating services, like cloud-delivered SD-WAN and security services from their cloud. End customers, on the other hand, are looking for a single point of contact to deploy these services.

Solution:

- Service providers are taking advantage of SDN and NFV to build software-based network services in their data centers, points of presence, and central offices.

- Palo Alto Networks VM-Series firewalls and VeloCloud multi-tenant gateways are deployable as VNFs within service provider NFV/SDN environments, which can be instantiated and easily delivered to customers as security and "last mile" optimization services from the cloud.

- Last mile optimization is delivered between VeloCloud Edge (physical/virtual) and gateways hosted in service provider environments. SP NFV solution then service chains the VM Series VNF for delivering Security as a Service (SecaaS).
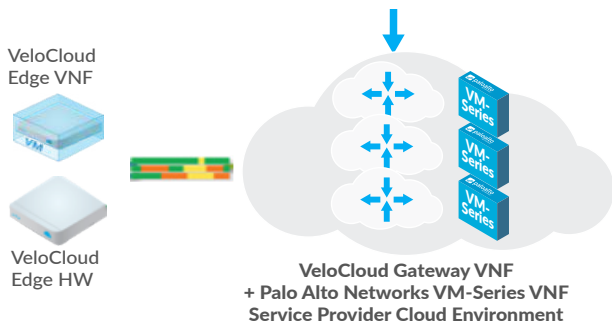
About VeloCloud Networks

VeloCloud Networks, Inc., the Cloud-Delivered SD-WAN™ company, Gartner Cool Vendor 2016 and a winner of Best Startup of Interop, simplifies branch WAN networking by automating deployment and improving performance over private, broadband Internet and LTE links for today's increasingly distributed enterprises. VeloCloud SD-WAN includes: a choice of public, private or hybrid cloud network for enterprise-grade connection to cloud and enterprise applications; branch office enterprise appliances and optional data center appliances; software-defined control and automation; and virtual services delivery. VeloCloud has received financing from investors including NEA, Venrock, March Capital Partners, Cisco Investments and The Fabric, and is headquartered in Mountain View, Calif. For more information, visit **www.velocloud. com** and follow the company on **Twitter@VeloCloud**.

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**

VeloCloud Edge VNF

VeloCloud Edge HW

VeloCloud Gateway VNF + Palo Alto Networks VM-Series VNF Service Provider Cloud Environment