

CHECK POINT + VELOCLOUD

SECURE CLOUD-DELIVERED SD-WAN

BENEFITS

- An integrated WAN and Security solution, which provides secure and optimized WAN connectivity over Internet links or hybrid WAN connections
- Eliminate expensive backhaul and deliver application assurance with security for enterprise and cloud applications
- Enable VNF deployments in the cloud or on-premise with simple service insertion, thus dramatically simplifying deployments and reducing costs

INSIGHTS

A common practice used by Enterprises today is to tunnel traffic over a private wide area network (WAN) that assures application performance, but is very expensive at the same time. Backhaul of cloud traffic, guest Wi-Fi, and more bandwidth-intensive applications, such as video and virtual desktop integration (VDI), further increases private WAN bandwidth consumption.

Software Defined Wide Area Network (SD-WAN) is a new and emerging technology that aims to utilize inexpensive high-speed internet as a transport mechanism to support bandwidth-intensive applications within reasonable costs. However, public internet links provide a “best effort” service and are more susceptible to cyber-attacks. A secure, cloud-delivered SD-WAN solution delivers ubiquitous security and enterprise-grade application performance for cloud and on-premises applications.

SOLUTION

VeloCloud and Check Point can jointly assure the performance and security of enterprise and cloud applications over the internet and hybrid-WAN while dramatically simplifying deployments and reducing costs.

VELOCLOUD NETWORKS

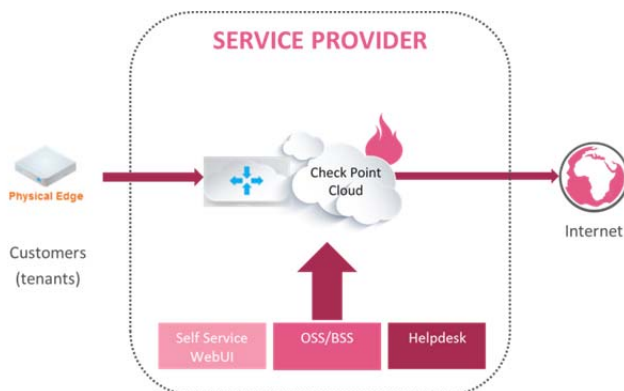
VeloCloud Cloud-Delivered SD-WAN™ is an overlay solution between VeloCloud Edges in distributed sites/data centers and cloud-hosted VeloCloud Gateways. The overlay is independent of physical transport and providers, enabling unified control/visibility, business-level abstraction and incremental migration.

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 Check Point 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.

Use Case #1: Secure SD-WAN for Service Providers (clean-pipe)

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

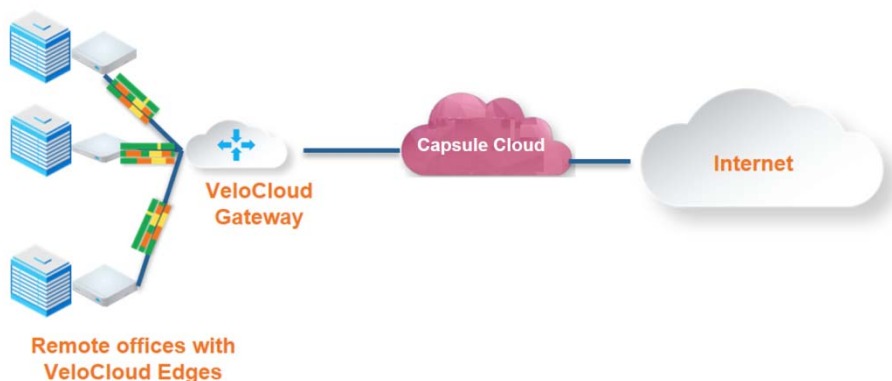


Solution:

- Check Point multi-tenant cloud security for service providers and VeloCloud multi-tenant gateways are deployable as VNFs within service provider environments, which can easily be delivered to customers as security and “last mile” optimization services from the cloud.
- VeloCloud provides last mile optimization between VeloCloud Edge (physical/virtual) and gateways hosted in service provider environments.
- Check Point multi-tenant cloud service provides Check Point’s award winning advanced threat prevention, web based self-care portal for subscribers and seamless integration to a service provider’s network, OSS/BSS systems and customer portal.

Use Case #2: SD-WAN enabled Security-as-a-Service for Businesses

Challenge: Organizations with geographically dispersed remote offices are faced with the challenge of securing their corporate network from attacks and monitoring/managing these offices in a simplified manner. They need to provide the same level of protection across all offices irrespective of whether they are inside or outside the confines of the corporate network perimeter.



Solution:

- Branches and Remote offices of an organization can benefit from the optimized connectivity offered by VeloCloud SD-WAN from the remote site all the way to the VeloCloud gateways.
- VeloCloud gateways connect remote offices to Check Point Capsule Cloud, where they are able to leverage Check Point’s advanced threat prevention as a cloud-based service, protecting the network and their users from known and unknown threats.
- Network administrators can easily monitor and manage these sites from a central VeloCloud Orchestrator. They can seamlessly distribute enterprise business and security policies to each of these sites.

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 Check Point vSEC (virtual firewall) on the VeloCloud Edge, and program and manage this from remote locations. vSEC can be inserted on the VeloCloud Branch Edge with the click of a button, thus delivering a cost-effective and secure SD-WAN.

Use Case #4: 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 to 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:

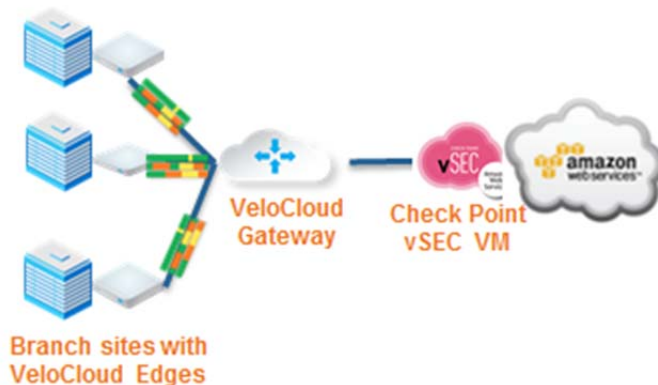
- VeloCloud business policy framework enables one-click service insertion, eliminating complex configurations. These business policies can be based on applications and business objectives.
- Can easily forward traffic from multiple branches to a selected regional data center with a VeloCloud Edge and Check Point firewall installed.
- Forwarding traffic to a regional data center for Check Point security service insertion can also be accomplished without SD-WAN hardware in the data center. The Check Point 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 Check Point 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 #5: Secure SD-WAN for Optimized Access to IaaS

Challenge: Organizations are moving data center workloads to IaaS (e.g., Amazon Web Services). To access “N” VPC instances from “N” branches, customers would need to manually configure “NxN” secure overlay tunnels, which is operationally complex. Furthermore, customers would like to enable private WAN with 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, Check Point vSEC on AWS can be deployed on-demand for advanced security services such as Firewall, IPS, Antivirus and Anti-Bot, thus safeguarding cloud applications and critical assets in the cloud.

SUMMARY

By dramatically simplifying deployments and reducing costs, Check Point and VeloCloud provide enterprise security and performance for cloud applications over the internet and hybrid-WAN. Our integrated SD-WAN and Advanced Threat Prevention platform provides secure and optimized WAN connectivity over Internet links and hybrid WAN connections.

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (<https://www.checkpoint.com>) is the largest network cyber security vendor globally, providing industry-leading solutions and protecting customers from cyber-attacks with an unmatched catch rate of malware and other types of threats. Check Point offers a complete security architecture defending enterprises – from networks to mobile devices – in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes.

ABOUT VELOCLOUD

VeloCloud Networks™, Inc. 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. For more information, visit www.velocloud.com and follow the company on Twitter @VeloCloud.