CHECK POINT + VMWARE SD-WAN
SECURE CLOUD-DELIVERED SD-WAN

As more applications move to the cloud, business users increasingly rely on them to do their jobs. From virtual meetings to file-sharing to collaboration through tools like Skype, Slack, and Office 365, including voice and video traffic, they require consistent, high-quality bandwidth, all the time. For IT organizations that are managing remote and branch offices, it can be a challenge to accommodate these needs in a way that's efficient, secure, and cost effective. For branch office users who are consuming more Wide-Area Network (WAN) bandwidth than ever, the user experience is often suboptimal. Traditional WAN architectures weren't designed to support cloud and SaaS applications. WAN traffic is carried through expensive leased lines that drive up costs or unreliable public Internet lines that frustrate end users.

CHECK POINT VMWARE SD-WAN SOLUTION

Now there's a better option. Software-Defined WAN (SD-WAN) enables enterprises to support application growth and simplify branch operations while streamlining access to cloud services and private data centers over both ordinary broadband Internet and private links, regardless of the transport mechanism. SD-WAN is critical for today's hybrid cloud environments because it brings enterprise-level manageability, performance, and reliability across branch offices.

Private links backhauled to the data center can be secured in a hub and spoke model, but the local Internet breakout to the cloud is susceptible to cyber-attacks. Check Point secures these links with the same advanced threat prevention available in our on-premises security gateways. Together VMware SD-WAN™ by VeloCloud® and Check Point jointly assure the performance and security of enterprise and cloud applications over the Internet and hybrid-WAN while dramatically simplifying deployments and reducing costs.

VMWARE SD-WAN NETWORKS

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

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

CHECK POINT INTEGRATED ADVANCED THREAT PREVENTION

Check Point provides organizations of all sizes with integrated, advanced threat prevention, reducing complexity and lowering the total cost of ownership. Check Point security products protects SaaS, IaaS and now branch office assets from sophisticated threats with dynamic scalability, intelligent provisioning and consistent control across physical and virtual networks.

WELCOME TO THE FUTURE OF CYBER SECURITY

Unlike other solutions that only detect threats, Check Point prevents threats from detonating their payload on their target host. Check Point SandBlast Zero-Day Protection is our cloud-based sandboxing technology where files are quickly quarantined and inspected, running in a virtual sandbox to discover malicious behavior before it enters your network. We detect malware at the exploit phase, even before hackers can apply evasion techniques attempting to bypass the sandbox. This innovative solution combines cloud-based CPU-level inspection and OS-level sandboxing to prevent infection from the most dangerous exploits, and zero-day and targeted attacks.

The Check Point solution also includes Application Control and URL Filtering to enforce safe web use. IPS, Anti-Bot and Antivirus protect you from known threats. HTTPS inspection safeguards you from threats trying to hide inside encrypted HTTPS channels.

Furthermore, Check Point is a fully consolidated and connected cyber security architecture protecting on premises, cloud and branch networks as well as endpoint and mobile devices from Advanced Persistent Threats. Threats identified on one device can be automatically propagated as an IoC (Indicator of Compromise) to protect your branch, mobile and cloud-based assets from the same zero-day threat.

Small Branch Offices	Small to Midsized Branch Offices
VMware SD-WAN Edge	VMware SD-WAN Edge Services Platform
Check Point NSaaS	Check Point Branch VNF

SD-WAN ENABLED NETWORK SECURITY-AS-A-SERVICE (NSaaS)

Organizations with thousands of small, 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. A cost-effective, easy to maintain and always up to date with the latest security is needed.

Small Branch Office Solution

Branches and remote offices of an organization can benefit from the optimized connectivity offered by VMware SD-WAN from the remote site all the way to the VMware SD-WAN Gateways. VMware SD-WAN Gateways connect remote offices to the Check Point Cloud Network Security Security-as-a-Service, 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 VMware SD-WAN Orchestrator.

Cloud NSaaS doesn't burden your IT staff with deploying or maintaining dedicated hardware and supports adding advanced threat prevention capabilities on top of existing SD-WAN Edge deployments. With a simple and easy setup process, network traffic from your SD-WAN Edge device is connected over a low latency GRE or IPsec tunnel to a primary cloud-based network security service at a location near you.

A second connection provides redundancy. With cloud-based security, hardware or software updates are completely transparent, providing maintenance-free security for hundreds and thousands of physical devices, reducing your overall CAPEX and OPEX costs.

Simplified central management provides an intuitive, simple on-boarding process, security policy configuration and monitoring. Powered by Check Point SmartEvent you see the most important threats with a single view across your entire infrastructure. Take control of security events with real-time forensic and event investigation, compliance and reporting. Respond to security incidents immediately, reducing the time you spend remediating incidents.

The Cloud Connection

VMware SD-WAN Gateways improve application performance by bringing your users closer to the cloud with cloud-hosted SD-WAN gateways. This also simplifies the Check Point NSaaS configuration where the packets flow from branch to SD-WAN Gateway to Check Point NSaaS. In the Check Point NSaaS portal you create just two SD-WAN Gateway site objects instead of creating one site per branch. The close proximity of the cloud VMware SD-WAN Gateways and NSaaS guarantees high bandwidth.

CHECK POINT BRANCH VNF ON VMWARE SD-WAN SERVICES PLATFORM

Deploying a distributed firewall with the click of a button with SD-WAN CPE (Customer Premise Equipment) to avoid the truck rolls, costs and inflexibility associated with a stack of appliances.

Small to Midsized Branch Office Solution

Many customers prefer to have control of their data or must comply with regulations such as GDPR. Check Point Branch Virtual Network Firewall (VNF) on the VMware SD-WAN Edge provides you with granular control of your security and data. Service Providers and large enterprise customers can easily deploy Check Point Branch VNF and manage security from corporate headquarters. Check Point Branch VNF can be inserted on VMware SD-WAN Edge with the click of a button, thus delivering a cost-effective and secure SD-WAN.

SUMMARY

By dramatically simplifying deployments and reducing costs, Check Point and VMware SD-WAN 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. (www.checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

ABOUT VMWARE SD-WAN BY VELOCLOUD

VeloCloud, now part of VMware has been named a Leader in the 2018 Gartner Magic Quadrant for WAN Edge Infrastructure and placed furthest on Completeness of Vision. VMware SD-WAN™ by VeloCloud® simplifies branch WAN networking by automating deployment and improving performance over private, broadband Internet and LTE links for today's increasingly distributed enterprises. VMware 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.