SD-WAN: Fortifying Security across the WAN

How Unity EdgeConnect Provides Unmatched Protection for the Modern WAN

EXECUTIVE SUMMARY

Software-defined wide area networks (SD-WAN) are a better fit than traditional router-centric WANs for today's geographically distributed enterprises – especially those pursuing a cloud-first strategy for application delivery. By enabling organizations to augment or replace legacy, private line networks with broadband internet services, leading solutions – like Silver Peak Unity EdgeConnect – not only improve application performance and increase network/business agility, but also shrink related capital and operational expenditures. Achieving these gains, however, depends on having a solution that also addresses security. At a *minimum*, this means incorporating sufficient capabilities to ensure the confidentiality and integrity of essential application traffic. But, is a minimum level of security all your organization really wants, or needs?

This paper discusses why today's enterprises are embracing SD-WAN at an accelerating pace, along with the need for an effective solution to account for security. It then goes on to reveal the extensive set of security capabilities incorporated in the EdgeConnect SD-WAN solution from Silver Peak. As you'll soon come to appreciate, the net result is an SD-WAN solution that – by accounting both for key use cases (e.g., internet breakout to improve SaaS application and IaaS performance) and

A key benefit delivered by an SD-WAN is the ability to actively utilize low-cost broadband services. However, because broadband services are "public" instead of "private," advanced security capabilities are required to ensure the confidentiality and integrity of application traffic traversing such connections.

the key principles of a software-defined computing environment (e.g., being application-driven and enabling automation) – delivers a level of security that meets or exceeds the actual security and compliance needs of the modern enterprise.

Why SD-WAN Matters

The primary job of the WAN is connecting distributed users to the applications they need to do their jobs. But, applications have changed significantly over the past handful of years. For instance, they are no longer predominately hosted in a regional/centralized, corporate data center. In fact, the percentage of those that are is steadily dwindling as modern organizations continue to embrace the cloud in general, and SaaS applications in particular.

> "Enterprise IT executives expect 60% of workloads will run in the cloud by 2018"
>
> – 451 Research[1]

Many other modern applications feature real-time, peer-to-peer communication, which is driving the need for higher performance and increasingly meshed connectivity. Then there's the Internet of Things (IoT) and big data apps, which are representative on the whole of both the increasing diversity of applications and growing volume of data today's WAN must be able to handle … ideally in a differentiated manner that ensures each is treated according to its individual characteristics/needs (e.g., relative to QoS, security, etc.).

The impact of these changes to the application landscape is that the enterprise WAN needs to change too. Traditional, private line connectivity options (such as multi-protocol label switching, or MPLS) and routing practices – backhauling, in particular – are clearly a poor match for cloud-apps, burgeoning amounts of internet traffic, and peer-to-peer interactions. Key shortcomings include the high cost of such network services and architectures, the negative impact they have on performance (especially for internet or cloud-destined traffic), and the fact that they are too rigid. Making all but the most basic configuration changes is typically a slow, complex exercise that is nothing short of stifling from an IT responsiveness and business agility perspective.

In comparison, SD-WAN enables enterprises to leverage multiple types of network connectivity – including broadband internet services – when connecting users to applications. But using broadband services for enterprise WAN connectivity introduces new security challenges that must be addressed. A best-of-breed SD-WAN solution will promote an application-driven approach to the utilization and management of the resulting WAN including configuration and enforcement of security policies. The outcome, in concise terms, is substantially:

- Improved application performance and availability
- Reduced WAN total cost of ownership (TCO)
- Increased network and business agility
- Enhanced security (as it turns out)[2]

Backhauling and Internet Breakout

The practice of backhauling is where branch office application traffic destined for (or returning from) the internet is routed via a WAN connection between the branch and a corporate headquarters location. This allows it to benefit from the security controls and countermeasures deployed at the headquarters site before being routed to the internet. However, backhauling application traffic results in poor performance due to added latency. The alternative, referred to as local internet breakout for the purposes of this paper, is where selected branch office application traffic is routed directly to/from the internet (i.e., without the need to traverse the WAN and pass through a set of centrally deployed security tools before ultimately reaching the cloud-based application).

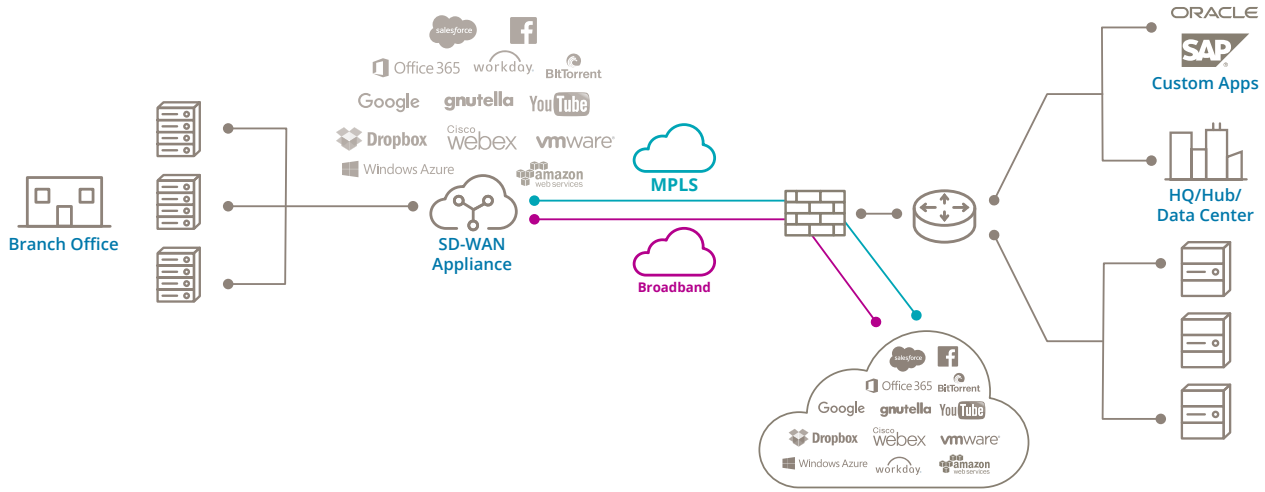

Figure 1: Basic SD-WAN solutions that cannot identify applications on the first packet must either send all web traffic directly to the internet, potentially exposing the branch to vulnerabilities or backhaul all internet-bound traffic to a headquarters-based firewall for additional security inspection. Inefficient backhauling adds latency and impacts application performance.

Why Security Is Critical to SD-WAN Success

For IT departments considering an SD-WAN implementation, the one "twist" to realize is the handful of security challenges and issues that are introduced by or otherwise associated with such an approach.

For instance, the use of broadband internet as low-cost connectivity option is core to the SD-WAN value proposition. However, the fact that broadband is "public" instead of "private" introduces the need for capabilities to ensure the confidentiality and integrity of application traffic traversing such connections. And let's not forget, too, that inline deployment of SD-WAN devices places them "in the line of fire" – at least compared to the scenario where a traditional WAN optimizer is implemented in an out-of-path configuration.

Enabling internet breakout is another good example. Although it's essential for enhancing performance and reducing the bandwidth (i.e., dollars) needed for backhauling, it also exposes branch users and their local networks directly to the internet and its myriad threats. So now you need a way to limit outbound destinations, block unwanted/unsolicited inbound traffic and filter allowed/expected traffic for threats.

However, not all web applications are created equal, and some web traffic can expose the enterprise to viruses, trojans, DDoS attacks and other vulnerabilities. Therefore, direct internet breakout must also be secure. For example, a web traffic security policy might be defined as follows

- Send all known, trusted business SaaS and web app traffic such as salesforce.com, Office365, G-Suite and Box directly to the internet
- Send "home from work" recreational applications like Facebook, Twitter, YouTube and Netflix to a secure web gateway service
- Send all untrusted, suspicious and unknown traffic such as peer-to-peer or traffic from countries in which the company does not do business back to a hub or headquarters-based next-generation firewall

To implement such a policy, web traffic must be steered granularly to its correct destination. This requires identifying the application on the first packet because once an application session has been established, it cannot be redirected to an alternate destination without breaking the flow resulting in application disruption. And because IP address ranges utilized by SaaS applications change almost continuously, address table updates must be automated and implemented on a daily basis.

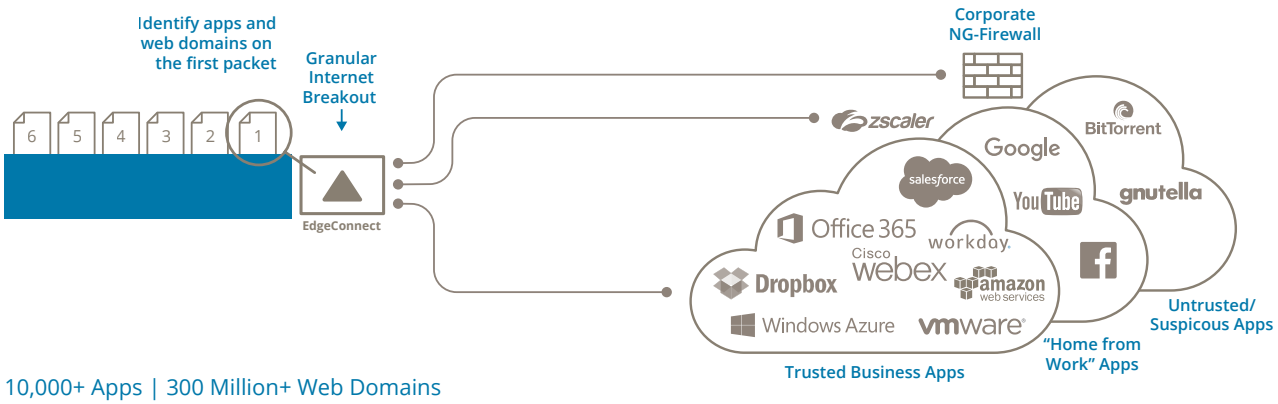

Figure 2: Secure cloud breakout of trusted web-based applications requires application classification on the first packet. Silver Peak First-packet iQ enables granular traffic steering based on application-specific security policies to deliver the highest SaaS and web application performance while protecting branch offices from vulnerabilities.

Additional areas where security is applicable to the success of an SD-WAN implementation include:

- Enabling applications with different security requirements to share the same physical connectivity
- Enabling faster deployment and more efficient management – for example, with secure, automated provisioning of SD-WAN devices, automated security policy enforcement, and a secure management plane
- Enabling consistent enforcement of an application's specific security policies regardless of where that application is located, or accessed from

Introducing Silver Peak EdgeConnect

The industry's most complete SD-WAN solution, EdgeConnect provides enterprises with the flexibility to use any combination of transport technologies to connect users to applications – including public broadband services – without compromising application performance or security. The three main components of the solution are:

- EdgeConnect zero-touch physical or virtual appliances, which are deployed at an organization's branch offices, central sites, and/or cloud data centers
- Unity Orchestrator centralized management system, which enables simplified configuration and orchestration of the entire WAN and provides unprecedented visibility into both legacy and cloud applications; QoS and security policies are defined centrally and automatically deployed globally to all appliances in the SD-WAN, increasing operational efficiency and minimizing human errors which can jeopardize branch security
- Unity Boost, an optional performance pack that enables IT teams to engage Silver Peak market-leading WAN optimization capabilities, where needed, simply by checking a box in the Orchestrator interface

Woven throughout the solution, too, is an extensive set of capabilities that accounts for the security challenges and requirements that are inherent to an SD-WAN implementation.

How EdgeConnect Delivers a Secure SD-WAN

EdgeConnect goes well beyond the basics of ensuring the confidentiality of application traffic traversing public networks. An extensive set of security capabilities provides coverage across four essential areas: the data plane, the management plane, partner integrations, and compliance. The net result is the full-spectrum of protection needed for enterprises to fully realize the benefits of an SD-WAN architecture – enhanced application performance, lower WAN TCO, and increased business agility – without being exposed to greater security risks.

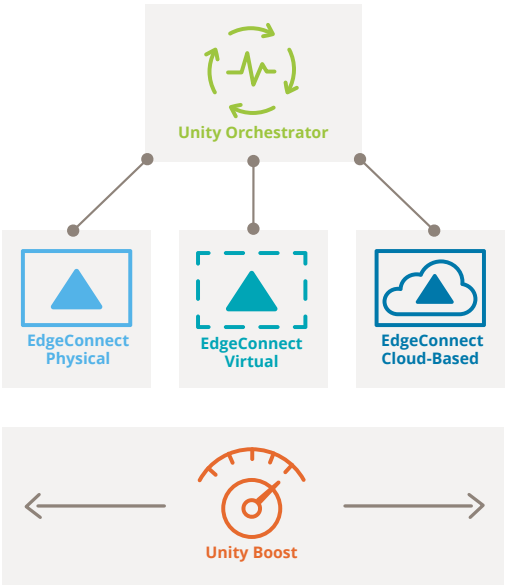

Figure 3: Silver Peak EdgeConnect SD-WAN solution

APPLICATION-DRIVEN DATA PLANE SECURITY

Different applications deserve – or perhaps even require – different treatment when it comes to how they are handled from a security perspective (not to mention other "perspectives," such as QoS, performance optimization, and tunnel bonding policy). For example, a major financial application processing sensitive transactions might require encryption regardless of the type of transport being used to meet compliance requirements, while SaaS applications could be left to rely on their own native capabilities (e.g., TLS). This is why it's important to have an *application-driven* SD-WAN, where policies and configuration settings can be implemented on a per-application basis.

Relevant security capabilities available with EdgeConnect include:

Data-in-Transit Protection: A base-level (yet essential) capability, the EdgeConnect data path is protected by IPSec tunnels that use AES 256-bit encryption to maintain app/data confidentiality. Automatic key rotation and integral message authentication deliver further protection against sophisticated attackers and attempts to tamper with any of the information being transmitted.

Micro-segmentation: EdgeConnect utilizes a virtual WAN overlay model to enable differentiated treatment – including security policies and controls – for different applications. And, because each overlay has its own set of encrypted tunnels, the result, effectively, is the ability to produce a zero-trust architecture where fine-grained segmentation is maintained not only within the corporate data center and branch office networks, but also across the WAN. Derivative benefits include attack surface reduction, containment of any threats that make it past perimeter defenses, and better support for regulations/standards where the intention (if not requirement) is to isolate sensitive transactions and data (e.g., credit card and healthcare information) from all other types of traffic as it traverses the WAN.

Zone-based Firewall: EdgeConnect protects your infrastructure by segmenting the network into zones spanning the LAN and WAN. Each zone is a collection of physical interfaces, VLAN-tagged interfaces or logical interfaces. With the integrated zone-based stateful firewall, granular security policies enabled by First-packet iQ application identification can be applied to secure access to specific zones and micro-segments. It is also essential to enable secure internet breakout from branch offices – not to mention consolidation of branch office WAN infrastructure. The EdgeConnect zone-based firewall further hardens the enterprise WAN by blocking unwanted or unauthorized internet traffic attempting to enter a branch network. By default, the only inbound sessions allowed are responses corresponding to branch-initiated requests and interactions. For organizations that are interested in doing so, the firewall capability can also be used to:

- Help enforce an application whitelist policy, where outbound communications are restricted to only those apps/services that are explicitly allowed (i.e., listed in the policy)
- Allow inbound access for known, trusted applications that require it (e.g., remote management of a printer or teleconferencing system)

DDoS Protection: With the rising frequency of distributed denial-of-service (DDoS) attacks, it is imperative that enterprises establish cost-effective defenses for any and all sites that might be affected. With EdgeConnect deployed at branch locations, that's

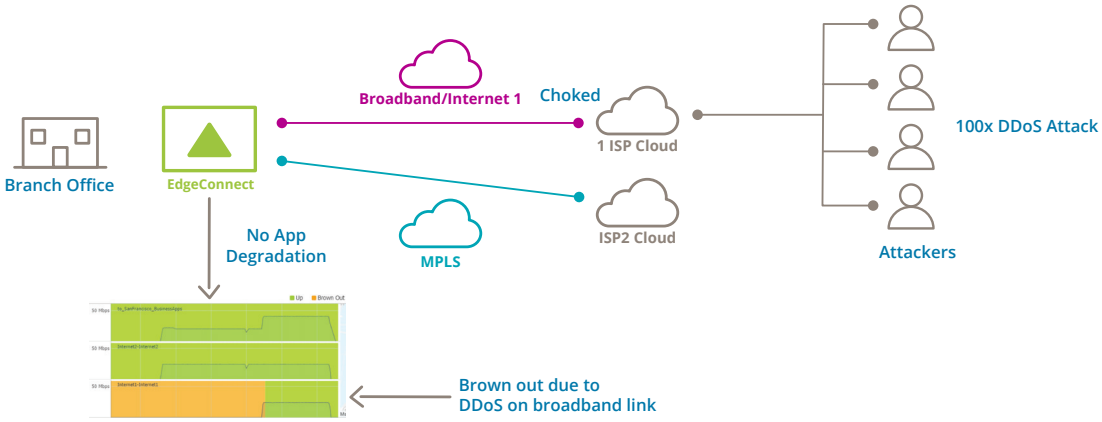

Figure 4: EdgeConnect protects the SD-WAN from DDoS attacks and routes traffic across an alternate transport service to keep applications running enhancing business continuity.

precisely what you get. In the event a broadband connection is flooded by a DDoS attack, EdgeConnect dynamically leverages other available connections to sustain operations with no degradation to application performance or impact to SD-WAN manageability. EdgeConnect protects not only itself, by dropping the offending traffic, but also protects all of the users and systems both on the local network and over the remaining, operational WAN connections.

Data-at-Rest Protection: All blocks of data that persist within EdgeConnect appliances as a result of the Boost WAN optimization data de-duplication capability are protected with AES 128-bit encryption.

Intelligent, Secure Traffic Steering

Although it's not a security capability per se, EdgeConnect First-packet iQ classification plays an important role in the overall effectiveness of the Silver Peak SD-WAN solution. By identifying applications on the first packet of a session, it enables application-driven traffic steering that not only ensures efficient use of WAN resources, but also helps automate security policy enforcement. For example, with First-packet iQ, trusted SaaS and web traffic can be sent directly to the internet (avoiding the performance impact and cost of backhauling), while unknown or untrusted web traffic can be service chained to more advanced corporate or web-based security services. Automated SaaS IP address updates described previously ensure that application traffic is directed correctly according to defined security policies.

MANAGEMENT PLANE AND SYSTEM-LEVEL SECURITY

Despite being less top-of-mind than its data plane counterpart, system and management plane security is no less important. Relevant EdgeConnect capabilities in this area include:

Secure, Zero-Touch Provisioning: A key part of the EdgeConnect value proposition is a plug-and-play deployment model that enables rapid installation, without the need for a distributed IT presence. Security for this process takes the form of a two-step authentication and authorization procedure. Before receiving its settings and policies and becoming an active part of the SD-WAN, each newly connected EdgeConnect appliance first must be authenticated by the Silver Peak Cloud portal and then "approved" by an IT administrator using Orchestrator. In addition, Orchestrator can also be used to subsequently revoke access for a given appliance (e.g., if it is stolen or otherwise compromised). This results in any in-flight traffic being dropped, and the specified appliance being unable to download configuration information or join the SD-WAN.

Encrypted Management Communications: All communication sessions between EdgeConnect appliances, Orchestrator, the Silver Peak cloud portal, and administrators' web browsers are protected with TLS. Furthermore, all weak protocols (e.g., SSLv2, SSLv3), weak hashes (e.g., MD5), and weak encryption algorithms (e.g., DES, RC4) are disabled by default.

System Hardening: Numerous capabilities are available to help minimize the exposure and potential for

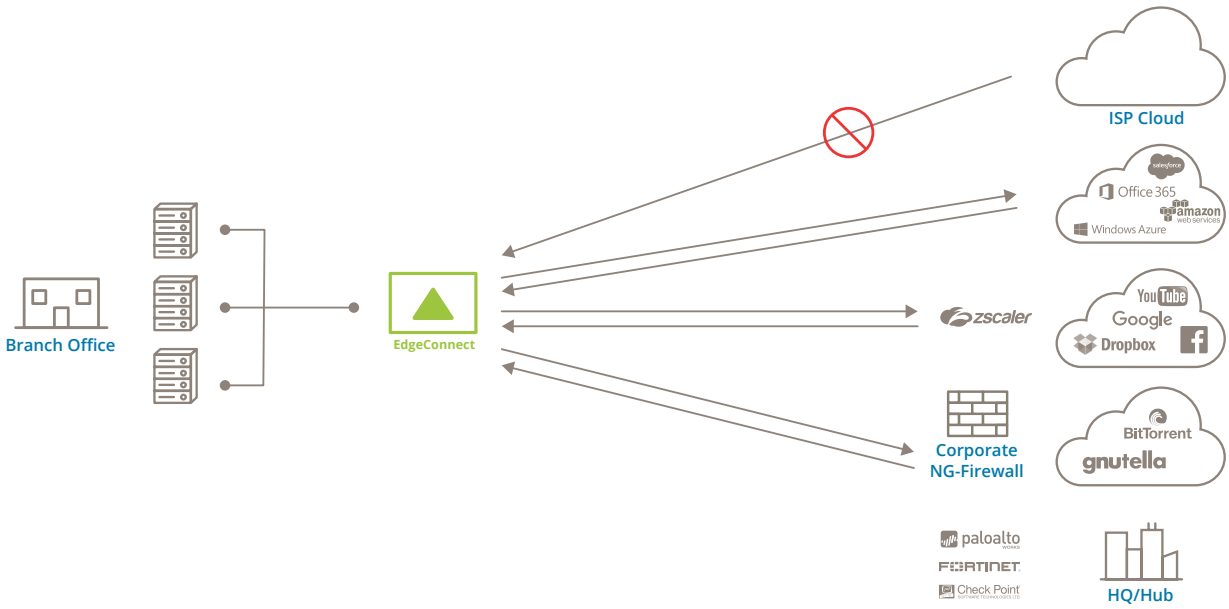

Figure 5: EdgeConnect integrated stateful firewall and simplified service chaining to secure web gateways and next-generation firewalls provides a comprehensive security solution for branch offices.

misuse of management-plane functionality, including:

Robust user authentication and authorization

- Support for local, RADIUS, and TACACS+ authentication and authorization
- Role-based access control with read-only users and administrators
- Whitelisting for Orchestrator that restricts administrative access to a specific set of IP addresses or subnets

Extensive logging for both Orchestrator and EdgeConnect

- Event logs/alarms – for system errors pertaining to memory, CPU, network interfaces, routing, and management plane connectivity
- Threshold crossing alerts – configurable, rising and falling thresholds to signal imminent/approaching conditions for concern, such as high memory or bandwidth utilization
- Audit logs – for tracking all access to an activity conducted via any of the available management interfaces (CLI, WebUI, or REST APIs)
- Netflow/traffic logs – for capturing full (non-sampled) flow data for analysis within Orchestrator, or so that it can be streamed to a third-party tool (e.g., SIEM)

SECURITY TECHNOLOGY PARTNERSHIPS AND SERVICE CHAINING

Third-party security products and services are – or, at least should be – another big part of the overall effectiveness equation for an SD-WAN solution. EdgeConnect supports the integration of third-party security technologies into the SD-WAN architecture as follows:

Security Partners: Most organizations already have an existing set of security tools and infrastructure in which they've made a considerable investment. Plus, when it comes to security, it's simply not realistic for a single solution provider to do everything on its own. The scope of threats, risks, and corresponding technologies is simply too great. The net result is that it's not only advisable to work with third-party security solutions, but also necessary. This is why Silver Peak maintains technology partnerships covering several solution areas, including industry-leading next-generation firewalls (e.g., Check Point, Fortinet, and Palo Alto Networks), secure web gateways (e.g., Zscaler), and secure DNS (e.g., Infoblox).[3]

Service Chaining: To more closely align with the ease-of-use, automation, and flexibility objectives of today's enterprises, EdgeConnect also enables sim-

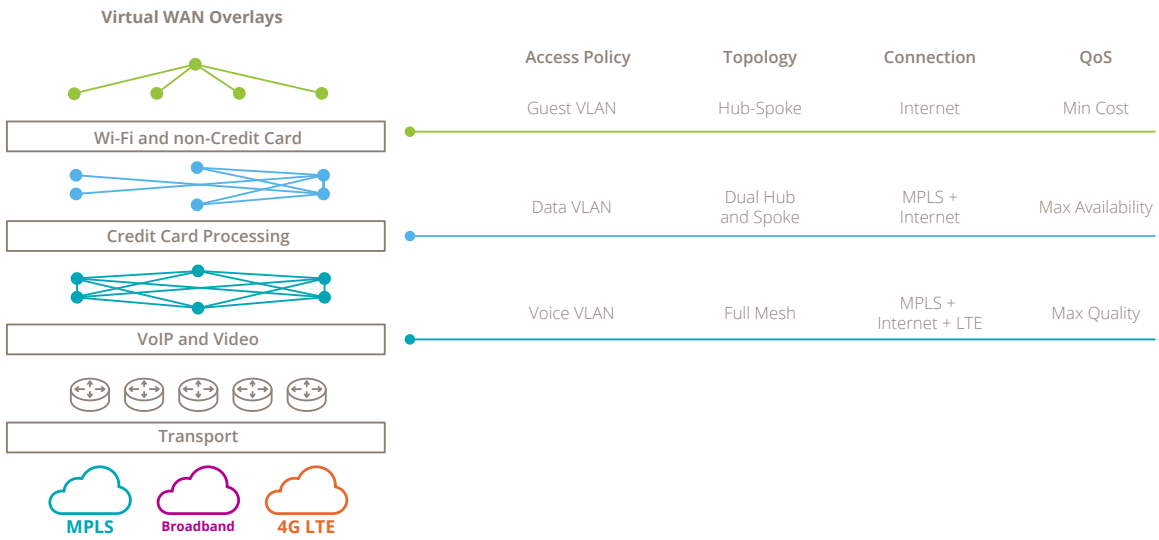

Figure 6: EdgeConnect extends micro-segmentation across the WAN to help enterprises meet compliance mandates.

plified service chaining. With this capability, administrators can take advantage of a drag-and-drop interface to logically interwork a combination of Silver Peak and partner security capabilities in whatever arrangement best meets their needs. A few, straightforward (yet powerful) examples include:

- A service chain where internet-bound traffic is routed through Zscaler cloud-based services for layer 7 access control, threat filtering, and analytics (with optional active-passive or active-active connection to multiple Zscaler points of presence for added resiliency)
- A service chain where EdgeConnect and a next-generation firewall are collocated in select branch offices that are locally hosting one or more enterprise applications
- A service chain where EdgeConnect and a next-generation firewall are collocated at regional hub/office to provide advanced security screening for untrusted applications that are still being backhauled

SECURITY CERTIFICATION AND COMPLIANCE

Last but not least are the many ways EdgeConnect helps ease the burden of complying with relevant industry regulations, including: Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS)[4], Sarbanes-Oxley Act (SOX), and others.One example is certification to the Federal Information Processing Standards (FIPS 140-2), which provides assurance of correct implementation and failure handling for supported cryptographic functions.[5]

Then there are all of the security features covered so far, most of which are applicable to multiple requirements spanning multiple regulations. Authentication, authorization, and auditing capabilities, for instance, are a fundamental requirement of NIST Special Publication 800-53 (Security and Privacy Controls for Information Systems and Organizations) – and, therefore, of practically every regulation that invokes it. Notable too, especially for its uniqueness among SD-WAN solutions, is EdgeConnect's support for micro-segmentation. With the ability to create encrypted, application-specific overlays at their disposal, IT teams can, for example, segment off credit transactions and associated systems as a way to substantially reduce the scope of their PCI DSS compliance efforts.

Conclusion

Fully realizing the many compelling benefits of an SD-WAN depends to no small extent on having a solution that accounts for the security issues, challenges, and opportunities that such an approach presents. In this regard, the extensive security capabilities of Silver Peak EdgeConnect go well beyond the minimum-required level of protection afforded by transport-level encryption and message authentication. By combining robust data and management plane security features with numerous security technology partnerships, and simplified service chaining, EdgeConnect delivers a level of security that better meets the *actual* protection and compliance needs of today's enterprises.

For more information about the EdgeConnect SD-WAN solution from Silver Peak, click here.

FOOTNOTES:

1. https://451research.com/blog/764-enterprise-it-executives-expect-60-of-workloads-will-run-in-the-cloud-by-2018

2. For details of how SD-WAN delivers improved application performance and other benefits, click here.

3. Related solution briefs are available here.

4. For details on how EdgeConnect supports PCI DSS compliance, click here.

5. For details on FIPS certification status, click here.

Company Address

Silver Peak Systems, Inc
2860 De La Cruz Blvd.
Santa Clara, CA 95050

Phone & Fax

Phone: +1 888 598 7325
Local: +1 408 935 1800

Online

Email: info@silver-peak.com
Website: www.silver-peak.com

© Silver Peak Systems, Inc. All rights reserved. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners. 01/2018