Secure SD-WAN for the Cloud-First Enterprise without Compromise

Zscaler and Silver Peak automate consistent security policies for all users, all applications and across all locations with true zero-touch provisioning

CLOUD-FIRST SECURITY CHALLENGES

Unpredictable application performance
Inability to prioritize traffic and enforce business-driven security policies can rob performance from business-critical applications

Time-consuming, error-prone policy configurations delay deployments
Ever-changing cloud applications require constant manual reconfiguration of routers and firewalls at every location

Inconsistent policy enforcement
Maintaining consistent security policy definitions across hundreds or thousands of sites is arduous

SOLUTION BENEFITS

Secure, uninterrupted access to business-critical applications
Prioritize business-critical applications, delivering the highest quality of experience to users

Accelerate deployments of new branch locations and applications
Centralized policy definitions and true no-touch provisioning accelerate deployments of new branch locations and applications

Deliver consistent business and security policies globally to all users
Automated security and cloud application updates ensure consistent network and security policy enforcement across all locations

Executive summary

As applications continue to migrate to the cloud, changing traffic patterns drive the need for a new Wide Area Network (WAN) approach and security model. When all applications resided in enterprise data centers, life was simpler for IT; all traffic from the branch was backhauled to the data center over MPLS circuits, with the entire stack of security services enforced at data center egress points, requiring only fundamental security services at the branch.

Now, applications reside everywhere and may be hosted in the data center, in public and private clouds, or delivered by myriad Software-as-a-Service (SaaS) providers. To further complicate the security model and the IT challenge, users now access applications from anywhere, from any device and across diverse WAN transports, including the internet. This increases the attack surface, significantly increasing the need for more advanced security services to protect the branch from threats.

While enterprises could deploy next-generation firewalls at every branch, that model is untenable. The hardware is too expensive, and deploying and managing dedicated security appliances at hundreds or thousands of branch locations requires far too many IT resources. In addition, branch locations need advanced security controls, like sandboxing, intrusion prevention (IPS) and Data Loss Prevention, as well as SSL inspection to protect against advanced threats.

To address the security and cost challenges, centrally orchestrated cloud-hosted security services, such as those available from Zscaler™, have emerged and are experiencing hyper-growth. The Zscaler Cloud Security Platform combined with the application-aware, business-driven Silver Peak Unity EdgeConnect™ SD-WAN edge platform provides a powerful solution that protects the enterprise from threats, delivers the highest application performance and user experience and keeps costs in check.

Application migration to the cloud compels a new WAN security model

Enterprises face several challenges when migrating applications to the cloud. To deliver the highest performance, users should connect to cloud-hosted and SaaS applications directly over the internet. However, that increases the attack surface at branch locations and exposes the enterprise to threats and vulnerabilities without the deployment of strong security measures.

In the device-centric model based on routers and discrete firewalls, this has meant a hub-and-spoke architecture and backhauling all internet-bound traffic to a headquarters site for inspection by next-generation firewalls. This backhaul consumes bandwidth, adds latency and negatively impairs application performance. Alternatively, an enterprise can deploy next-generation firewalls at every branch location, but that adds tremendous IT complexity and is cost-prohibitive.

Cloud-first IT security challenges

Any device, anywhere: IT faces another security challenge in a cloud-first strategy. Users access cloud and SaaS applications from everywhere — home, hotels, the local coffee shop — not just the branch office. To address this challenge, enterprises must arm workers with a security service solution that follows them wherever they go, providing a fast and secure experience for all users wherever they connect.

Not all apps are created equal: Some SaaS offerings, such as VoIP services, are jitter-sensitive, support robust security measures and therefore don't expose risk to the enterprise. Connecting users directly to these applications provides the best user experience. However, other cloud or web-based applications may not be as secure or may expose the enterprise to threats or intellectual property leakage. For example, an employee could inadvertently — or maliciously — transfer company IP in a Facebook message. Therefore, IT must be able to support granular security policies based on the applications and based on business requirements or "intent."

Applications change constantly: SaaS application definitions and the range of IP addresses used to access them change continuously, especially for popular SaaS applications, such as Office 365, UCaaS applications and recreational apps, such as Facebook, Instagram and others. IT must keep pace with constant changes to provide uninterrupted access to business-critical applications.

Deploying new branch locations and applications: To maintain competitiveness in today's global markets, IT must respond quickly to deploy new applications as well as bring new sites online. Bringing up new sites under the traditional WAN model based on routers, discrete firewalls and MPLS connections typically takes three months or longer. To address business growth, whether organic or through acquisitions, and to meet application demands, enterprises now require the ability to automate deployment of new WAN and security services with true zero-touch provisioning.

Remediating WAN performance and security issues: The emergence of the cloud, coupled with increasing use of internet and 4G/LTE services as active WAN transports, makes it more difficult for IT to resolve security, network and application performance issues. However, end-user expectations for always-on, high-performing applications is higher than ever. Enterprises need tools that enable faster troubleshooting so that IT can be more responsive to the business.

Addressing these challenges requires a re-architecting of the WAN and WAN security infrastructure models.

Secure SD-WAN without compromise

Cloud-hosted security services, such as Zscaler Internet Access™, have emerged to provide a superior security alternative for cloud-first enterprises. Centrally managed and supporting a full security stack, including next-generation firewall, IPS, sandboxing, UTM, URL filtering, DLP and more, Zscaler delivers identical protection for all users and consistent policies and policy enforcement across hundreds or even thousands of sites — without any security appliances to buy, deploy or manage.

Cloud-hosted security services, coupled with an application-aware, business-driven SD-WAN edge platform, such as Unity EdgeConnect, also greatly streamline WAN edge infrastructure at the branch. Enterprises no longer need to deploy expensive, complex-to-manage next-generation firewalls at every branch location.

Silver Peak First-packet iQ™ application identification enables intelligent, granular traffic steering. This facilitates granular security policy enforcement based on business intent, securing the organization while delivering the highest performance for all applications. For example, a set of business-driven security policies might be as follows:

1. Send enterprise data center-hosted application traffic directly to headquarters
2. Send only UCaaS traffic directly to providers' cloud services
3. Send all other internet-bound traffic, including Salesforce, Facebook, YouTube, Box and web browsing traffic to a Zscaler cloud point of presence (PoP) for security inspection prior to handing off to providers' cloud or web services

Centrally Managed: Not only does the Zscaler/Silver Peak solution simplify WAN infrastructure at the branch, the solution is centrally managed. Policies are defined once and pushed to all sites. This provides the ability to deploy new policies quickly across hundreds or even thousands of sites. Bringing new sites online or making policy changes or updates is equally easy. Centrally managed policy configuration and administration eliminates device-by-device configuration inherent to the discrete firewall model and minimizes the potential for human errors. The result is consistent, end-to-end security policy enforcement.

Fully Automated Onboarding: Zscaler and Silver Peak have partnered to greatly simplify cloud-security service onboarding. Fully automating IPsec tunnel configuration between EdgeConnect SD-WAN appliances and Zscaler Enforcement Node (ZEN) PoP eliminates manually defining IPsec tunnels at every branch site. Location information from the Zscaler portal is "learned" by Silver Peak Unity Orchestrator™ and used to connect branch sites to the closest primary and backup ZEN PoPs.

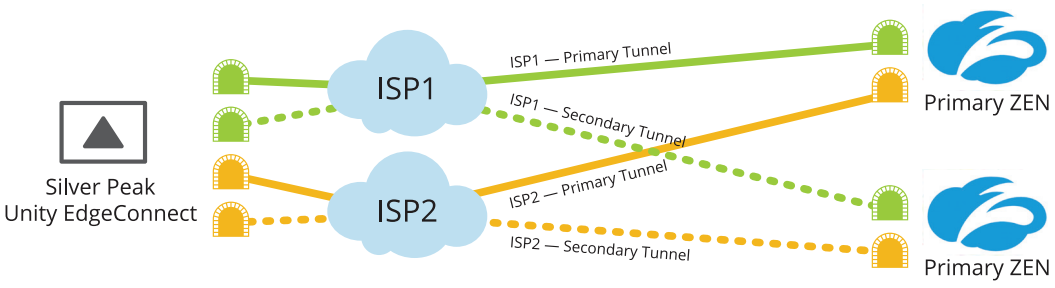


Figure 1: Four IPsec tunnels configured per site to support full WAN transport and ZEN POP redundancy

From the Unity Orchestrator console, IT simply validates a company's Zscaler subscription credentials and selects branch locations to connect to ZEN PoPs. Orchestrator automatically configures primary and optional secondary IPsec tunnels to the closest primary and secondary ZEN PoP to each branch location, delivering the highest quality of cloud application performance. The EdgeConnect SD-WAN continuously monitors the state of connections and ZEN PoPs, automatically re-directing traffic to the backup node if necessary. If a new ZEN PoP closer to a branch site becomes available, the configured tunnels are updated automatically, ensuring that the Zscaler/Silver Peak solution continuously adapts to deliver the peak application performance for users.

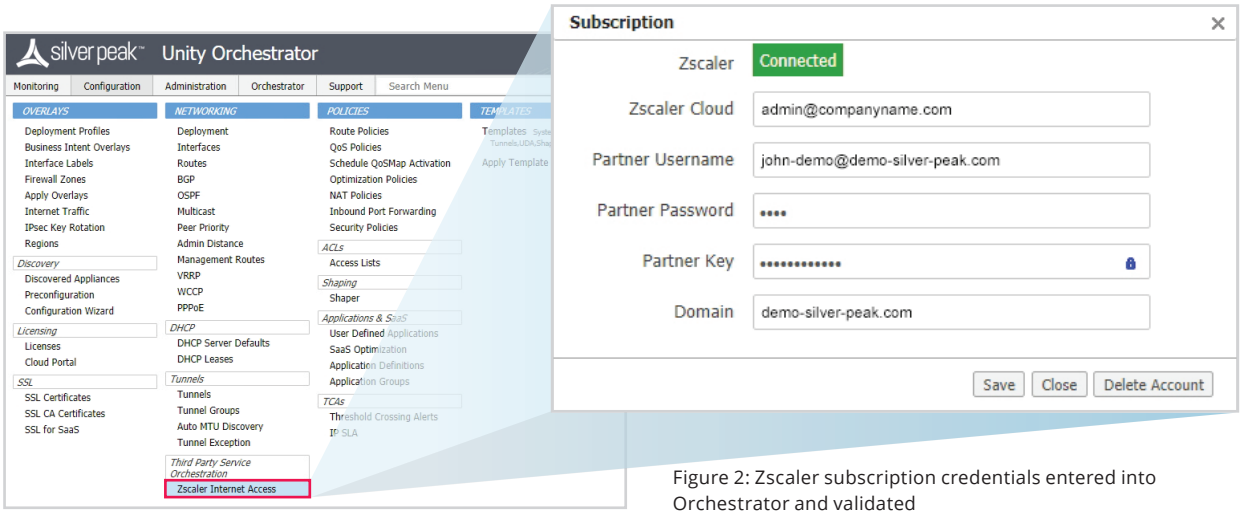


Figure 2: Zscaler subscription credentials entered into Orchestrator and validated

IT then selects the application traffic to forward to Zscaler ZEN PoPS and simply "drags-and-drops" the preferred primary and secondary traffic handling policies into the configuration screen; this is typically all internet-bound traffic except whitelisted traffic, such as UCaaS. Future policy changes may be updated easily and pushed to all locations with a single mouse click.

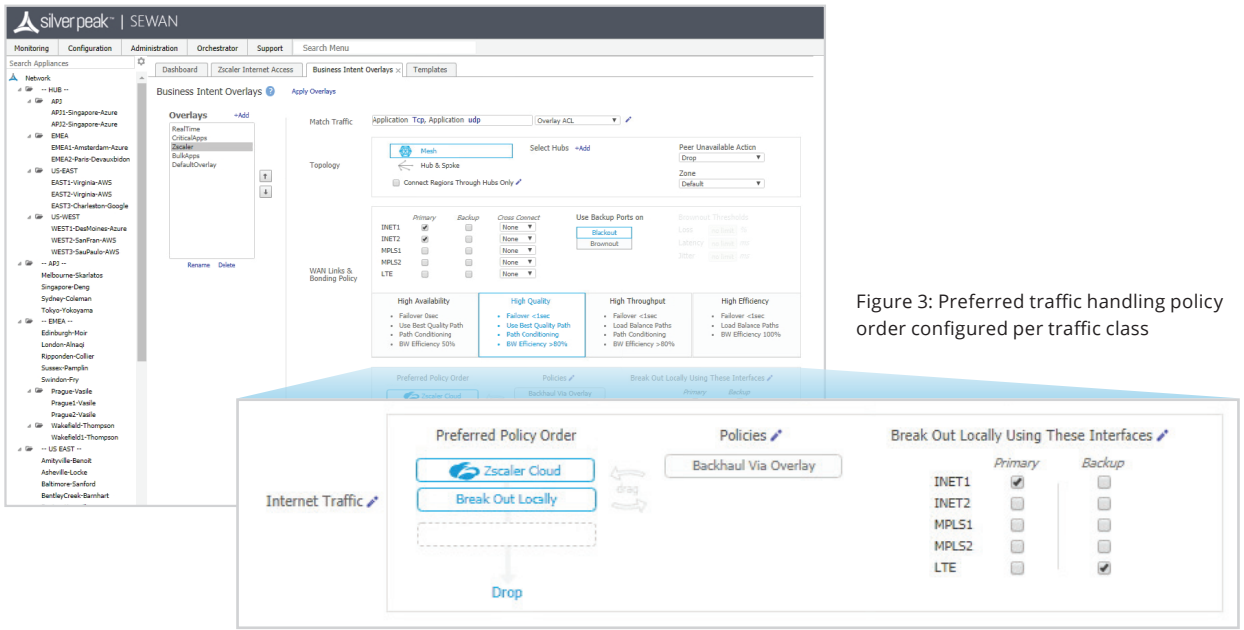


Figure 3: Preferred traffic handling policy order configured per traffic class

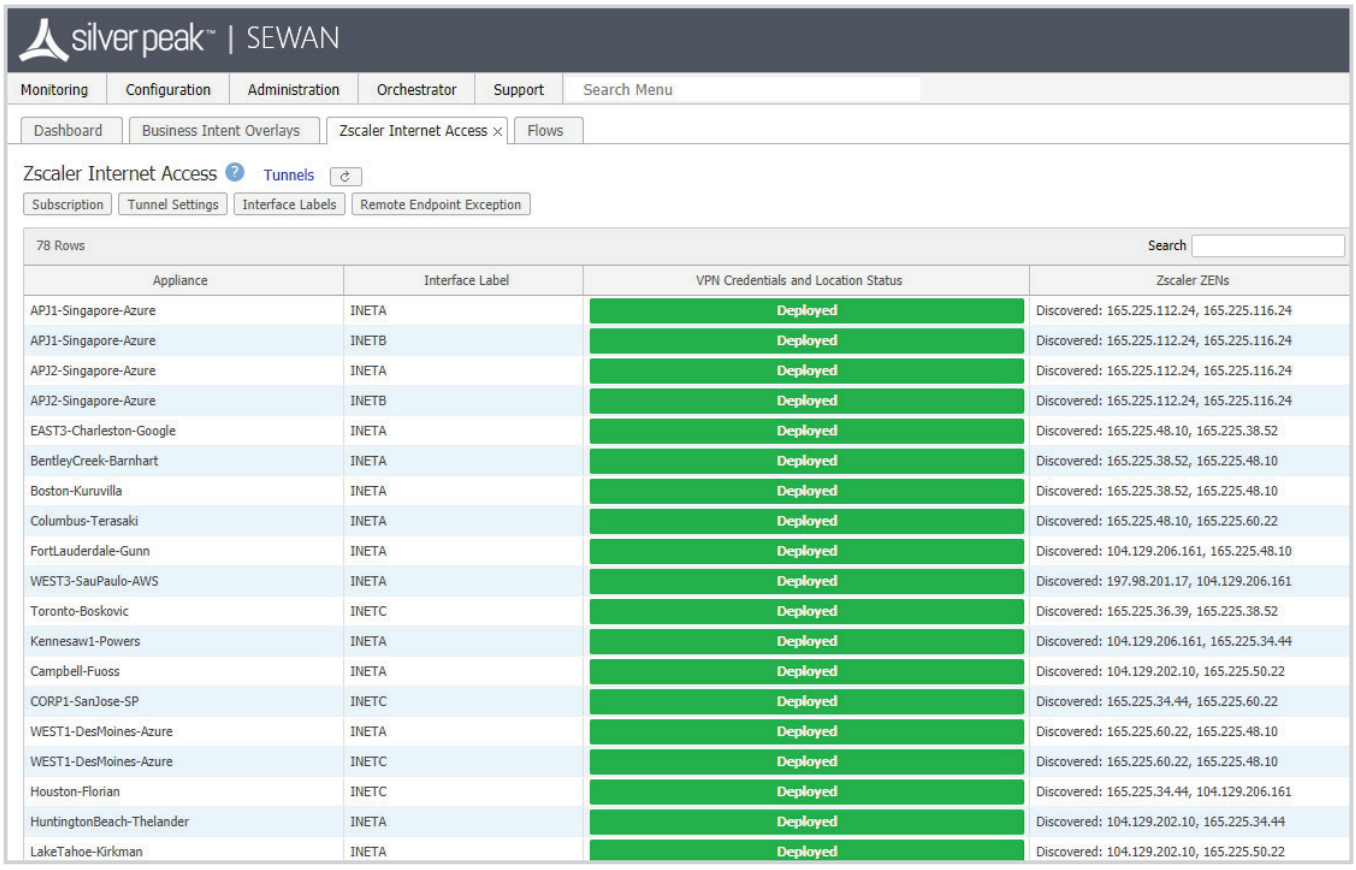
Silver Peak leveraged the Zscaler API to integrate and automate the process of connecting branch locations in the SD-WAN fabric to the closest primary and optional secondary ZEN PoPs. With this integration, hundreds of sites can be automatically connected within minutes, generating significant IT OPEX savings. The integration delivers the added benefit of consistent policy enforcement across the SD-WAN, keeping the enterprise safe from threats and vulnerabilities.

In addition to enabling full automation for establishing IPsec tunnels to secure branch locations, the Silver Peak/Zscaler solution provides the flexibility to support major branch locations that require Gigabit speed bandwidth for internet-bound traffic. IT uses Orchestrator to centrally configure and monitor GRE tunnels between these locations and the closest primary and secondary ZEN PoPs.

Zscaler + Silver Peak = better business outcomes

With the Silver Peak Self-Driving Wide Area Network™ platform and Zscaler Cloud Security Platform, branches going direct to cloud can be provisioned and secured in minutes. Enterprises can deliver faster deployments, optimal performance from applications, and secure SD-WAN connectivity that automatically adapts to changing business requirements. For IT, that means lower costs and simplified operations. End users enjoy fast, secure and uninterrupted access to the business-critical applications they need.

> Provide fast, secure and uninterrupted access to business-critical applications, increasing overall business productivity and user experience



Appliance	Interface Label	VPN Credentials and Location Status	Zscaler ZENs
APJ1-Singapore-Azure	INETA	Deployed	Discovered: 165.225.112.24, 165.225.116.24
APJ1-Singapore-Azure	INETB	Deployed	Discovered: 165.225.112.24, 165.225.116.24
APJ2-Singapore-Azure	INETA	Deployed	Discovered: 165.225.112.24, 165.225.116.24
APJ2-Singapore-Azure	INETB	Deployed	Discovered: 165.225.112.24, 165.225.116.24
EAST3-Charleston-Google	INETA	Deployed	Discovered: 165.225.48.10, 165.225.38.52
BentleyCreek-Barnhart	INETA	Deployed	Discovered: 165.225.38.52, 165.225.48.10
Boston-Kuruvilla	INETA	Deployed	Discovered: 165.225.38.52, 165.225.48.10
Columbus-Terasaki	INETA	Deployed	Discovered: 165.225.48.10, 165.225.60.22
FortLauderdale-Gunn	INETA	Deployed	Discovered: 104.129.206.161, 165.225.48.10
WEST3-SauPaulo-AWS	INETA	Deployed	Discovered: 197.98.201.17, 104.129.206.161
Toronto-Boskovic	INETC	Deployed	Discovered: 165.225.36.39, 165.225.38.52
Kennesaw1-Powers	INETA	Deployed	Discovered: 104.129.206.161, 165.225.34.44
Campbell-Fuoss	INETA	Deployed	Discovered: 104.129.202.10, 165.225.50.22
CORP1-SanJose-SP	INETC	Deployed	Discovered: 165.225.34.44, 165.225.60.22
WEST1-DesMoines-Azure	INETA	Deployed	Discovered: 165.225.60.22, 165.225.48.10
WEST1-DesMoines-Azure	INETC	Deployed	Discovered: 165.225.60.22, 165.225.48.10
Houston-Florian	INETC	Deployed	Discovered: 165.225.34.44, 104.129.206.161
HuntingtonBeach-Thelander	INETA	Deployed	Discovered: 104.129.202.10, 165.225.34.44
LakeTahoe-Kirkman	INETA	Deployed	Discovered: 104.129.202.10, 165.225.50.22

Figure 4: Within minutes, every SD-WAN branch location is automatically connected to the closest Zscaler ZEN POPs

- Streamline branch architecture and eliminate the need to buy, deploy, and manage security appliances or VNFs for all branch locations by delivering the entire security stack as a cloud-based service, including native SSL inspection at scale
- Quickly add and secure new branches with automated deployments and true zero-touch provisioning, increasing business agility and accelerating time-to-revenue
- Make changes easier, minimize human errors and enable faster troubleshooting so that IT is more responsive to the business
- Centrally define security requirements once, and automatically deliver identical security for all users, wherever they connect
- Minimize risk by delivering consistent network and security policies based on the needs of the business, not the limitations of the infrastructure
- Reduce the time required for troubleshooting network and application bottlenecks and for fielding support/help desk calls day and night
- Reduce dependence on high-cost MPLS services and eliminate costly security appliances

About Zscaler

Zscaler enables organizations to securely transform their networks and applications for a mobile and cloud-first world. Zscaler cloud-delivered services securely connect users to their applications and cloud services, regardless of device, location, or network, while providing comprehensive threat prevention and a fast user experience. All without costly, complex gateway appliances. Learn more at zscaler.com or follow us on Twitter @zscaler.

About Silver Peak

Silver Peak, the global SD-WAN leader, delivers the transformational promise of the cloud with a business-first networking model. The Unity EdgeConnect™ self-driving wide area network platform liberates enterprises from conventional WAN approaches to transform the network into a business accelerant. EdgeConnect replaces routers, unifying SD-WAN, firewall, segmentation, routing, WAN optimization and application visibility and control in a single platform. EdgeConnect continuously learns and adapts to meet the requirements of the business, delivering the highest quality of experience to enterprise users and IT organizations. Thousands of globally distributed enterprises have deployed Silver Peak WAN solutions across 100 countries. Learn more at silver-peak.com.

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

SP-SB-SECURE-SD-WAN-WITH-ZSCALER-050219