Simplified, Consistent Security for Applications

No Matter Where They Reside

CHALLENGES

Inflexible to secure all types of applications
Complex to setup and configure policies for distributed and cloud-based applications

Inefficient to configure and manage
Fragmented policy management unable to quickly respond to changing business requirements

Expensive
On-going support and management are time consuming and expensive to maintain

SOLUTION

Simplified configuration with drag-and-drop approach
Drastic reduction in IT time required to configure and manage security policies

Intelligent app-driven security policy model
Reduces errors, increases efficiency and reduces cost

Easy to manage with a single dashboard
Accelerates deployment of applications through centralized app-driven policy orchestration

Traditional WANs were not designed to easily and simply secure distributed and cloud-based applications.

The cloud-first branch must be able to dynamically secure applications based on defined policies whether the application are hosted in public or private clouds. Once an application security policy is defined, the intelligent application-driven WAN edge must automatically apply and enforce the policy as it steers traffic across the WAN – without any further IT intervention.

Traditional security model in the branch

Traditional security architectures in branch offices (Figure 1) are not centrally managed and configured. Security policies – and any subsequent changes to them – in this model must be configured manually, resulting in management complexity. This is especially true when it comes to supporting distributed and cloud-based applications. In the traditional model, all branch office traffic is backhauled to the data center for thorough security inspection before being redirected to its destination. In cases where security provisioning is required for a specific application, the IT security team must update policies on individual security appliances. This manual configuration process is lengthy, cumbersome, costly and prone to human error.

Some branch offices include on-site security appliances to connect

Traditional Security Model

1 Inflexible
Inflexible in supporting cloud-based and distributed apps

2 Inefficient
Complex to configure and manage; can't respond fast enough to business needs

3 Expensive
Costly to support and maintain

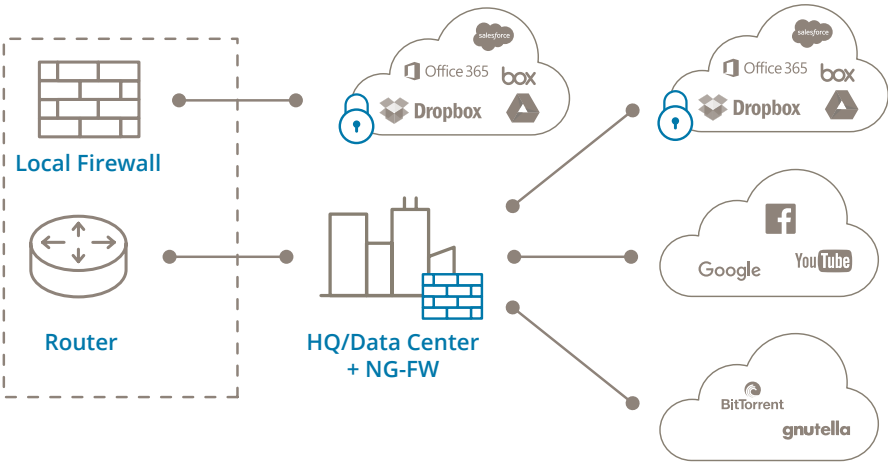

Figure 1: Traditional security model at the branch

directly to the internet. This enables application performance efficiencies by eliminating internet traffic backhaul and support for secure hosting of applications at the branch DMZ. However, operational inefficiencies lie in the individual provisioning of applications to the firewall and the ongoing management of devices at the branch in addition to the added capital cost.

Simplified, integrated application-driven security

In the application-driven security model, the Silver Peak Unity EdgeConnect SD-WAN solution can greatly simplify the architecture and the process of applying policies to applications. Application policies are defined centrally in the EdgeConnect business intent overlay template within Unity Orchestrator and then applied to applications in an automated manner. Policies may be a combination of ACL rules with a built-in stateful firewall that is included in EdgeConnect plus the option to service chain with third-party security appliances for additional traffic inspection. EdgeConnect makes it easy to stitch these security services together, whether the security appliances are located in the branch, at headquarters or in the cloud. Using a simple, drag-and-drop interface from a business intent overly template (Figure 2), security services are easily chained and applied to defined applications. Once policies have been defined, they are programmed in an automated manner to all appliances in the SD-WAN. This accelerates application deployment and provisioning while reducing errors.

As shown in Figure 3, EdgeConnect automatically steers traffic to its destination on an application-by-application basis according to policies configured to meet enterprise security requirements. For example, trusted SaaS and web traffic may be steered directly to the internet while backhauling or service chaining untrusted or unknown traffic to more advanced security services located at a hub or headquarters site.

However, to steer traffic granularly and to its correct destination, applications must be identified on the first packet. Once traffic starts flowing, it cannot be redirected to alternate path without breaking the flow and causing application disruption.

Silver Peak First-packet iQ enables EdgeConnect to intelligently direct traffic to the correct SD-WAN overlay based on enterprise security policies and across the underlying WAN circuit(s) utilized by that overlay. First-packet iQ incorporates a dynamic map of the internet to identify and classify more than 10,000 SaaS applications, hundreds of thousands of IP ad-

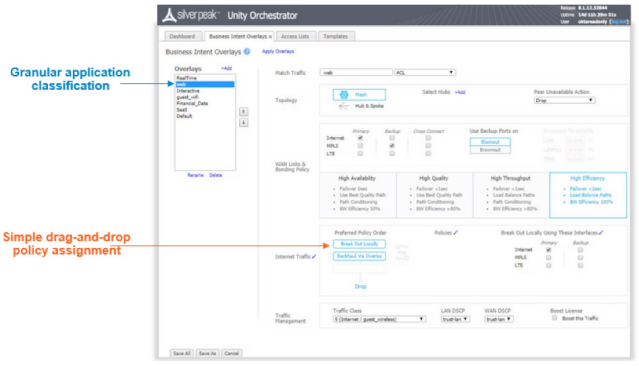

Figure 2: Business intent overlay policy screen securing applications via simplified drag-and-drop service chaining with third-party security appliances

Simplified Security Model

1 Simple
Drag-and-drop approach drastically reduces IT time required to configure and manage security policies

2 Intelligent
App-driven security policy model that reduces error, increases efficiencies and reduces cost

3 Easy to Manage
Single dashboard for orchestrating and maintaining policies resulting in accelerated deployment of apps

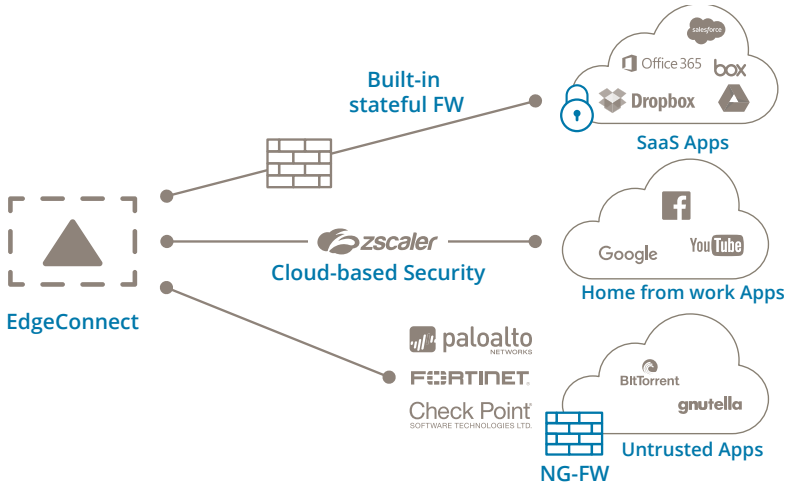

Figure 3: EdgeConnect simplifies applying application-driven security policies

dresses and geo-location data, and 300 million web domains on the very first packet. To keep up with constantly changing IP address tables used by SaaS and web applications, Silver Peak employs a variety of technologies including RSS feeds, DNS snooping and machine learning to keep the internet map up to date on a continuous basis. EdgeConnect appliances receive a daily download of the latest SaaS and web application IP address information, required for first-packet application steering.

In practice, IT security administrators usually define more than one application security policy in their network. For example, trusted SaaS traffic could be sent directly to the internet. The built-in stateful firewall in the EdgeConnect solution is ideal for inspecting traffic generated by users in the branch when accessing trusted SaaS applications like Office365 or Salesforce. Recreational web traffic such as Facebook or YouTube could be directed to a cloud-based security gateway like Zscaler, and untrusted or suspicious traffic could be sent to a next-generation firewall like Palo Alto Networks, Check Point or Fortinet located at a headquarters site for further security inspection.

Conclusion

Security is a major concern for enterprises, and the new cloud-first model requires a different, application-driven approach to securing the branch. The Silver Peak Unity EdgeConnect SD-WAN solution enables simplified orchestration of application-driven security policies and integrates with best-of-breed ecosystem partners while protecting current investments. The outcome is the automation of granular security policies which dramatically reduces amount of time and the complexity in managing and controlling applications across the distributed enterprise.

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