Centrally Orchestrated End-to-End Segmentation

The Unity EdgeConnect SD-WAN Edge Platform Enforces Granular Security Policies across the LAN-WAN-LAN, LAN-WAN-Data Center and LAN-WAN-Cloud

Network Security has been a Manual, Device-Centric Approach

Software-defined Wide Area Networks (SD-WAN) have transformed the way users connect to applications. In contrast to the traditional router-centric approach that uses TCP/IP addresses and Access Control Lists (ACLs), an SD-WAN employs a more intelligent and more automated application-driven model to control how traffic traverses the WAN.

With the Silver Peak Unity EdgeConnect™ SD-WAN edge platform, enterprises create multiple application-specific virtual WAN overlays. Each virtual overla — or business intent overlay — specifies priority and quality of service requirements for application groups based on business requirements or intent. With these definitions in place, EdgeConnect automates traffic steering on an end-to-end basis across all underlying WAN transport services including MPLS, broadband and 4G/LTE, providing the ability to deliver an application quality of experience that is better than what can be provided by any of the underlying transport services individually.

However, to date, security policy definition and enforcement across the traditional WAN remains a manual, fragmented, device-centric approach. Multiple disparate policies must be defined for the LAN, WAN, Data Center and the Cloud. Current zone-based firewalls and other security devices must be individually programmed, device-by-device and then stitched together with separate policies defined across the WAN. Not only is this time-consuming and expensive, it leads to inconsistent security policies that expose the enterprise to unnecessary risks due to inconsistent configurations and errors.

Consistent Policies with End-to-End Network Segmentation

EdgeConnect centrally orchestrates end-to-end segmentation spanning the LAN-WAN-LAN, LAN-WAN-Data Center and LAN-WAN-Cloud.

The Silver Peak Unity Orchestrator™ enables distributed enterprises to easily segment users, applications and WAN services into secure end-to-end zones[1] in compliance with predefined security policies, regulatory mandates and business intent. This results in consistent security policies and automates enforcement across the enterprise. Orchestrator centralized security administration pares down the task of defining multiple end-to-end zones to a matter of minutes.

The example shown in Figure 1 below represents typical zone or segment definitions for a retail chain. In this example, independent end-to-end segments have been defined for Point of Sale (POS) traffic, HVAC control applications, resource planning and for internet-bound traffic with independent policies for guest Wi-Fi, trusted SaaS applications and recreational web applications. Segments extend from the LAN, across the WAN and to the data center or to the cloud service provider. Traffic within a segment is isolated from traffic in other segments, preventing unauthorized access. If a threat were to surface, its impact is contained to to the compromised segment. Zone-based security policy definitions also define the transport topology and failover policies for each segment.

The segmentation described in this example would have likely prevented the now-famous Target credit card breach that occurred in 2013. Attackers used stolen HVAC credentials to gain access to Target's internal data network, exploited a vulnerability to gain control of Target servers and injected malware onto POS data servers. Attackers exploited the security breach and misappropriated personal identifiable information for more than 40 million credit and debit card holders[2]. While the Target attack was sophisticated and involved multiple security enforcement breakdowns, secure, end-to-end zone-based segmentation could have prevented access to the POS applications from any other zones or segments.

Centralized Orchestration Improves Operational Efficiency

Using an intuitive graphical user interface, an IT administrator can define segments spanning the LAN and the WAN. Each LAN-side zone may be mapped to a business intent overlay, extending micro-segmentation across the WAN. Multiple LAN-side zones may be mapped to a single business intent overlay. However, the traffic from a single LAN-side zone can be mapped only to a single business intent overlay.

Application traffic within a zone is enabled across the LAN and mapped to the corresponding WAN segment, but all other traffic is denied by default. IT can allow trusted applications or allow specific applications to access users or devices in a different zone.

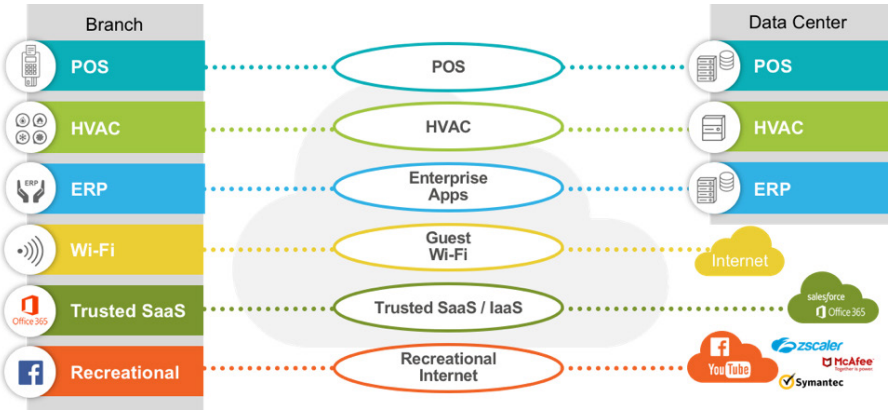

Figure 1: Sample configuration designed for a retail organization to create isolated segments for Point of Sale traffic, HVAC application traffic, resource planning traffic and internet-bound traffic.

[1]A zone is a collection of interfaces and network segments attached to the interfaces. A zone may comprise VLANs, physical and/or logical interfaces and sub-interfaces. Each zone is mapped to one and only one EdgeConnect business intent overlay (BIO). However, multiple zones may be mapped to a single BIO.

[2]https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

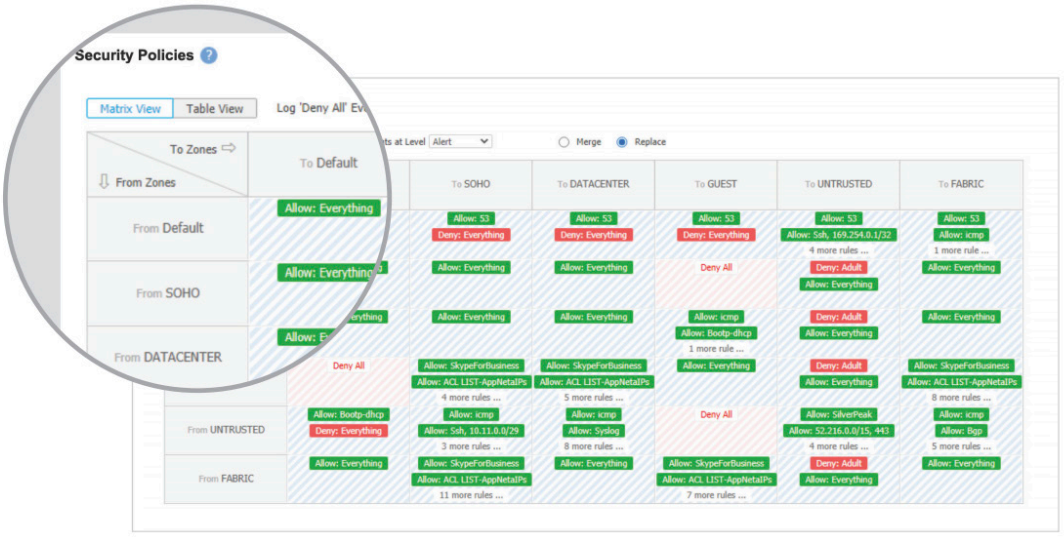

Figure 2: Security policies enable LAN to WAN traffic within a zone (segment) but deny traffic between zones until IT explicitly allows specific communication between zones.

This may include policies for traffic that remains within the branch LAN such as that for a printer shared between multiple zones. A matrix view from Orchestrator, shown in Figure 2, provides an easy-to-read, intuitive visualization of configured zones and defined whitelist exceptions. Orchestrator also supports a standard table view, similar to that provided by firewall management applications, making the transition to the end-to-end segmentation model seamless for security professionals.

Automated Enforcement and Threat Containment Reduces Risk

Once end-to-end segments, zone-based policies and any exceptions have been defined, Orchestrator programs the policies automatically to every EdgeConnect SD-WAN appliance, eliminating time-consuming manual configuration of routers and firewalls. EdgeConnect automates consistent security policy enforcement across the LAN and WAN and to the data center to help enterprises meet compliance requirements, reduce threat risks and ensure continuous business operations.

Advanced Segmentation with Virtual Routing and Forwarding (VRF)

Silver Peak has reimagined virtual routing and forwarding (VRF) for the modern cloud-first enterprise, thoughtfully unifying advanced segmentation capabilities into the EdgeConnect SD-WAN edge platform.

VRFs allow multiple instances of a routing table to co-exist within the same router/switch, operating at the same time. One or more logical or physical interfaces may have a VRF, and these VRFs do not share routes. Hence packets are only forwarded between interfaces on the same VRF. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other. Network functionality is improved because network paths can be segmented without requiring multiple routers.

By combining new VRF capabilities with the existing EdgeConnect zone-based stateful firewall and Network Address Translation (NAT) capabilities, network managers can apply advanced segmentation definitions to routes and application traffic with just a few mouse clicks within the Orchestrator management interface. Network managers can now configure and manage separate addressing, routing and security policies consistently across end-to-end segments and micro-segments for traffic traversing the networks of large-scale multinational enterprises and federations of independent companies. Advanced segmentation eliminates the arduous task of manually stitching together VRF, firewall and NAT policies in a consistent manner, dramatically simplifying the management of diverse scenarios and providing unprecedented flexibility when contending with overlapping IP address spaces.

Solution Benefits

CONSISTENT POLICIES
Enforce end-to-end zone-based security policies spanning LAN-WAN-LAN, LAN-WAN-Data center and LAN-WAN-Cloud.

SEPARATE LINES OF BUSINESS (LOB)
Provide selective access to relevant data and applications to business units or departments based on access privileges; restrict access to specific segments of the network for subsidiary and business partner companies.

SIMPLIFIED MANAGEMENT AND VISIBILITY
Separate authenticated users from guest users, isolate different traffic types more efficiently, e.g., video surveillance traffic from transactional traffic.

IMPROVED OPERATIONAL EFFICIENCY
Centrally orchestrate consistent security policies with fewer human programming errors.

REDUCED RISK
Contain threats with end-to-end segmentation of users, applications and WAN services.

BETTER COMPLIANCE
Segment applications and data to help maintain compliance with regulatory mandates like PCI and HIPAA.

GREATER IP ADDRESS USABILITY
Support overlapping IP address ranges in different segments.

AGILITY AND SCALABILITY
Easily configure multiple end-to-end segments spanning the LAN/WAN/Data center or LAN/WAN/Cloud.

Conclusion

The unified stateful zone-based firewall within EdgeConnect addresses the security requirements of most branch offices. End-to-end segmentation and security policy enforcement introduces no additional latency in the data path and has no impact on application performance.

By combining routing, firewall, segmentation, virtual routing and forwarding (VRF), optional WAN optimization, application visibility and control and SD-WAN in a single solution, EdgeConnect can greatly simplify branch WAN edge architecture. A centralized, automated architecture is inherently more robust and reliable than one that relies on traditional, fragmented, site-by-site manual configuration. In addition to consistent end-to-end security policy enforcement spanning the LAN, WAN, data center and cloud, enterprises can realize significant operational efficiencies through the centralized orchestration of all essential wide area network functions from a single pane of glass.

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-END-TO-END-SEGMENTATION-091620