SOLUTION OVERVIEW

Local Internet Breakout

Why it is imperative that service providers deliver the best possible user experience for cloud-hosted applications

Silver Peak was acquired by Aruba, a Hewlett Packard Enterprise company, in 2020. You may see references to Silver Peak in this document.

Enterprises continue to migrate applications to the cloud. In fact, it is estimated that 92%[1] of enterprise workloads are use multi-cloud, i.e. multiple public and private cloud services and platforms to support their ever-expanding application requirements.

In today's cloud-first world where SaaS and IaaS become extensions of the enterprise network, it is critical for the business to reach these cloud services by the most efficient and highest performing means. Frequently, cloud applications perform better from home than from the branch. The router-centric model employed at branch offices backhauls web-bound traffic to headquarters-based security infrastructure such as next generation firewalls and IDS/IPS solutions to protect the branch from vulnerabilities. Backhauling traffic adds latency which negatively impacts application performance.

An unmanaged broadband internet connection delivers higher band- width and direct access for all cloud applications (direct to net). However, applications require different quality of experience and security considerations. Service providers are challenged to offer services that control the traffic to applications hosted in the cloud with a managed secure local internet breakout solution. Not all local internet breakout solutions include the ability to enforce application-specific security policies in real-time, and not all solutions provide daily SaaS/IaaS IP address updates to keep pace with the dynamically changing nature of cloud applications.

With the right solution, service providers can offer the best SaaS and IaaS performance while optimizing underlying network resources, and ultimately, guarantee a superior user experience at lower cost.

SERVICE PROVIDER CHALLENGES

- **Securing "untrusted" broadband** Difficult to offer local internet breakout without exposing branch users and their local networks directly to the internet and its myriad threads
- **Application traffic steering based on business intent** Unable to granularly steer traffic to a specific destination based on the application type
- **Lack of integrated security and application policy administration** Manual provisioning and configuration on every appliance is complex and error-prone

SOLUTION

- **Simplified, integrated application- driven security** An application-driven SD-WAN solution extends micro-segmentation across the WAN to enable differentiated QoS and security policies for different applications
- **Granular traffic steering based on application classification and cloud intelligence** Intelligently traffic steer on the first packet to the correct SD-WAN overlay based on predefined application-driven business and security policies
- **Centralized security policy administration and automated updates**
- **Aruba Orchestrator** Ensures consistent, unified policies across applications and predictable application performance for multi-tenant environments

[1] Flexera 2021 State of the Cloud Report

SERVICE PROVIDER CHALLENGES

Service providers want to deliver the best possible user experience for cloud-hosted applications and must address the following challenges:

- **Securing "untrusted" broadband** – Local internet breakout exposes branch users and their local networks directly to the "untrusted" broadband internet and potentially to its myriad threats. Service providers that support broadband internet services as an SD-WAN connectivity option must support granular service policies that can restrict application traffic to certain outbound destinations and enforce granular security policies.
- **Application traffic steering based on security policies** – Not all web traffic is equal, and security policies must enforce different security policies. For example, a security policy might specify sending trusted traffic directly to the internet while redirecting untrusted traffic to a security web gateway, cloud-hosted security service or next generation firewall. To implement such policies, web traffic must be granularly steered to its correct destination based on the application. This requires identifying the application on the first packet; once a destination has been selected for a given flow, it cannot be changed without restarting the session.

  Existing application classification techniques using a combination of well-known IP addresses, port numbers and Deep Packet Inspection (DPI) are unable to consistently enable granular traffic steering to a specific destination based on the application. A security policy might work when initially configured but might fail when the SaaS application IP addresses change.

  A managed SD-WAN service offering must be able to dynamically secure applications based on defined policies whether the applications are hosted in public or private clouds.
- **Lack of integrated security and application policy administration** – Traditional security architectures in branch offices 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.

  Service providers offering a managed network security service, are required to provision, monitor and update security policies on individual security appliances for any new application. This manual configuration process is lengthy, cumbersome, costly and prone to human error.

Service Provider Solution Requirements

As service providers assess the challenges of delivering the highest SaaS and IaaS performance to their customers, they need to evaluate and consider the following requirements for enabling local internet breakout:

- Support granular, application-driven security policies (IPsec, TLS) for all applications over broadband internet
- Automate application visibility for classifying trusted and untrusted applications based on enterprise security requirements and policies
- Optimize performance, without compromising security, with granular application traffic steering and optimal traffic delivery
- Enforce security with an integrated firewall to protect the branch from incoming threats and that will enforce granular security policies
- Centralize security and policy management easy integration with any service provider's service
- orchestration platform
- Enable service chaining to complementary network security solutions like next generation firewalls and secure web gateways

ARUBA EDGECONNECT LOCAL INTERNET BREAKOUT SOLUTION

A Secure, Adaptive Application- driven Internet Breakout

Different applications often require different treatment when it comes to how they are handled from a security perspective. For example, a major financial application processing a sensitive transaction 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 base managed SD-WAN services on an application-driven SD-WAN solution, where policies and configuration settings can be implemented on a per-application basis.

Aruba EdgeConnect utilizes a virtual WAN overlay model and enforces end-to-end micro-segmentation to enable differentiated treatment – including security policies and controls – for different applications. For example (Figure 1), a security policy might be defined as follows:

- Send all known, trusted business SaaS traffic directly to the internet
- Send "home from work" recreational applications to a secure web gateway service or cloud-hosted security service such as Zscaler, Netskope, Forcepoint, McAfee or Symantec
- Send all untrusted, suspicious and unknown traffic to a hub or headquarters-based next-generation firewall from Palo Alto, Fortinet or Check Point

An integrated zone-based stateful firewall is essential for a complete, secure local internet breakout solution enabling direct internet connectivity to trusted SaaS applications and IaaS from branch offices. The EdgeConnect zone-based firewall further hardens the enterprise WAN by blocking unwanted or unauthorized traffic attempting to enter the branch network from the enterprise LAN.

EdgeConnect supports simplified service chaining, using a drag-and-drop interface, to enable service providers to automate and accelerate the integration of security partners' advanced firewall services (e.g. Check Point, Fortinet, Palo Alto Networks) secure web gateways (e.g., Zscaler, McAfee, Symantec, Netskope, Forcepoint and secure DNS (e.g., Infoblox) utilizing private secure encrypted IPSec tunnels.

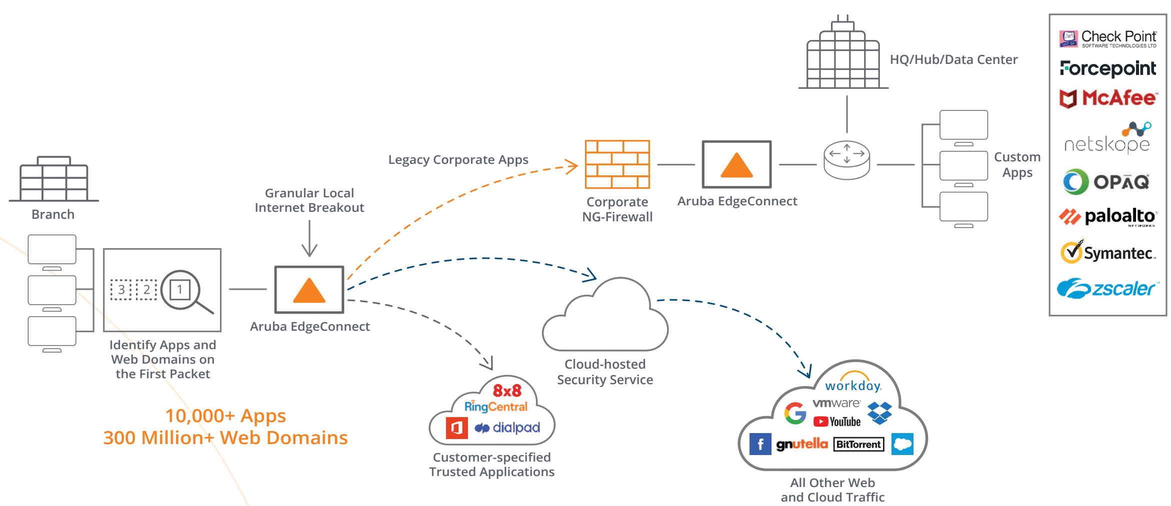

Figure 1: Granular traffic steering requires application identification and classification on the first packet.

Granular Traffic Steering Based on Application Classification and Cloud Intelligence

As described previously, not all web applications are created equal and they require different application-specific security policy enforcement in accordance to security policies. To enforce those policies, traffic must be classified and steered appropriately on the first packet.

Aruba first-packet classification technology (First-packet iQ™) enables EdgeConnect to intelligently traffic steer on the first packet to the correct SD-WAN overlay based on predefined application-driven business and security policies and across the underlying WAN circuits utilized by that overlay. The overlays may be configured with a built-in zone-based stateful firewall that is included in the EdgeConnect[SP] SD-WAN solution plus the option to service chain with third-party security appliances for additional traffic inspection. Application-specific Business Intent overlays (Figure 2) may also be defined to enable micro-segmentation across the SD-WAN to help organizations meet compliance mandates.

First-packet iQ uses Cloud Intelligence to maintain an up-to-date database of IP addresses used by SaaS applications. In addition, automated daily updates of the application IP address database to EdgeConnect appliances keep pace with dynamic SaaS and web address changes.

The solution eliminates the potential for wasted bandwidth and performance bottlenecks for trusted SaaS and web traffic. Trusted traffic gets treated appropriately while questionable traffic is automatically sent to more robust security appliances in accordance with corporate security policies.

For branch sites not served by internet connections or if corporate security policies require backhaul of SaaS applications for additional security screening, Aruba Cloud Intelligence includes information to help the service provider optimally route traffic for the best performance.

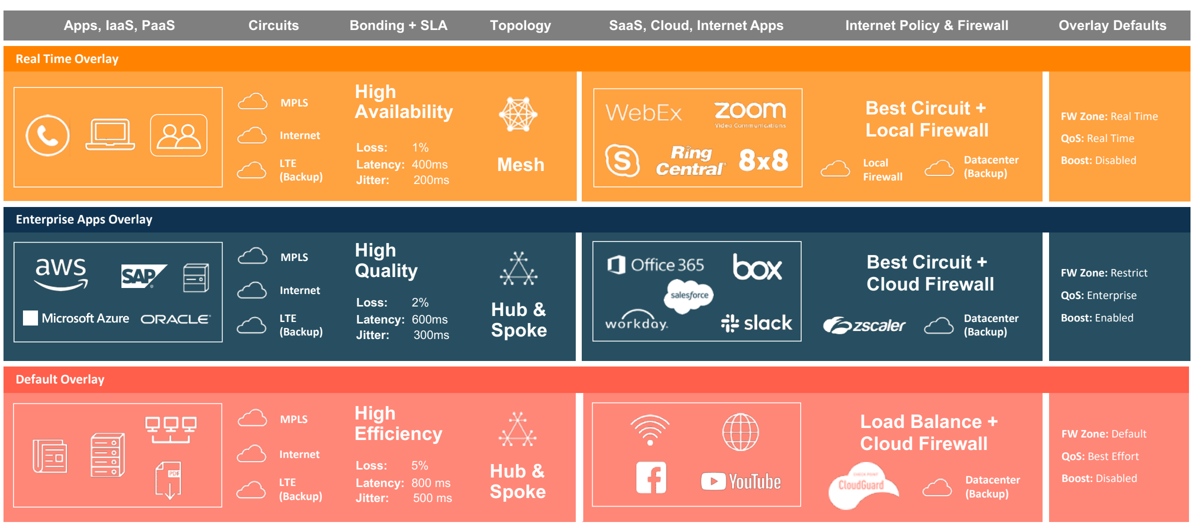

Figure 2: Application-driven, Business Intent Overlay SD-WAN policies enable differentiated treatment, including security policies and controls for different applications.

Centralized Security Policy Administration and Automated Updates

A key benefit of a comprehensive SD-WAN solution is simplified, centralized orchestration.

Aruba Orchestrator[SP] (Figure 3) empowers service providers to centrally define and orchestrate granular security policies and create secure end-to-end zones across any combination of users, application groups and virtual overlays, automatically pushing configura- tions to sites in accordance with business intent.

This accelerates application deployment and provisioning while reducing errors, ultimately enforcing granular security across the LAN and WAN and increasing operational efficiency.

Additionally, EdgeConnect appliances and Orchestrator can be fully managed and integrated with service provider OSS/BSS and/or northbound orchestration systems with REST APIs. Any feature or capability that is available on the Orchestrator GUI is available via REST APIs.

Benefits and Business Outcomes

Service providers have an opportunity to offer enterprises an application migration strategy to securely connect to cloud services, as enterprises increasingly adopt a “cloud-first” SD-WAN architecture. Service providers need to provide the highest levels of SaaS application and IaaS performance to retain and grow their managed services. The tangible benefits and business outcomes for service providers are:

- Deliver increased enterprise SaaS application and IaaS performance and availability
- Improve service agility with flexible security control and policy management that can be easily integrated into any service providers’ service orchestration platforms via open APIs
- Enable comprehensive integration of managed SD-WAN and managed security services
- Drive customer retention enabling optimization of cloud connectivity to any SaaS provider
- Enhance MPLS services and solutions by breaking out internet traffic locally at the branch
- Increase customer loyalty by enhancing their business productivity, user experience and competitiveness

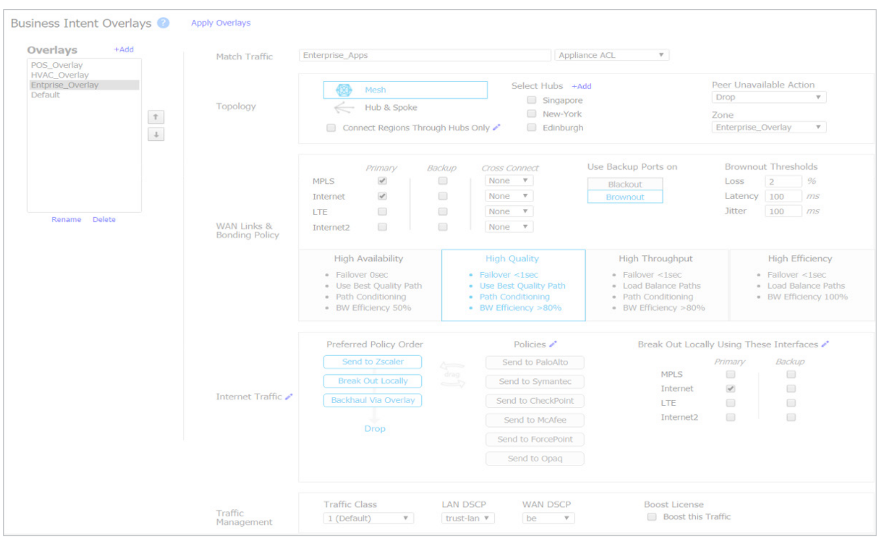

Figure 3: Aruba Orchestrator – simplified drag-and-drop policy assignment and service chaining.

a Hewlett Packard Enterprise company

SO_LocalInternetBreakout_102221 a00118989enw

Contact Us