BUSINESS PAPER

a Hewlett Packard Enterprise company

Architecting a secure business-driven SD-WAN

LEARN HOW THE ARUBA EDGECONNECT ENTERPRISE SD-WAN PLATFORM DELIVERS UNMATCHED PROTECTION ACROSS THE CLOUD-CONNECTED ENTERPRISE WAN

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Software-driven wide area networks (SD-WAN) are enabling today's geographically distributed enterprises to realize the transformational promise of cloud computing, reduce capital and operating costs, provide the highest quality of experience for employees and customers, and adapt quickly to changing business requirements.

But cloud computing and business-first networking introduce new security challenges. These include:

- Users connecting from anywhere and from any device
- Increasing cybersecurity risks
- More sensitive data hosted in the cloud
- Proliferation of IoT devices increasing the attack surface
- Complying with regulations and industry standards

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. By segmenting networks into zones that span LANs and WANs, SD-WANs isolate traffic, and minimize the attack surface to help compliance with industry standards.

This paper discusses why enterprises are embracing SD-WAN platforms at an accelerating pace, and how a comprehensive SD-WAN security deployment can better safeguard today's dynamic, cloud-first enterprises. It then goes on to reveal the extensive set of security capabilities incorporated in the Aruba EdgeConnect Enterprise Software Defined WAN (SD-WAN) platform.

Network security in the cloud era

85% of organizations will embrace a cloud-first principle by 2025.

Gartner 2021[1]

As more applications and workloads migrate to the cloud, the role of the corporate data center has been significantly reduced. The security perimeter is also dissolving as users connect from anywhere and from any device, accessing sensitive data hosted in the cloud.

Organizations that try to manage WANs using traditional routers are faced with continual compromises and trade-offs. Manual processes and complex architectures prevent organizations from establishing a secure architecture and effectively respond to malicious threats such as denial of service (DoS) attacks. Security concerns can hamper the use of low-cost broadband connections and slow the move toward the cloud in general, and SaaS applications in particular.

The impact of these changes is that enterprise WAN architecture must change too. In August 2019, Gartner defined "Secure Access Service Edge" (SASE) as the combination of advanced WAN edge network capabilities with network security functions such as SWG, CASB, FWaaS, and ZTNA delivered in the cloud. A SASE architecture brings a more secure and flexible way to connect to cloud-hosted applications by not backhauling application traffic to a data center before forwarding it to the cloud. With a SASE architecture, the SD-WAN can steer application traffic directly to a trusted SaaS provider or first to a cloud-hosted security service where more advanced security inspections can be performed before forwarding to the SaaS provider, all according to enterprise security policies

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-based apps. Key shortcomings include the negative impact they have on performance (especially for internet or cloud-destined traffic), the high cost of such network services and architectures, and the fact that they require to maintain a myriad of security equipment in branch locations.

[1] Gartner Says Cloud Will Be the Centerpiece of New Digital Experiences, November 2021

The proliferation of Internet of Things (IoT) devices has become another major concern for organizations, significantly increasing the attack surface. Based on a simple design, these devices usually cannot host a security agent, and therefore they cannot be easily protected. Organizations require a different security solution for IoT devices to protect their networks from potential vulnerabilities that could breach the network. That's why SASE must be complemented with a zero trust, identity-based access control security framework, segmenting traffic so that users and IoT devices can only reach network destinations consistent with their role in the business.

WHY SD-WAN IS CRITICAL TO SECURITY

Strong security is a prerequisite and integral element of many of the benefits of a business-driven SD-WAN. 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.

BACKHAULING AND LOCAL 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 application traffic 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, 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).

Although local internet breakout is essential for enhancing performance and reducing the bandwidth needed for backhauling, it also exposes branch users and their local networks directly to the internet and its myriad of 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 could be defined as follows:

- Send known, trusted business SaaS traffic such as Microsoft 365 and Unified Communications-as-a-Service (UCaaS) directly to the internet.
- Send enterprise data center-hosted application traffic directly to headquarters.
- Send all untrusted, suspicious, and unknown web traffic (for example, peer-to-peer network traffic and traffic from countries in which the company does not do business) to a cloud-hosted security service.

To implement such a policy, web traffic must be steered granularly to its intended 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.

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 Aruba SD-WAN platform. 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.

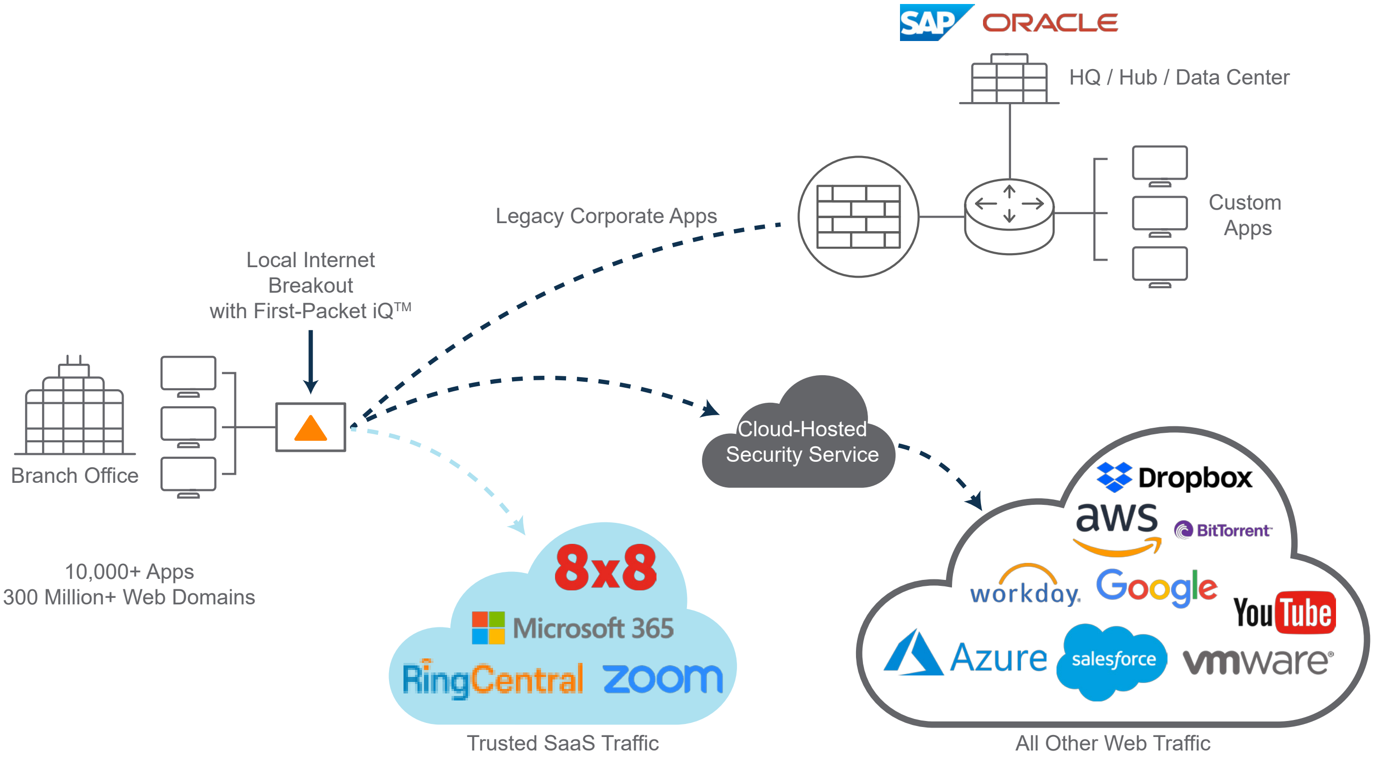


Figure 1. Application traffic is identified on the first packet to steer traffic to its correct destination to enable granular security policy enforcement.

INTRODUCING ARUBA EDGECONNECT ENTERPRISE

The Aruba EdgeConnect Enterprise SD-WAN platform provides enterprises with the flexibility to use any combination of transport technologies — including public broadband services — to connect users to applications without compromising application performance or security. The four main components of the platform include:

- Aruba EdgeConnect Enterprise zero-touch physical or virtual appliances, which are deployed at an organization's branch offices, central sites, and cloud data centers
- **Aruba WAN Orchestrator**, a centralized management system that enables simplified configuration and orchestration of the entire WAN and provides complete observability 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
- **Aruba WAN Boost**, an optional WAN optimization performance pack that enables IT teams to engage market-leading WAN optimization capabilities, where needed, simply by checking a box in the Orchestrator interface

- **Aruba Advanced Security**, an optional security license that enables intrusion detection and prevention functions (IDS/IPS) in Aruba EdgeConnect Enterprise appliances

Aruba EdgeConnect Enterprise is designed with an extensive set of capabilities to address all of the branch WAN edge security challenges and requirements inherent in SD-WAN implementations.

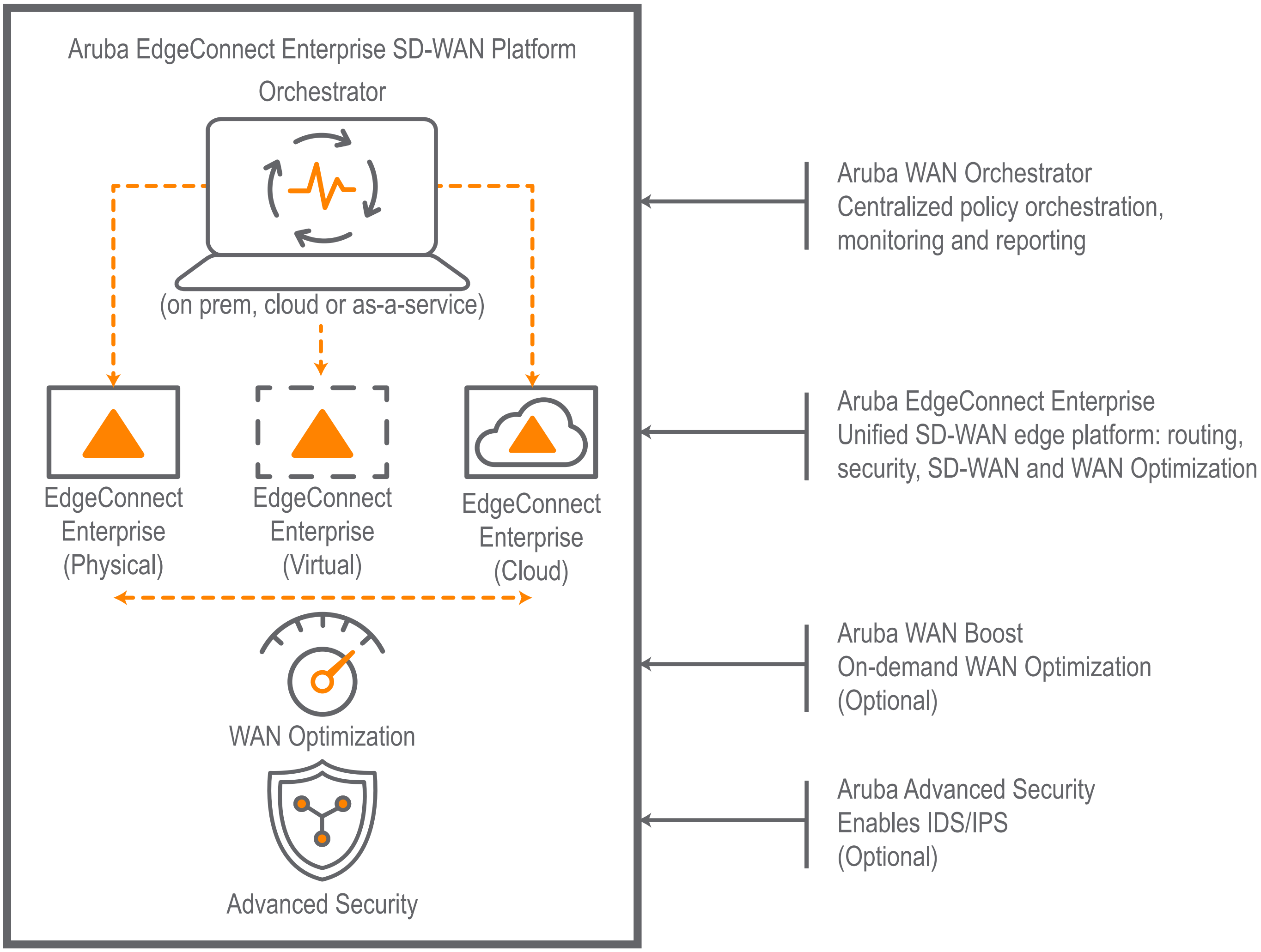

Aruba EdgeConnect Enterprise SD-WAN Platform
Orchestrator
(on prem, cloud or as-a-service)
EdgeConnect Enterprise (Physical)
EdgeConnect Enterprise (Virtual)
EdgeConnect Enterprise (Cloud)
WAN Optimization
Advanced Security
Aruba WAN Orchestrator
Centralized policy orchestration, monitoring and reporting
Aruba EdgeConnect Enterprise
Unified SD-WAN edge platform: routing, security, SD-WAN and WAN Optimization
Aruba WAN Boost
On-demand WAN Optimization (Optional)
Aruba Advanced Security
Enables IDS/IPS (Optional)

Figure 2. Aruba EdgeConnect Enterprise SD-WAN Platform

HOW ARUBA EDGECONNECT ENTERPRISE DELIVERS A SECURE SD-WAN

Aruba EdgeConnect Enterprise 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, integration with cloud-security partners to enable best-of-breed SASE, and compliance. The net result is the full-spectrum of protection needed for enterprises to fully realize the benefits of an advanced SD-WAN — enhanced application performance, lower overall WAN cost, and increased business agility — without being exposed to greater security risks.

APPLICATION-DRIVEN DATA PLANE SECURITY

Different applications deserve — or perhaps even require — different treatments 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 business application that is 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.

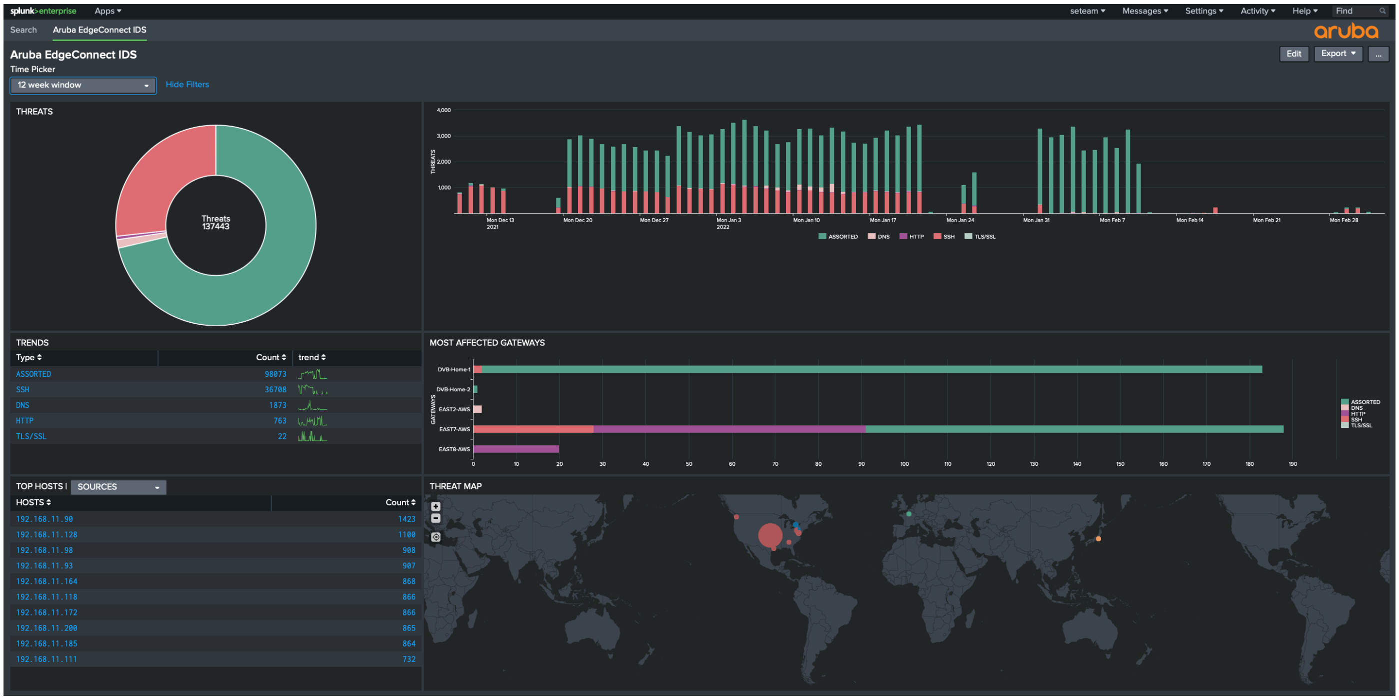
Relevant security capabilities available with Aruba EdgeConnect Enterprise include:

Next-generation Firewall: Aruba EdgeConnect Enterprise includes a next-generation firewall that provides in a single entity, advanced security features such as deep packet inspection, intrusion prevention, as well as application and user identity awareness. It gives IT leaders the ability to block malware from entering the network based on application, identity, and context, regardless of the port/protocol used. Additionally, IT leaders benefit from an increased visibility into network activity and potential risks.

Intrusion Detection and Prevention (IDS/IPS): Aruba EdgeConnect Enterprise integrates a rule-based Intrusion Detection and Prevention System (IDS/IPS) and utilizes the common Aruba Unified Threat Management (UTM) framework. The signature-based system monitors network traffic to find patterns that match a particular attack signature. Integrated with the EdgeConnect Enterprise next-generation firewall, the system allows application-level selection for inspection based on firewall zones and provide actions such as drop, inspect, and allow traffic when an intrusion is detected.

The system can operate either in strict mode or performant mode. In strict mode, the traffic passes through the sensor so that the traffic is immediately blocked when an intrusion occurs. In performant mode, a copy of the traffic is sent for analysis, providing more efficiency without impacting network performance. Using this mode, an intrusion is blocked after its detection. Depending on their security requirements, organizations can choose between the strict or performant modes.

Threat logging provides network and security analytics back to Aruba Central or a third-party SIEM such as Splunk to monitor threats in real time. The Aruba EdgeConnect Security App for Splunk provides a dashboard view of all security event notifications exported from EdgeConnect devices within an enterprise’s SD-WAN. IT managers can easily configure EdgeConnect to forward all security event notifications to Splunk, centralizing logging, visualization, and analysis of security events alongside other telemetry or network events. From Splunk, users can filter, sort, navigate and view the collective security event notifications generated across the entire SD-WAN fabric, overall trends, and top talkers to help them pinpoint network events that require further investigation.



Aruba EdgeConnect IDS

Time Picker: 12 week window

Hide Filters

TRENDS

Type	Count	trend
ASSORTED	98073	
SSH	36708	
DNS	1873	
HTTP	763	
TLS/SSL	22	

TOP HOSTS | SOURCES

HOSTS	Count
192.168.11.90	1423
192.168.11.128	1100
192.168.11.98	908
192.168.11.93	907
192.168.11.164	868
192.168.11.118	866
192.168.11.172	866
192.168.11.200	865
192.168.11.185	864
192.168.11.111	732

Figure 3. Splunk security dashboard

DDoS Defense: With the rising frequency of distributed denial-of-service (DDoS) attacks, it is imperative that organizations establish cost-effective defenses for any and all sites that might be affected. With EdgeConnect deployed at branch locations, that's precisely what you get. In the event of a DDoS attack, EdgeConnect limits the number of malicious requests with actions such as rapid aging, drop excess and block source.

Actions are based on preset or configurable DoS thresholds set for traffic parameters including flow rate, concurrent flows, and embryonic flows. Additionally, the solution can dynamically route the traffic over unaffected network links in case of a DDoS attack with no degradation to application performance or impact to SD-WAN manageability. EdgeConnect protects not only itself, but also protects all of the users and systems both on the local network and over the remaining, operational WAN connections.

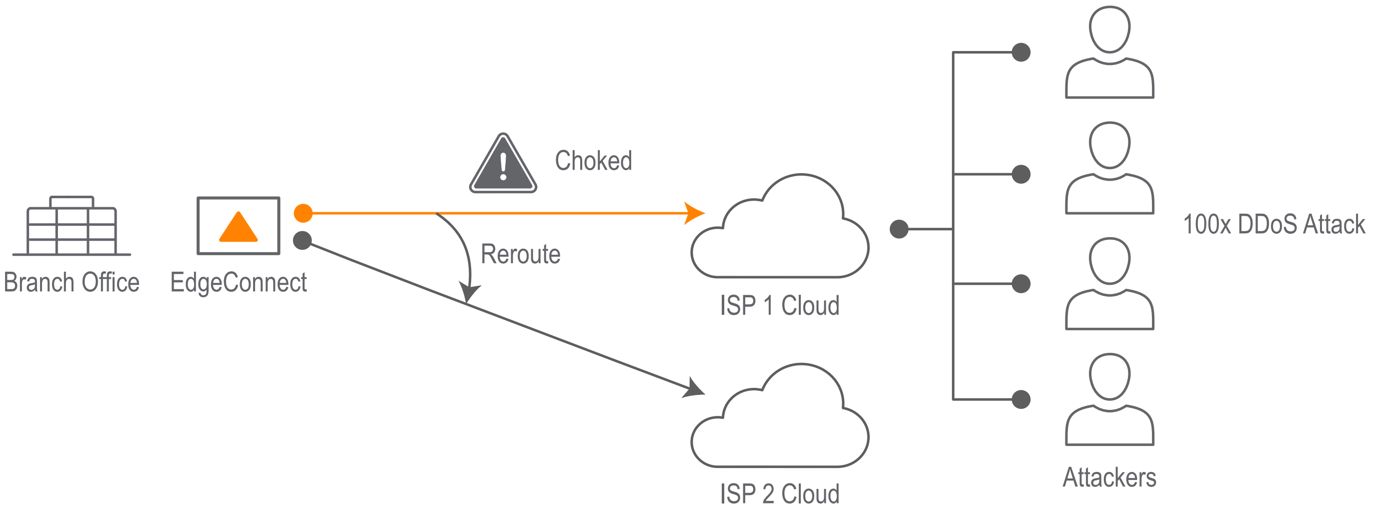


Figure 4. EdgeConnect Enterprise protects the SD-WAN from DDoS attacks and routes traffic across an alternate transport service to keep applications running, enhancing business continuity.

Data-in-Transit Protection: Each EdgeConnect data path is protected by IPsec tunnels that use AES 256-bit encryption to maintain application and data confidentiality. EdgeConnect uses an "IKE-less" IPsec UDP protocol; that is, it employs standards-based IPsec UDP encryption but doesn't require Internet Key Exchange pre-shared keys. Encryption keys are never repeated and are directionally unique. Aruba WAN Orchestrator manages the encryption keys and rotations automatically, which reduces tunnel setup time without a loss of service. This protocol avoids problems encountered when deploying NAT (Network Address Translation) with IKE, such as failures when branch offices have multiple devices with different VPN requirements. Because IKE-less tunnels use different ports over IPsec, they are unlikely to be limited or blocked by upstream firewalls. These advanced features for protecting data in transit increase the flexibility, security, and robustness of secure communication between remote endpoints.

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

Zero-trust segmentation: Aruba EdgeConnect Enterprise creates secure end-to-end zones across any combination of users, devices, application groups and virtual overlays, propagating configuration updates to sites in accordance with business intent. Paired with Aruba ClearPass Policy Manager, Aruba EdgeConnect enforces a zero-trust architecture that dynamically segments the network and applies least privileged access principles. It ensures that users and devices only communicate with destinations consistent with their role based on identity, access rights, and security posture.

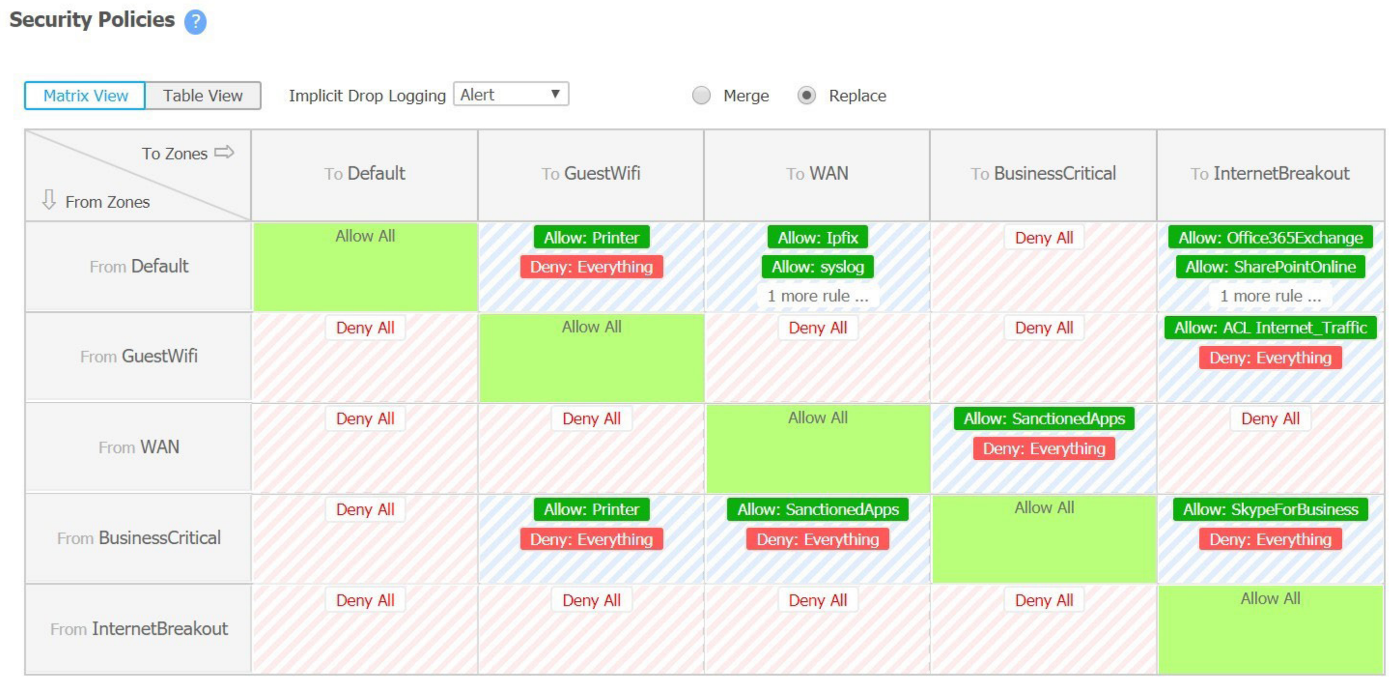
Additionally, Aruba EdgeConnect Enterprise allows organizations to create multiple application-specific virtual WAN overlays (also called business intent overlays). Each virtual overlay specifies priority and quality of service requirements for application groups based on business requirements. Using these specifications, EdgeConnect automates traffic steering end-to-end across all underlying WAN transport services.

Each virtual overlay is mapped to a LAN-side zone or zones. A zone may be comprised of VLANs, physical and logical interfaces, and sub-interfaces. Each zone can be assigned security policies that limit connectivity with other zones. For example, a policy could allow only outgoing traffic, or allow incoming traffic only from approved applications and services or block all traffic from less secure zones.

With zero-trust segmentation:

- Users and IoT devices access resources based on role and context using least privileged access principles
- Traffic within each zone is isolated from traffic in other segments, reducing unauthorized access and limiting the scope of incidents
- Micro-segmentation is extended from the LAN, across the WAN, and to data centers and cloud platforms
- High-priority applications enjoy faster, more reliable performance across the WAN, increasing application availability and improving the experience and productivity of end users

Simple policy creation: IT administrators can create network segments in minutes using an intuitive graphical user interface. These segments can connect LANs with other LANs (LAN-WAN-LAN) and with data centers (LAN-WAN-data center). The virtual WAN overlays are defined based on business requirements and intent, not infrastructure details like IP addresses. Zone-based security policies are displayed in a configuration matrix that makes them easy to understand.



Security Policies ?

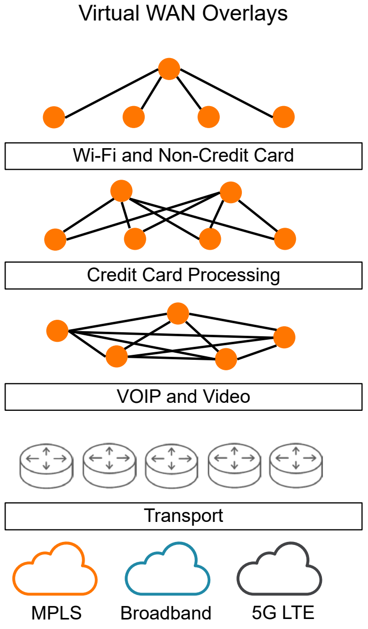
Matrix View | Table View   Implicit Drop Logging: Alert ▼   ○ Merge ● Replace

To Zones ⇨ / ⇩ From Zones	To Default	To GuestWifi	To WAN	To BusinessCritical	To InternetBreakout
From Default	Allow All	Allow: Printer Deny: Everything	Allow: Ipfix Allow: syslog 1 more rule ...	Deny All	Allow: Office365Exchange Allow: SharePointOnline 1 more rule ...
From GuestWifi	Deny All	Allow All	Deny All	Deny All	Allow: ACL Internet_Traffic Deny: Everything
From WAN	Deny All	Deny All	Allow All	Allow: SanctionedApps Deny: Everything	Deny All
From BusinessCritical	Deny All	Allow: Printer Deny: Everything	Allow: SanctionedApps Deny: Everything	Allow All	Allow: SkypeForBusiness Deny: Everything
From InternetBreakout	Deny All	Deny All	Deny All	Deny All	Allow All

Figure 5. A security policy configuration matrix greatly simplifies the creation and management of segmentation rules.

Central orchestration and automated enforcement: Once virtual WAN overlays and zone-based firewall policies have been defined, Orchestrator deploys them to all EdgeConnect SD-WAN appliances, where they are automatically enforced. This replaces the time-consuming manual configuration of routers and firewalls every time a policy changes. The benefits include:

- Consistent security policy enforcement across LANs and WANs
- Fewer configuration errors
- Improved compliance with regulations and industry standards
- Increased productivity for security and operations staffs



Access Policy	Topology	Connection	QoS
Guest VLAN	Hub Spoke	Internet	Min. Cost
Data VLAN	Dual Hub and Spoke	MPLS – Internet	Max. Availability
Voice VLAN	Full Mesh	MPLS – Internet – LTE	Max. Quality

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

INTEGRATION WITH BEST-OF-BREED SASE PARTNERS

With the continuously evolving threat landscape, organizations must take a best-of-breed approach toward security. It is simply not realistic for a single SASE vendor to do everything on its own and truly deliver best-in-class network and security technologies across a single platform. It may require compromises that organizations cannot afford at a time when cybersecurity has become a major concern. Plus, most organizations already have an existing set of security tools in which they've made a considerable investment.

Gartner indeed stated in a report[2] that: *"Choosing a single-vendor SASE solution is challenged by the lack of solutions that offer "best of breed," and for many enterprises, not even "good enough"' functionality across all of SASE's functional domains."*

Aruba EdgeConnect can seamlessly connect to a variety of best-in-class cloud security services, to deliver a best-of-breed SASE architecture. Aruba maintains technology partnerships with leading SSE (Security Service Edge) vendors covering solution areas such as secure web gateways (SWG), cloud access security broker (CASB), zero-trust network access (ZTNA) and remote browser isolation (RBI) from security companies like Zscaler, Netskope, Check Point, McAfee, Palo Alto Networks and Symantec.

By offering the freedom of choice to integrate best-of-breed SASE, Aruba EdgeConnect Enterprise prevents organizations from being locked-in to proprietary single vendor solutions or having to settle for basic features and capabilities.

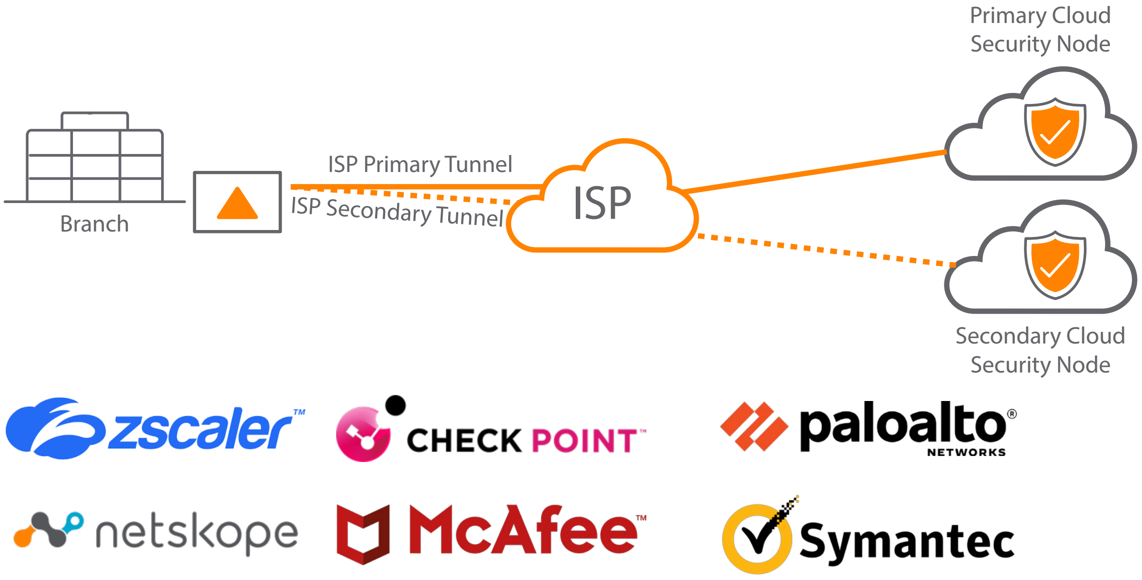


Figure 7. Automate service orchestration with best-of-breed cloud-security vendors

Automated integration and orchestration: To more closely align with the ease-of-use and flexibility objectives of today's organizations, EdgeConnect automates the orchestration with third-party cloud security (SSE) vendors, and the configuration of IPsec tunnels between EdgeConnect and SSE vendors. With this capability, First-packet iQ™ application classification feature first identifies applications and web domains based on the first packet. The traffic is then intelligently steered to SSE services based on security policies defined by the organization. Administrators can also take advantage of a simple drag-and-drop interface that makes it easy to assign policies to traffic from specific applications and to route the traffic to specific security tools. For example, an internet-bound traffic is automatically routed through cloud-based security services for Layer 7 access control, threat filtering, and analytics.

[2] How to Align SD-WAN Projects with SASE Initiatives, Gartner April 2022

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 Aruba EdgeConnect Enterprise 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 Aruba Cloud portal and then "approved" by an IT administrator using Aruba 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 Aruba cloud portal, and administrators' web browsers are protected with TLS 1.2. Furthermore, all weak protocols (e.g., SSLv2, SSLv3, TLS 1.0, TLS 1.1), weak hashes (e.g., MD5), and weak encryption algorithms (e.g., DES, RC4) are disabled by default.

System Hardening: EdgeConnect is a hardened appliance that ships with the factory default "harden" mode. This approach ensures out-of-the-box security for appliances plugged in for the first time."

Subsequently, on zero touch provisioning and configuration, a strong password per standard FIPS 140-2 guidelines is always enforced on the appliance. This prevents malware from using default passwords to gain unauthorized access to the appliance. All non-essential management services like SSH, FTP are closed by default.

Other management plane protections include:

Robust user authentication and authorization

- Support for local, RADIUS, TACACS+, and Oauth for authentication and authorization with identity management systems such as Active Directory and Okta.
- Granular role-based access control with read-only users and multiple administrator roles
- 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)
- Firewall logs — traffic flows inspected by the EdgeConnect next-generation firewall generate deny, accept, and drop events, as well as reasons for those events. Firewall logs can then be streamed to a third-party SIEM tool (e.g., Splunk).
- Netflow/traffic logs — for capturing full (non-sampled) flow data so that it can be streamed to a third-party tool (e.g., Netflow-collector)

In addition to being critical for network management and incident response, log data can be valuable for complying with standards such as HIPAA.

SECURITY CERTIFICATION AND COMPLIANCE

As users connect from anywhere using connections that are inherently insecure such as broadband internet and 5G, and access sensitive data online, the need to certify an SD-WAN for security has become more pressing. Aruba EdgeConnect Enterprise has earned the ICSA Labs Secure SD-WAN certification based on a comprehensive and robust set of SD-WAN functionality and platform security requirements.

ICSA Labs Secure SD-WAN certification requirements include:

- **Advanced SD-WAN features** such as tunnel bonding, dynamic path selection and zero-touch provisioning
- **Native support (or via service chaining) for advanced security** functions such as anti-malware, intrusion prevention and DoS protection
- **Encryption** of sensitive data, as well as administrative and operational communications
- **Policy enforcements** for both WAN-specific functions and security policies
- **Security events logging**

With the assurance of using a secure SD-WAN, certified by a globally recognized independent, third-party organization, enterprises can simplify network architecture in branch locations by replacing branch firewalls with Aruba EdgeConnect Enterprise.

Last, but not least, there are many ways Aruba EdgeConnect Enterprise 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), Sarbanes-Oxley Act (SOX), the European Union GDPR, 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[3].

Most of the security features covered so far 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 support for micro-segmentation. The ability to create encrypted, application-specific overlays can help IT teams control access to systems that store and process electronic private health information (ePHI) to support HIPAA compliance, segment off credit transactions and associated systems to substantially reduce the scope of their PCI DSS compliance efforts and reduce the risk of unauthorized access to information about customers to meet GDPR and other privacy rules.

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 the Aruba EdgeConnect Enterprise SD-WAN platform go well beyond the minimum-required level of protection afforded by transport-level encryption and message authentication.

Thanks to its advanced SD-WAN capabilities paired with the highest security features like IDS/IPS and DDoS protection, EdgeConnect Enterprise has earned the secure SD-WAN certification from ICSA Labs. This certification allows organizations to improve security in branch locations and accelerate compliance to regulations or security frameworks such as NIST CSF, HIPAA and PCI DSS.

By combining an SD-WAN featuring robust data and management plane security with leading cloud-delivered security partnerships, supported by automated integration and orchestration, EdgeConnect Enterprise enables a best-of-breed SASE architecture that meets the security requirements of today's cloud-first organizations. With the increasing use of IoT devices, EdgeConnect complements SASE with a zero-trust architecture to segment the network based on identity so that users and IoT devices can only reach network destinations consistent with their role in the business.

[3] **For details on FIPS certification status, click here.**

aruba
a Hewlett Packard
Enterprise company

BP_SecureBusiness-DrivenSD-WAN_RVK_083122 a00126522enw

Contact us at www.arubanetworks.com/contact