Aruba Software Defined Branch Solution Validation and Performance Assessment

February 2020

DR191218C

Miercom

Miercom.com

Contents

1.0 Executive Summary

Software Defined Wide Area Networks (SD-WAN) help simplify, optimize and control multiple local branch office deployments of a corporate network or data center. Traditionally, networks used a centralized Virtual Private Network (VPN) management architecture over Multiprotocol Label Switching (MPLS), T1/ T3, Broadband or Cellular (4G/LTE) links to connect branch offices across the WAN. However, there are also challenges related to the Local Area Network (LAN), particularly with the large increase in client devices. This leads to issues of segmentation and management in the branch LAN.

The Aruba SD-Branch solution meets both WAN and LAN challenges head on with unified management, monitoring, and security from Aruba Central Management. Aruba, a Hewlett Packard Enterprise Company, engaged Miercom to independently assess its SD-Branch solution for management, SD-WAN, SD-LAN and security features.

By subjecting the Aruba solution to a real-world deployment, Miercom engineers validated each feature using a custom methodology which focused on real-world use cases. Test results shown in this report prove how businesses can achieve higher performance, quality, control and visibility of their local and wide area networks, regardless of device count or geographical location by using Aruba SD-Branch.

The Aruba SD-Branch solution addresses not only common WAN challenges but also simplifies management of branch networks and cloud-based applications.

Key Findings of the Aruba SD-Branch Solution

- **Aruba Central Management.** Cloud-based single point management of LAN, WLAN and WAN delivers simple, secure communication to scale for thousands of branches. The SD-Branch solution maintains unified access roles and policies for cohesive deployment beyond traditional SD-WAN, by creating an overlay network over the MPLS network, and saving time and effort even for the long-term as the network expands.
- **Simplified Deployment.** Automatic device detection and provisioning options make setting up the branch network quick and simple. Zero-Touch Provisioning (ZTP) or One-Touch Provisioning (OTP) eliminates needs for costly, error-prone user interaction with configurations and access policy rules. The Aruba Installer application scans devices to automatically onboard with device-specific configurations.
- **Automated SD-WAN Orchestration.** Web native, horizontally scalable multi-tenant tunnel and route orchestration that can scale to very large networks while providing simplicity. Automatically creates and sets up IPsec tunnels between gateways, building the SD-WAN overlay. Routes are automatically learned and distributed from the SD-WAN Orchestrator to all gateways.

- **Dynamic Routing Policies.** Leverages awareness of application-based routing for enhanced visibility, orchestration and security for LAN and WAN. Route policy can be configured centrally, and Dynamic Path Steering (DPS) optimizes communications in real-time, regardless of transport, even during black-out and brown-out conditions.
- **Very High Gateway Performance.** Up to 1.3Gbps of encrypted throughput and 4Gbps of firewall throughput on the Aruba 7005 gateway (the smallest model for small businesses).
- **Cloud Provider Integration.** Aruba virtual gateways can serve as headends in public cloud infrastructure. In scenarios with multiple virtual private networks, a transit gateway can route traffic between multiple individual cloud regions.
- **Role-Based Policies**. Integrated with Aruba ClearPass Policy Manager, the gateway's built-in firewall provides consistent role-based enforcement across the LAN for IoT devices. Role-based policies are used not only to enforce security but also to define WAN policies. Automated security policies remove the need for manual configuration.
- **Unified Security.** Aruba branch gateways revolutionize how zero-trust is enforced in the branch. All network traffic within a branch is forwarded to gateways for deep packet inspection (DPI) using the built-in firewall or a third-party solution such as Zscaler. Aruba Dynamic Segmentation eliminates the need for numerous VLANs with a single VLAN deployment. This also adds the ability to isolate endpoints while also stopping any malicious activity. Security and forwarding policies can be applied to both north-south traffic and east-west traffic.

Based on our findings, the Aruba SD-Branch solution goes beyond traditional SD-WAN solutions by unifying LAN, WLAN and WAN with unique and impressive capabilities. Our results revealed Aruba SD-Branch to be a simplified approach for complex environments, making it a valuable purchase for branch network administrators. We proudly certify the Aruba SD-WAN solution as **Miercom Performance Verified**.

Robert Smithers

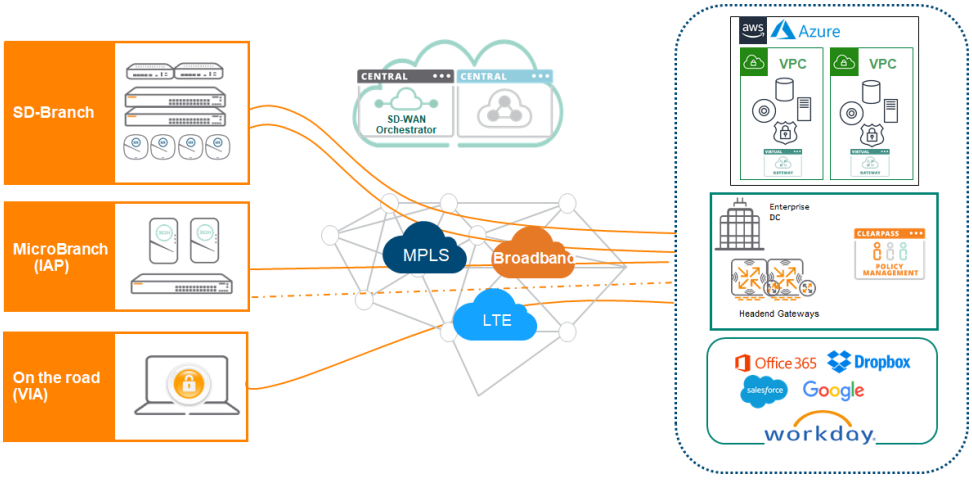
CEO, Miercom

2.0 Introduction

The Aruba SD-WAN solution incorporates Aruba Gateways for a robust SD-WAN architecture that is flexible for any sized branch environment.

Branch size types are as follows:

- **Small to Large Branches**: Branches that deploy a single or dual active gateway. Aruba offers a flexible portfolio of gateways from the 9004 that can handle 4Gbps of firewall and encrypted throughput, up to the 7240 that can handle 40Gbps throughput. The gateways can be deployed in branch sites or as headend gateways. At the data center, it's recommended to deploy the Aruba 7200 Series Gateway as the headend gateway, which can also be a virtual gateway (vGW).
- **Micro-Branch**: For micro-branches, Aruba provides an AP-based SD-WAN solution. In this deployment, a branch gateway is not required—an AP is used instead to establish secure IPsec connections with the headend.
- **Remote Branch**: Remote or travelling workers using Aruba Virtual Internet Access (VIA).



Source: Aruba, a Hewlett Packet Enterprise Company

Typical deployment topology of an Aruba SD-Branch site with Aruba BGWs, a micro-branch with Aruba APs, and VIA.

Aruba Central

Aruba Central is a cloud-based platform which simplifies deployment, management, service and security of wired, wireless and SD-WAN environments. The single-pane-of-glass interface features multiple tools that simplify deployment and management of a large system of devices and users with a quick onboarding process via Zero-Touch Provisioning, available through the Aruba Installer application.

Network operations can be streamlined and optimized using AI-based analytics, high availability features, automated configuration design, and granular visibility. The platform has been built from the ground up as a web-native, container-based solution designed to be fully horizontally scalable and multi-tenant with Service Provider (SP) or Managed Service Provider (MSP) support as foundational capabilities of the service.

Aruba SD-WAN Orchestrator

The SD-WAN Orchestrator uses a cloud-based, multi-tenant control plane for automatable scalability of growing business IT processes. Other SD-WAN solutions do not have automated scalability across the entire topology; they tend to be single-tenant solutions with manual scaling and are generally Virtual Machine (VM)-based control plane elements requiring costly and error-prone manual tunnel configurations when scaling to hundreds or thousands of locations.

Using SD-WAN Orchestrator, branches and headends automatically and rapidly set up overlay tunnels and exchange routes through an unlimited, elastic environment. And while other SD-WAN vendors take advantage of wizards, Aruba specializes in a sustainable coordination and scalability that saves administrators time and effort for the long-term.

Aruba ClearPass Policy Manager

Aruba ClearPass integrates with Aruba SD-WAN to provide enhanced profiling for appropriate rule enforcement, traffic isolation and protection against attacks. ClearPass provides visibility and dynamic, role-based control across all branch networks in real-time. Using ClearPass Policy Manager, roles and policies are set for all users and devices authenticated on the network.

Virtual Intranet Access (VIA)

The VIA client is part of Aruba's VPN services – a hybrid of IPsec and SSL VPN – that provides secure remote network device connectivity. Supported on Windows, Android, MAC OS X, Apple iOS and Linux, this feature automatically builds a secure connection to the corporate network directly from the end host. Thousands of remote users can access the network with user-friendly connectivity that uses the same role-based access policy framework as the local network.

Summary of Aruba Advantages

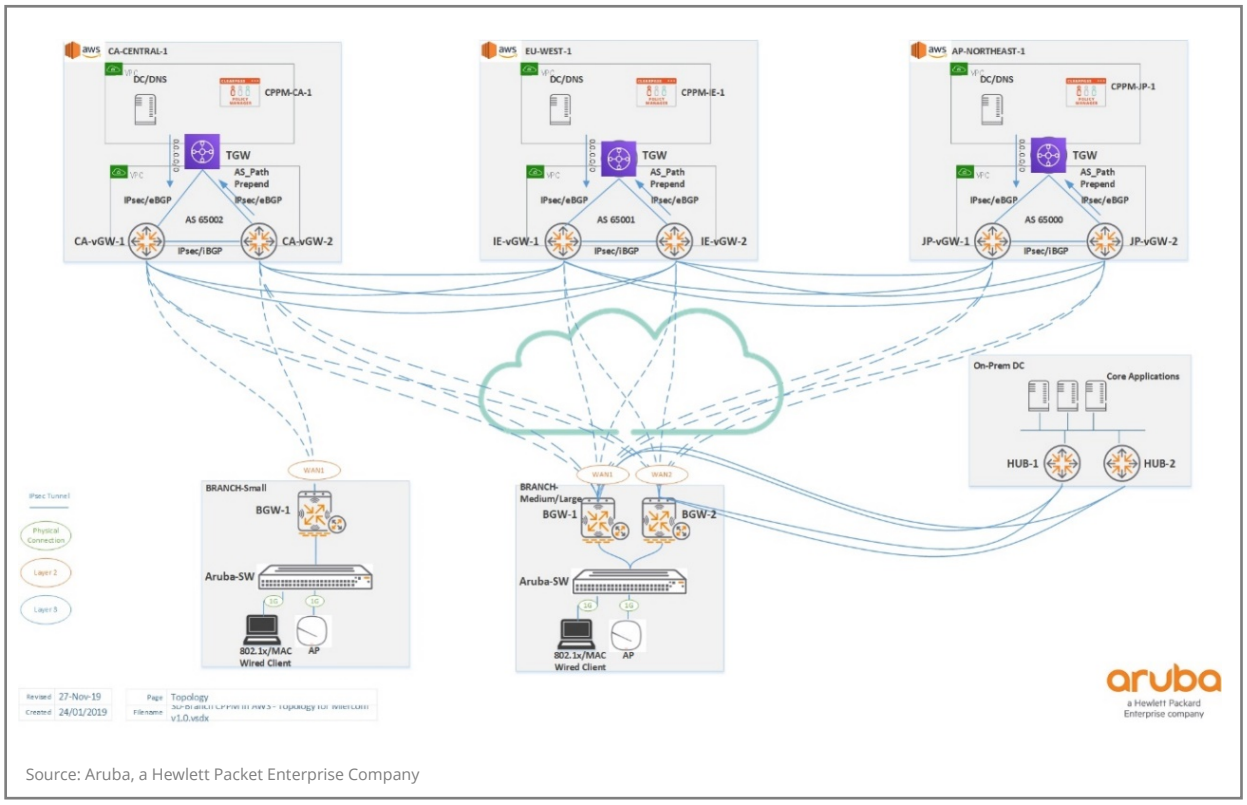
- Onboarding with the Aruba Installer application on Android and Apple iOS saves time and cost, as it can be done by any partner. A device can now be added in minutes rather than hours.
- Zero-Touch or One-Touch Provisioning automatically maps configurations for every infrastructure device. Eliminating manual provisioning reduces errors and makes deployment highly scalable – for up to thousands of branches. Administrators have a global network view at the WAN level and can then drill all the way down to a single device, client and application—all from a single pane of glass.
- Aruba SD-WAN Orchestrator supports complex overlay architectures by automatically building tunnels between all gateways in the network; the SD-WAN Orchestrator takes care also to dynamically distribute routing information learned from each branch or headend.
- Aruba Virtual Gateways along with SD-WAN Orchestration allows customers to easily extend SD-WAN to their public cloud infrastructure with a few clicks and facilitates connectivity between branches, on-premise data centers, or public cloud. Aruba also supports integration with AWS transit gateway (TGW) and Azure virtual WAN for optimizing connectivity in multiple virtual private clouds.
- Rich set of native security services including session- and role-aware stateful firewall, turnkey VPN access, application-based filtering, web content (URL), geolocation or reputation filtering, and simple cloud security provider integration.

- Routing protocol support for BGP, OSPF, and RIP for customer LAN and WAN facing interfaces.
- No need to spend time troubleshooting configuration errors. Aruba finds the last configuration that kept the system running smoothly and reverts to it automatically in instances of failure, eliminating maintenance and downtime.
- Application-aware policy-based routing provides tremendous flexibility and cuts congestion while boosting security. Aruba Branch Gateways use a built-in firewall to inspect packets or work with a third-party application (e.g., Zscaler) to filter content for high performance, low-risk communications.

3.0 How We Did It

Our hands-on testing used a real-world branch environment, challenging product performance for a realistic assessment of unique features and capabilities. The following topology was used for all performed tests.

Test Topology



Source: Aruba, a Hewlett Packet Enterprise Company

The test topology includes physical branch gateways, virtual headends (vGWs) and on-premise physical headends (VPNCs) that are connected to the SD-WAN overlay network.

Three headend gateways represent globally dispersed data centers hosted in Amazon Web Services (AWS) – a useful depiction of typical worldwide customer locations. Inside every data center is an integrated AWS Transit Gateway (TGW). By presuming the customer's services are inside AWS, headends are placed in front of each data center for tunnel termination, load balancing and redundancy. A data center was placed in each of three different regions. For instance, "CA" (Canada) represents North America and will serve mainly all branch locations from North America, "EU" is Europe and surrounding areas, and "AP" for Asia-Pacific (e.g. Japan). The headends are virtual gateways hosted in the AWS cloud. (The solution also works similarly with Microsoft Azure.) In the on-premise data center, the gateways are Aruba physical gateways (VPNCs).

The solid blue lines are IPsec tunnels that form the SD-WAN overlay. The underlay network (dashed lines) represents the IPsec tunnel mesh which builds the connectivity between the headends and the branch gateways. On the top of IPsec tunnels which are interconnecting the headends, BGP is used to advertise the data center routes to all data centers.

Device (firmware version)

Aruba Branch Gateway 9004 (8.5.0.0-1.0.7.2)

Aruba Branch Gateway 7000 (8.5.0.0-1.0.6.2)

Aruba ClearPass (6.7)

Aruba Central (2.4.9)

Aruba Headend Gateway 7200 (8.5.0.0-1.0.6.2)

Aruba Switch 2930F 8-port (16.10)

Aruba Access Point AP-515 (8.5.0.4)

Test Tool Descriptions

Ixia IxNetwork	A scalable performance test solution used to simulate devices and large networks to evaluate routing, switching and software defined networking capabilities. Generated traffic flows emulate real-world applications and scenarios used on today's networks.

4.0 Management

Aruba Central is key in the management of the LAN, WLAN and WAN from a single pane of glass.

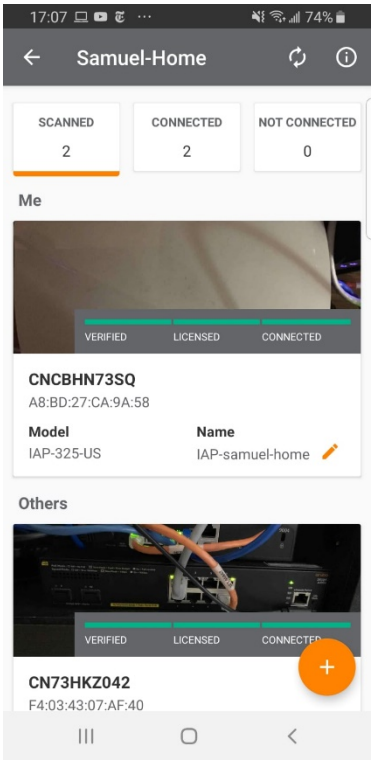
Aruba Central simplifies provisioning, configuration and visibility. This section reviews features such as Install Manager, Zero-Touch Provisioning, One-Touch Provisioning, Configuration Auto-Recovery and Application Visibility.

4.1 Install Manager Workflows

Aruba Central supports a restricted, read-only role designated for an installer. Installers can be engineers, partners, contractors, store managers, and office managers that are responsible for installing physical gear at the site. Installers don't have access to Aruba Central, but have access to the Aruba Installer application that is supported on IOS (iOS 9.0 or later) and Android (Android 5.0 or later).

Install Manager allows users to manage, monitor and optimize workflows. To test this, we created the new site and assigned to the devices which will be provisioned using the following steps:

1. Associate a group to the site.
2. Give the installer rights for the sites to be provisioned.
3. Once the installer has been added and associated to the corresponding sites, the application prompts the user to sign in. A text message is sent which instructs the installer to download the application (for iOS or Android).
4. Select the site and scan the branch devices (gateways, switches or APs) which need to be installed and onboarded to Aruba Central.

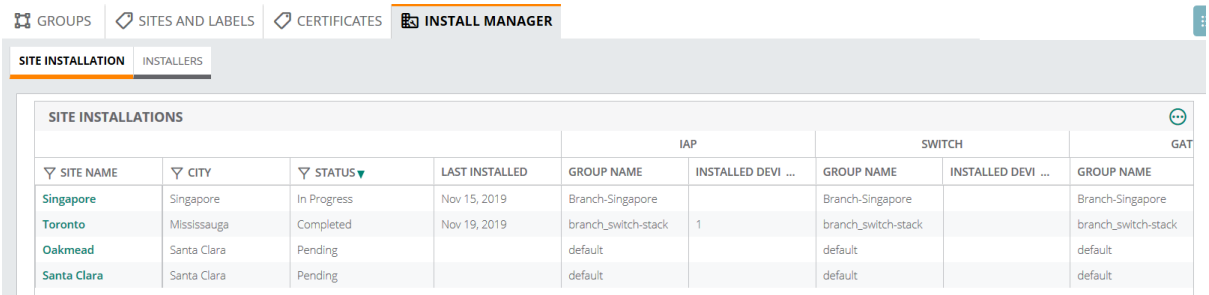


The Aruba Installer app shows all devices scanned and connected.

Results

The Aruba Installer app successfully scanned the branch devices and connected them to the network via Aruba Central.

Upon connecting to Aruba Central, the device was automatically mapped to the site with its appropriate group configuration.



After configuration is pushed successfully to the device, Install Manager marks the status of the installation as Completed (within Aruba Central) for that device.

The approach of centralized management, consistent across the distributed enterprise, ensures there is no longer a need for traditional LAN segmentation. Traditional means of authentication and access control assigns groups of users or devices to VLANs that require manual configuration with static IP address ranges. This challenges administrators in terms of tracking, management, time and human error. As IoT device connections increase, scalability gets increasingly complex.

Aruba Install Manager streamlined the installation of new devices such as gateways, switches and wireless access points.

Source: Aruba, a Hewlett Packet Enterprise Company

The installer can take a picture of the new device installed in the corresponding site and upload the photo in Aruba Installer app. The app sends a photo to Aruba Central, displaying it under Install Manager as "proof" that the device was properly installed.

Aruba Advantage

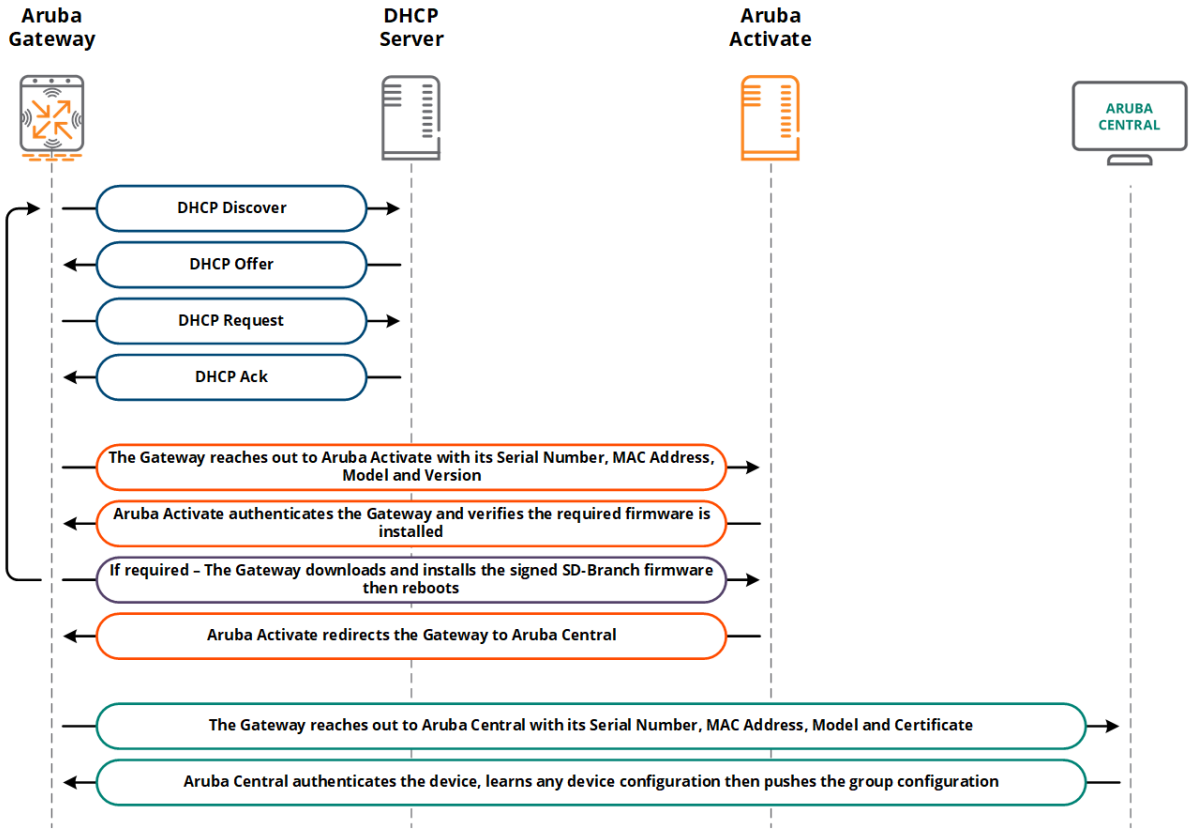
Onboarding with the Aruba Install Manager saves time and cost, as it can be done by any partner. A device can now be added in minutes rather than hours. Using Aruba Install Manager, contractors or subcontractors do not even need access to Aruba Central to pre-stage the equipment.

4.2 Zero-Touch and One-Touch Provisioning

Traditional SD-WAN deployment requires many steps to map access policies and configurations for every endpoint. Aruba uses a combination of Zero-Touch Provisioning (ZTP) or One-Touch Provisioning (OTP) to automate this process, eliminating manual user interaction and risk of human error.

With ZTP, all Aruba Gateways, Access Points (APs) and ArubaOS switches are automatically deployed using a cloud-based activation service, Aruba Activate, with Aruba Central. Deployment requires no user interaction to onboard and provision each branch device.

OTP is more commonly used for provisioning headend gateways, since static IPv4 addresses, specific VLANs, and switch port configurations are required, and DHCP is typically not available in the data center.



Source: Aruba, a Hewlett Packet Enterprise Company

Automated processes in branch site deployment. The process uses Aruba Activate, a cloud-based service that helps provision Aruba devices and maintain inventory.

This test verified the ability to deploy a branch site with minimal configuration steps.

Results

New devices were subscribed using serial number, MAC address and corresponding site. Gateway subscriptions could be set automatically or manually. With ZTP and a network connectivity, the device automatically came online, connected to Aruba Central and downloaded its configuration without any manual intervention. ZTP is complete once the full configuration is pushed to the device. From then on, it was entirely managed by Aruba Central.

Aruba Advantage

Zero-Touch and One-Touch Provisioning automatically maps configurations for every endpoint. This eliminates manual provisioning, reduces errors, and makes deployment highly scalable, for up to thousands of branches.

4.3 Configuration Auto-Recovery

If an erroneous configuration is pushed to a branch gateway, which would make it lose connectivity with the cloud, the gateway should automatically roll back to its previous configuration. This allows the administrator to remediate the configuration mistake and regain control of the "lost" device.

The configuration auto-recovery feature is enabled by default. Testing its functionality can be achieved, for example, by administratively shutting down the uplink interface or changing the default gateway in order to break the connectivity with Aruba Central. Once the configuration is applied, the branch gateway will check if it still has connectivity with Aruba Central and roll back to the previous working configuration if it has been broken.

Results

The branch gateway automatically rolled back to the last known working configuration, allowing the network administrator to correct the configuration mistake. The automatic rollback mechanism guarantees that an erroneously pushed configuration doesn't isolate a branch or a group of branches from the network. This was tested by verifying the device's configuration after pushing the wrong configuration.

Aruba Advantage

No need to spend time troubleshooting configuration errors. Aruba finds the last working configuration that kept the system running smoothly and reverts to it automatically in instances of failure, eliminating maintenance and downtime.

4.4 Application Visibility

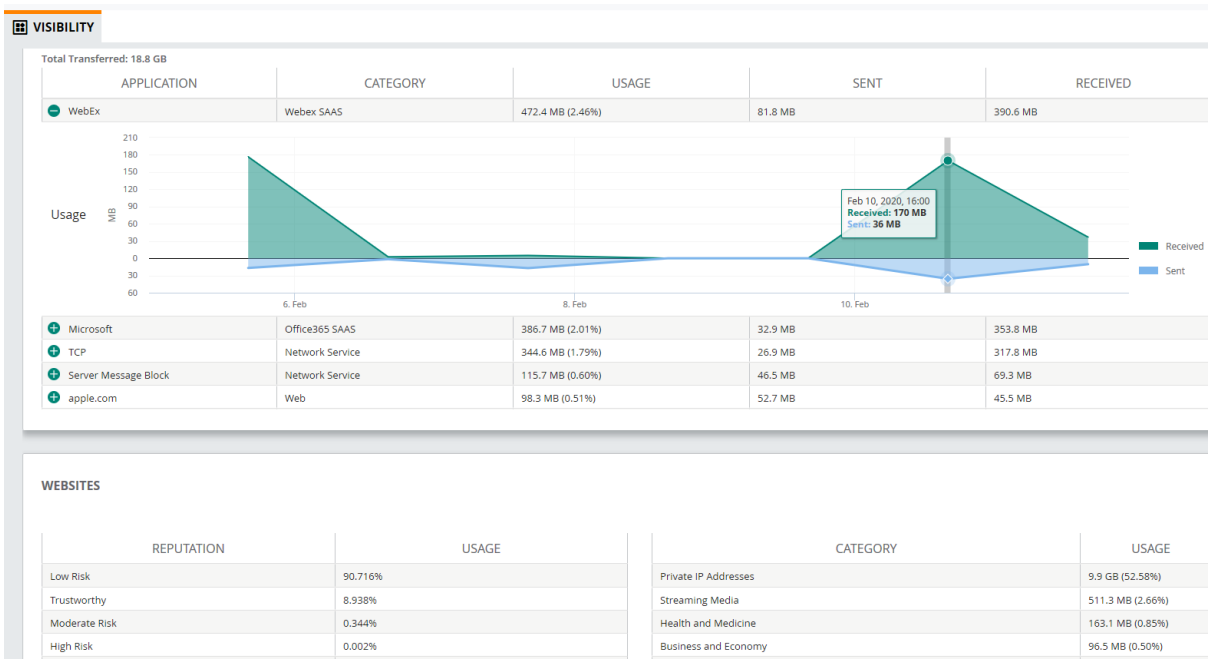
One of the ways Aruba assesses application traffic is with its custom-built, Layer 4-7 firewall capability. This feature includes Deep Packet Inspection (DPI) which is used for creating firewall policies based on application type.

The DPI feature analyses data packets to identify applications in use and create access rules for clients across applications, application categories, web categories or URLs. Traffic shaping policies (e.g., bandwidth or Quality of Service) can be defined for client roles.

The built-in Layer 7 firewall provides application visibility of client traffic flows that are displayed in Aruba Central, with details, for every device and client.

Results

Aruba has awareness for over 3,200 applications across 21 categories. Our testing of application visibility showed application performance, latency and other characteristics that help optimize the network's role-based policies.



Aruba Central's Visibility into WebEx performance, latency, and other characteristics over time.

Aruba Advantage

Application recognition and visibility helps IT to fine-tune WAN link management and proactively mitigate performance issues. Aruba provides this visibility for a huge library of applications.

5.0 SD-WAN Features

In this section we reviewed how the following features contribute to successfully building an overlay network using Aruba SD-WAN Orchestrator and smart routing application traffic based on latency and jitter of the paths.

- Tunnel and Route Orchestration
- Data center Failover
- Active-Active WAN Gateways
- Micro-Branch with AP-VPN
- Application-Aware Routing
- Dynamic Path Steering (DPS)
- Policy-Based Routing (PBR)

5.1 Tunnel and Route Orchestration

The Aruba SD-Branch solution is designed from the ground up to be both simple and scalable. To simplify routing and allow SD-Branch deployments to build a scalable and secure overlay network, the Aruba SD-Branch solution supports an SD-WAN Orchestrator for centralized orchestration of tunnels and routes.

In order to avoid maintaining complex underlay architectures, the Aruba SD-WAN solution:

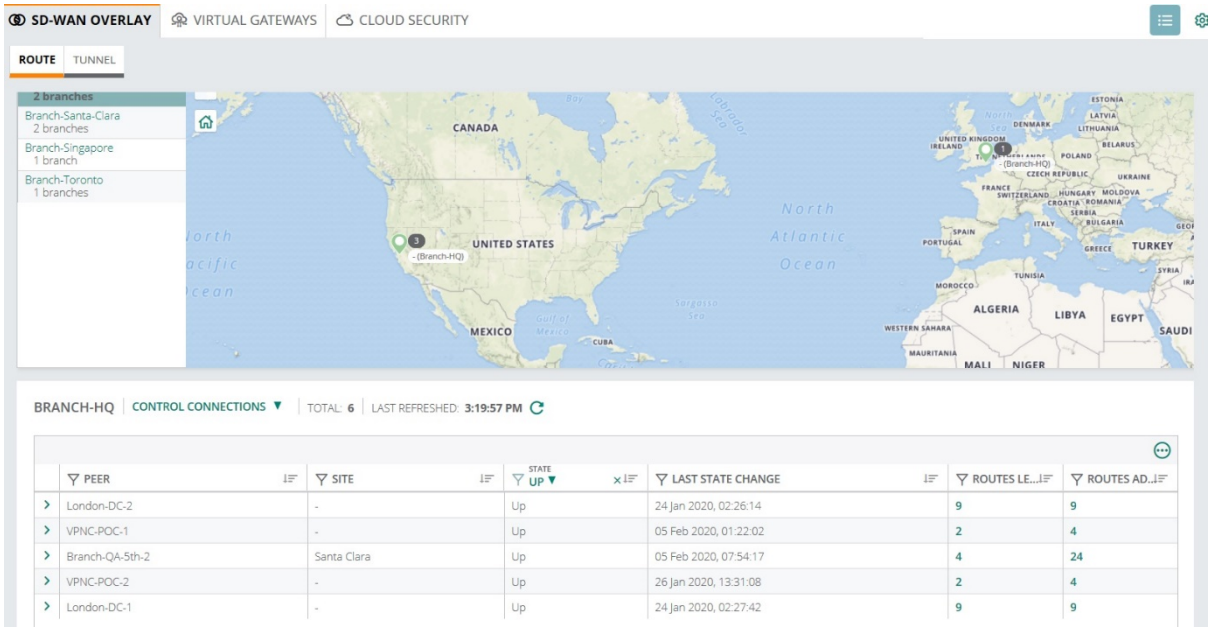
- Leverages an SD-WAN Orchestrator to automatically build an overlay of tunnels between the nodes in the network.
- Automates the routing process and distributes routing information learned from each connected branch in a dynamic way as per the routing segmentation requirements.

Results

When the SD-WAN Orchestrator is enabled, it seamlessly brings up all required tunnels, setting up the overlay network with headends and branch gateways. The SD-WAN Orchestrator handles the creation and re-keying of those IPsec tunnels. It was verified that tunnels were properly established.

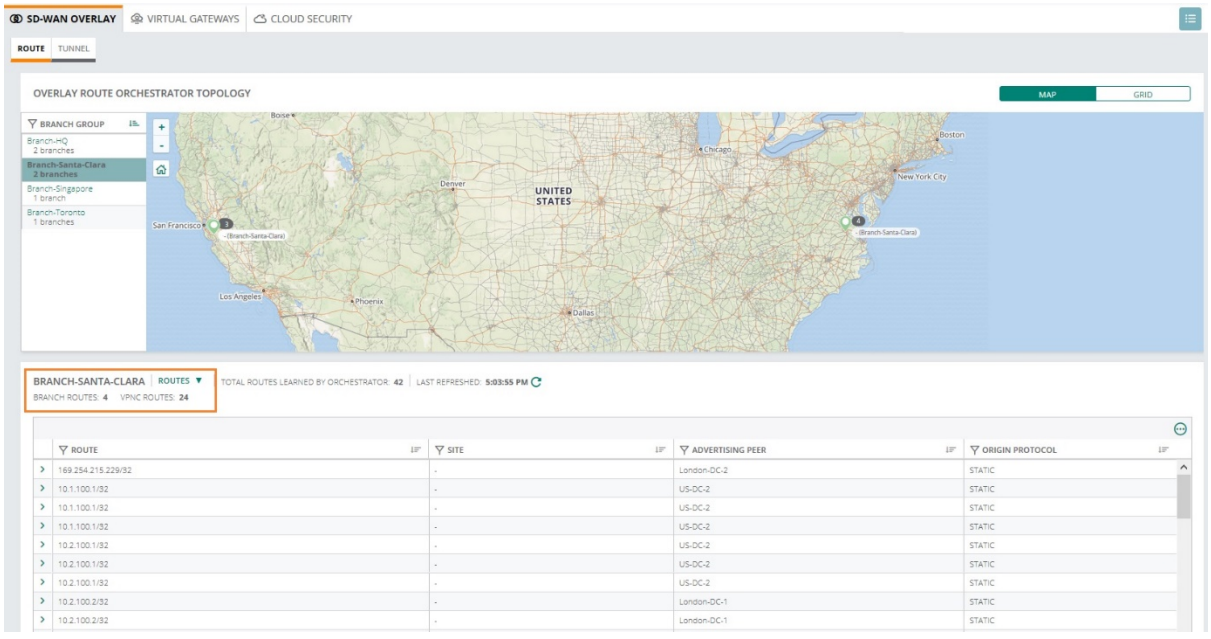
Once the SD-WAN overlay was established, the solution was able to dynamically advertise branch subnets into the headend gateways and data center networks were advertised into the branch locations. This redistribution of routes across the overlay is dynamic and does auto-costing of metrics based on data center (DC) preference configured by the user. To ensure symmetric routing across the WAN, auto-costing ensures that the branch route costs are appropriately reflected within the DC to comply with the configured DC preference.

The following figure illustrates how customers can monitor overlay connectivity using the Aruba SD-WAN Orchestrator dashboard.



SD-WAN Orchestrator under Aruba Central. Tunnels are established between headends and branch gateways, and routes advertised. As such, customers can globally view the details of the control connection, orchestrated overlay tunnels and routes.

The following screen shows a centralized view of all the overlay routes that are exchanged between the selected group of branch sites and the VPNCs.



Aruba Central's SD-WAN Orchestrator (Routes View). This provides a global view of routes.

Aruba Advantage

SD-WAN Orchestrator automatically creates the overlay network between the branch gateways and headends by building IPsec tunnels and dynamically exchanging the routes throughout the overlay network.

5.2 Data Center Failover

In the rare event that a disaster should occur and a whole data center would go down, the branch solution should have a mechanism to re-provision itself to a backup data center. Aruba supports Layer 3 or Layer 2 failover for deployments where the IPsec tunnels are established to headends deployed at each hub site. In this redundancy model the branch groups in Central are configured with multiple headends. The IPsec tunnels are established from each BGW to their designated headends.

Each headend is assigned with a data center preference. The headend with the highest DC preference is advertising the branch routes at a lower route cost than the headend with the second DC preference. The IPsec tunnels are already established to the secondary headend if the primary headend fails or becomes unreachable.

This test assessed the failover of a headend gateway, where traffic is routed through a second active headend gateway as soon as the tunnel becomes non-operational.

Results

Failover between the two headends across data centers took approximately 35 seconds to re-establish the traffic via the new headend. The time interval for route switching is dependent on how fast the tunnels are brought down and on route convergence. Generally, less than 40 seconds is the expected time.

Aruba Advantage

Aruba SD-WAN provides extremely rapid data center failover. The policy is very easy to set up and the feature ensures symmetric routing. All of this can be achieved with a single view of your overlay topology and the overlay routes that are exchanged.

5.3 Active-Active WAN Gateways

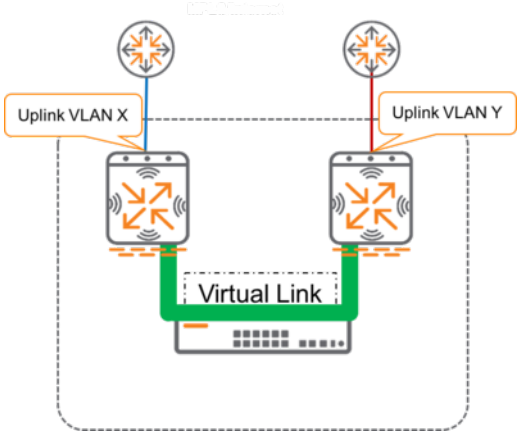
The active-active redundancy of Branch Gateways (BGWs) means SD-WAN gateways can use each other's WAN uplinks. Active-active redundancy gateways have one uplink connected to each gateway over which a virtual uplink is created.

This test addresses how redundant WAN gateways can share the WAN uplinks.

Results

A virtual link is established between BGWs, over the uplink which is interconnecting the gateways, allowing the gateways to share uplinks. The virtual link is a GRE tunnel that's automatically established between the branch gateways configured in HA.

Once the virtual link is established, the branch Gateway will share uplink interfaces with their peer.



Source: Aruba, a Hewlett Packet Enterprise Company

A logical diagram of active-active redundancy.

Aruba Advantage

Active-active redundancy means that high availability is guaranteed with the Aruba SD-WAN solution. Both link and device level redundancy are provided with this solution.

5.4 Micro-Branch with AP-VPN

The Aruba SD-Branch solution provides a complete suite of solutions for all the needs of a distributed enterprise. This often includes a need for micro-branches (SOHO), where a branch network might be built using just access points (APs) and switches.

Micro-branches serve the needs of road warriors who require VPN connectivity to access corporate resources. Solutions may be achieved with redundant gateways or with a complete cloud-managed LAN/WLAN.

For micro-branch deployments, Aruba offers an AP-based SD-WAN solution. Micro-branch deployments can be teleworkers or very small branch locations. Typically, in a micro-branch deployment, a BGW is not required. An AP can be used as a branch gateway and establish secure IPsec connections with the headend.

Results

Aruba APs have the capacity to establish IPsec tunnels to tunnel traffic from wired and wireless users to the headend in the data center. In this simplified topology for micro-branches, APs become the branch gateway for the entire branch network, including both wired and wireless users.

Route exchange for all branch networks was automatically done as part of the tunnel negotiation. Using the IPsec tunnel created, users can access corporate networks, and can also have an AP firewall available for all LAN and WLAN traffic and all the usual WLAN services.

Aruba Advantage

Aruba SD-WAN supports branch offices of all sizes, including micro-branches. For micro-branches, Aruba offers an AP-based SD-WAN solution that does not require a branch gateway; this provides a convenient, lower-cost solution for micro-branches.

5.5 Application-Aware Routing

For most SD-Branch deployments, the BGW will forward traffic via the overlay network or to the Internet using destination-based routing. Each BGW has routes in its routing table for the corporate subnets that point to their respective headend overlay tunnels as well as default gateways for each WAN uplink.

The solution is expected to determine the path of each traffic flow based on following parameters:

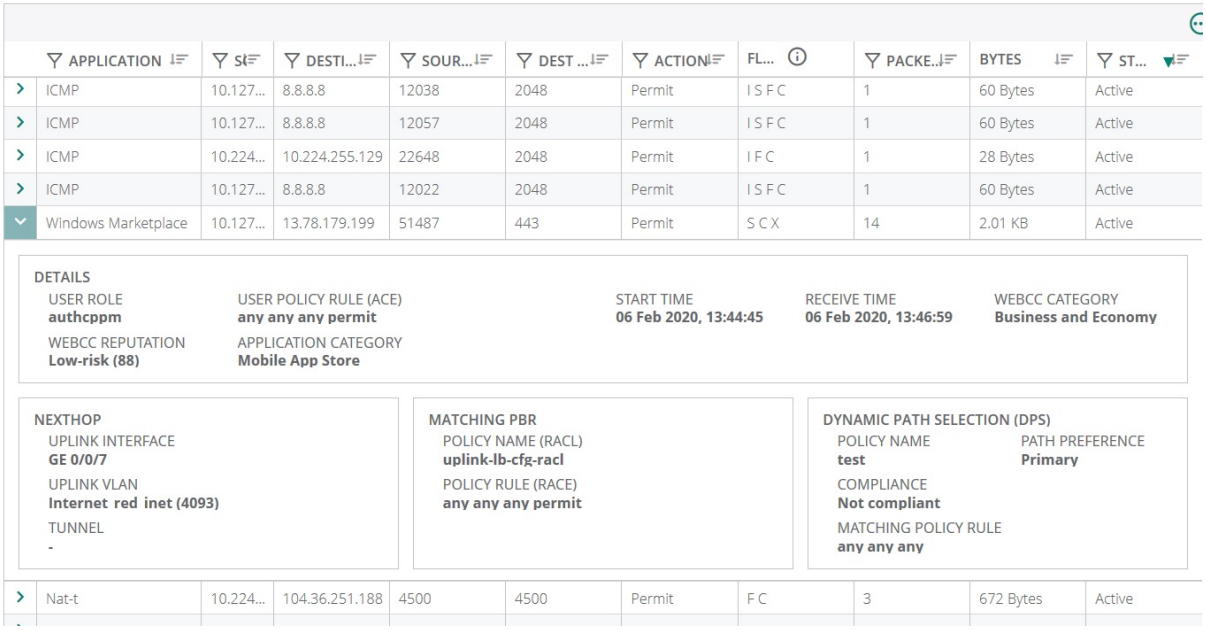
- User role
- Source/Destination IP address or port
- Application category
- Fully Qualified Domain Names (FQDN)

Also, as Software as a Service (SaaS) applications are increasingly deployed in the cloud and have servers and data centers across different geographical locations, SD-WAN devices must discover SaaS servers that are geographically closer, continuously monitor the reachability of these servers and application performance, and dynamically steer traffic via the best available path.

Results

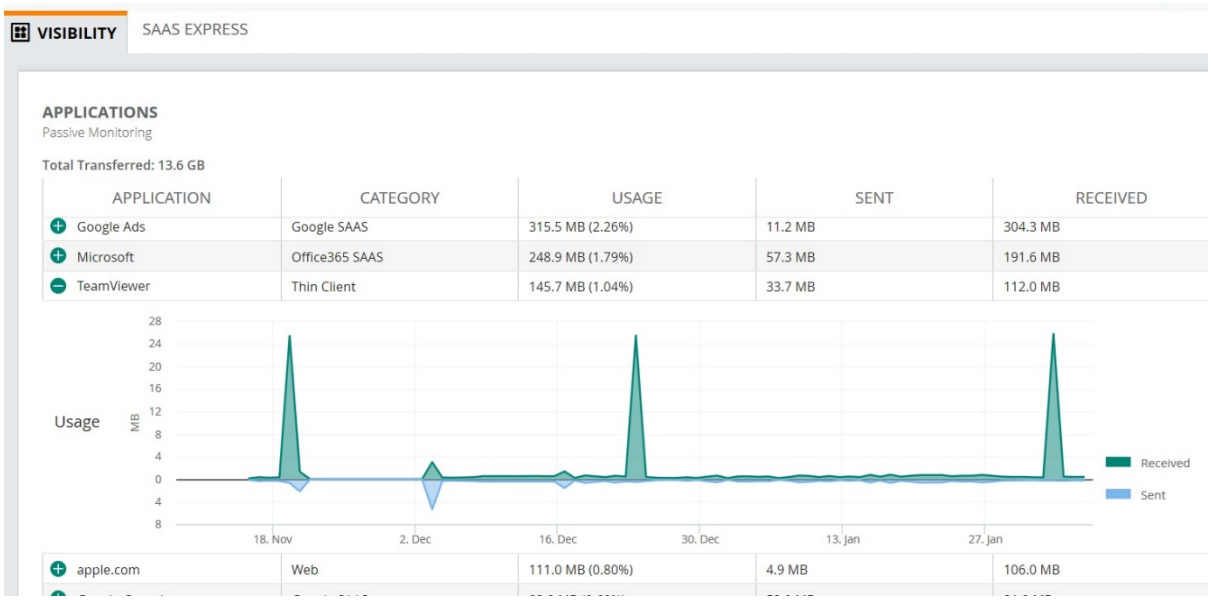
Aruba's SD-WAN solution offers enhanced traffic visibility and automated application-based routing. Aruba Application Awareness encompasses categorization based on name, category, web site reputation, or performance requirements (such as jitter, loss and latency). The BGWs are capable of routing traffic based on Layer 3-7 applications, FQDN, source VLAN or even source user role.

The following screen from Aruba Central illustrates the next hops, policy rules, and dynamic path preference for a Windows Marketplace application.



Application routing details viewed from Aruba Central.

The following Aruba Central screen shows usage over time for the TeamViewer application.



Application visibility under Aruba Central.

For SaaS applications, we set a WAN policy with path steering criteria based on key performance indicators such as jitter, latency, and packet loss and attached it to the relevant SaaS application profiles. The applications performed optimally.

Aruba Advantage

It is extremely powerful and flexible to be able to determine traffic paths based on user roles, application categories, source/destination or FQDN. Aruba SD-WAN provides this capability for thousands of applications and does so with detailed visibility.

5.6 Dynamic Path Steering

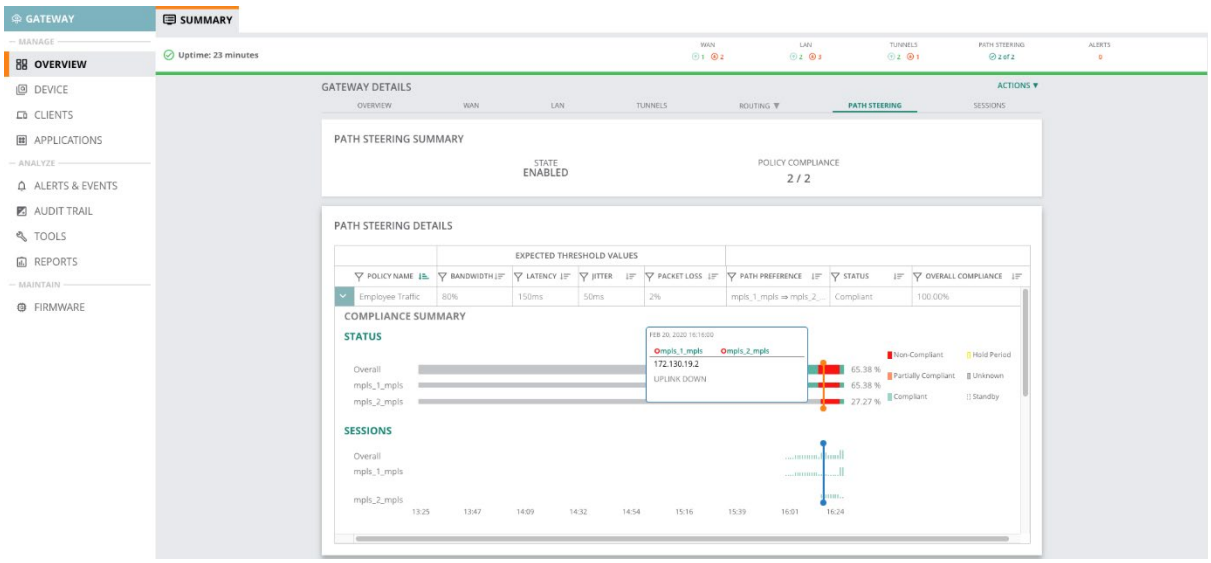
Branch gateways (BGWs) should monitor different WAN interfaces, steering traffic in the event of a path failing to meet the required service level agreement (SLA) for each traffic flow. IPsec tunnels are formed over all WAN circuits to build an SD-WAN fabric independent of the transport type.

Aruba SD-Branch is expected to work across different types (and speeds) of links using Dynamic Path Steering (DPS), as opposed to the traditional destination-based routing with load-balancing required to accomplish transport-independent routing. Using DPS, Aruba BGWs can select which upstream path is used by every traffic stream using real-time information.

Results

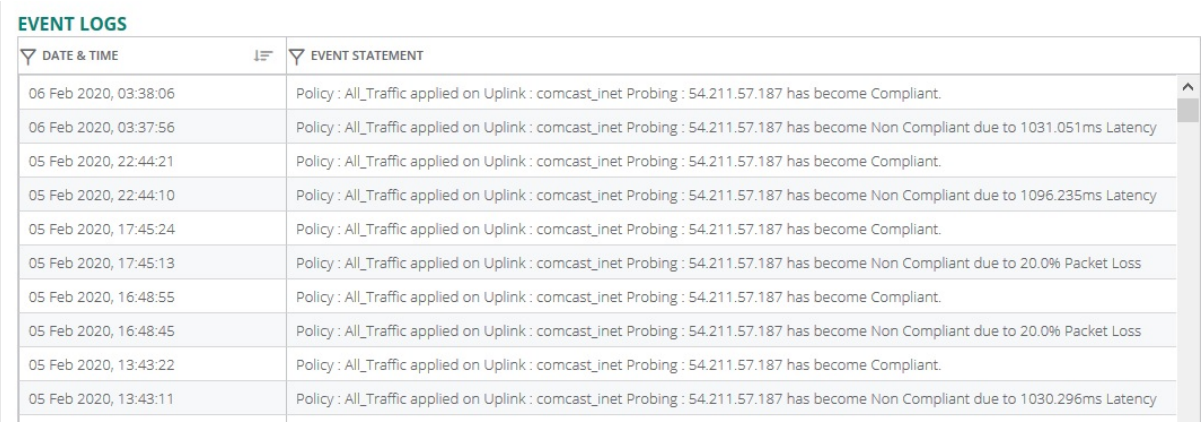
The WAN policies that we verified included the following use cases:

- **Brownout:** Steer traffic to a secondary link if the primary link is non-compliant with the configured SLA for a given traffic flow. Using a WAN emulator, we increased the latency by 300ms for the primary link, which resulted in the voice policy (which had an SLA of 150ms) to become noncompliant; as such, it failed over to the secondary link.
- **Blackout:** Simulate complete uplink failure to observe how the session is steered.
- **Smart Load-Balancing:** Configure a utilization threshold for a non-critical traffic flow and observe how traffic for that policy is steered to preserve critical application bandwidth. The load balancing options include round robin (equally distributing traffic), session count (balancing based on number of sessions), and uplink utilization (balancing based on utilization percentage).



The path steering details under Aruba Central display the threshold values and the path preference for the specified policy.

The Aruba Central event logs screen is shown below.



EVENT LOGS

DATE & TIME	EVENT STATEMENT
06 Feb 2020, 03:38:06	Policy : All_Traffic applied on Uplink : comcast_inet Probing : 54.211.57.187 has become Compliant.
06 Feb 2020, 03:37:56	Policy : All_Traffic applied on Uplink : comcast_inet Probing : 54.211.57.187 has become Non Compliant due to 1031.051ms Latency
05 Feb 2020, 22:44:21	Policy : All_Traffic applied on Uplink : comcast_inet Probing : 54.211.57.187 has become Compliant.
05 Feb 2020, 22:44:10	Policy : All_Traffic applied on Uplink : comcast_inet Probing : 54.211.57.187 has become Non Compliant due to 1096.235ms Latency
05 Feb 2020, 17:45:24	Policy : All_Traffic applied on Uplink : comcast_inet Probing : 54.211.57.187 has become Compliant.
05 Feb 2020, 17:45:13	Policy : All_Traffic applied on Uplink : comcast_inet Probing : 54.211.57.187 has become Non Compliant due to 20.0% Packet Loss
05 Feb 2020, 16:48:55	Policy : All_Traffic applied on Uplink : comcast_inet Probing : 54.211.57.187 has become Compliant.
05 Feb 2020, 16:48:45	Policy : All_Traffic applied on Uplink : comcast_inet Probing : 54.211.57.187 has become Non Compliant due to 20.0% Packet Loss
05 Feb 2020, 13:43:22	Policy : All_Traffic applied on Uplink : comcast_inet Probing : 54.211.57.187 has become Compliant.
05 Feb 2020, 13:43:11	Policy : All_Traffic applied on Uplink : comcast_inet Probing : 54.211.57.187 has become Non Compliant due to 1030.296ms Latency

Event logs under Aruba Central show the policy events that cause traffic to be steered to another path.

This test was performed using the Ixia IxNetwork tool to manually increase the throughput on the main link up to the rate set by a policy.

Aruba Advantage

To monitor performance requirements, the gateway tests link performance on a regular basis. This data is available for optimizing link quality routing. When SLA conditions (such as latency, jitter or loss values) were not met, then the application switched to a better-performing uplink. In this way, for instance, a voice call will not be interrupted. In general, whenever link utilization exceeded a specified threshold, the Dynamic Path Steering feature successfully selected a different path with better throughput.

5.7 Policy-Based Routing

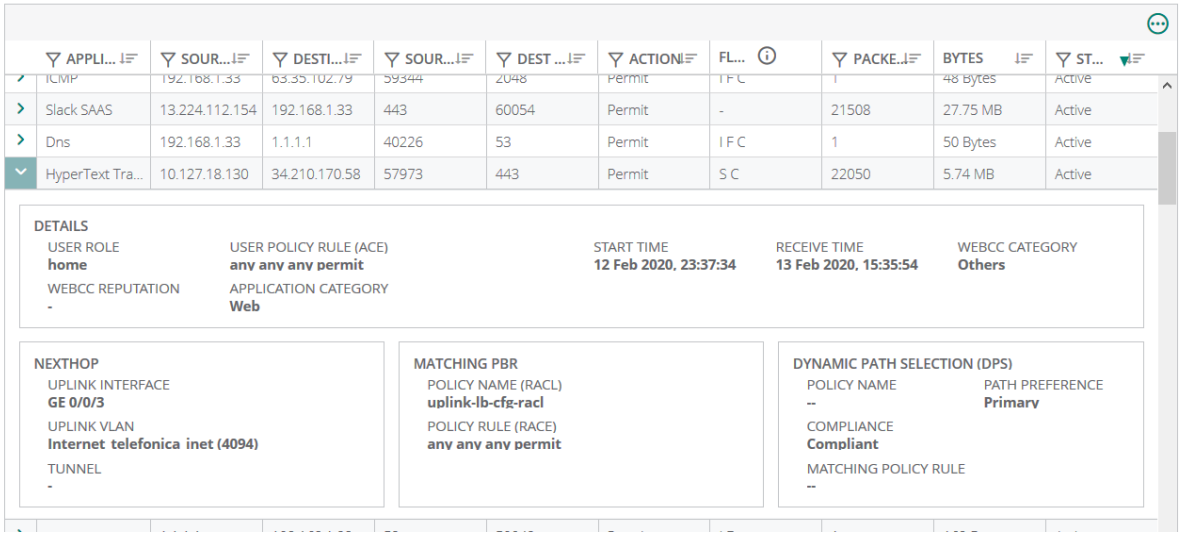
Aruba supports both split tunnel and full tunnel policies to direct Internet-bound traffic at the BGW. In the case of split tunnel, we configured an application-aware and role-aware policy based route (PBR) to directly peel off traffic on Internet circuits. For instance, all guest traffic is typically split-tunnelled.

In the case of full tunnel, we configured an application-aware and role-aware policy based route (PBR) to direct the traffic over the tunnel towards the data center. In this case, all Microsoft Office application traffic is full-tunnelled.

In either case, customers can make use of more than one path at a time and leverage DPS to achieve intelligent path selection.

Results

In full-tunnel mode, we used a PBR rule that is applied to the LAN VLAN to forward all traffic destined to the Internet via the overlay IPsec tunnels. When PBR is applied, the branch gateway will ignore the default gateways in its routing table and will instead forward the Internet traffic to the overlay IPsec tunnels.



Under Aruba Central's Session Monitoring tab, the exit interface can be viewed in real-time and the PBR is matched by each packet.

Aruba Advantage

Aruba SD-WAN's policy-based routing functionality eliminates congestion in the network and boosts security. This functionality offers the flexibility of working with both split tunnel and full-tunnel traffic.

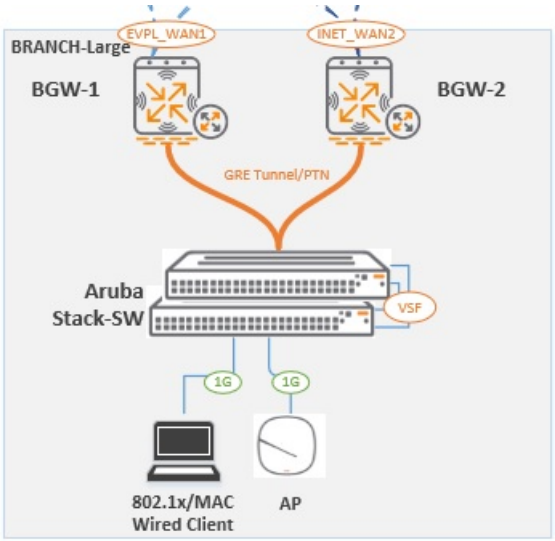
6.0 SD-LAN Features

Aruba branch gateways provide enhanced visibility, control and security for the LAN side across multiple network layers. Unlike traditional SD-WAN solutions, Aruba eliminates the need for complex VLAN architectures. Port tunneling and dynamic segmentation provide role-based access right from the branch gateway for a unified and consistent management of endpoints.

6.1 Stack of Switches with LACP

The SD-Branch gateway is acting as default gateway for the branch network, which means that redundant connections should be used to facilitate the availability for a higher bandwidth. Therefore, the solution should support Link Aggregation Control Protocol (LACP) for link aggregation in LAN-facing interfaces.

The Aruba SD-Branch solution supports stacking of up to 8 switches, providing additional bandwidth, as well as more available ports. The following topology diagram shows how the gateways are connected to stacked switches.



Source: Aruba, a Hewlett Packet Enterprise Company

Connections between gateways and stacked switches.

Results

Link aggregation using LACP was configured using LAN facing ports between the branch gateway and the stacked switch. The gateway correctly establishes an LACP port channel and traffic was tunneled over the port channel.

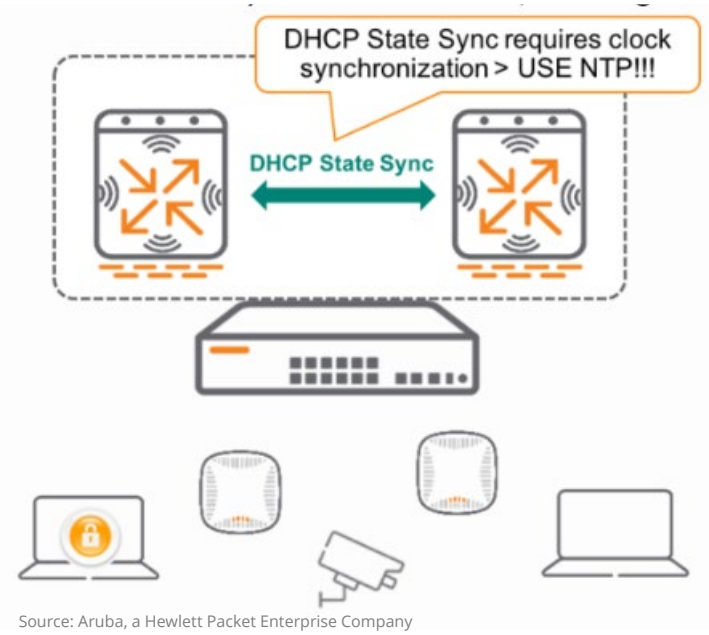
Aruba Advantage

With Aruba SD-Branch, you can stack up to eight switches for additional bandwidth and more available ports. In a simplified configuration, traffic is tunnelled over and LACP port channel.

6.2 DHCP State Sync

Branch gateways (BGWs) which are configured in high availability (HA) mode can be configured to synchronize their DHCP databases to be dynamic and avoid overlapping IP address assignments. The pool scope under the DHCP database is shared for both branch gateway peers, and each branch gateway is capable of assigning IP addresses from the common DHCP pool.

The normal functioning of the DHCP server on both branch gateways is dependent on NTP clock synchronization and network connectivity (given by the virtual interconnecting link) between branch gateway peers in a high availability (HA) setup.



Source: Aruba, a Hewlett Packet Enterprise Company

Diagram of DHCP state synchronization

Results

The DCHP database was successfully synchronized for dynamic IP assignments for the devices connected in the branch LAN. The database was updated with the timestamp to which provides the most current DHCP lease of IP addresses, allowing allocation based on which IP address is available from the DHCP pool.

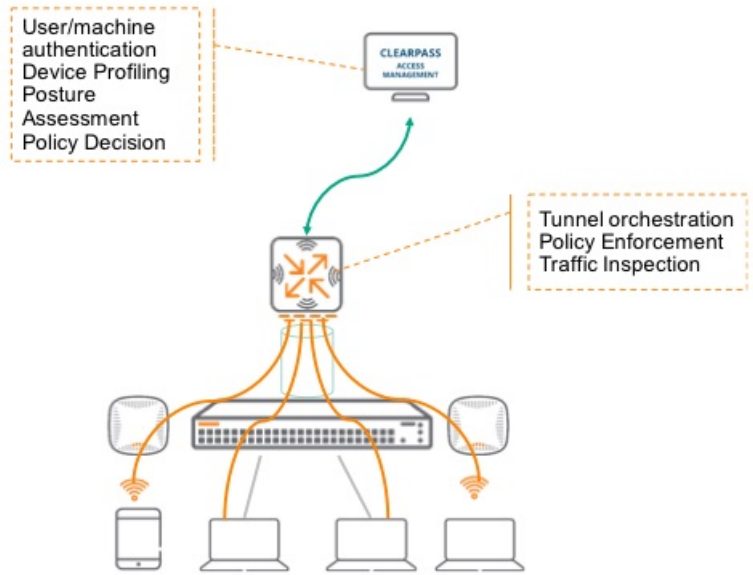
Aruba Advantage

Aruba SD-Branch provides a simplified way to avoid overlapping IP addresses with DHCP state synchronization. By sharing the DHCP database, each gateways can assign IP addresses from the common DHCP pool.

6.3 Dynamic Segmentation via Port-Based Tunneling (PBT)

The branch infrastructure should provide role-based access for branch users without the need to separate them in different subnets. Deploying Aruba switches at the branch allows for simple, Zero Touch, onboarding of the network infrastructure. When integrated with Aruba branch gateways, the combined solution can also offer a single point of access control and enforcement from the branch gateway.

Aruba switches support "Tunneled-Node," a feature that allows the access switch to tunnel all traffic in a port or set of ports to the branch gateway. Security policies are applied and enforced in the branch gateway. This allows an administrator to configure a common set of policies on a central ClearPass server and use a single policy enforcement point, the branch gateway, to inspect every communication in the branch, even when communication is happening between devices in the same subnet.



Source: Aruba, a Hewlett Packet Enterprise Company

Aruba Tunneled Node allows the access switch to tunnel all traffic in a port or set of ports to the branch gateway.

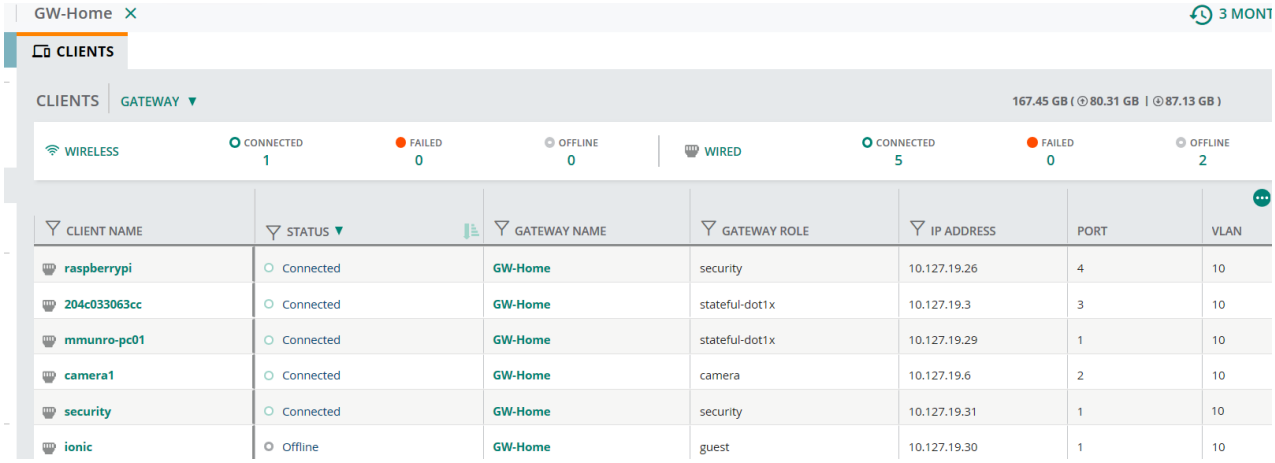
In the above diagram, all traffic is tunnelled to the gateway for device isolation and policy enforcement. The BGW's Layer 3-7 stateful firewall can enforce very granular policies. Policies are assigned by ClearPass, based on posture and device profiling.

Results

The dynamic segmentation model dramatically simplified branch infrastructure by eliminating the traditional method of having a VLAN per user or per device. Using Aruba's dynamic, policy-based tunnelling, we needed only one VLAN for all branch devices while still ensuring complete isolation between devices in the same VLAN if necessary.

ClearPass Policy Manager further profiled and assessed devices for more granular distinction. Combined with a firewall, branch user-roles were extended to corporate firewalls for complete role-based access to the rest of the organization.

These results show the advantage of Aruba's colorless ports.



CLIENT NAME	STATUS	GATEWAY NAME	GATEWAY ROLE	IP ADDRESS	PORT	VLAN
raspberrypi	Connected	GW-Home	security	10.127.19.26	4	10
204c033063cc	Connected	GW-Home	stateful-dot1x	10.127.19.3	3	10
mmunro-pc01	Connected	GW-Home	stateful-dot1x	10.127.19.29	1	10
camera1	Connected	GW-Home	camera	10.127.19.6	2	10
security	Connected	GW-Home	security	10.127.19.31	1	10
ionic	Offline	GW-Home	guest	10.127.19.30	1	10

With colorless ports, it doesn't matter which access port an IoT device is connected to: the branch gateway applies appropriate policies to the device based on the associated role that is dynamically assigned to it. This is illustrated here under Aruba Central.

Aruba Advantage

Dynamic segmentation provides secure and simplified access for users and devices. This allows a flat network without an explosion of VLANs and multiple DHCP scopes. This ensures simplified operations and an improved security posture by enforcing all the policies on the gateway.

6.4 AAA Survivability

Even a branch solution designed with redundant uplinks cannot guarantee 100 percent uplink availability. To ensure this, even without an uplink, the branch solution should be able to cache last authentications when the RADIUS server is unreachable.

When authentication servers are not accessible, clients cannot access the network because they cannot authenticate. Authentication survivability allows branch gateways to provide client authentication and authorization survivability when remote authentication servers are not accessible. When this feature is enabled, the branch gateway stores access key reply hash values whenever clients are authenticated. When external authentication servers are not accessible, the branch gateway uses its internal survival server to continue providing authentication and authorization functions by using the user access credentials and key reply attributes that were stored earlier.

Results

We tested AAA survivability using a RADIUS server which had enabled the caching of RADIUS information for seven days.

When the user reconnected to the network and the RADIUS server was unavailable, local authentication was needed. The RADIUS server was marked as "Out of service" and the client was able to use the user's cached information in the Internal Server.

Aruba Advantage

Aruba SD-Branch implementations can cache authentication information for use even when the RADIUS server is unreachable, allowing clients to use this cached information for up to a week.

6.5 Performance Testing

This section reviews testing of gateway performance capabilities during ideal and degraded scenarios to determine how well the SD-WAN solution can maintain connectivity and quality.

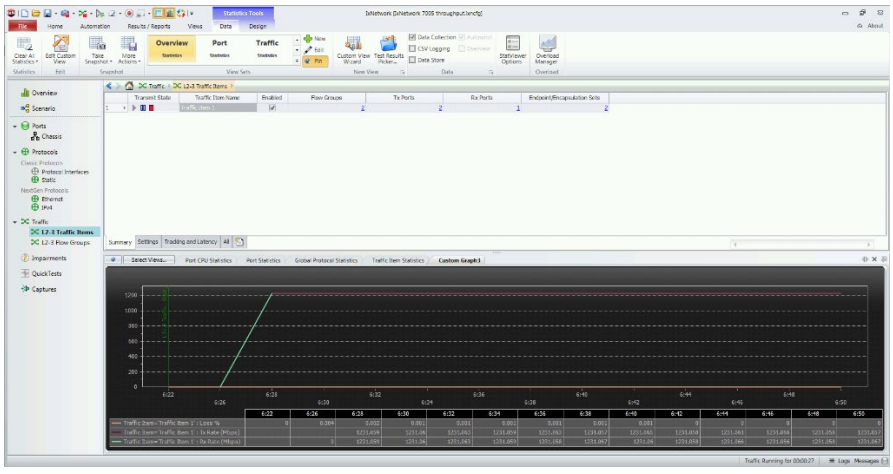
Results

Using the Aruba 7005 (smallest model for small businesses), we verified the following:

- Supported line rate of tunnels to data center using 2x1-GbE ports
- Supported line rate of tunnels to data center with same configuration with encrypted throughput.

Following use cases were tested:

Test Case	Performance
Throughput	
Case 1: Max throughput • Send traffic over 2x1-GbE links	• Successfully supported line rate: 1.24 Gbps • Max crypto throughput: 1.24 Gbps at 95% CPU
Case 2: Application failover in Branch HA scenario • Master BGW Rebooted • 2000 users connected	• 1.24 Gbps throughput • 6 seconds to switch over for the applications • 2 seconds ping loss
Case 3: Steer Video steaming • Video streaming via WebEx • Main uplink SLA getting degraded	• No video streaming loss, no calls dropped • Failover to the second uplink did not result in dropped calls • Seamless WebEx traffic



Throughput results on Ixia IxNetwork

Aruba Advantage

Aruba SD-Branch provides very high-performance gateways, with up to 1.3 Gbps throughput on the Aruba 7005 gateway (the smallest model for small businesses).

7.0 Security

As security threats evolve into internally launched attacks, customers are looking for the ability to separate and restrict traffic, especially for specific device types or user groups. Aruba is in a unique position to provide this separation thanks to the user-centric role-based approach to security that has been present since Aruba was founded. With a true role-based approach, complex designs with tens of VLANs would no longer be necessary, as all east-west traffic goes through the stateful inspection of the firewall.

7.1 Control Plane Policy

Aruba Gateways support stateful firewall packet inspection, providing an additional security layer for network connections. By tracking connection states and using information from previous connections, the gateways monitor and control all control plane sessions.

To protect against external attacks and unauthorized communication attempts the Aruba SD-WAN gateways are configured with match conditions and packet filtering criteria. Additionally, access lists allow, deny or rate-limit the desired control plane traffic.

Results

The branch gateway uses the stateful firewalls to monitor and control traffic throughout the branch network. Control Plane Policies (CoPP) determine, based on traffic profile characteristics, which traffic can be permitted.

Aruba Advantage

Aruba SD-Branch gateways with stateful firewall packet inspection provides protection against external attacks and unauthorized communication attempts. Sophisticated packet filtering means users can allow, deny, or rate-limit control plane traffic.

7.2 Application-Based Security Policies

Aruba's branch gateway incorporates a stateful firewall capable of identifying and controlling traffic based on IP addresses, ports, and applications. The Aruba branch gateway identifies over 3,200 different applications and can selectively apply policies for any of them.

In this test, we configured application visibility to detect and prioritize business applications such as Skype for Business, Jabber, Citrix or GoToMeeting. We then blocked peer-to-peer applications for both employees and contractors; beyond that, we established different rules for employees and contractors:

- For employees, we rate-limited Windows updates.
- For contractors, we blocked Apple application updates but allowed Windows and anti-virus updated; we also rate-limited cloud-based applications.

Results

The branch infrastructure correctly prioritizes key applications such as unified communications, and correctly blocks, as specified, risky or forbidden applications. As users within a VLAN may not all need the same access rules, these rules are applied on a per-role basis.

Aruba Advantage

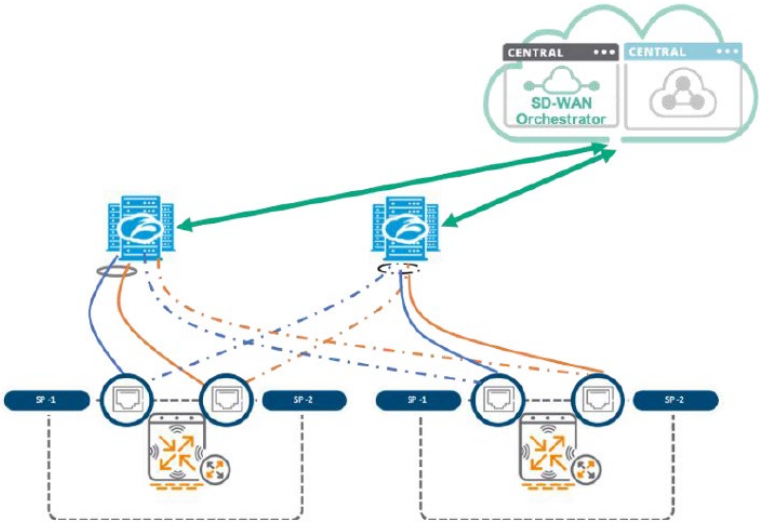
Aruba's SD-Branch gateways can identify over 3,200 different applications and identify and control traffic based on these applications and on IP addresses and ports. Selected treatments include blocking or rate-limiting applications.

7.3 Integration with Cloud Security Providers

For faster delivery and efficient use of bandwidth, Aruba SD-WAN customers can route local traffic to the Internet. However, for branch devices to directly connect to the Internet, users must keep the branch network secure from threats. The most common approach to secure the branch Internet traffic is to enable branch devices to route all Internet traffic through a cloud security platform, such as the Zscaler cloud security service.

The Zscaler Cloud Security Platform provides fast and secure connections between users and applications, regardless of device, location, or network. Branch gateways can interoperate with Zscaler's cloud network to provide a secure branch network connectivity with threat detection capabilities.

To integrate with this service, SD-WAN solution needs to do is establish tunnels with the nearest Zscaler Internet Access (ZIA) node(s) to send Internet-bound traffic through them.



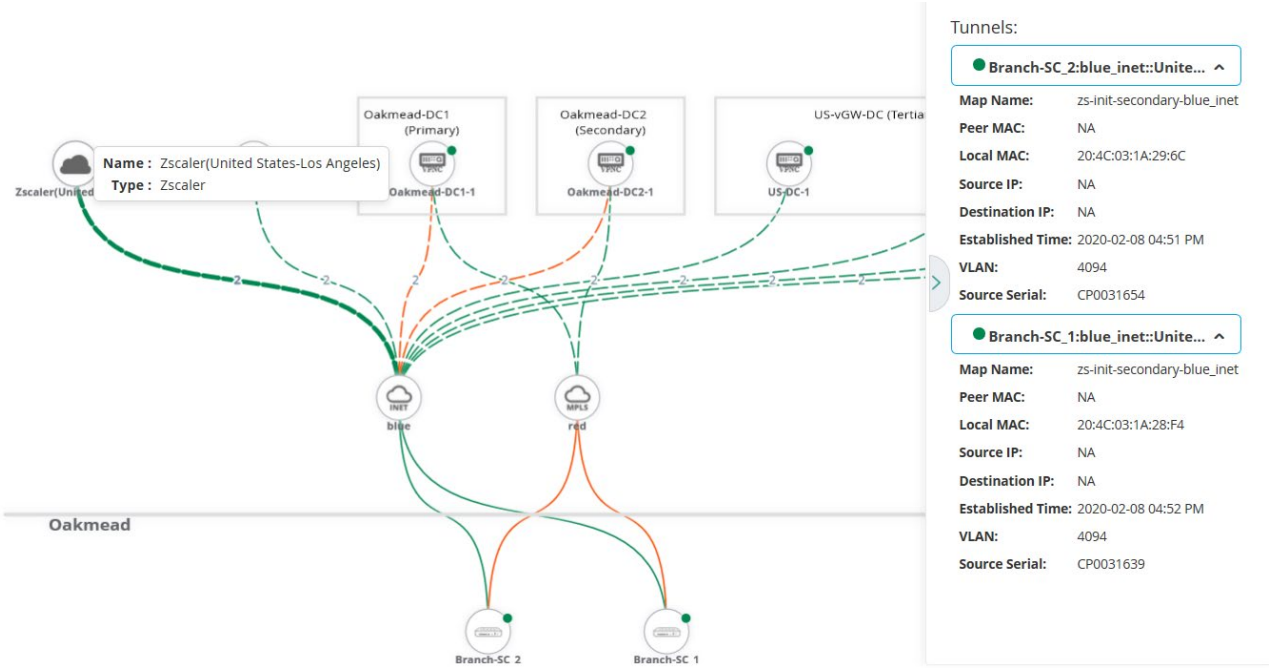
Source: Aruba, a Hewlett Packet Enterprise Company

Aruba WAN Orchestrator integration with Zscaler Cloud Security Platform.

The Aruba SD-WAN Orchestrator is a cloud-native, multi-tenant control plane that is included as part of Aruba Central to automate SD-WAN deployments. The benefit of the SD-WAN Orchestrator is that WAN links are automatically discovered and tunnels and routes are orchestrated based on business and topological needs.

Results

The SD-WAN Orchestrator automated the creation of tunnels to the nearest Zscaler Enforcement Note (ZEN) nodes. To enable automatic orchestration of the tunnels was required to set up the accounts in Zscaler for the branch gateways and have them authenticate themselves. As such the tunnels are established by using the SD-WAN Orchestrator service available in the Aruba SD-Branch solution.



Tunnels are established via Aruba Central's SD-WAN Orchestration for Zscaler Cloud Security platform integration.

Aruba Advantage

Aruba's SD-Branch gateways enforce zero-trust in the branch through integration with third party solutions such as the Zscaler Security Cloud Platform. Aruba also provides orchestration of the tunnels to set up the accounts in Zscaler for the gateways.

8.0 Resources

The following resources are available for more information:

- Aruba SD-WAN Technical Notes on Aruba Support Portal:
    1. Aruba SD-Branch and Zscaler Internet Access Integration
    2. Aruba SD-Branch Hardening
    3. Aruba SD-Branch with Palo Alto Prisma Access
    4. Aruba SD-WAN Integration with AWS Public Cloud
    5. Aruba SD-WAN Orchestrator
- Aruba SD-WAN and SD-Branch Online Help under Aruba Central
- Aruba SD-WAN Home Page:
    - Functionality and benefits of Aruba's SD-WAN solution
    - Functionality and benefits of Aruba's SD-Branch solution
- Aruba SD-WAN Datasheet: Includes ordering information for Aruba Virtual Gateways
- Aruba 7000 Series Datasheet
- Aruba 7200 Series Datasheet
- Aruba 9000 Series Datasheet
- Software-Defined Branch for Dummies: Aruba SD-Branch Solution
- Aruba SD-Branch and SD-WAN Technical Briefs
    - Dynamic Path Steering with Service Level Agreements
    - Seamless SD-WAN Orchestration
    - Optimizing SaaS with Aruba SD-WAN
    - Using Aruba SD-WAN with Microsoft Azure Virtual WAN
    - Orchestrating Virtual Gateways in Public Cloud Infrastructure
    - Unified Policy and Management for the Distributed Enterprise
    - Using Aruba SD-WAN with AWS Transit Gateway Network Manager
    - Advanced Threat Defense with Aruba SD-Branch

About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable™, Certified Reliable™, Certified Secure™ and Certified Green™. Products may also be evaluated under the Performance Verified™ program, the industry's most thorough and trusted assessment for product usability and performance.

Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report, but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

By downloading, circulating or using this report this report in any way you agree to Miercom's Terms of Use. For full disclosure of Miercom's terms, visit: https://miercom.com/tou.