
# Secure SD-WAN

Certification Testing Report

## Aruba
## Aruba EdgeConnect Enterprise

**Tested against this standard**
ICSA Labs Secure SD-WAN Criteria Version 1.0

August 9, 2022

Prepared by ICSA Labs
1000 Bent Creek Blvd., Suite 200
Mechanicsburg, PA 17050
www.icsalabs.com

# ICSA Labs Secure SD-WAN
## Certification Testing Report

a Hewlett Packard Enterprise company

## Aruba EdgeConnect Enterprise SD-WAN Platform

www.arubanetworks.com/products/sd-wan/edgeconnect/

| SD-WAN Components Tested | |
|---|---|
| SD-WAN Edge Devices: | EC-M-P<br>EC-XS |
| Other Component(s): | Orchestrator |

Certified
Since August 2022

ICSA labs CERTIFIED SECURE SD-WAN

## Summary of Test Results

| | |
|---|---|
| Support for multiple WAN paths | ✓ |
| Dynamic path selection | ✓ |
| Auto-provisioning of SD-WAN edge devices | ✓ |
| Single pane-of-glass administrative interface | ✓ |
| Configure, deploy firewall policies on SD-WAN edge devices | ✓ |
| Capability to perform secure remote upgrades of SD-WAN edge devices | ✓ |
| Identification and authentication of administrative users | ✓ |
| Secure remote administration | ✓ |
| Confidentiality of in-transit administrator communications | ✓ |
| Confidentiality of in-transit sensitive data | ✓ |
| Real-time metrics, reporting of data items & relevant status information | ✓ |
| Logs with relevant data for select security, operational & administrative events | ✓ |
| Industry-accepted crypto protecting remote admin sessions, in-transit administrative data & in-transit sensitive data | ✓ |
| Support for advanced security functions (either built-in or via service chaining) | ✓ |
| Properly enforces policies applied to SD-WAN edge devices | ✓ |
| Stateful inspection of permitted network traffic | ✓ |
| Invulnerable to known attacks including DoS attacks | ✓ |
| Introduces no vulnerabilities to any systems | ✓ |

## About ICSA Labs

The goal of ICSA Labs is to significantly increase user and enterprise trust in information security products and solutions by establishing publicly vetted requirements and developing robust test methodologies. For over thirty years, ICSA Labs has performed independent, third-party security certification testing of computer and network security products, beginning with anti-malware testing in 1991.

## SD-WAN Technology

A software-defined wide-area network (SD-WAN) is a WAN edge technology that improves an organization's application performance, reduces its WAN implementation costs and simplifies deployment and administration. Across SD-WAN networks, SD-WAN edge devices dynamically select the best path for application traffic when there is path degradation independent of the underlying WAN connection types (e.g., broadband Internet, private MPLS and fixed wireless). Deployment and management of these edge devices is simplified with auto-provisioning and single-pane-of-glass administration.

## ICSA Labs Secure SD-WAN Certification Testing

In annual ICSA Labs Secure SD-WAN Certification testing, ICSA Labs tests the functional aspects of the components comprising an SD-WAN solution. Among other things, the methodology includes test cases to determine whether or not the SD-WAN devices under test support multiple WAN paths and if they dynamically select another WAN path when there is jitter, increased latency or bandwidth degradation.

As SD-WAN edge devices may replace on-premise routers, firewalls and next-gen firewalls, they must also provide the same kinds of security protections as these network security devices. Thus, an ICSA Labs Certified Secure SD-WAN solution has been tested to demonstrate that it is invulnerable to attacks including denial-of-service (DoS) attacks, encrypts communication and sensitive in-transit data with industry-accepted cryptographic algorithms, properly enforces security and other policies applied to SD-WAN edge devices, and provides stateful inspection of permitted traffic.

## Product Overview

In the recently completed Secure SD-WAN test cycle, ICSA Labs tested the Aruba EdgeConnect Enterprise SD-WAN platform. Aruba describes the Aruba EdgeConnect Enterprise as follows:

Aruba EdgeConnect Enterprise SD-WAN platform powers a secure self-driving wide area network for cloud-first enterprise organizations to dramatically reduce the cost and complexity of building a Secure SD-WAN. By empowering organizations to use broadband connections to augment or replace their current MPLS networks, Aruba improves IT efficiency and responsiveness, increases application performance, and significantly reduces capital and operational expenses by up to 90 percent. The Aruba EdgeConnect Enterprise SD-WAN enables organizations to implement consistent QoS and security policies on an end-to-end network comprising WLAN, switching, SD-WAN, and remote access, all protected by common Zero Trust and SASE security frameworks, built-in from the start. Advanced SD-WAN with identity-based traffic segmentation and built-in NGFW ensures consistent security policies are applied from the access edge to the WAN edge to the cloud enabling organizations to retire on-premises routers and firewalls.

## Testbed

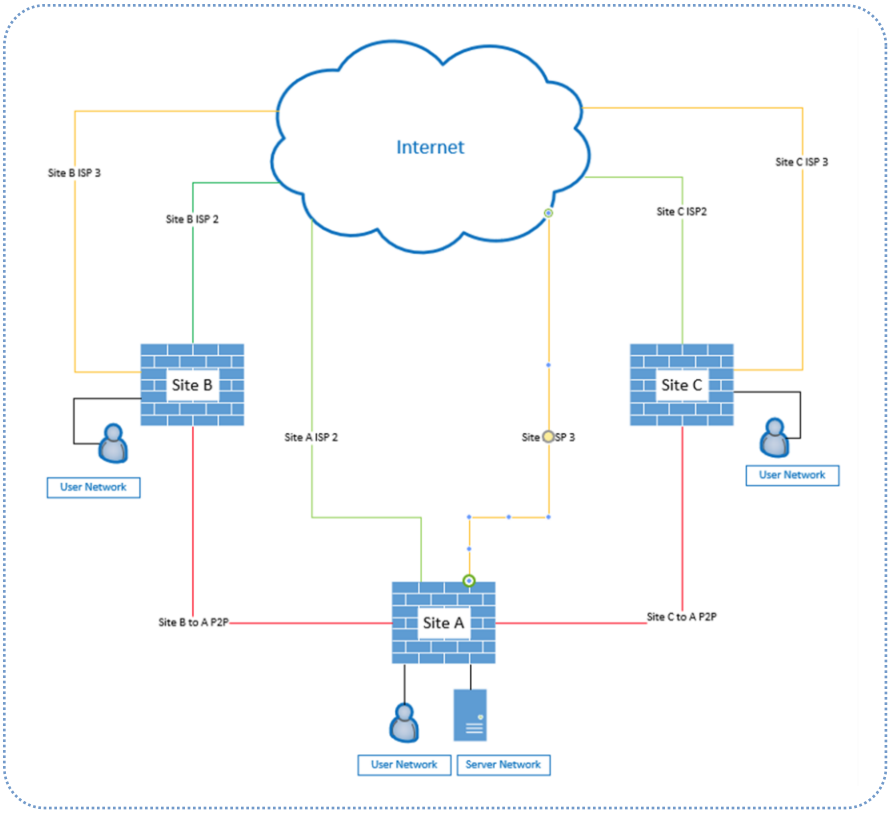


Fig. 1 – ICSA Labs SD-WAN Network Diagram

The testbed for ICSA Labs Secure SD-WAN Certification testing was developed to simulate a data center with two remote branches. The testbed therefore typically requires a minimum of three SD-WAN edge devices.

Having a minimum of three devices is necessary in order for ICSA Labs to emulate the complexity of SD-WAN edge devices that employ a variety of WAN connection types, that need to be auto-provisioned and that dynamically select the best path for application traffic if/when path degradation occurs.

In Figure 1, on the left, Site A represents the headquarters with users and hosting various servers, while Sites B and C represent the two remote branches with users in the SD-WAN test network.

## Tested Components – Secure SD-WAN Solution

Aruba provided or otherwise made available the following hardware, firmware and/or software to ICSA Labs for the recent and successfully-completed ICSA Labs Secure SD-WAN certification test cycle.

| | Site | Hardware/Component | Initial Version | Final Version |
|---|---|---|---|---|
| Data Center | A | EC-M-P | 8.2.1.0-77228 | 9.2.0.0-93688 |
| Branches | B | EC-XS | 8.2.1.0-77228 | 9.2.0.0-93688 |
| | C | EC-XS | 8.2.1.0-77228 | 9.2.0.0-93688 |
| | | | | |
| Administration | | Orchestrator | 8.8.6.40118 | 9.2.0.4031 |

Note that if the final version of either the firmware or software in the table above differs from the initial version from the beginning of testing, then the reason for this version difference is explained in the Criteria Violations and Resolutions section of this report.

## SD-WAN Functionality – Configuration & Findings

### WAN Paths

ICSA Labs configured the Aruba EdgeConnect Enterprise devices through the cloud-based Orchestrator to permit traffic flows as shown in Figure 2 below. In Aruba EdgeConnect Enterprise parlance, Site A was set to be the "HUB" as it

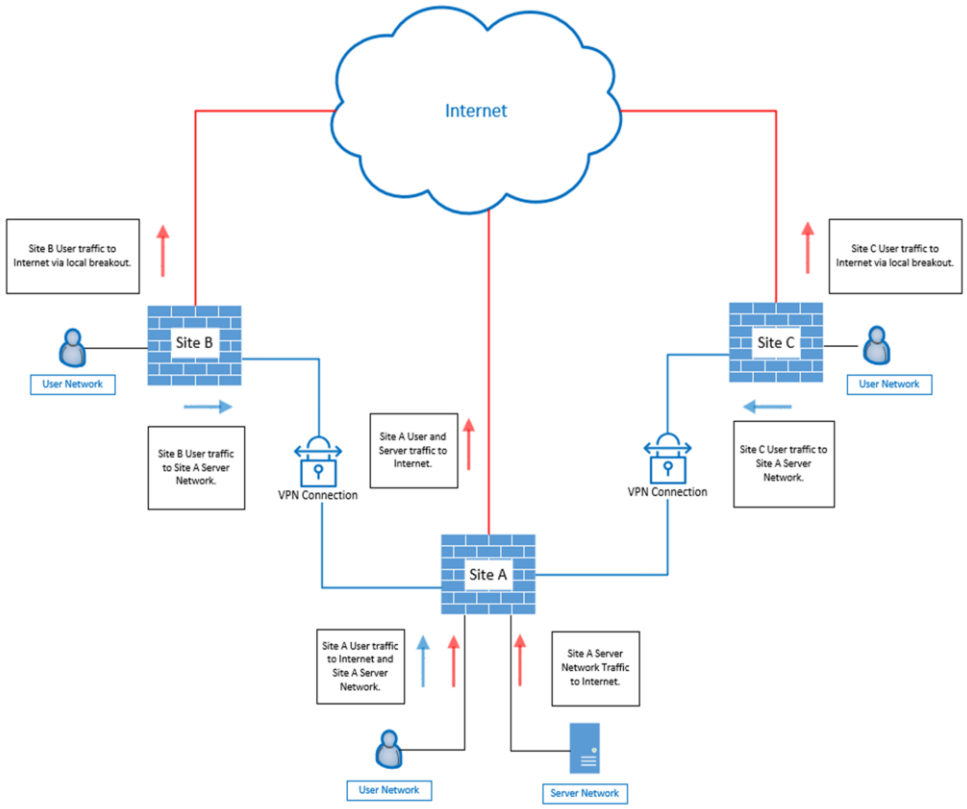


Fig. 2 – ICSA Labs SD-WAN Traffic Flows

represents the main location or headquarters, while Sites B and C were set to be "SPOKES" as they represent remote branches. Between Sites A and B as well as between Sites A and C (there is no connection between Sites B and C), ICSA Labs configured the products to use three WAN paths:

1. P2P link (aka STS1) – simulating a leased line from a Telco;
2. ISP2 (aka INET1) – simulating a cable modem type Internet connection from an ISP;
3. ISP3 (aka INET2) – simulating a LTE cellular back up connection from a wireless provider.

Depicted in Figure 3 below is an image taken from the Orchestrator showing Site B's deployment profile. Deployment profiles set which interfaces are tied to which firewall zones, the interface's bandwidth and the firewalling mode (whether or not NAT is used) for outbound connections. Deployment profiles also control how the Aruba EdgeConnect appliances interconnect. EdgeConnect employs "IKEless" IPSEC tunnels. The "IKE" layer of IPSEC is handled through the EdgeConnect Orchestrator which manages and distributes IPSEC key material to SD-WAN appliances.

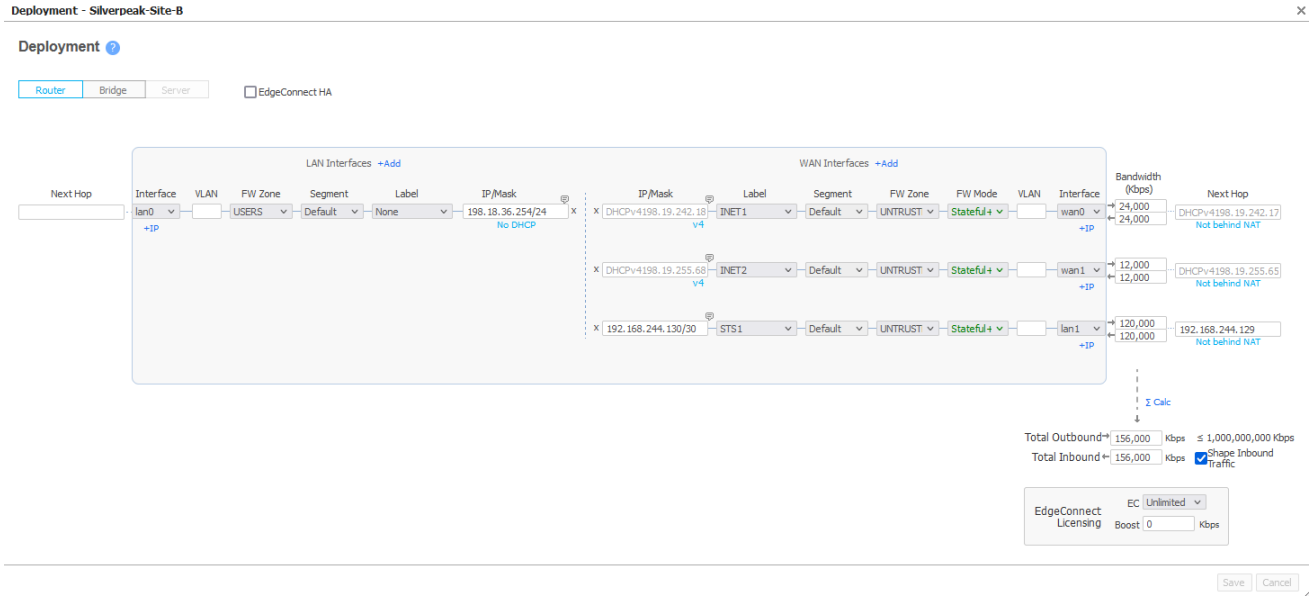


Fig. 3 – Site B's Deployment profile

## Dynamic Path Selection

ICSA Labs configured dynamic path selection in the Orchestrator using the Business Intent Overlay. For example, ICSA Labs configured the RealTime view such that traffic would "breakout" and "waterfall" into ISP2 when the P2P link degraded. Figure 4 below depicts traffic changing WAN paths after degradation and "waterfalling" into another path. Then, after the degradation ends, the figure shows pictorially how traffic is restored to the initial P2P WAN path.

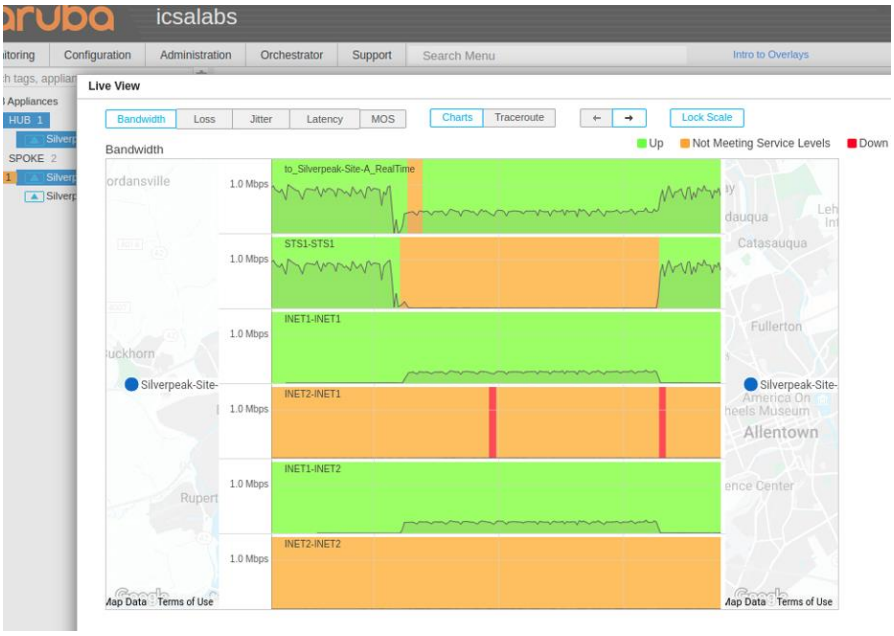


Fig. 4 – Traffic "Waterfalls" from one WAN path to another after degradation

### Auto-Provisioning SD-WAN Edge Devices

In terms of other SD-WAN functionality, ICSA Labs tested to confirm that Aruba EdgeConnect devices can be properly and securely configured and that they thus support zero touch automatic provisioning.

## Administration, Logging, Analytics

### Single Pane-of-Glass Admin Interface

Aruba EdgeConnect Enterprise SD-WAN platform devices are remotely and securely administered with the cloud-based Orchestrator. Aruba's Orchestrator provides a single pane-of-glass interface from which admins provision all SD-WAN edge devices Through Orchestrator, admins decide which WAN paths will be used, what security policy(ies) will be deployed, etc.

Through this single pane of glass, administrators - after being properly identified and authenticated - can additionally review log data related to all logged events as well as various analytics including real-time metrics such as those shown in Figure 5 below.

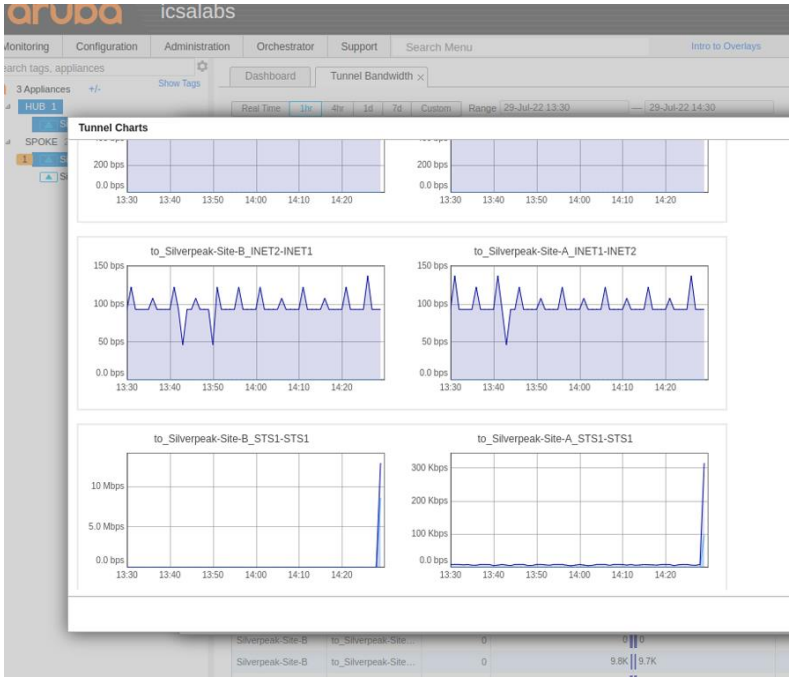


Fig. 5 – Real-time metrics for one of the paths

### Logging Security, Operational and Administrative Events

ICSA Labs tested that the Aruba EdgeConnect Enterprise devices log both allowed and denied traffic, administrative changes to both the security policy and non-security-related policy data.

Among the logs is an interesting one with counters recording DDoS profile hits. This log is viewed by launching a shell from the Orchestrator and issuing the following command:

```
show ddos profile src-zone <zone number> stats detail
```

Figure 6 below shows this DDoS profile log. Its contents persist until an admin clears it. Depicted, one can see hits for out-of-state ICMP packets and Invalid TCP connections, among other things. Of the counters are indications that since the last time these log counters were cleared, the Aruba EdgeConnect Enterprise device at Site B saw 37 out-of-state ICMP error packets and 4 where an ICMP echo reply was seen before the echo request.

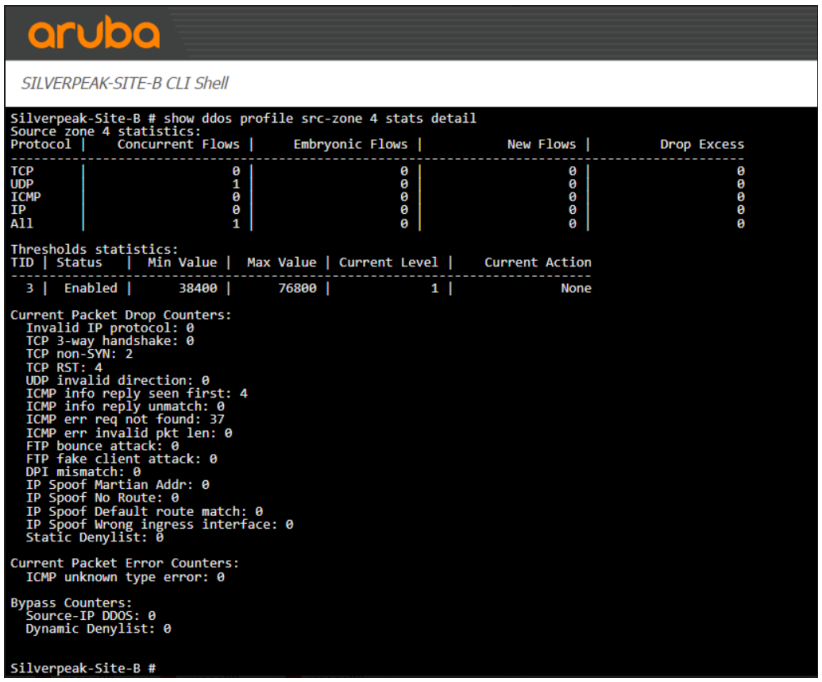


Fig. 6 – DDoS Profile Log for Site B

As a final note about logging, when the WAN interfaces are set to stateful+snat, Aruba EdgeConnect Enterprise devices will not log traffic aimed for and arriving at its external interface. Aruba indicated that this is by design, given that no traffic is permitted inbound in this configuration.

## Secure SD-WAN Testing

ICSA Labs Secure SD-WAN Certification Testing is much more than an SD-WAN functionality test. As SD-WAN Edge Devices may replace network security devices, they must also provide the same kinds of security protections as would a firewall. In fact, the policy configuration requirement to set security policies for network traffic in ICSA Labs Secure SD-WAN testing is equivalent to ICSA Labs Corporate Firewall Certification. Thus while the network topologies differ for the two testing services, the ICSA Labs security testing is the same.

The Aruba EdgeConnect Enterprise was tested to confirm that:

- The SD-WAN Edge devices are invulnerable to attack;
- The communications between SD-WAN Edge devices are secure;
- The SD-WAN Edge devices are stateful and properly enforce all policies – both those that are security policies and those that are WAN-specific.

### Policy Enforcement

As in its firewall testing, ICSA Labs tests that Secure SD-WAN edge devices are stateful, that they are not susceptible to trivial denial of service attacks, that the edge devices themselves are invulnerable to known threats, and that they each properly enforce the configured security policy. As a result, ICSA Labs Secure SD-WAN testing includes rigorous security-related test cases.

Figure 7 below shows Site B's Firewall Protection Profile. As a result of this ICSA Labs test cycle, Aruba made significant improvements to its stateful inspection and DoS protections. In fact, all of the checked boxes under "Security Settings" in the figure were added as a result of testing.

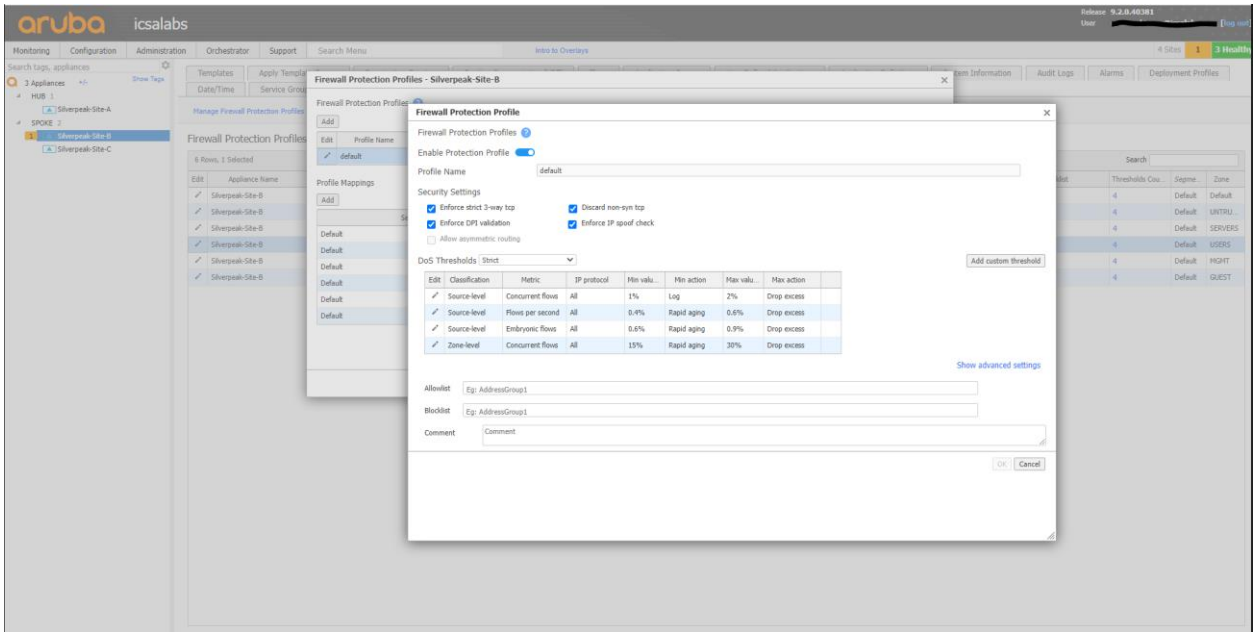


Fig. 7 – Site B's Firewall Protection Profile

The Aruba EdgeConnect Enterprise Orchestrator depicts the state of sessions in a Flow Table. ICSA Labs found this table, shown below in Figure 8, useful for troubleshooting active traffic issues. Seeing traffic that should be blocked or vice versa came in handy during the test cycle. One can also see other things in the Flow Table including how much bandwidth is in use for a particular connection. Clicking on any line item in the table, an admin can drill down to see which firewall security policy rule is being triggered.

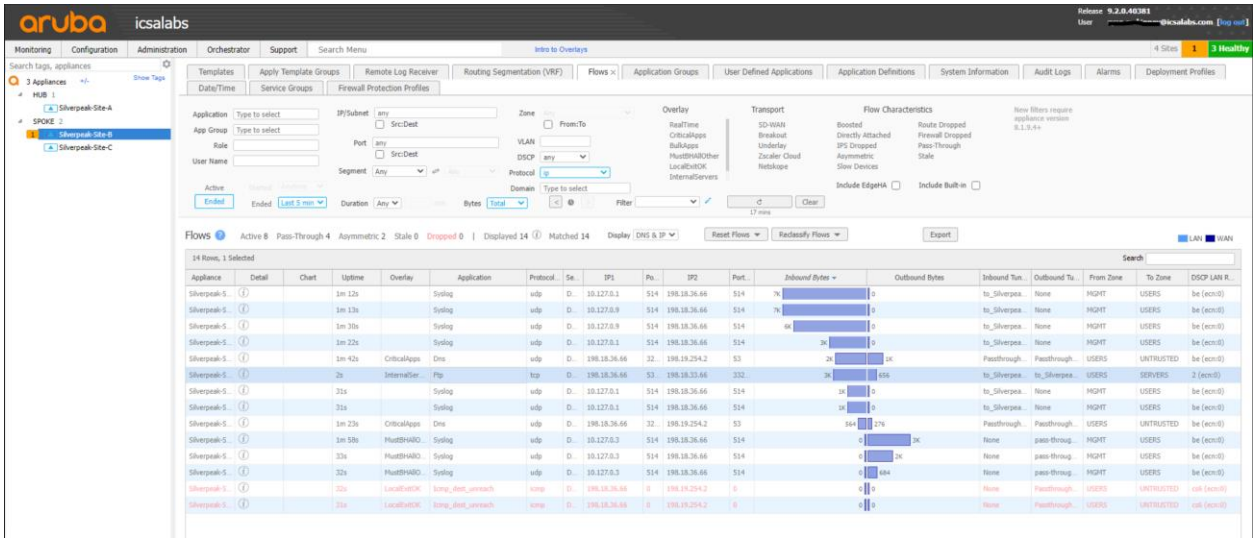


Fig. 8 – Site B's Flow Table

## Cryptographic Protection of Admin & Operational Communication

The Aruba EdgeConnect Enterprise devices supported just one TLS v1.2 cipher suite. No others were supported. In testing, the server selected only the following NIST-approved cipher suite:

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

## Additional Security Protections

In addition to security testing, ICSA Labs tested to confirm that the SD-WAN Edge devices provide additional security functionality either inherently in itself or via an external mechanism such as service chaining one or more external security products (e.g., anti-malware, Secure Web Gateway, etc.). Note that ICSA Labs Secure SD-WAN testing does not include efficacy testing of these added security features but instead confirms their availability. To test the efficacy of these added security functions, like anti-malware, ICSA Labs offers separate security certification testing services for interested parties.

For the Aruba EdgeConnect Enterprise, added security functionality is provided via service chaining with Aruba partners, Zscaler or Netskope. To configure this, an administrator does so in the Business Intent Overlay in the Orchestrator. From there, partner cloud security services are available to Aruba customers via breakout traffic to the Internet and cloud.

## Criteria Violations and Resolutions

During initial testing of the Aruba EdgeConnect Enterprise, ICSA Labs discovered several shortcoming in the SD-WAN edge devices that needed to be corrected:

- did not properly enforce TCP session state inspection
  - allowed packets with improper TCP flags combinations prior to successful 3-way TCP handshake;
  - allowed replayed TCP RST packets
  - allowed spoofed TCP RST packets;
- was vulnerable to FTP fake Client attack.
- did not prevent spoofing attacks.
- did not allow valid ICMP response packets.
- did not properly mitigate trivial DoS attacks.

Once corrected by Aruba, ICSA Labs confirmed through additional re-testing that the identified issues were properly remediated and that no new issues were uncovered.

## ICSA Labs Secure SD-WAN Certification

Because Aruba's EC-M-P and EC-XS SD-WAN devices passed all of the functional and security test cases performed by ICSA Labs and as the tested devices met the entire set of testing criteria requirements, ICSA Labs is pleased to state that these models and the other models comprising the Aruba EdgeConnect Enterprise SD-WAN platform attained ICSA Labs Secure SD-WAN Certification.

## Authority

This report is issued by the authority of the General Manager, ICSA Labs. Tests are performed under normal operating conditions.

Darren Hartman

Darren Hartman, General Manager, ICSA Labs

### ICSA Labs

The goal of ICSA Labs is to significantly increase user and enterprise trust in information security products and solutions. For more than 30 years, ICSA Labs, an independent division of Verizon, has been providing credible, independent, 3rd party security product testing and certification for many of the world's top security product developers and service providers. Enterprises worldwide rely on ICSA Labs to set and apply objective testing and certification criteria for measuring product compliance and performance.

www.icslabs.com

### Aruba, a Hewlett Packard Enterprise company

Aruba, a Hewlett Packard Enterprise company, is a global leader in secure, intelligent edge-to-cloud networking solutions that use AI to automate the network, while harnessing data to drive powerful business outcomes. With Aruba ESP (Edge Services Platform) and as-a-service options, Aruba takes a cloud-native approach to helping customers meet their connectivity, security, and financial requirements across campus, branch, data center, and remote worker environments, covering all aspects of wired, wireless LAN, and wide area networking (WAN).

www.arubanetworks.com