

# Arista Remote Access Point Design Guide

## Introduction

Arista's Remote Access Point can be leveraged to extend corporate managed Wi-Fi access to remote teleworkers, eliminating the complexities of software client VPN access and providing a simple, fast and secure remote access solution. Leveraging a hardware based standards approach that allows corporate security policies to be extended directly to the user base anywhere there is a reliable internet connection.

## Key features

Ability to extend Corporate SSID to a remote workplace

- Teleworkers' office

IPSec VPN tunnel from the AP to the Data Center (DC)

- Traffic from Wi-Fi devices connecting to the SSID to the DC to flow via the tunnel
- VPN setup not required individually on the Wi-Fi devices
- Split tunnel functionality limits only corporate traffic through the tunnel
  - › Internet and web traffic can be split directly to the internet from the AP
  - › Preserves precious VPN throughput at the head-end

Works with industry standard firewalls

- No additional investment required at the DC
- Tested with firewalls from Palo Alto Networks, Juniper, Cisco, CheckPoint, and Fortinet

Ease of configuration and ease of deployment with cloud based remote management & visibility. Zero Touch Provisioning (ZTP) can be leveraged for rapid deployment at massive scale. CloudVision CUE (CV-CUE) allows very flexible configurations utilizing hierarchical configuration management allowing consistent configuration to be deployed based on use case requirements.

Leverage the same AL/ML capabilities that are utilized on CloudVision CUE (CV-CUE) on the campus are extended to the remote office, enhancing administrators visibility and ability to troubleshoot common connectivity issues.

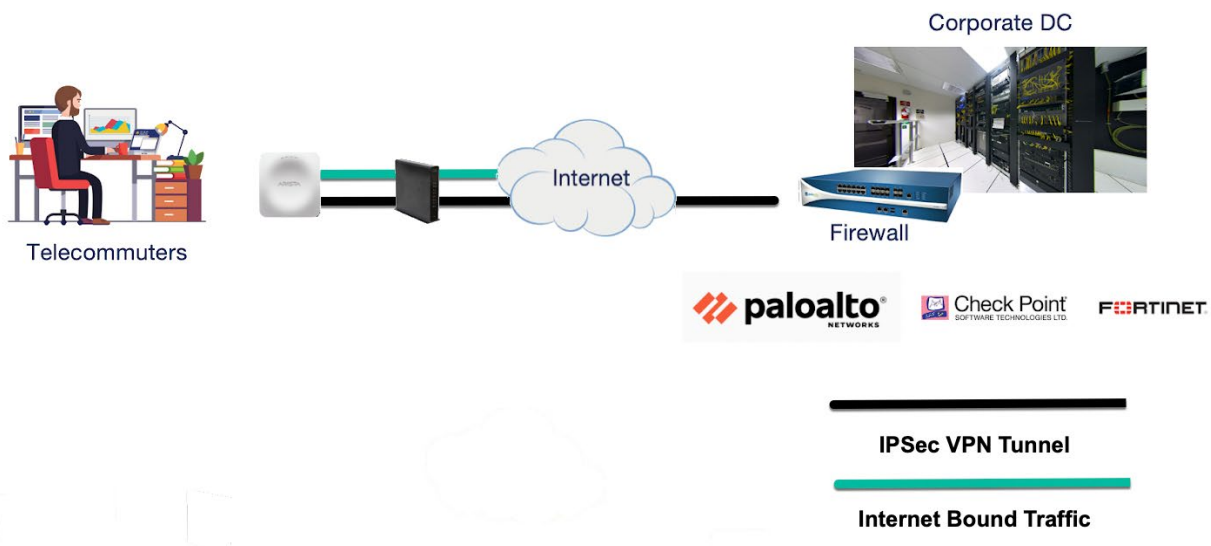
- Application QoE / Single Client Inferencing
- Automatic Packet Capture / Visual Packet Capture Analysis
- Client Journey
- Network Baselining
- Root Cause Analysis / Inference Engine

## Benefits of CV-CUE Remote AP Solution

- Brings the enterprise connectivity paradigm to any workspace
  - › 802.1x and other mechanisms all continue to work.
- Keeping up the controller-less model APs terminate encrypted tunnels on standard firewalls/VPN concentrators
  - › No specialized devices
  - › No scale limitations; easily scales to 10s of 1000s of remote APs

- Multiple Tunnel Options
  - › Tunnel
  - › Split-Tunnel
- No flooding or other unwanted broadcast storms over WAN/Internet
  - › Existing solutions limited by controller architecture forces to stretch VLANs across Internet/WAN
  - › Cleaner solution, keeping up with Arista's open standards models
- Flexible client authentication
  - › Enterprise RADIUS Servers
  - › Okta
  - › Google Authentication
  - › SecureW2
  - › Captive Portal
  - › Pre-Shared Key

## Arista Remote Access Point - Typical Deployment

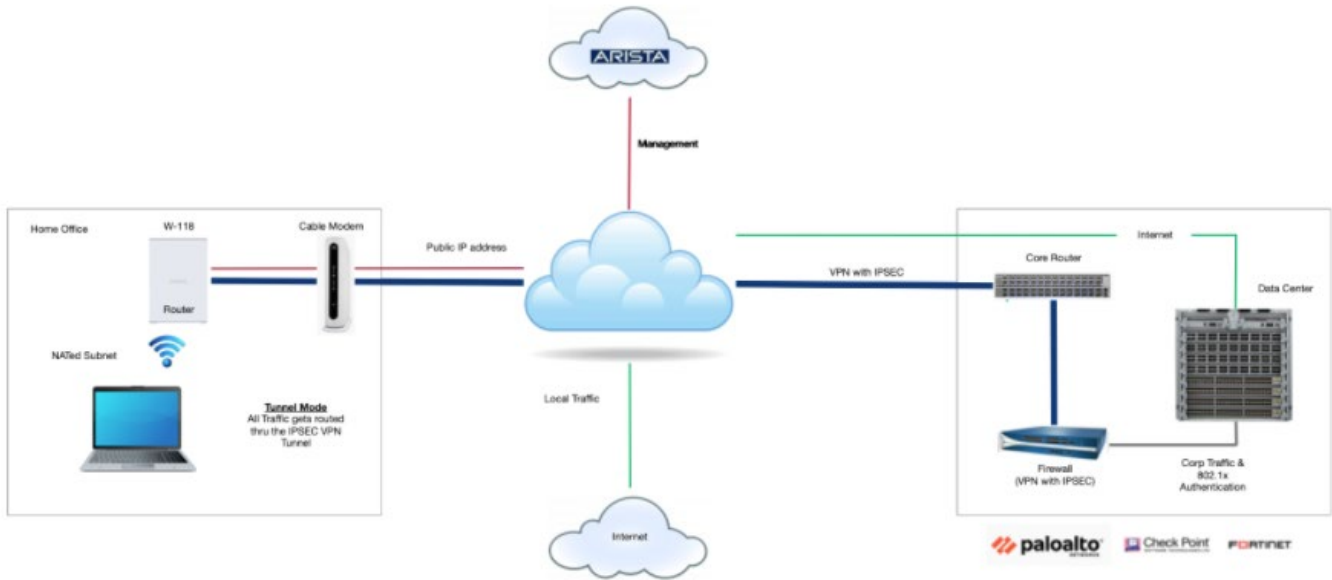


### Use Cases

The Arista Remote Access Point can be configured to tunnel all traffic over standards based IPsec tunnels. The protocol is an industry standard L2 encapsulation method that can be terminated on any router, firewall or WLAN controller that supports IPsec. In theory any device that supports IPsec can be used at the head end but we have verified that we can terminate an IPsec tunnel originating on an Arista Remote Access Point on a Palo Alto Firewall, Juniper SRX, Cisco ASA or Aruba Controller.

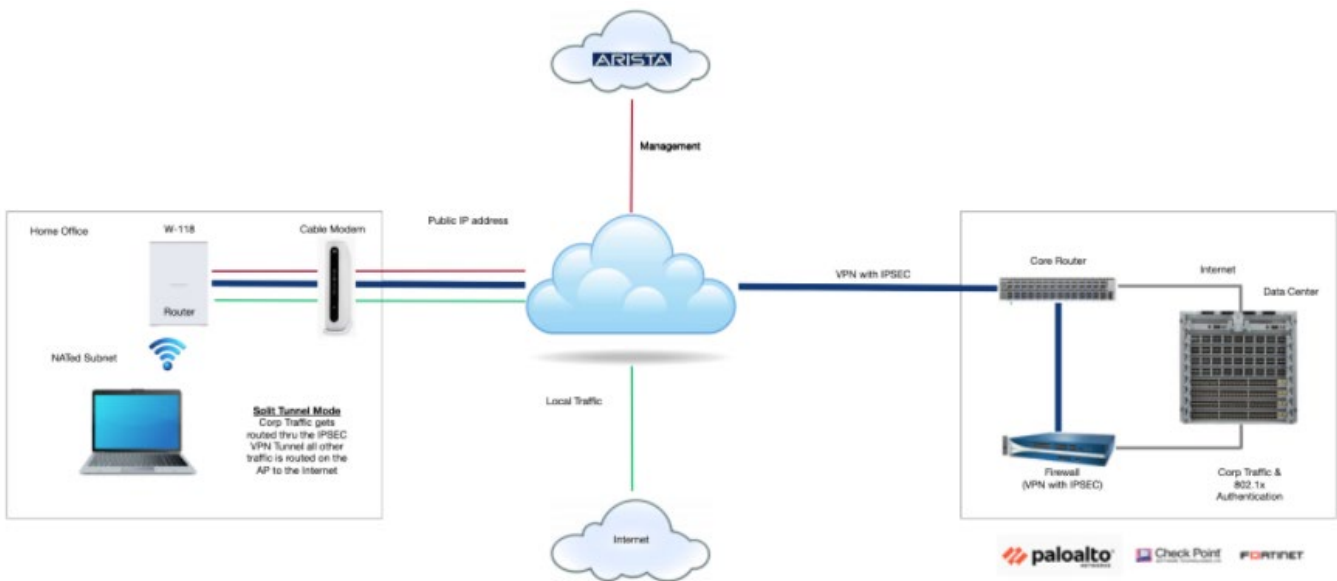
### Home Office Use Case #1 (Tunnel Mode):

The Arista Remote Access Point that is Cloud Managed and has an IPsec tunnel to a head end Tunnel Terminator (Palo Alto Firewall, Juniper SRX, Cisco ASA) utilizing flexible authentication options via a 802.1x, Pre-Shared Key or Captive Portal. All traffic is sent to the head end and processed by existing corporate security tools.



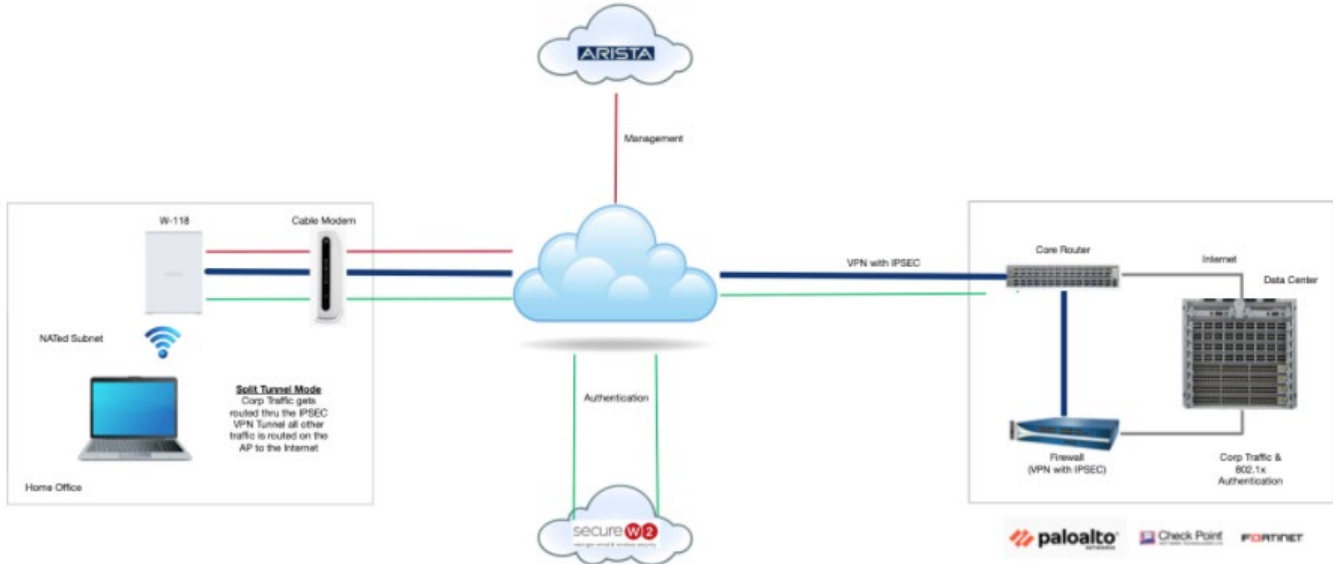
### Home Office Use Case #2 (Split-Tunnel Mode):

The Arista Remote Access Point that is Cloud Managed and has an IPsec tunnel to a head end Tunnel Terminator (Palo Alto Firewall, Juniper SRX, Cisco ASA) utilizing flexible authentication options via a 802.1x, Pre-Shared Key or Captive Portal. Corporate traffic is sent to the head end via the tunnel while all other traffic is routed through the local network.



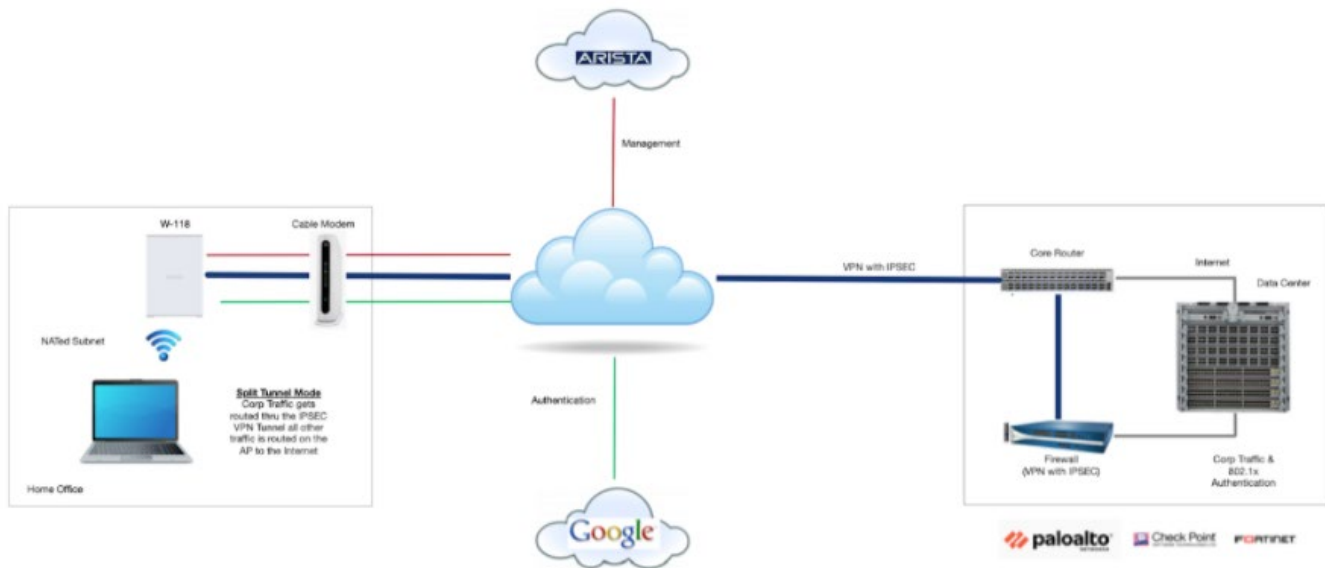
### Home Office Use Case #3 (Cloud Based Strong Authentication):

Arista Remote Access Point that is Cloud Managed and has an IPSec tunnel to a head end Tunnel Terminator (Palo Alto Firewall, Juniper SRX, Cisco ASA). Clients can be 802.1x authenticated via an internet authentication cloud service like Secure W2. The cloud authenticator would have to have a federated identity management service to authenticate users.



### Homeschool Use Case #1 (Google Authentication):

Arista Remote Access Point that is Cloud Managed and has the option to use an IPSec tunnel to a head end Tunnel Terminator (Palo Alto Firewall, Juniper SRX, Cisco ASA) or go directly to the Internet with student traffic. Clients can use a Pre-Shared Key or 802.1x authentication via G Suite for Education using the Arista Enforce feature that integrates G Suite and Wireless Manager. Enforce allows the school to restrict which devices are allowed on the network by assigning VLANs, firewall rules, bandwidth control, and redirection based on user roles.



## Example Configuration Steps

The screenshot shows the Arista configuration interface for a Tunnel Interface. The left sidebar contains navigation options: ARISTA, DASHBOARD, MONITOR, CONFIGURE (highlighted), TROUBLESHOOT, REPORTS, FLOOR PLANS, SYSTEM, and Services. The main content area is titled 'Tunnel Interface' and includes tabs for WiFi, SSID, RADIUS, Tunnel Interface (selected), Role Profiles, Radio Settings, and Device Settings. The 'Tunnel Interface Name' section has an 'Enter Profile Name' field containing 'Tunnel Interface Name'. The 'Tunnel Type' dropdown menu is open, showing options: L2 TUNNEL, EoGRE, IPsec over EoGRE, VxLan, VPN TUNNEL, and VPN with IPsec. A blue hand icon points to 'VPN with IPsec'. Below the dropdown are fields for 'Remote Endpoint (IP / Hostname)', 'GRE Primary Key' (with a placeholder [0-65535]), and 'Local Endpoint VLAN' (with a placeholder [0-4094]). At the bottom right, there are 'Cancel' and 'Save' buttons. A callout bubble with a blue background and white text says: 'Create a new tunnel and choose "VPN with IPsec" as tunnel type.'

The screenshot shows the Arista configuration interface for a Tunnel Interface, continuing from the previous step. The 'Tunnel Type' dropdown is now set to 'VPN with IPsec - VPN Tunnel'. The 'Primary' and 'Secondary' tabs are visible, with a blue hand icon pointing to the 'Secondary' tab. Below the tabs is the 'Local Endpoint VLAN' field with a placeholder [0-4094]. The 'IPsec' section is expanded, showing 'Remote Endpoint (IP / Hostname)' fields for both Primary and Secondary destinations. A callout bubble with a blue background and white text says: 'Configure Primary and Secondary VPN destinations and parameters.'

The screenshot shows the Arista configuration interface for an SSID named "Spectrum". The interface is divided into a left sidebar with navigation options (ARISTA, DASHBOARD, MONITOR, CONFIGURE, TROUBLESHOOT, REPORTS, FLOOR PLANS, SYSTEM, Services, cvp admin) and a main configuration area. The main area has tabs for SSID, RADIUS, Tunnel Interface, Role Profiles, Radio Settings, and Device Settings. The "SSID" tab is active, and the "Network" sub-tab is selected. The "VLAN ID" is set to 0. The "Network Type" section has four radio buttons: Bridged (selected), NAT, L2 Tunnel, and VPN Tunnel. A callout box with a hand icon points to the "VPN Tunnel" option, with the text "Choose Network Type as 'VPN Tunnel' for SSID." Below this, there are checkboxes for "Layer 2 Traffic Inspection and Filtering", "Inter AP Coordination" (with options Layer 2 Broadcast, RF Neighbors, This Server), "Advertise Client Associations on SSID VLAN" (checked), and "DHCP Option 82". At the bottom right, there are "Cancel" and "Save" buttons.

## Remote Client Health and Performance Monitoring Application QoE / Single Client Inferencing

Know whether or not your users are happy with their experience of running VoIP and video conferencing applications on your network. In the event that users are experiencing poor application performance the system can do automatic root cause analysis and offer remediation recommendations.

The screenshot displays a dashboard for remote client health monitoring. At the top, there are four application-specific cards: GoToMeeting (3 clients, 12 affected), Hangouts (54 clients, 5 affected), MsTeams (33 clients, 6 affected), and Zoom (28 clients, 7 affected). Below these is a 'Clients' section with a bar chart and a table of characteristics: Associated SSID (Spectru... 49), Associated Access Point (Mojo\_01... 10), and Operating System (Microsof... 10). A table lists 5 clients with columns for Status, Name, User Name, MAC Address, No. of Sessions, Application Usage Time, Application Experience, and Potential Cause. A detailed view of a client connection log shows two events: 'Successfully Connected' at 10:23:12 AM and 'IP Failure' at 10:22:12 AM. A 'Recommendations' box suggests 'Dual-band clients operating in 2.4 GHz' and 'Enable band steering for following SSIDs'.

## Automatic Packet Capture / Visual Packet Capture Analysis

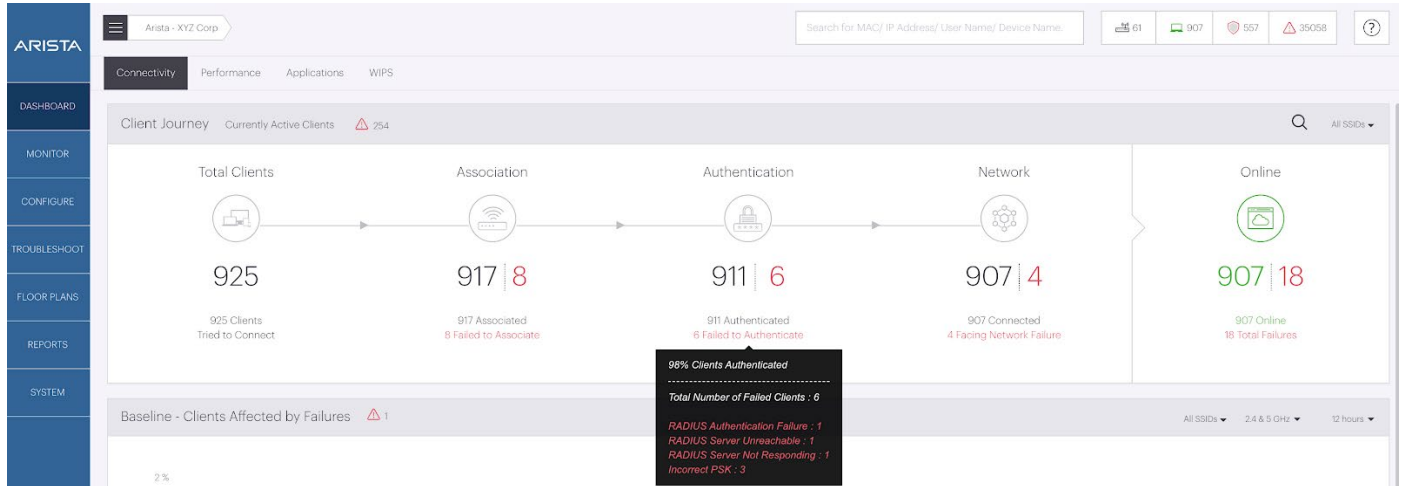
With real-time, inline packet capture, CloudVision CUE (CV-CUE) preemptively captures packet traces to help capture problems. The traces are stored alongside related failures or symptoms to simplify troubleshooting at a later time. Packet traces can be downloaded or directly visualized in Arista Packets, the cloud-based, visual Wi-Fi packet analyzer.

The screenshot shows the Arista Packets interface for visual packet capture analysis. On the left, a client connection log shows a 'RADIUS Authentication Failure' event at 3:07:30 PM and a 'Successfully Connected' event at 3:05:18 PM. The main area displays a packet capture visualization with a timeline of frame numbers (415 to 622) and data rates (0.00 Kbps to 781.25 Mbps). A specific event is highlighted: 'Deauthentication(Tx)' at frame 448, with destination 00:11:74:41:11:40 and time 107.435517000. The interface also includes a search bar and various status indicators.



## Client Journey

CloudVision CUE (CV-CUE) provides direct and real-time insight into the experience of Wi-Fi clients as they journey on the network. Client Journey tracks when and why clients fail to connect to the network, reporting latencies of network services such as AAA, DHCP, and DNS. Administrators can drill down and access live and historical client connection logs to aid troubleshooting.



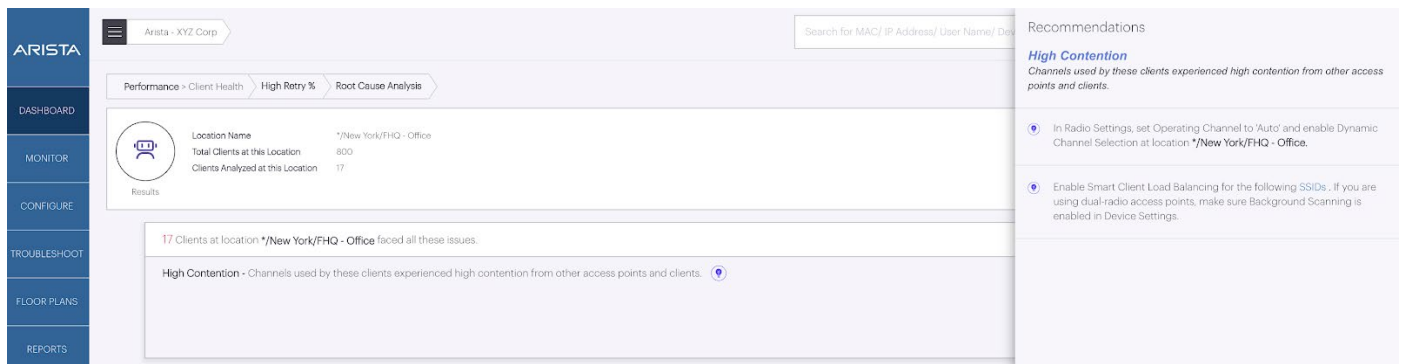
## Network Baseline

Using machine-learning algorithms on the telemetry it collects, CloudVision CUE (CV-CUE) baselines network traffic and automatically detects and highlights anomalies.



## Root Cause Analysis / Inference Engine

Using machine-learning algorithms on the telemetry it collects, CloudVision CUE (CV-CUE) baselines network traffic and automatically detects and highlights anomalies.



## Conclusion

The Arista Remote Access Point, allows for flexible and rapid deployment of corporate managed secure wireless remote access to anywhere in the world. Leveraging Arista's CloudVision-Wi-Fi management platform, IT administrator and helpdesk resources will have visibility to common network failures (Authentication, Authorization, Network Services), root cause analysis recommendations and remote packet captures that they desperately needed in today's predominantly work from home environments.

For more information on the Arista Remote Access Point solution, please visit our website: <https://www.arista.com>

### **Santa Clara—Corporate Headquarters**

5453 Great America Parkway,  
Santa Clara, CA 95054

Phone: +1-408-547-5500

Fax: +1-408-538-8920

Email: [info@arista.com](mailto:info@arista.com)

### **Ireland—International Headquarters**

3130 Atlantic Avenue  
Westpark Business Campus  
Shannon, Co. Clare  
Ireland

### **Vancouver—R&D Office**

9200 Glenlyon Pkwy, Unit 300  
Burnaby, British Columbia  
Canada V5J 5J8

### **San Francisco—R&D and Sales Office 1390**

Market Street, Suite 800  
San Francisco, CA 94102

### **India—R&D Office**

Global Tech Park, Tower A, 11th Floor  
Marathahalli Outer Ring Road  
Devarabeesanahalli Village, Varthur Hobli  
Bangalore, India 560103

### **Singapore—APAC Administrative Office**

9 Temasek Boulevard  
#29-01, Suntec Tower Two  
Singapore 038989

### **Nashua—R&D Office**

10 Tara Boulevard  
Nashua, NH 03062



Copyright © 2022 Arista Networks, Inc. All rights reserved. CloudVision, and EOS are registered trademarks and Arista Networks is a trademark of Arista Networks, Inc. All other company names are trademarks of their respective holders. Information in this document is subject to change without notice. Certain features may not yet be available. Arista Networks, Inc. assumes no responsibility for any errors that may appear in this document. June 1, 2022