Arista Remote Access Point Design Guide

Introduction

Arista's Remote Access Point can be leveraged to extend corporate managed Wi-Fi access to remote teleworks, 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.

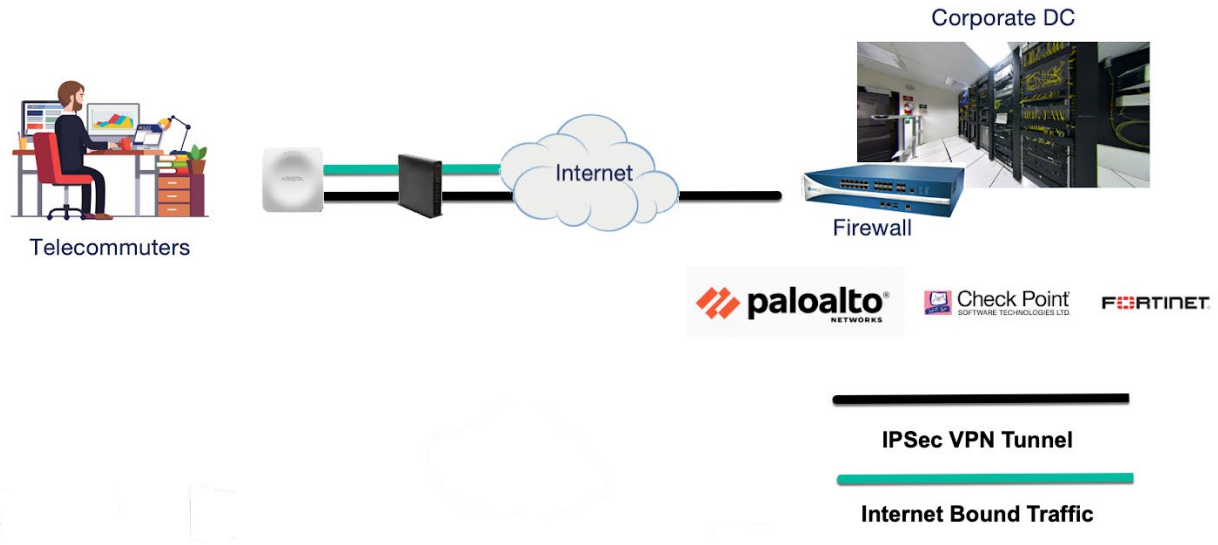
- Application QoE / Single Client Inferencing
- Automatic Packet Capture / Visual Packet Capture Analysis
- Client Journey
- Network Baselining
- Root Cause Analysis / Inference Engine

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

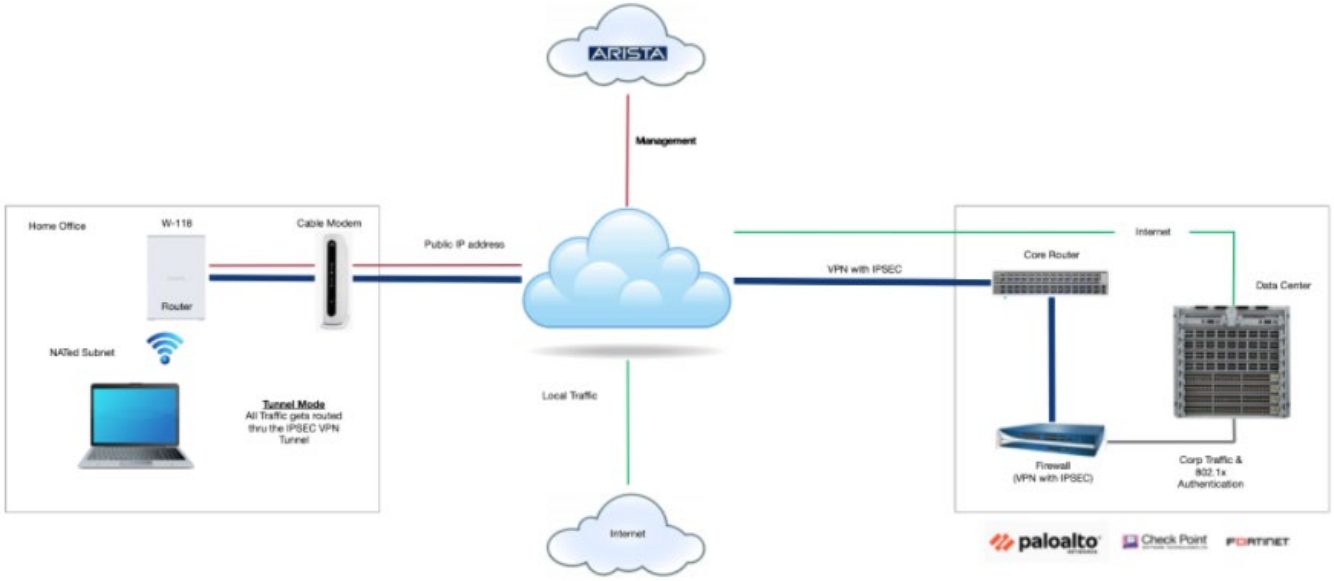


Use Cases

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.

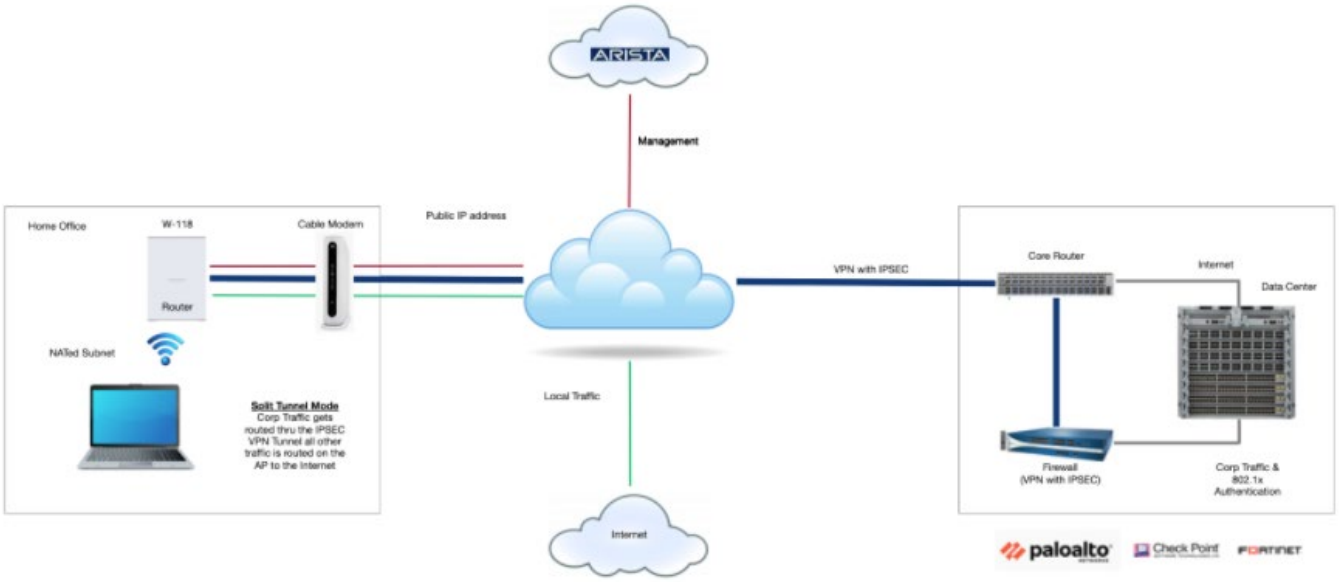
Home Office Use Case #1 (Tunnel Mode):

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.



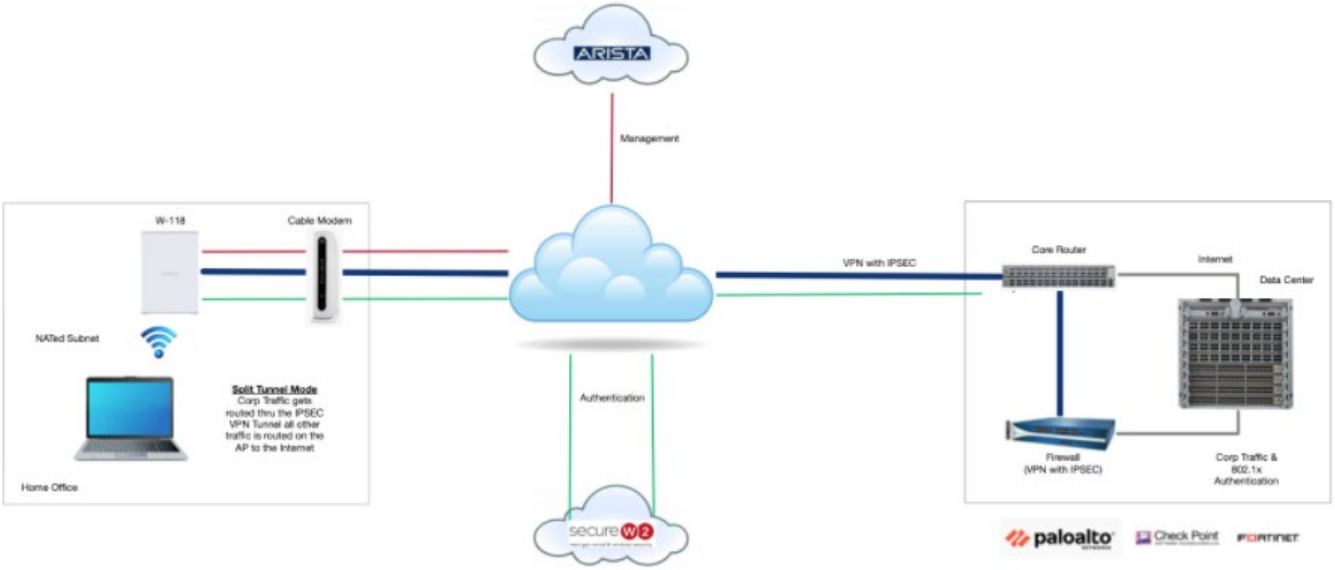
Home Office Use Case #2 (Split-Tunnel Mode):

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.



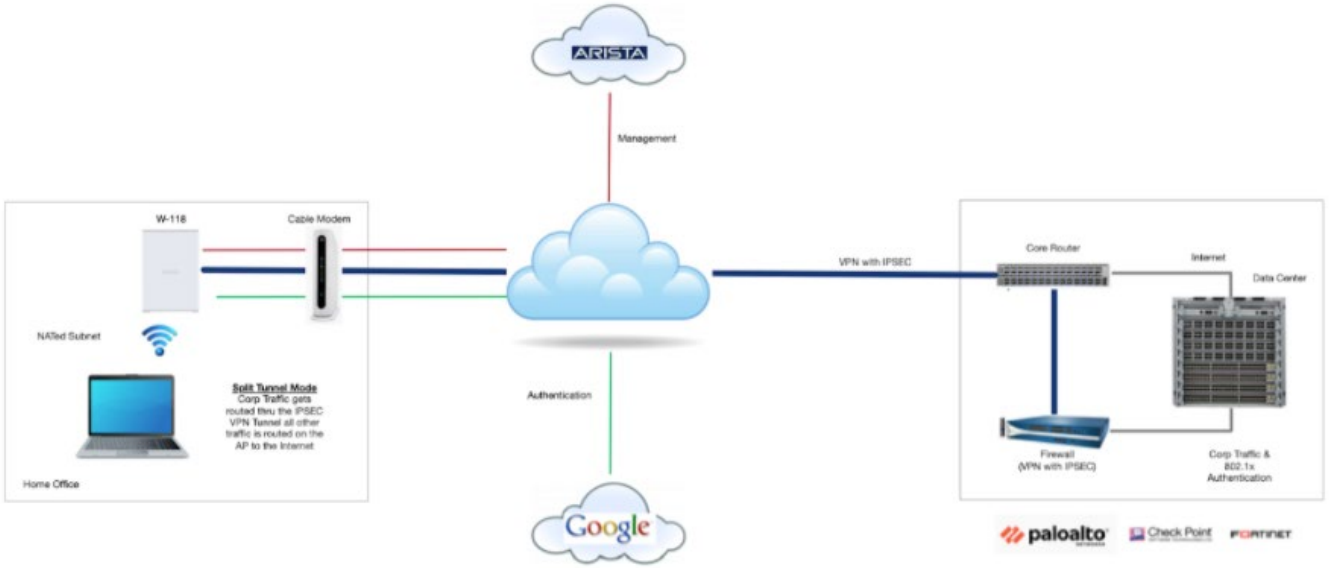
Home Office Use Case #3 (Cloud Based Strong Authentication):

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.

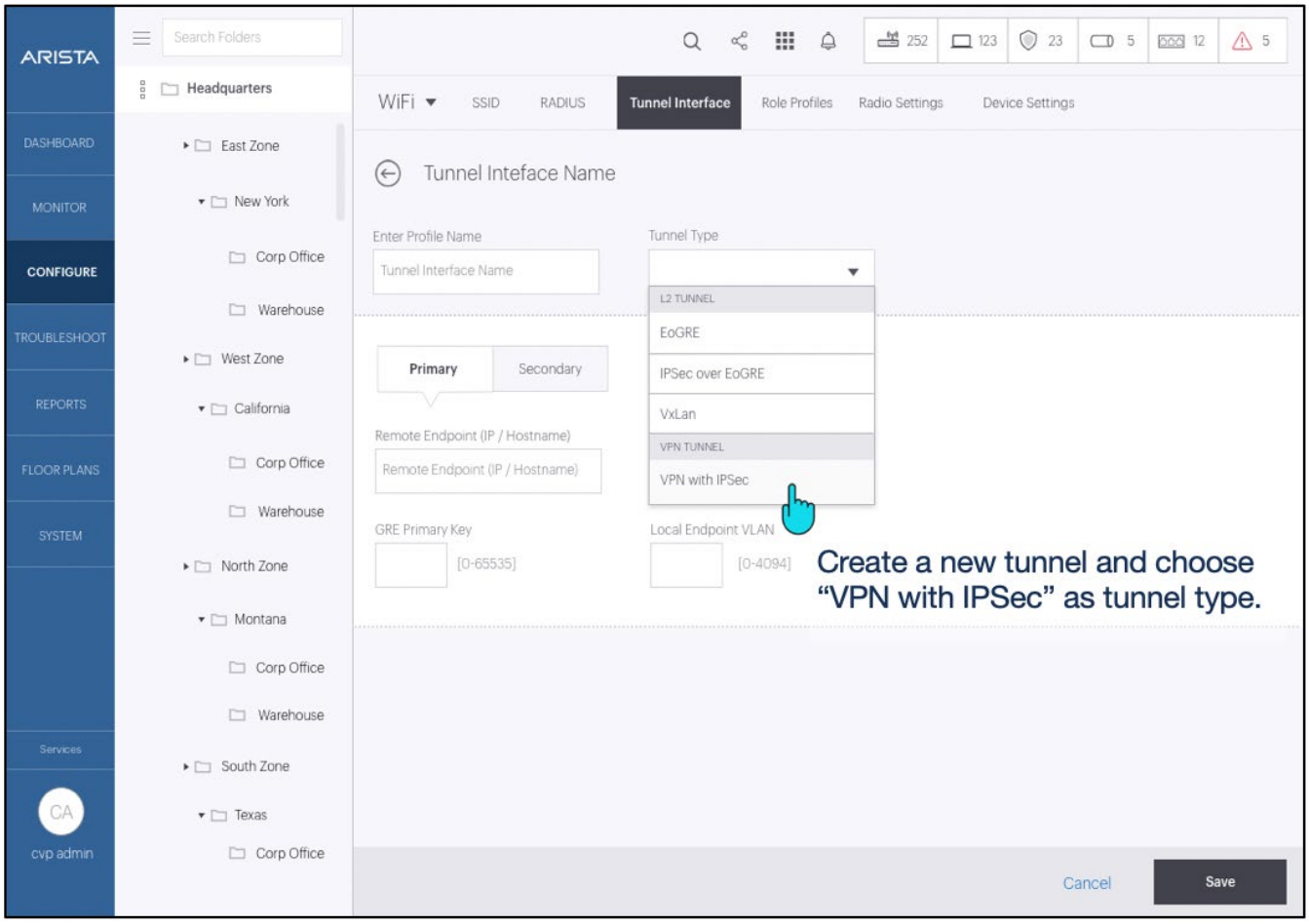


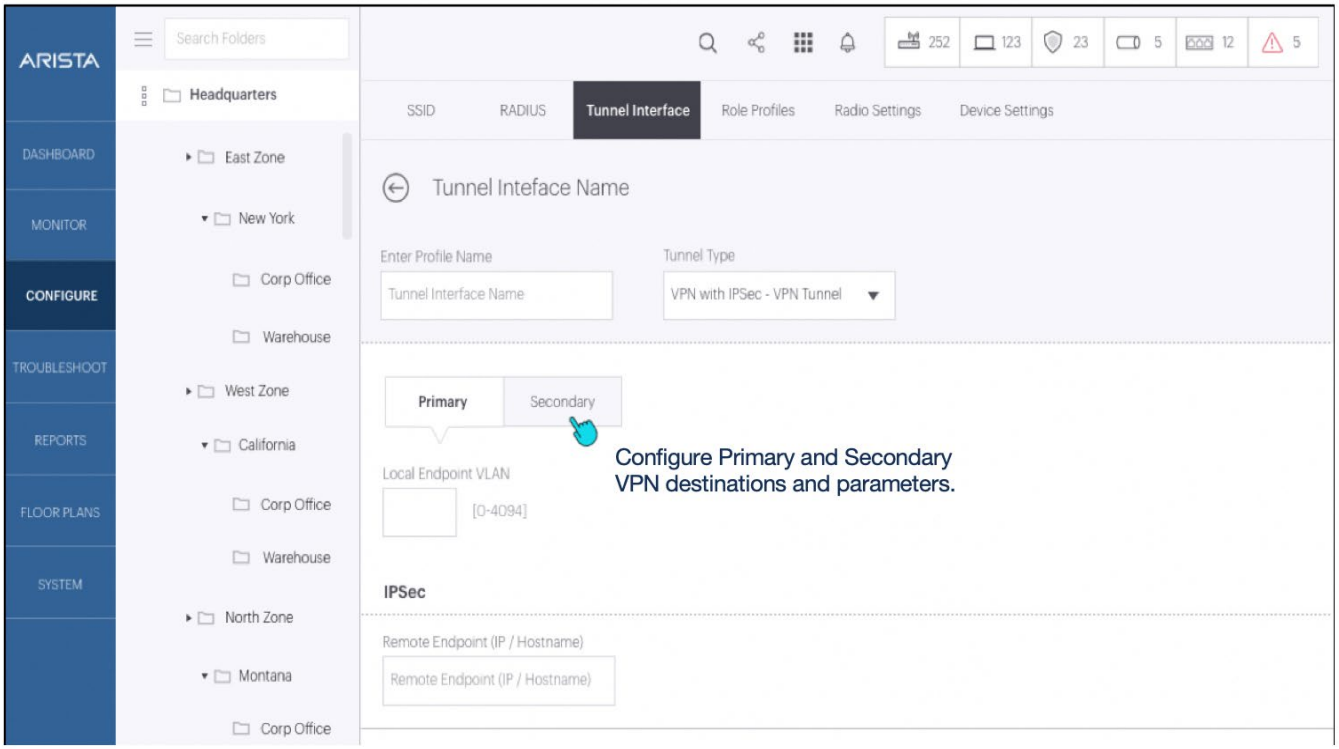
Homeschool Use Case #1 (Google Authentication):

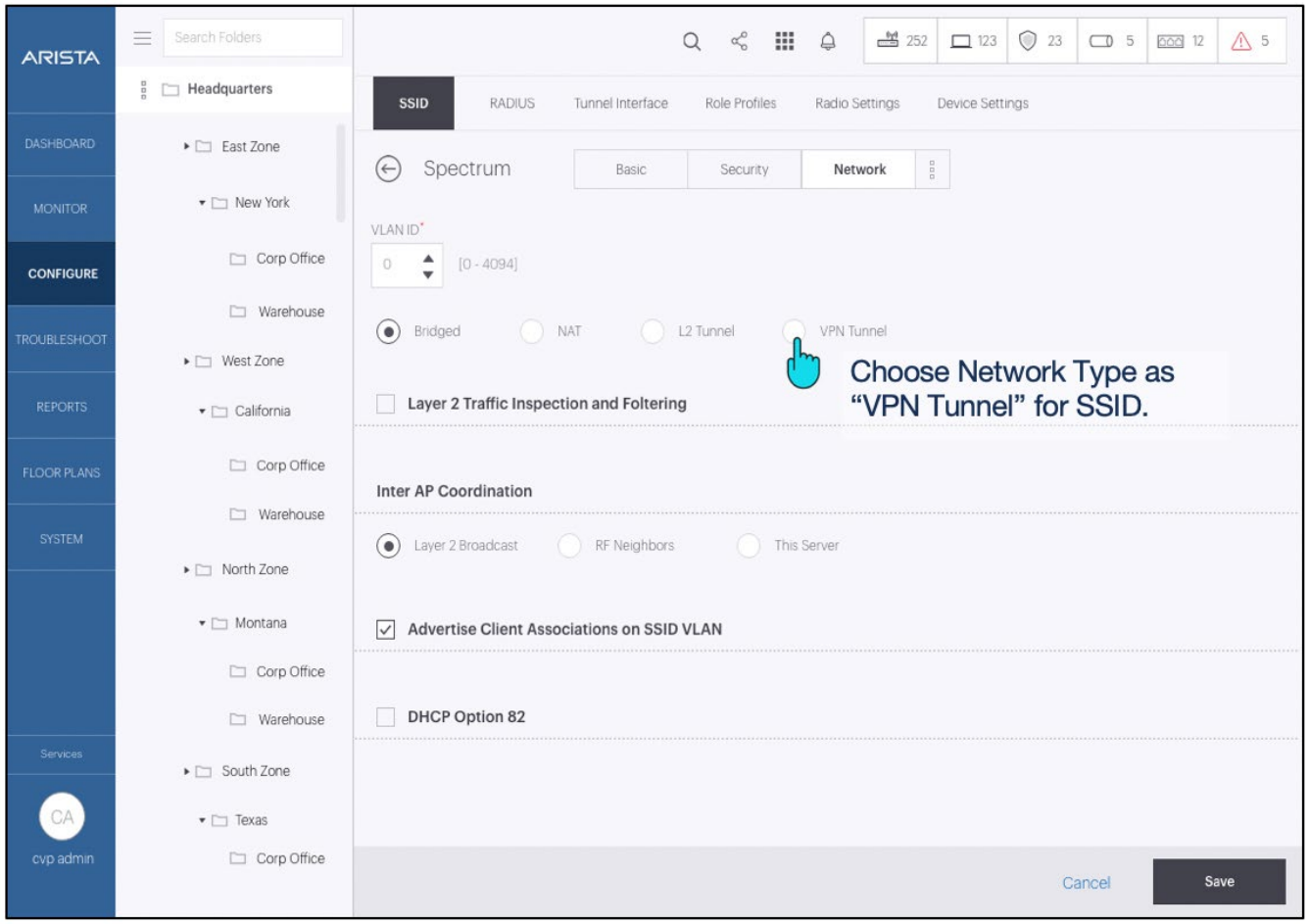
Arista Remote Access Point that is Cloud Managed and has the option to use an IPSec tunnel to a head end Tunnel Terminator (Palo Alto Firewall, Juniper SRX, Cisco ASA) or go directly to the Internet with student traffic. Clients can use a Pre-Shared Key or 802.1x authentication via G Suite for Education 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



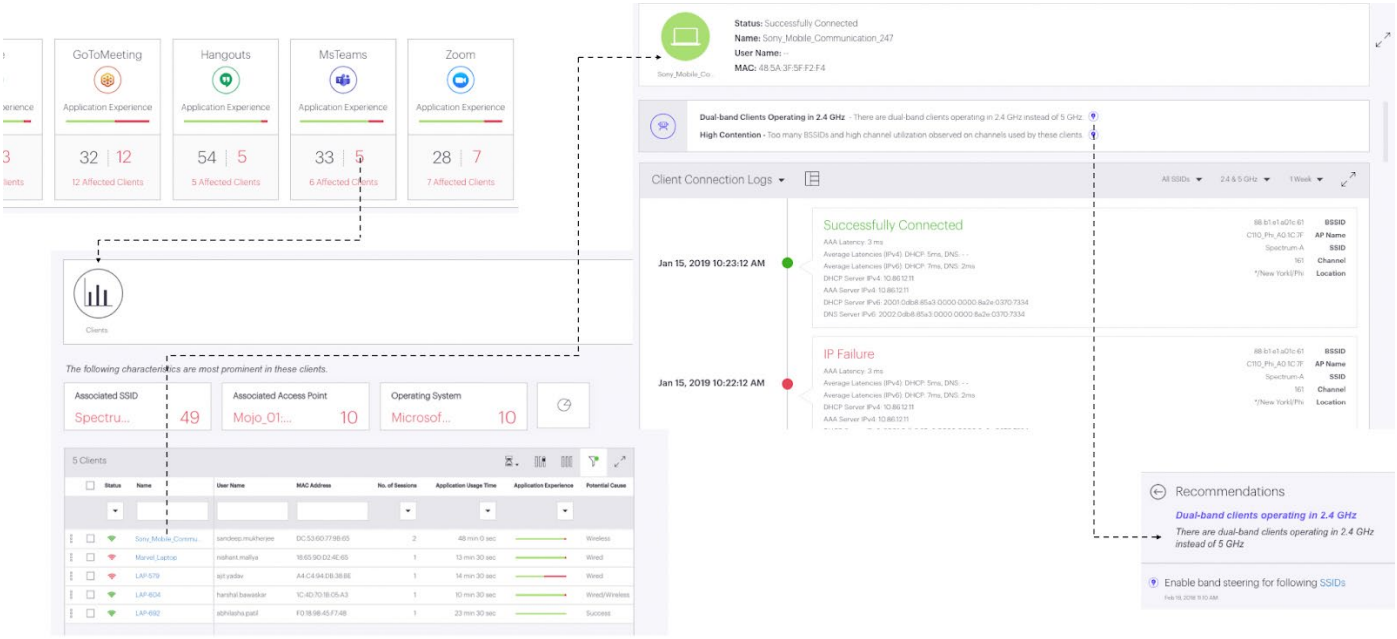



ARISTA
Search Folders
Headquarters
East Zone
New York
Corp Office
Warehouse
West Zone
California
Corp Office
Warehouse
North Zone
Montana
Corp Office
Warehouse
South Zone
Texas
Corp Office
DASHBOARD
MONITOR
CONFIGURE
TROUBLESHOOT
REPORTS
FLOOR PLANS
SYSTEM
Services
CA
cvp admin
252
123
23
5
12
5
SSID
RADIUS
Tunnel Interface
Role Profiles
Radio Settings
Device Settings
Spectrum
Basic
Security
Network
VLAN ID*
0
[0 - 4094]
Bridged
NAT
L2 Tunnel
VPN Tunnel
Choose Network Type as "VPN Tunnel" for SSID.
Layer 2 Traffic Inspection and Foltering
Inter AP Coordination
Layer 2 Broadcast
RF Neighbors
This Server
Advertise Client Associations on SSID VLAN
DHCP Option 82
Cancel
Save

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.

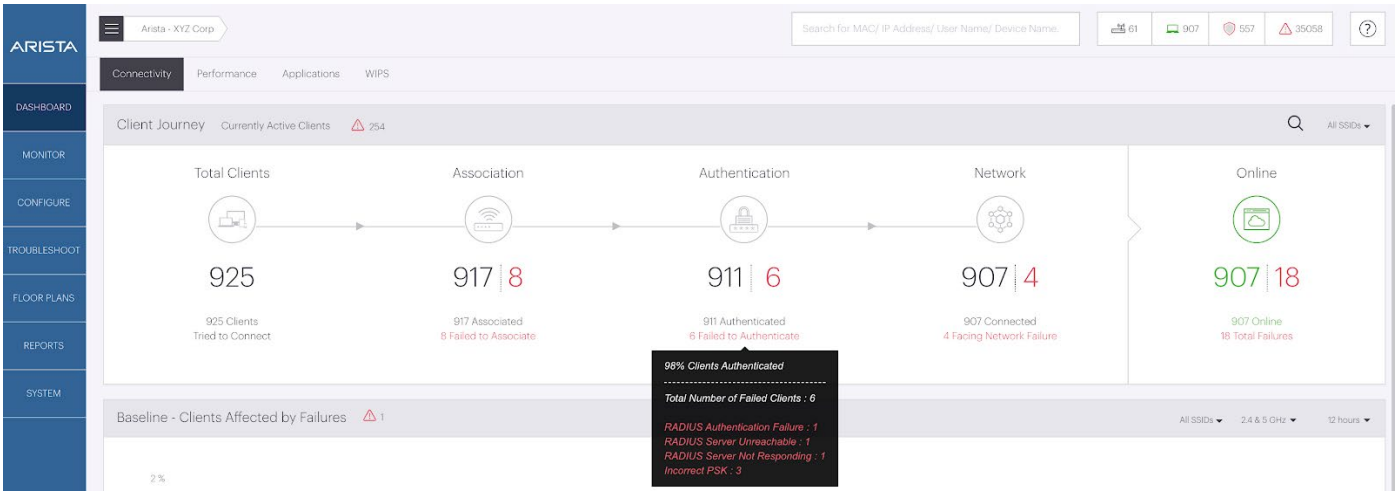


Automatic Packet Capture / Visual Packet Capture Analysis

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.

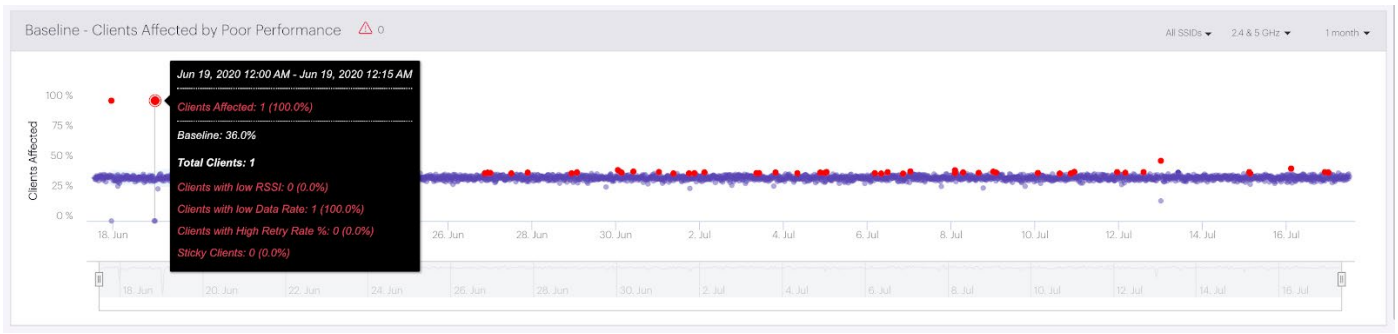
Client Journey

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.



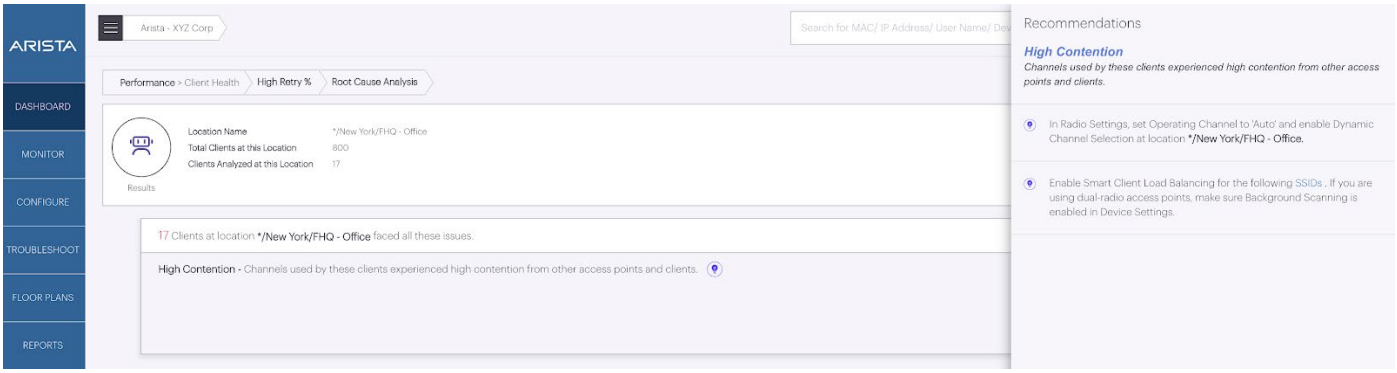
Network Baselining

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

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