The Remote Access Point (RAP)

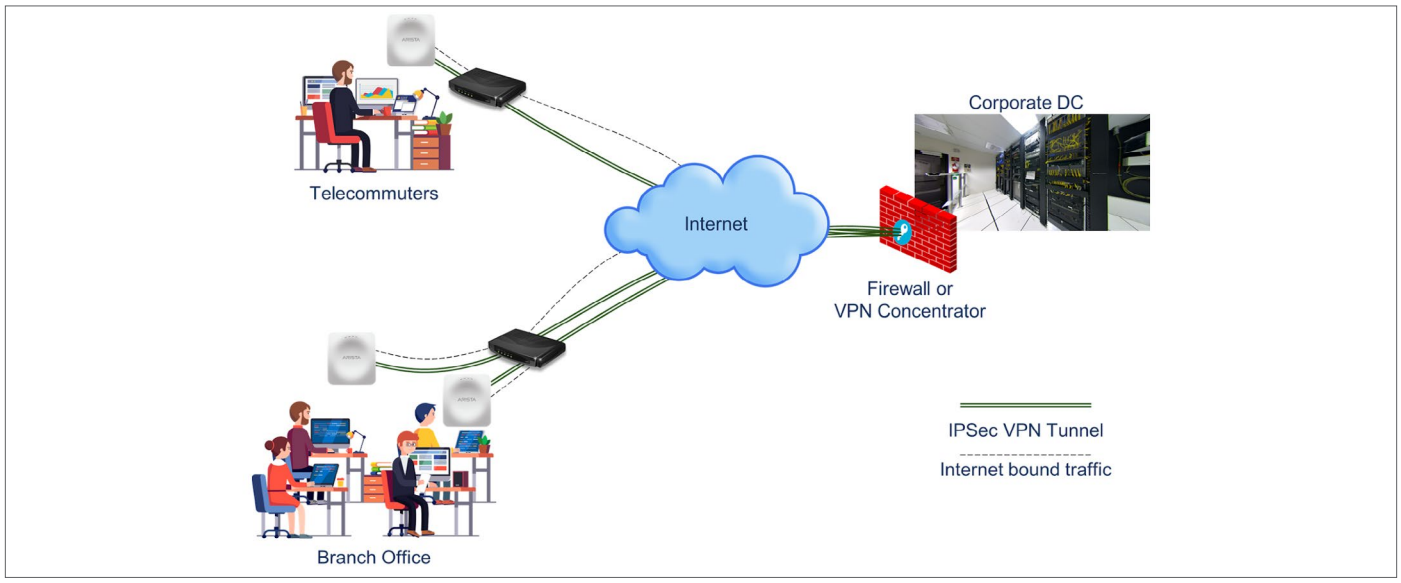
The Remote Access Point (RAP) solution empowers enterprise customers with the ability to extend Corporate SSID to a remote workplace such as a teleworkers' home office or a small remote branch office.

RAP offers the following benefits:

Enterprises	End Users
• Extension of the Enterprise SSIDs to the remote location with the same access controls and other policies. • Unified management and monitoring of APs deployed in the enterprise as well as RWAP devices. • Integrates seamlessly with industry standard firewalls. Hence, there is no need for additional investment.	• High-performance, enterprise-grade WiFi AP for employees working remotely from home or small branch offices. • Secure access to corporate network resources for users at the remote workplace.

RAP Overview

Arista's RAP solution uses industry-standard protocols to securely connect the AP deployed at a workplace with the Enterprise datacenter (DC) over the public Internet.



Secure Access

By establishing an IPSec VPN tunnel from the AP to the DC, traffic to/from Wi-Fi endpoints, connecting to the Corporate SSID, is securely forward from/to the DC. This eliminates the need for VPN setup on each WiFi endpoint. Note that the RADIUS exchange between the AP and authentication server located in the DC is also tunneled.

Flexible Data Forwarding

Leveraging Arista's flexible data plane architecture, only corporate traffic needs to be forwarded through the tunnel and Internet-bound traffic can be directly forwarded over the ISP network from the AP. This preserves precious VPN throughput at the head-end.

For operational flexibility, the following tunnel-SSID options are supported:

- One tunnel can be used for multiple SSIDs
- Each SSID can be defined with a separate tunnel

Ease of Integration

The solution is designed to integrate seamlessly with industry standard firewalls from leading vendors such as Palo Alto, CheckPoint etc. It has been tested with the following firewall products:

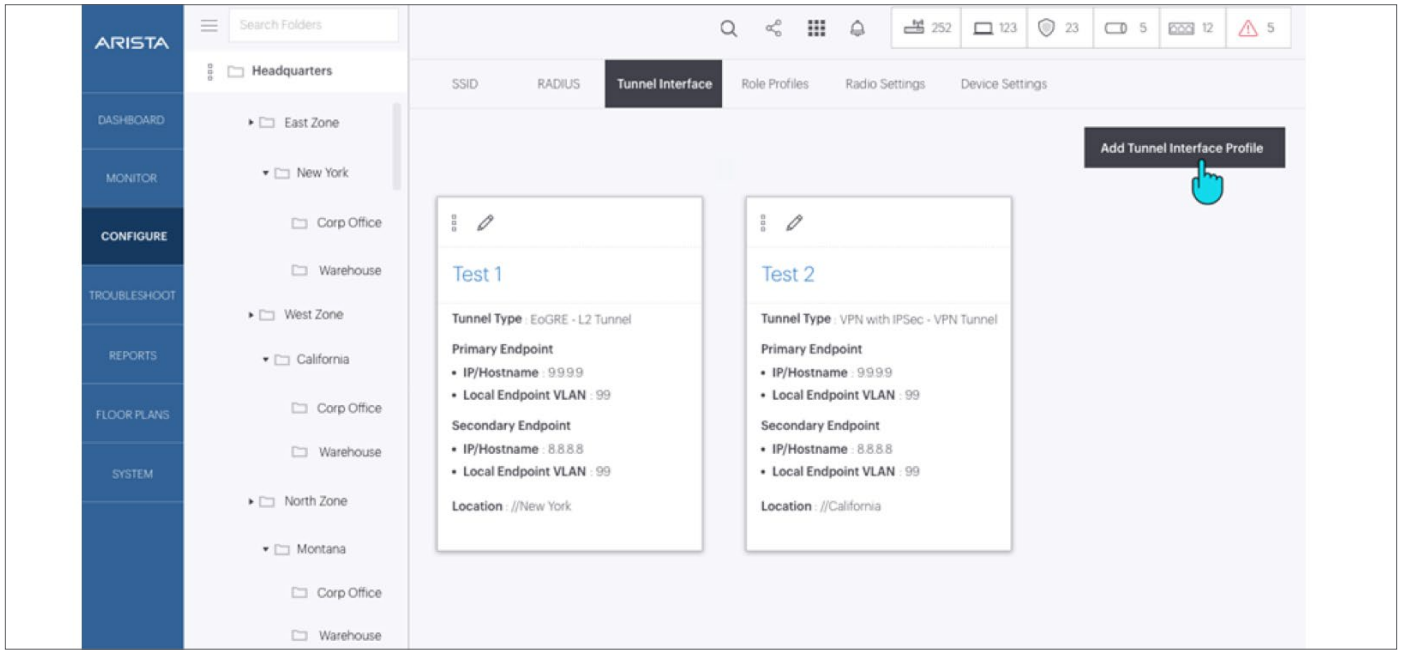
- Palo Alto PA220
- Juniper vSRX
- Cisco FirePower 1010
- CheckPoint SG1530
- FortiGate 30E

RAP Configuration

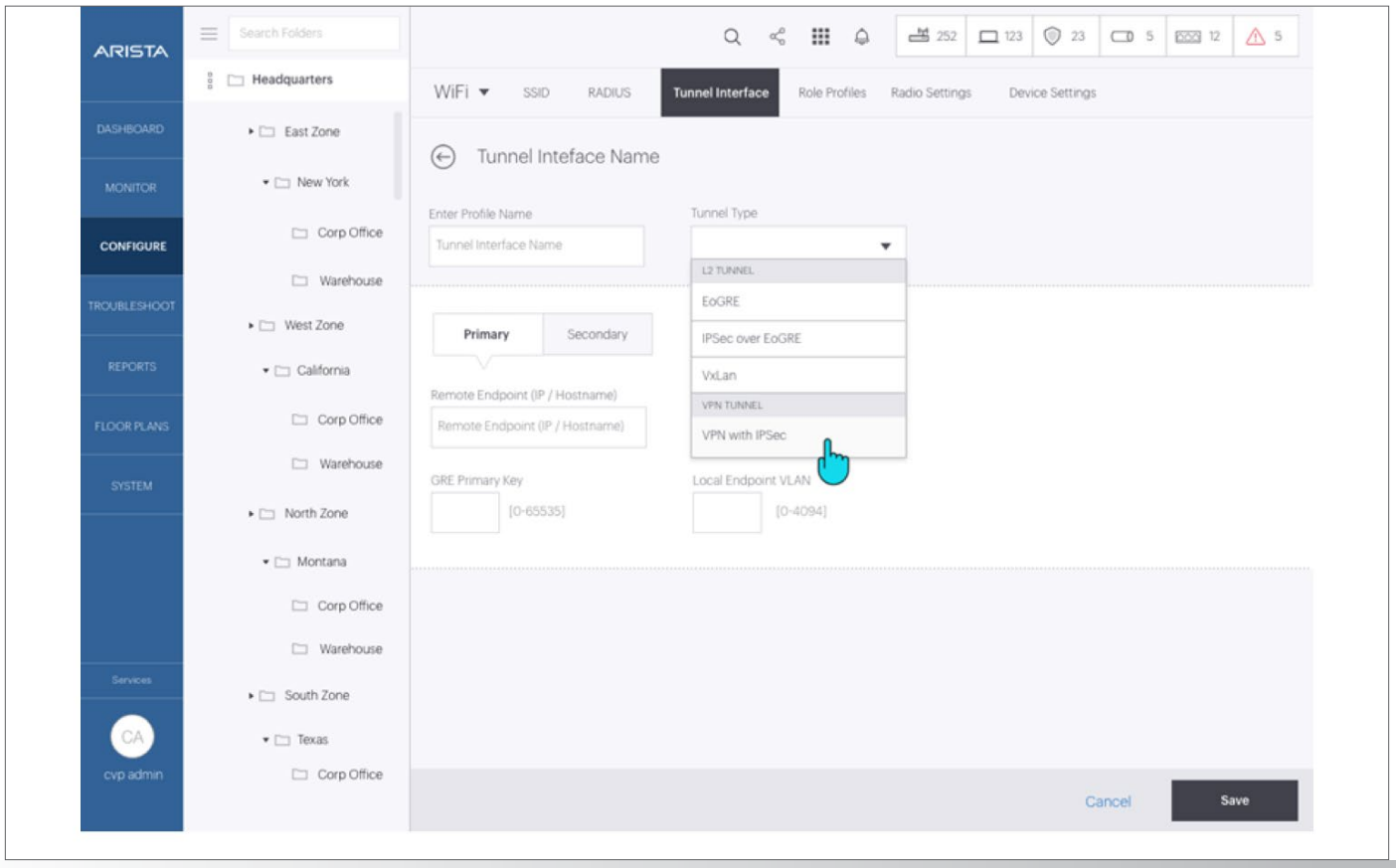
Just like any other Arista WiFi AP, the RAP device also needs to be provisioned first on the CV WiFi and then the RAP-specific configuration profile is created, as per the steps described below.

Step 1: Create Tunnel Profile

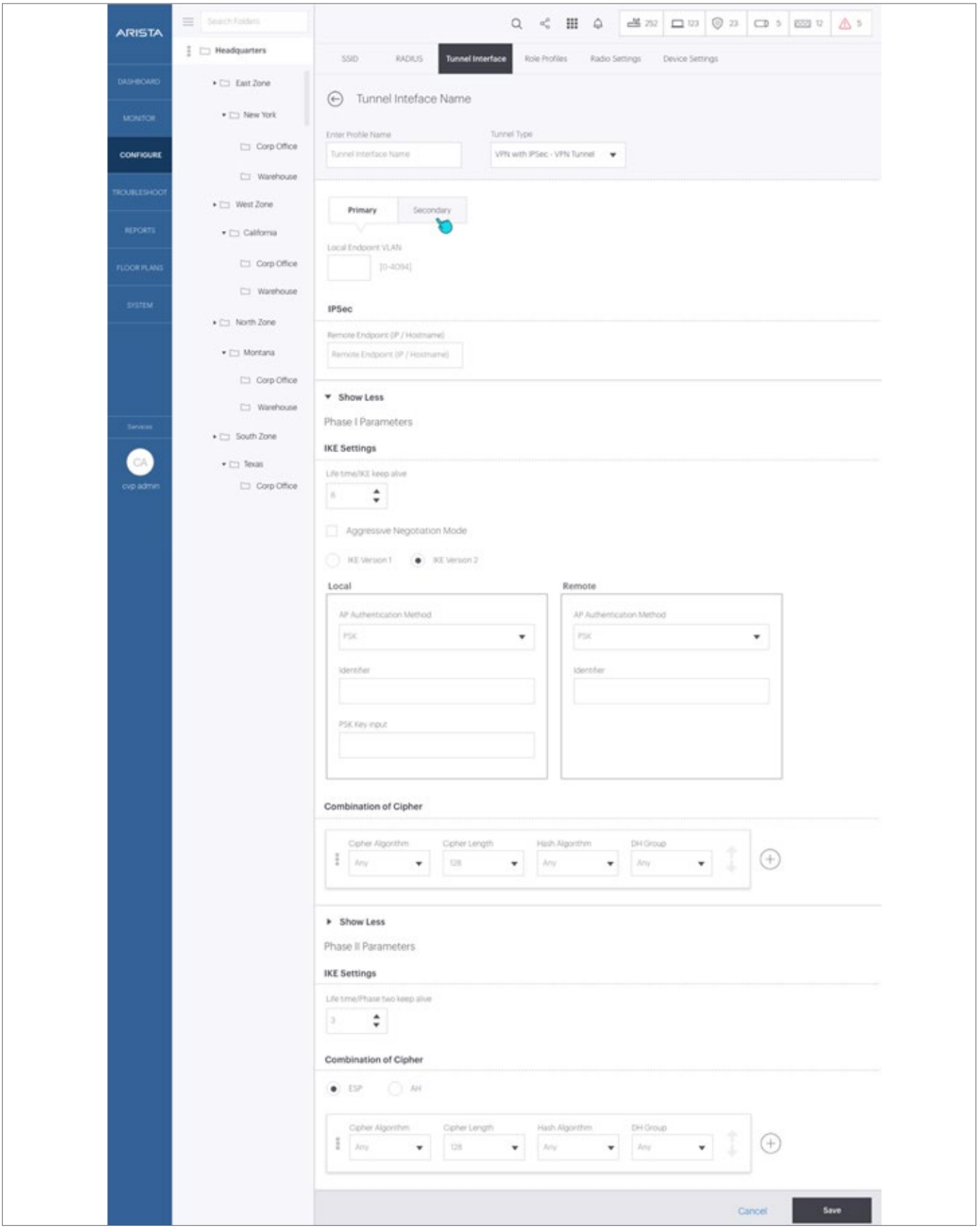
Navigate to the Configure->Tunnel Interface menu in CV WiFi and click on 'Add Tunnel Interface Profile'.



From the dropdown for the Tunnel Type field, select 'VPN with IPSec' option.

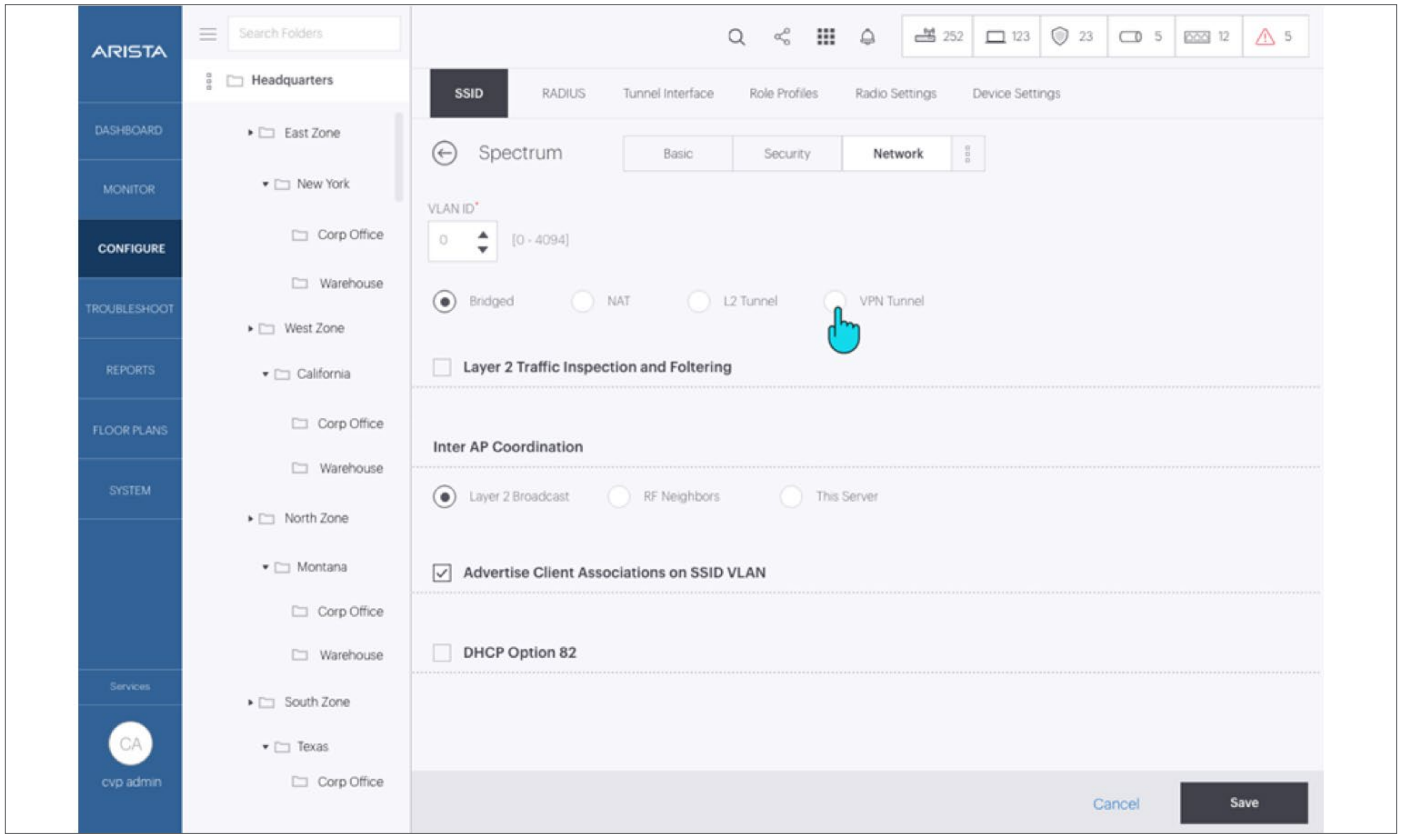


Provide the VPN Endpoint details

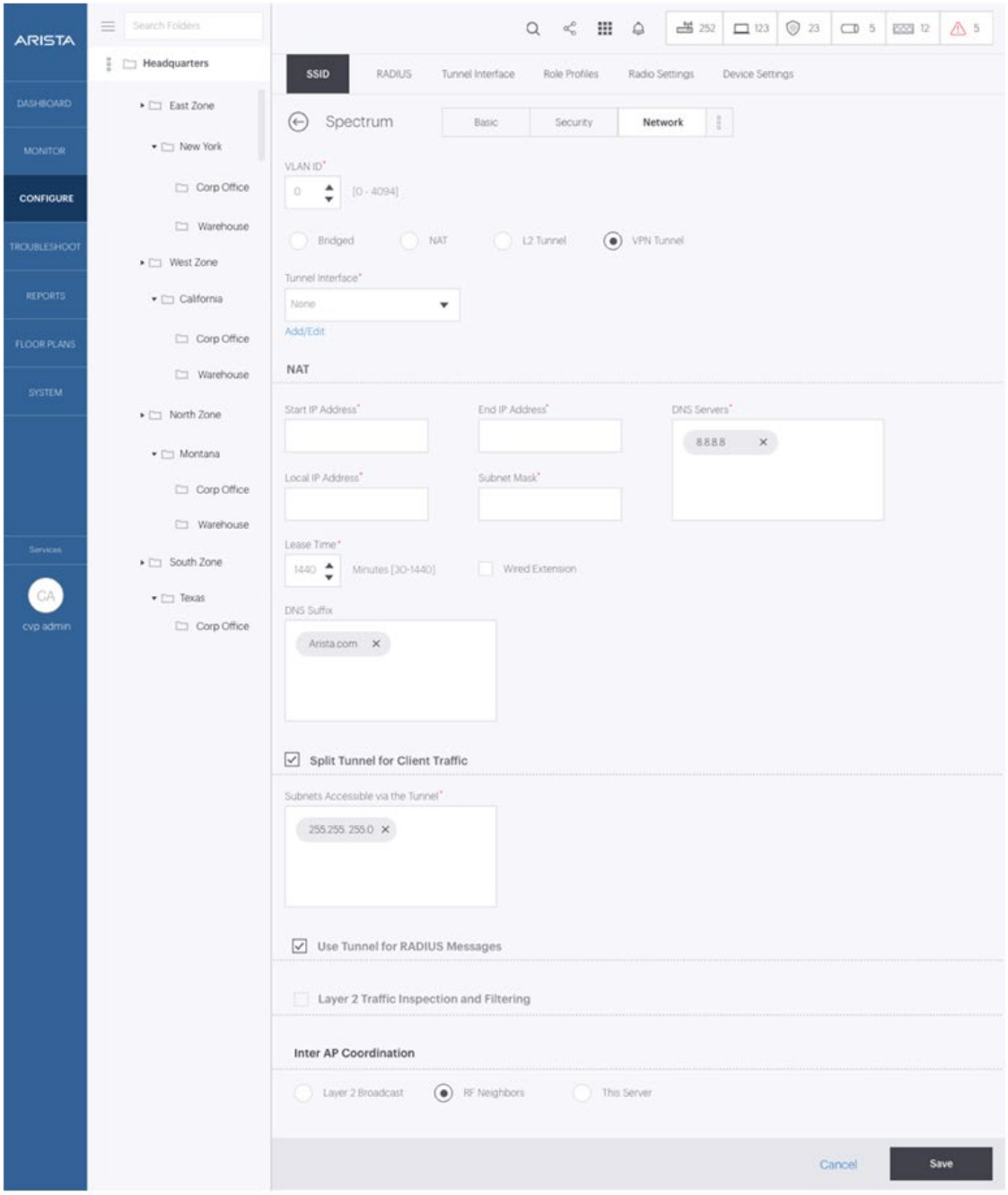


Step 2: Add the Tunnel to SSID Profile

Navigate to Configure->SSID and open the 'Network' configuration tab. Select 'VPN Tunnel' option.



This will result in display of additional configuration parameters. In the 'Tunnel interface' dropdown, select the tunnel defined in Step 1. Specify the NAT parameters for the SSID.



The following two additional options may also be enabled if required:
Split Tunnel for Client Traffic
Use Tunnel for RADIUS Messages

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 & B, 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 © 2020 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. 05-0046-01 September 30, 2020