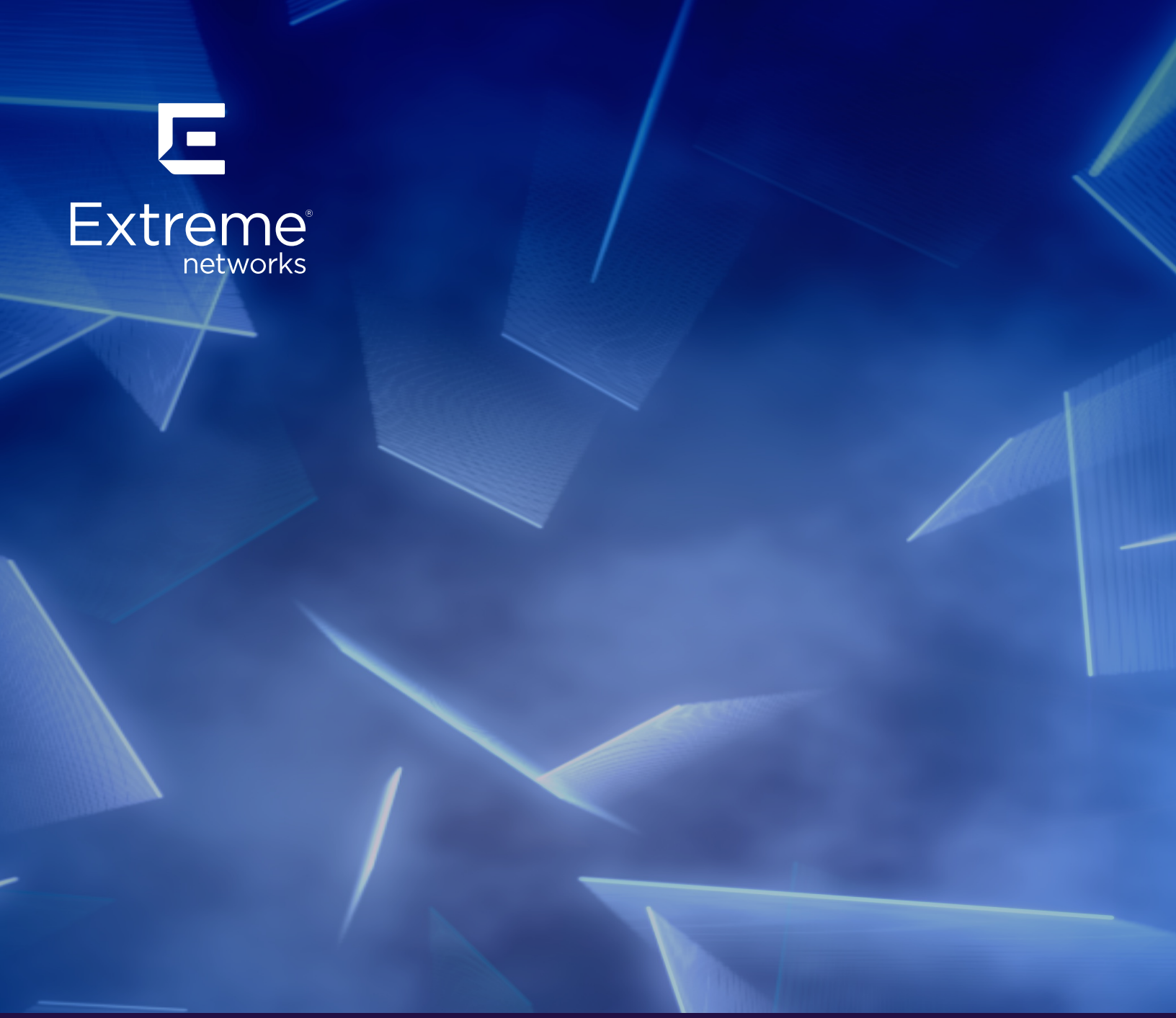


VPN Gateway Virtual Appliance (VGVA) for L2 VPN Installation Guide

March 2020

Table of Contents

Introduction 2
Overview of Solution 2
Document Control 3
Network Schematic 3
- VPN Gateway Virtual Appliance Server Prerequisites 3
- Deploying VMWare Infrastructure 4
- Initial Configuration and License Activation 6
- Create VGVA in ExtremeCloud IQ 7
- Configure Layer 2 VPN 7
- Step 1: Create a L2 IPsec VPN Object 8
- Step 2: Create or edit a Network Policy 10
- Step 3: Verify the IPsec Tunnel 12
- Step 4: Verify Client Connectivity 14

Summary 14

Introduction

This document has been created to provide a configuration walkthrough guide to allow technical staff to deploy Extreme Networks' VPN Gateway Virtual Appliance (VGVA) software in a VMWare environment and remote devices to provide Layer 2 VPN.

This document focuses on the creation of a Layer 2 VPN solution, deployed between an access point running IQ Engine (AP305C, AP510C, AP410C, AP30, AP150W, AP122, AP630, AP230, AP130) and a VGVA.

The document describes the configuration steps to prepare the VMWare environment for deployment of the VGVA, installation of VGVA software, Layer 2 VPN policy creation and its deployment to the VGVA and wireless access points.

Overview of Solution

The solution comprises of three elements; ExtremeCloud™ IQ Management Platform, remote access point network devices and VGVA software.

The ExtremeCloud IQ management platform is used to create configuration policies, distribute policies to network devices, and monitor connected devices and clients. The remote access point is used to provide local wireless services and initiate Layer 2 VPN tunnels to the VGVA software that runs as a virtual machine on VMWare ESX hosts. It is used to terminate Layer 2 VPNs and forward traffic from remote sites into the head office network and forward remote outbound traffic in VPN from the head office to the remote sites.

Document Control

Version Number	Date	Description	Author
1.0	February 2020	Configuration Guide - VPN Gateway Virtual Appliance (VGVA) for L2 VPN	Marko Tisler, Glyn Brice, Stuart Farmer

Network Schematic

The Layer 2 VPN solution requires the ability for the remote access point to create a Layer 2 VPN from the remote site to the centrally hosted VGVA. Figure 1 shows a typical deployment of the solution.

The remote access point is connected to the home router which provides IP addressing information. The VGVA software logically connects on Eth0, the host server is connected to the upstream firewall in a DMZ. The two ExtremeCloud IQ devices are configured and managed by the ExtremeCloud IQ instance.

The access point provides wireless connectivity to local devices, based on the configuration the traffic is forwarded in the VPN tunnel between the access point and the VGVA.

The head end firewall is configured to allow VPN traffic from the Internet, the data is decrypted by the VGVA and forwarded to the firewall from
the same interface, the firewall controls traffic to the internal network. The traffic once decrypted can be tagged with VLAN information to provide segregation.

The traffic from the head end follows the reverse path, forwarded by router to firewall, inspected and forwarded by firewall to VGVA, encrypted and forwarded across the Internet to the access point where it is decrypted and forwarded to wireless client.

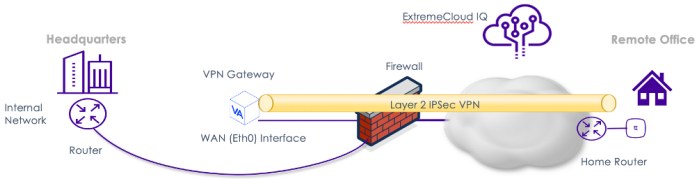


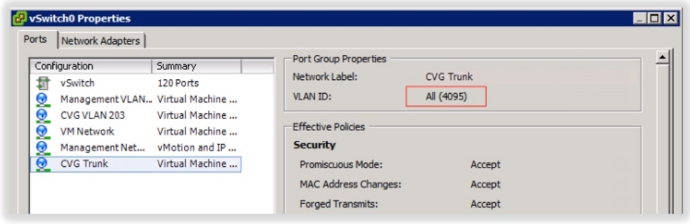
Figure 1 – Layer 2 VPN Solution

VPN Gateway Virtual Appliance Server Prerequisites

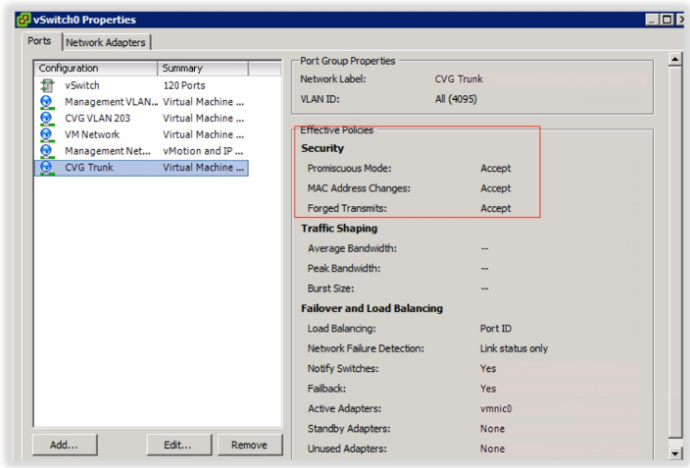
This section of the document describes the VMWare server requirements that are required to install and run VGVA, managed by ExtremeCloud IQ.

The VGVA software will require Internet access (http/https) for the purposes of license verification. This can also be achieved using a HTTP proxy server configured as a part of the initial configuration. The administrator will be prompted to enter the proxy server during the initial configuration wizard and will access to a DNS server.

If the intention is to place clients onto VLANs other the its management VLAN, you will need to configure the VM to support trunking inside the vSphere environment. This is achieved by setting the associated port group configuration with VLAN label 4095. Also make sure your network infrastructure is correctly configured with the required VLAN and trunk settings. You can learn more here.

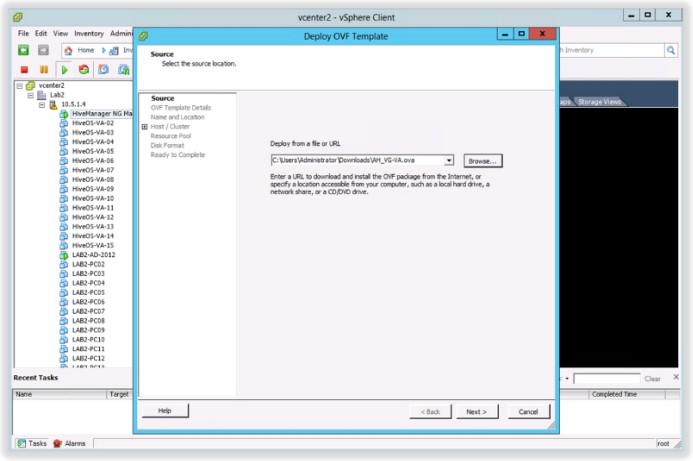


Ensure that the port group in vSphere allows promiscuous mode. If disabled L2 VPN clients may not be able to receive an IP address or pass any traffic. You can access these settings on your host > Configuration > Networking > <your vSwitch>.

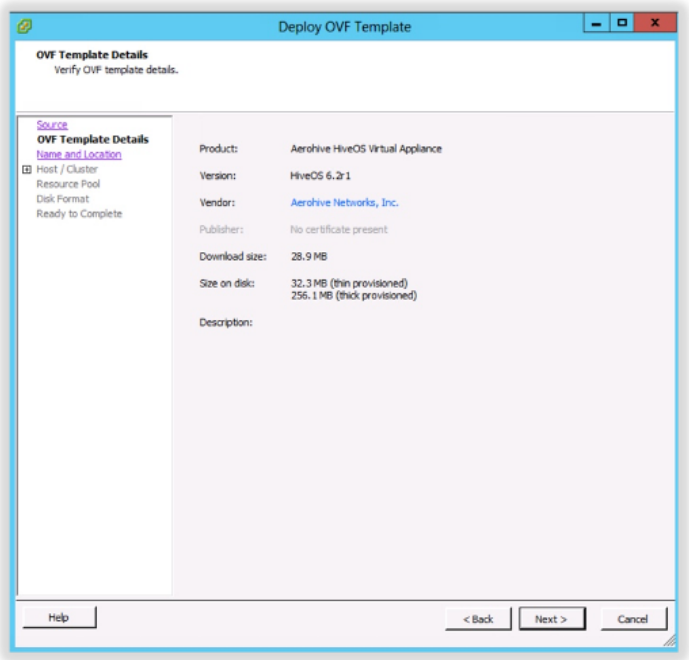


Deploying VMWare Infrastructure

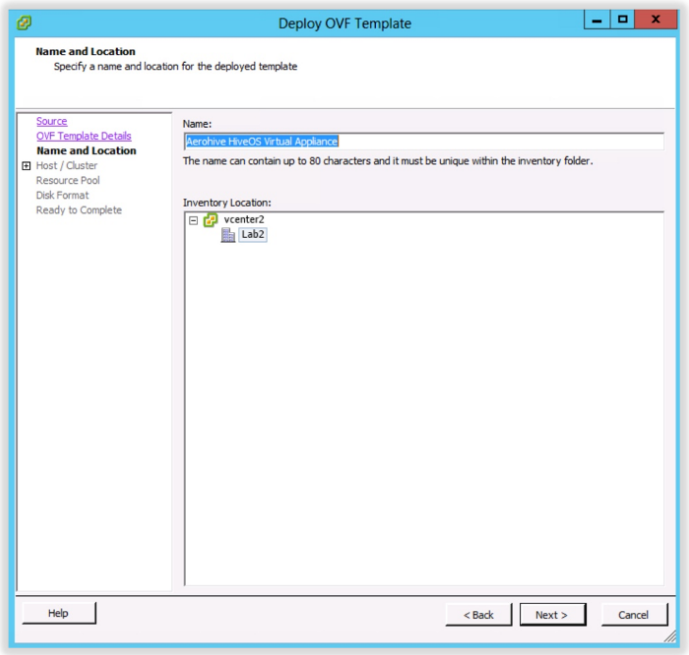
1. Once the VGVA firmware .ova file has been downloaded from the Extreme Networks' support portal, open the vSphere client. Go to File > Deploy OVF Template and locate the downloaded .ova file



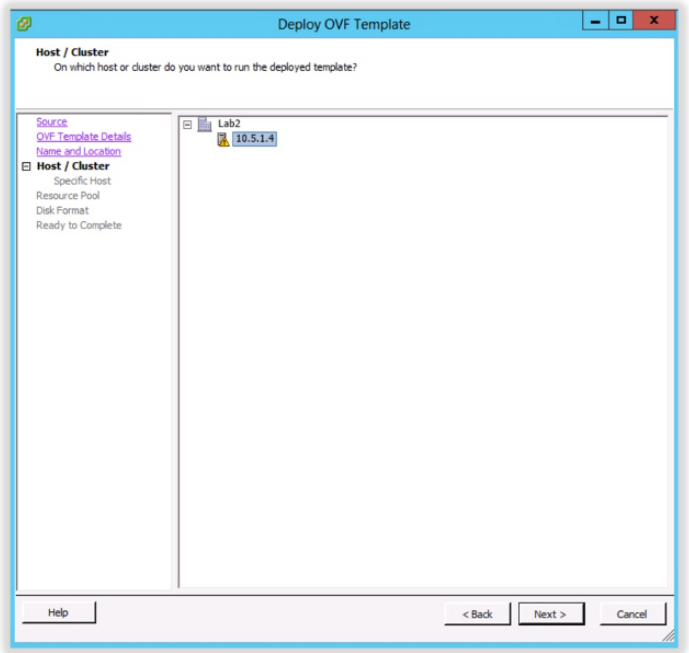
2. Click Next. Click next again on the following screen.



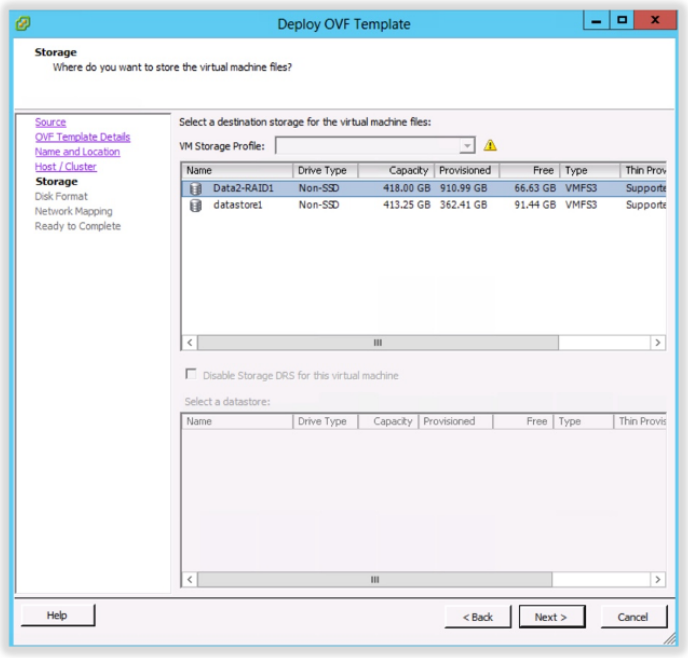
3. Give the virtual machine a name and select the inventory location.



4. Select the host server.

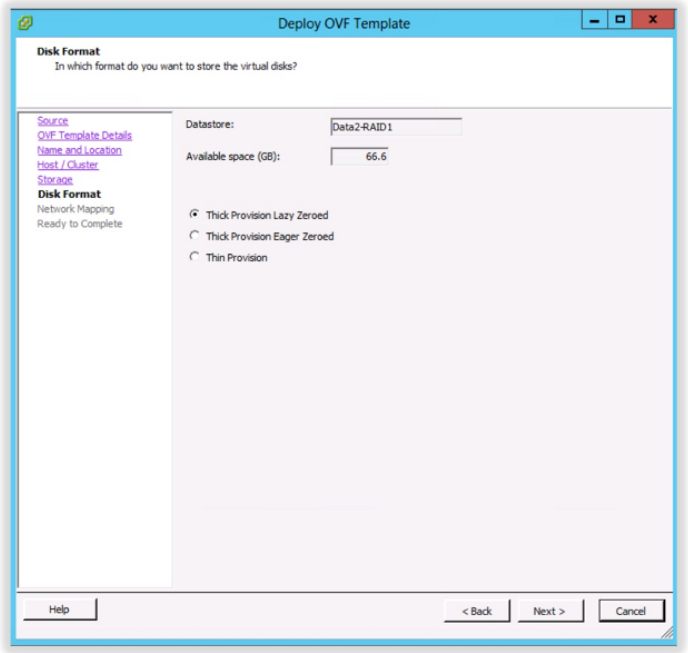


5. Select the datastore that will host the virtual machine.

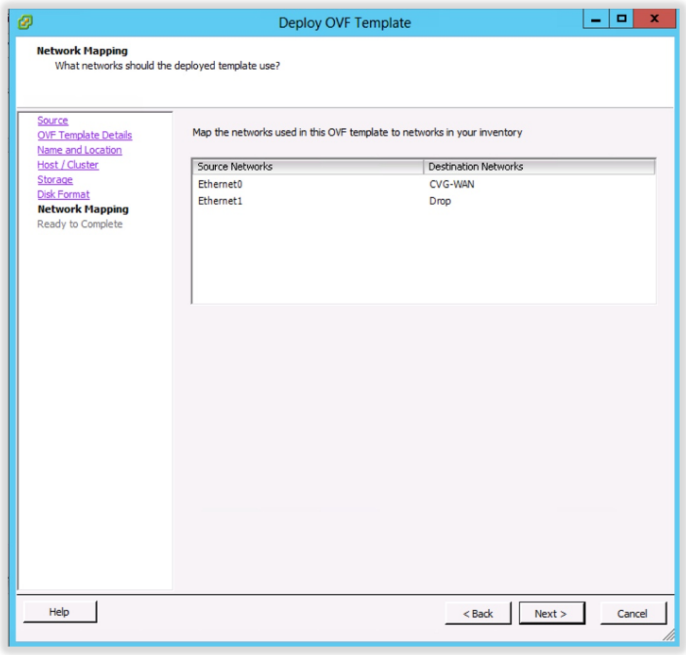


6. Select the disk format.

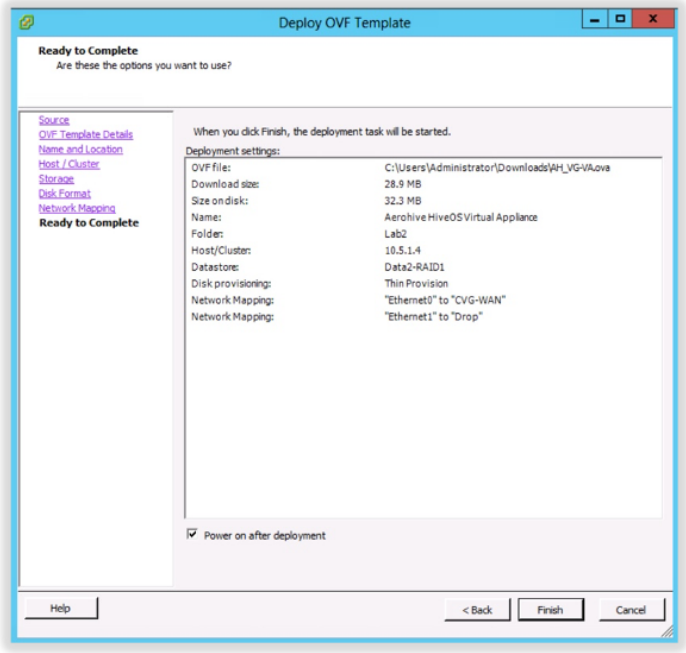
Note: Thick provisioning will reserve all the disk space needed by the virtual machine while thin provisioning will reserve the minimal amount and increase it later if needed.



7. Select the network for the virtual machine's Ethernet0 interface. This will be the network for the management interface of the virtual appliance (VA). In this case, we are connecting the VA to a Network called CVG-WAN.

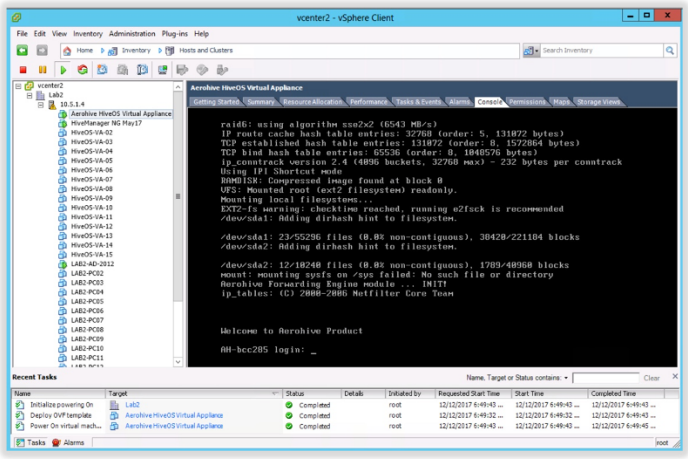


8. Review your settings and click Finish.

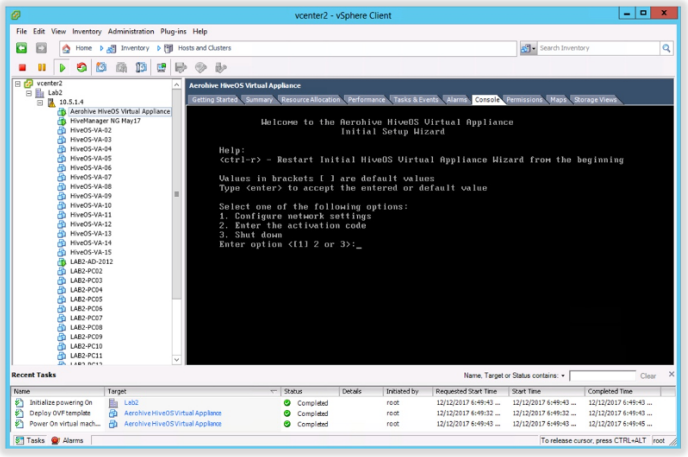


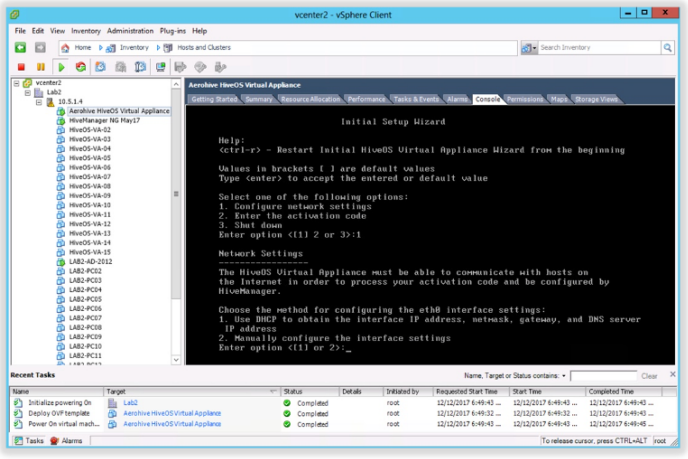
Initial Configuration and License Activation

Open the console access to the VGVA virtual machine in the vSphere client. Login using the username admin and password aerohive.



You will be greeted by the initial Virtual Appliance Wizard. Start with configuring the network settings (option 1).

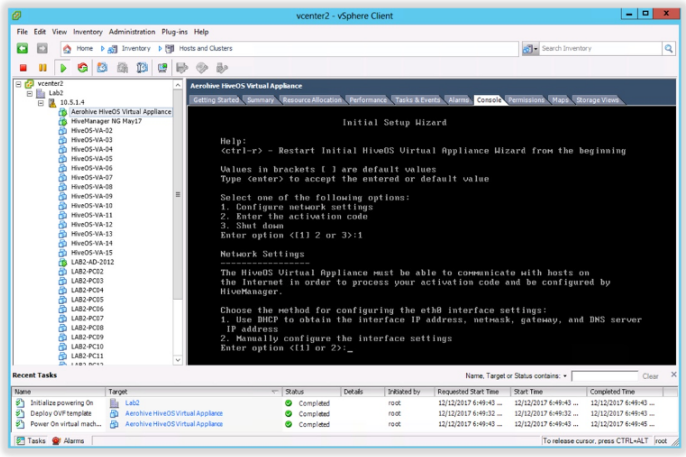




Configure either static or DHCP configuration for the IP address of the eth0 interface of the virtual appliance.

Note: eth0 interface will be used for the initial connectivity between the VGVA and ExtremeCloud IQ. It will be necessary to set the actual management interface settings for the VGVA from ExtremeCloud IQ once the VGVA is connected to it. After the management interface is configured from ExtremeCloud IQ, the eth0 interface will no longer have an IP address and will only be used for bridging traffic. The mgt0 interface IP settings will be used for all further communication including GRE and IPsec tunnels.

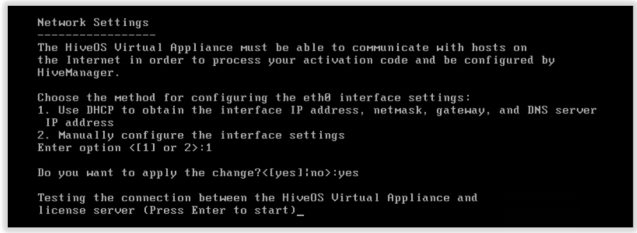
Note: For ease of use it is recommended to configure the eth0 interface IP settings using DHCP during this initial stage and set the static settings from within ExtremeCloud IQ once the VGVA is connected to ExtremeCloud IQ.



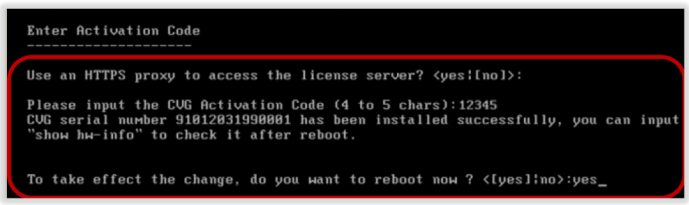
Once network settings have been entered manually and confirmed,
press “Enter” to start the connectivity test. The VA will then perform the following tests:

- Ping the default gateway
- Resolve a FQDN using the provided DNS server
- Try to contact the licensing server

Note: The management VLAN that the virtual machine is the untagged VLAN.



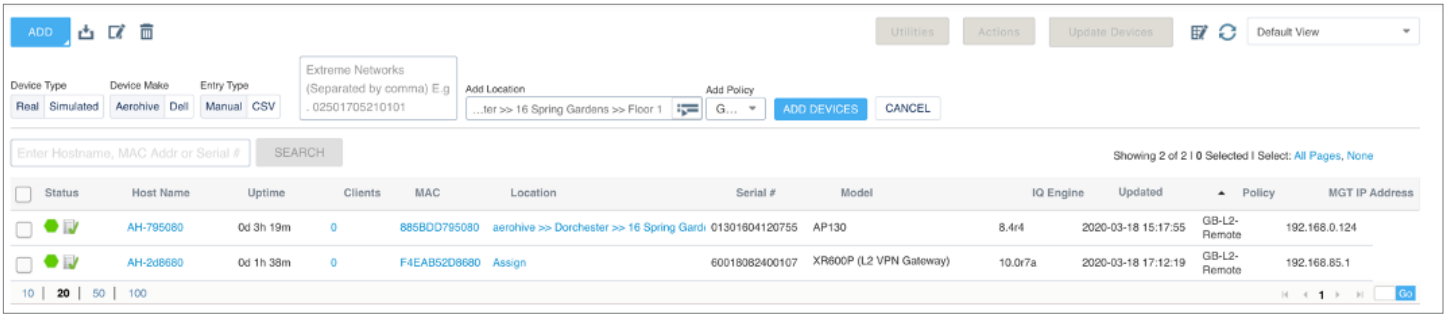
Enter the activation code and the system will create a Serial Number this will be entered into ExtremeCloud IQ in order to add the device for management.



Create VGVA in ExtremeCloud IQ

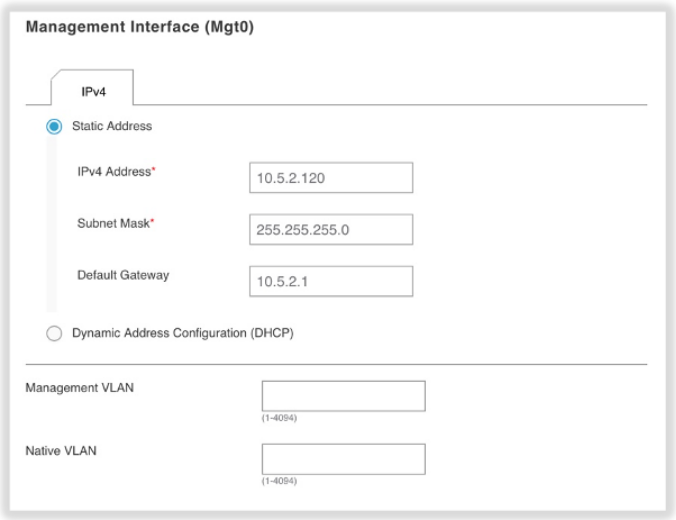
In order to add the VGVA, login to the ExtremeCloud IQ instance. If you are using the Local Cloud (VA) version of ExtremeCloud IQ this step can be skipped as the VGVA will try to locate the Local Cloud using the normal discovery mechanisms (DHCP, DNS, redirector).

In order to add the VGVA to the ExtremeCloud IQ instance as a new device click “Add” while in the Manage/Devices tab. This workflow allows the administrator to assign location and a Network Policy, that will be automatically assigned once the device connects to ExtremeCloud IQ.



Once the VGVA contacts and connects to your ExtremeCloud IQ instance, click on the device name while in the Manage/Device tab, and assign a static IP address.

Configure the management IP address depending on your environment. By default, the management IP address needs to come from the untagged (native) VLAN. This can be overridden. Once done click “Save”.



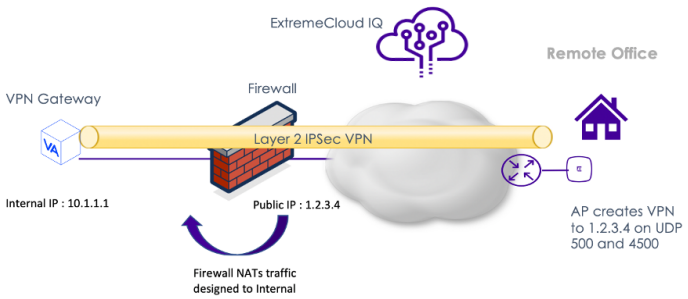
Next, you will need to decide what you are using the VGVA for. It could either be to terminate GRE tunnels for guest tunneling or IPsec tunnels from wireless access points acting as VPN clients.

Configure Layer 2 VPN

The configuration steps to deploy the Layer 2 VPN is completed within the Network Policy of ExtremeCloud IQ and deployed to the VGVA and wireless access points.

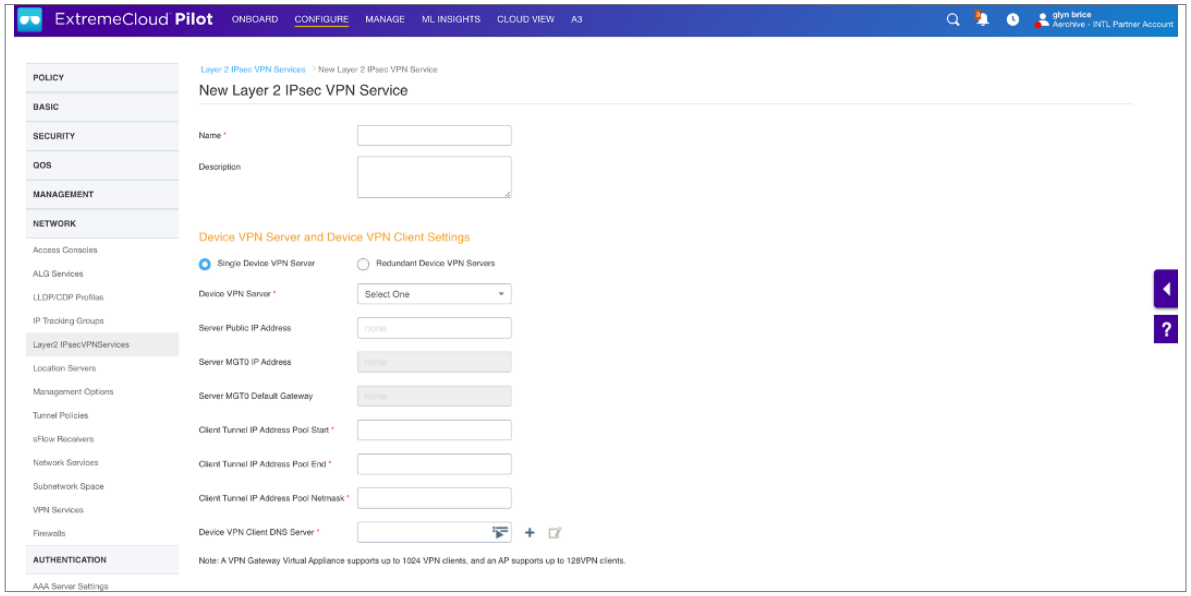
Requirements

- The VPN is created between access point(s) and the VGVA .
- The access points and VGVA are managed by the same ExtremeCloud IQ instance.
- The IP address assignment, L3 routing and firewalling is done by other network devices located at head end.
- The VGVA uses static IP addressing for the mgt0 interface. This is required in order to properly configure NAT on the firewall and forward the traffic coming from the AP to the correct IP address. Alternatively, you can create a static assignment on your DHCP server.
- All port forwarding/port mapping is configured on the local firewall/router.
- The firewall is configured to perform Network Address Translation and UDP forwards traffic to ports 4500 and 500 to the internal mgt0 (management interface) IP address of the VGVA.
- The VGVA HiveOS version is 6.9rx or later.

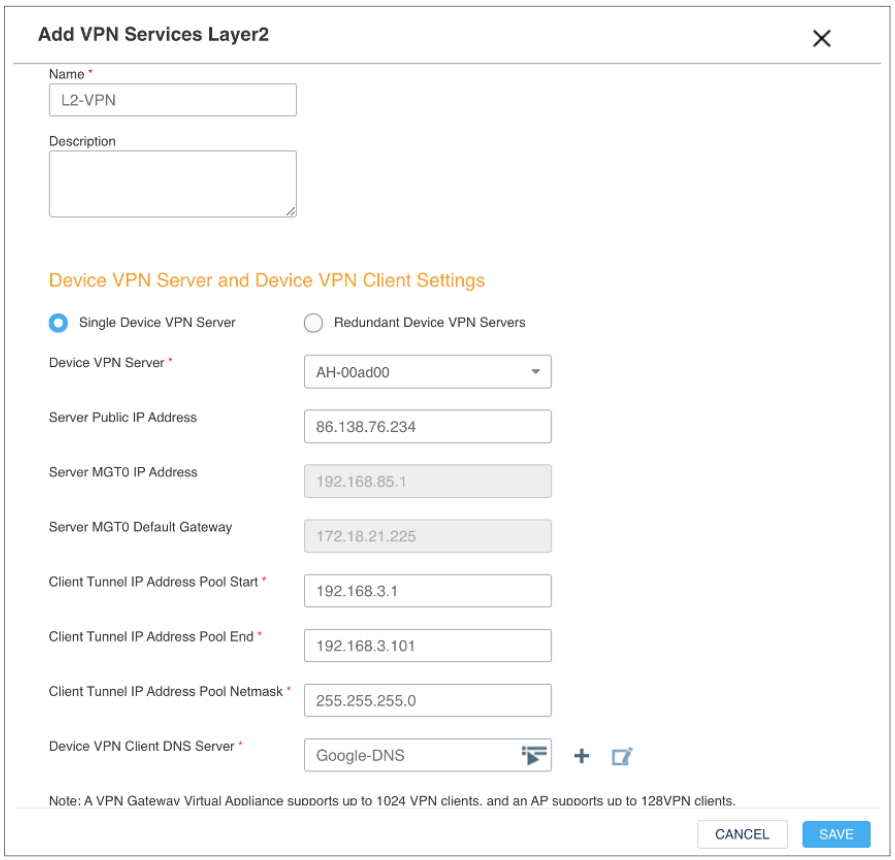


Step 1: Create a L2 IPsec VPN object

In ExtremeCloud IQ create a new L2 IPSec VPN object under Configuration > Common Objects > Network > Layer 2 IPSec VPN. Click “Add”.



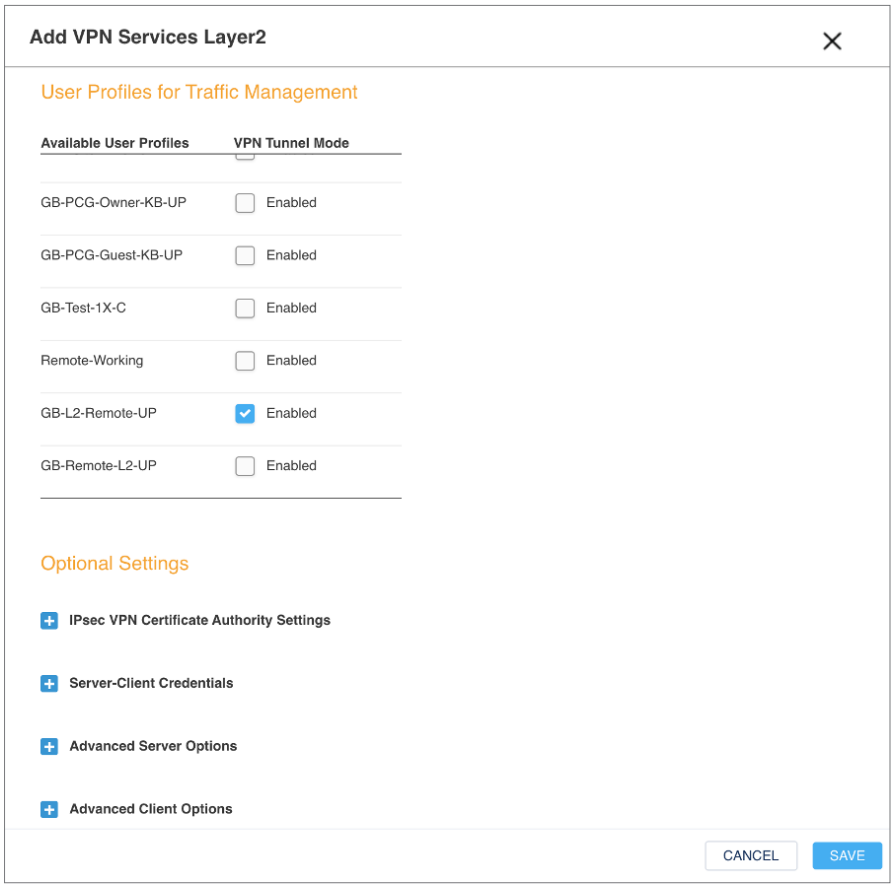
Name the VPN object e.g. L2-VPN and select a VPN server from the Device VPN Server dropdown menu. Up to two servers can be configured for redundancy purposes.



ExtremeCloud IQ will automatically determine the server's public IP address which will be used as the L2 IPsec VPN tunnel destination by the L2 VPN clients. Dedicate a non-existent IP Address Pool to be used for L2 VPN tunnel. These addresses will be used to create tunnel interfaces on the VPN clients.

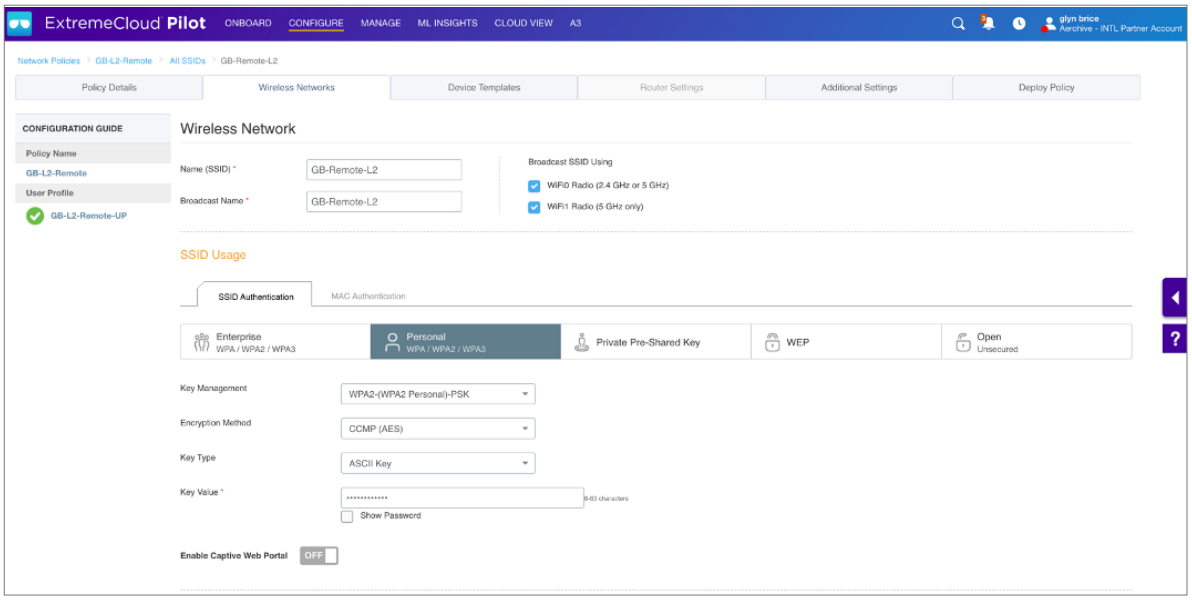
Scroll down on the same screen, the administrator is presented with the User Profiles for Traffic Management. This selects the user profiles which should have their traffic tunneled across the VPN tunnel. In this case we selected the traffic for the user profile "GB-L2-Remote-UP" to be tunneled back to the VPN server.

Click Save.



Step 2: Create or Edit a Network Policy

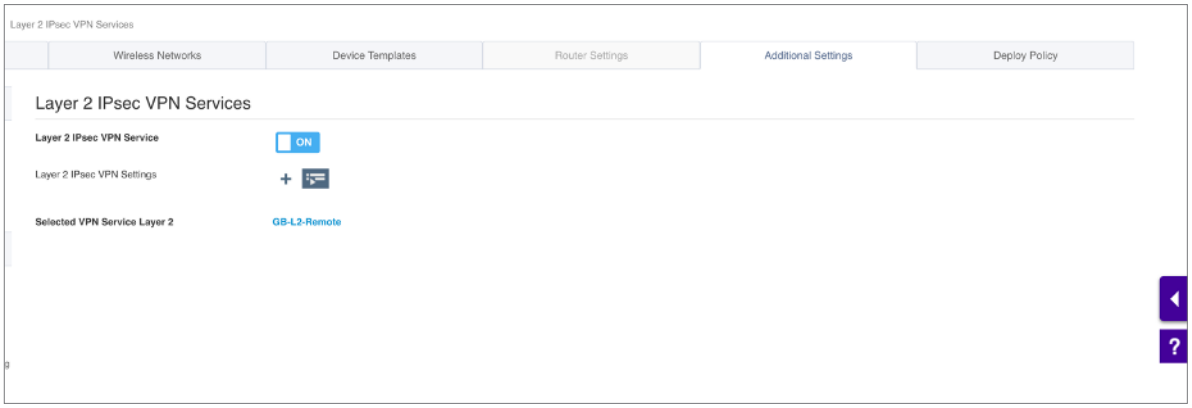
The next step is to create a Network Policy which will use this L2 IPsec VPN object. Create an SSID and select the appropriate authentication method. Example below uses WPA2-Personal.



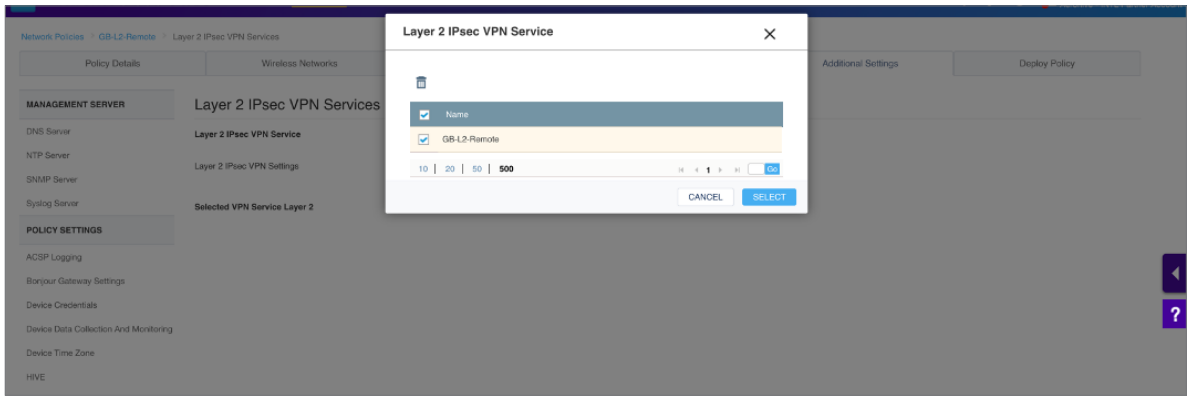
In this case we have created an SSID called GB-Remote-L2 utilizing a user profile called "GB-Remote-L2-UP". The user profile ties the L2 IPSec VPN tunneling rules to this SSID. Save the Network Policy.

Note: The user is mapped to VLAN 1 in this case. To place the connected client device in a different VLAN, make sure the VG VA virtual machine Ethernet 0 interface is configured as a trunk port in vSphere and that VLANs are actually being passed to the ESXi server.

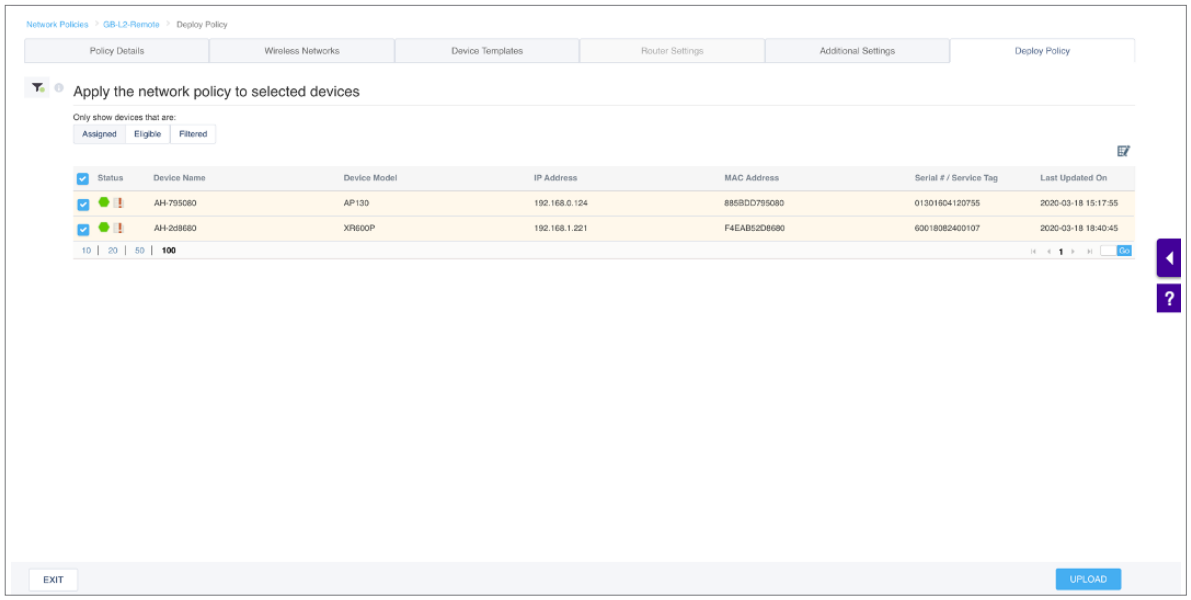
Click "Save" and go to the "Additional Settings" section. This is where we will assign a VPN Service to this network policy.



First, turn the Layer 2 IPsec VPN feature on. Then click to select the VPN Service we created under the Common Objects section. Click “Select” and click “Save”. Finally, upload this Network Policy to both the VGVA and the access point which will serve as the VPN Client.

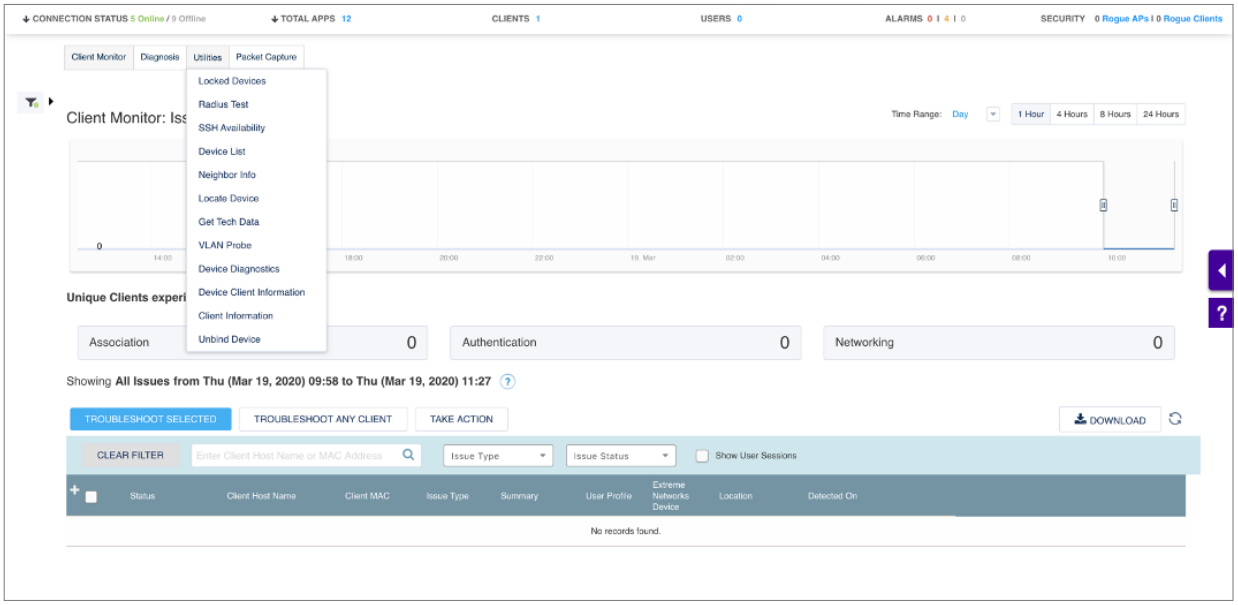


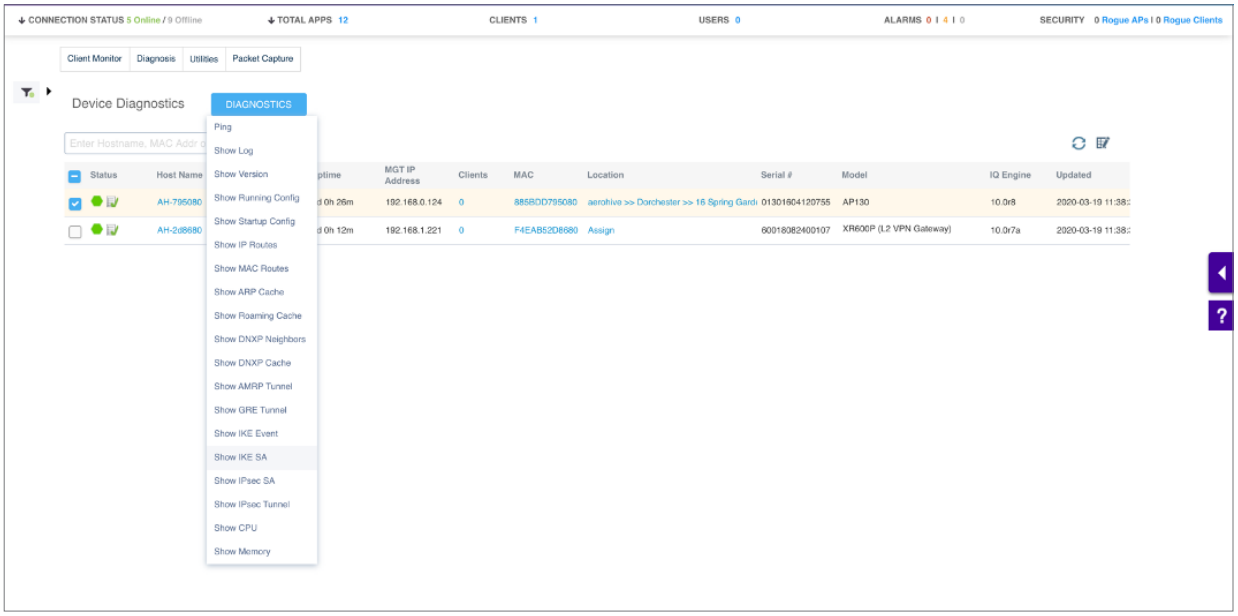
Click “Select” and click “Save”. Finally, upload this Network Policy to both the VGVA and the access point which will serve as the VPN Client.



Step 3: Verify the IPsec tunnel

To verify that the IPSec tunnel has been successfully established, navigate to the Monitor tab and select the Access Point. Click Manage > Tools > Utilities > Device Diagnostics.





This will display successfully established VPN tunnels. The following commands can be used to verify the VPN tunnels have been successfully created.

Show IKE SA

```
1:  phase 1 start;
2:  msg 1 received;
3:  msg 1 sent;
4:  msg 2 recived;
5:  msg 2 sent;
6:  msg 3 received;
7:  msg 3 sent;
8:  msg 4 received;
9:  phase 1 established;
10: phase 1 expired;
S=Side(I=Initiator;R=Responder):V=Version:E=Etype
Created=ISAKMP SA created time;Phase2=Counter of phase 2 rekey
-------------------------------------------------------
Destination            Cookies                          ST S  V  E Created              Phase2 Tu
nnel-ID
86.153.11.253[4500]    96882a08a02c4b0e:c39be48ac0f48b1b   9 I  10 M 2020-03-20 19:14:56      1
9
```

Show IPsec SA

```
IPsec Security Association Information:
192.168.1.221 [4500] 82.26.25.241 [1065]
        tunnel-id: 63
        esp-udp mode=tunnel spi=51453192(0x03111d08) reqid=2(0x00000002)
        Encryption: aes-cbc
        Authentication: hmac-sha1
        seq=0x00000000 replay=20 flags=0x20000000 state=mature
        created uptime: 1584731697      current uptime: 790
        diff: 18446744072124820709(s)   hard: 3600(s)   soft: 2880(s)
        last: 1584731698        hard: 0(s)      soft: 0(s)
        current: 1406(bytes)    hard: 0(bytes)  soft: 0(bytes)
        current: 19(pkts)       hard: 0(pkts)   soft: 0(pkts)
        failed: 0(pkts) replay: 0(pkts) replay window: 0(pkts)
        sadb_seq=1 pid=1791 refcnt=0
82.26.25.241 [1065] 192.168.1.221 [4500]
        tunnel-id: 63
```

Show IPsec Tunnel

```
IPsec Tunnel Duration:
Source                 Destination            Created             Duration
---------------------- ---------------------- ------------------- ---------------------------------------
192.168.1.221[4500]    82.26.25.241[1065]     2020-03-20 19:14:56  0 days 0 hours 3 minutes 30 seconds

Total IPsec Tunnel Sessions: 1

Tunnel Statistic Information::
Src IP                 Dst IP                 Pkts       Bytes      Auth-Err   Other-Err  SPI        Remaining-Lifetime
---------------------- ---------- ---------- ---------- ---------- ---------- ---------- ------------------
192.168.1.221[4500]    82.26.25.241[1065]     22         1628       0          0          0x03111d08  1584734473(s) expir
e
82.26.25.241[1065]     192.168.1.221[4500]    25         1863       0          0          0x0bacb864  1584734473(s) expir
e
```

Step 4: Verify Client Connectivity

You can now connect the WLAN client to the SSID you created and configure for L2 IPSec VPN. The client should get its IP address from the LAN subnet behind the VGVA. The VLAN can be different than the one used by the VGVA and the VLAN ID is defined by the User Profile object.

Summary

This solution provides a method to quickly and easily deploy a layer 2 VPN between the Virtual Gateway Appliance (VGVA) and a wireless access point. Once deployed, the solution will extend the head office network to remote locations and provide remote wireless users the abilituy to access head office based applications.