

New Features Guide for HiveOS and HiveManager 5.0r1

This guide describes the new features and feature enhancements that have been introduced in the HiveOS and HiveManager 5.0r1 releases, including Layer 3 routing support for the BR100, AP330, and AP350 devices.

New Features and Feature Enhancements

Several new features and feature enhancements have been introduced in the HiveOS and HiveManager 5.0r1 releases. You can read summaries of these features and enhancements below. Most of them are covered in more detail in individual sections later in this guide. For more information about addressed issues for these releases, refer to the *Aerohive Release Notes for HiveOS and HiveManager 5.0r1 Releases*.

New Features and Enhancements in the 5.0r1 Releases

HiveManager 5.0r1 in Enterprise mode and HiveOS 5.0r1 introduce routing features for the Aerohive BR100 Router and Aerohive AP 330 and 350 Access Points when configured to function as routers. With this functionality, you can construct and manage cloud-enabled networks using routers and a CVG (Cloud VPN Gateway) or a pair of CVGs, one as a primary and one as a backup. The CVG is a VMware ESXi version of HiveOS that terminates VPN tunnels from routers so that hosts at one site can make secure connections to hosts at the corporate site or at other branch sites. You can enable, configure, and monitor all of your Aerohive routing devices through HiveManager 5.0r1 in Enterprise mode.

The following features are supported in the HiveOS and HiveManager 5.0r1 releases:

Cloud VPN Gateway: The CVG is a virtual machine for HiveOS that runs on a VMware ESXi hypervisor. It terminates VPN tunnels from Aerohive routers at teleworker home or branch sites, allowing hosts at one site to communicate securely with hosts at the corporate site and at other remote sites. In addition, the CVG supports dynamic routing so that routes are automatically propagated between branch routers and the corporate site.

Aerohive Routers: You can use the BR100 and configure AP330 and AP350 devices to operate as Aerohive routers and VPN tunnel initiators so that your branch sites can connect securely to your corporate network or to other remote sites.

Dynamic IP Assignment for Remote Sites: It is not necessary to configure a network address scheme for each branch site. You only have to specify how many sites and how many hosts per site you need for any size subnetwork, and HiveManager divides the subnetwork into the appropriate portions and assigns one to each Aerohive router. You can even create a list of sites that must be included in a specific portion of the subnetwork and HiveManager will ensure that these sites receive the correct network information. The router at each site then can act as a DHCP server, supplying IP addresses to connected clients. This feature eliminates the need for an external DHCP server, setting up DHCP relay agents in each branch site, and configuring unique DHCP scopes for each site, which would all be necessary without this capability.

IPsec VPN: HiveOS provides the ability to build route-based IPsec tunnels between Aerohive routers and the CVG. Unlike software-based VPN solutions that must be installed and run on the clients themselves, a router with an established IPsec VPN tunnel allows multiple types of devices to connect through a secure SSID or authenticated LAN connection to your router, which then tunnels their traffic. There is no need to install any additional VPN software on the clients.

Network Firewall: Every Aerohive router has stateful firewall functionality built in. The network firewall is not applied through user profiles, but at the network policy level on the router. Because the firewall is applied at the network policy level, you can quickly see all of the firewall rules that apply to any device sending traffic through that router.

Dynamic Route Updates: Through RIPv2 or OSPF, the CVG can dynamically collect routing information from other routers on the corporate network and distribute the routes it learns to Aerohive routers at branch locations. In the reverse direction, it can also advertise route information about branch networks to other routers on the corporate network.

USB Modem with WAN Failover: Aerohive routers provide a USB port for a 3G or 4G modem that can be used as a WAN interface in case the Ethernet link fails or as the primary access method in situations where there is no Ethernet access.

DNS Proxy: You can configure a router to function as a DNS proxy server to provide domain name resolution for connected local clients. You can configure the router to send some domain name requests to local DNS servers and others to remote DNS servers on the corporate network. This assures that the router forwards all corporate-destined traffic through a VPN tunnel and provides security and added control of the name resolution process. This way you can use an internal DNS server to reach internal servers, and an external DNS for traffic non-corporate traffic.

Client Information on Ethernet Ports: In contrast to earlier releases, which displayed information only for wireless clients, HiveManager 5.0r1 displays information for all clients connected to the network, regardless of their access method.

Web Filtering: Aerohive routers can transparently send HTTP traffic destined for the Internet first to an external security vendor for verification and enforcement of URL filtering and other security policies before permitting the traffic to reach its originally targeted destination. Aerohive supports the following external security vendors:

Websense: Websense provides access to a database of over 95 web categories and 150 application protocols you can use to configure web use policies for employees. Websense web filtering services help minimize risks from rogue applications, viruses, drive-by downloads, data stealth, Trojans, and other security threats.

Barracuda: Barracuda web filtering services help protect against Internet threats, conserve bandwidth, and filter content for compliance and productivity. You can configure Barracuda policies based on group membership or individual user requirements. Barracuda policies use eight super-categories with 73 sub-categories to manage user access to content. By adding *quotas* to these policies, you can control connections, duration, or bytes used while users are browsing the web. For example, you can allow site access but block audio, video, executables, or other undesired functions. Your policy manages P2P/File Sharing, IM, and streaming media, and prevents the downloading or uploading of undesired content.

HiveManager Device Management: This release introduces a single interface from which you can monitor all Aerohive devices (HiveAPs, routers, and CVGs), modify or view policies across groups of devices, and manage large-scale distributed networks without the need for additional resources.

Setting up a Cloud VPN Gateway and a Router

You can construct and manage cloud-enabled networks using routers (BR100 devices and AP330 and AP350 devices configured as routers) and a CVG (Cloud VPN Gateway). You can enable, configure, and monitor all of your Aerohive routing devices through HiveManager 5.0r1 in Enterprise mode.

To enable hosts on branch networks to communicate securely with hosts on the corporate network, you can first install and configure a CVG to which the Branch Routers can build IPsec VPN tunnels. This process is described in the following sections.

Installing a Cloud VPN Gateway

The CVG is a virtual machine that you can download in an .ova (Open Virtual Appliance) file and deploy on an ESXi hypervisor running on a physical device on your corporate network. The ESXi hypervisor is a server dedicated to running VMs (virtual machines), and a VM is a container that can run its own operating system and execute applications. If you do not already have VMware ESXi deployed, you can obtain free VMware ESXi software from <http://www.vmware.com/products/vsphere/esxi-and-esx/overview.html>. You can download the AH_CVG.ova file from the HiveManager GUI: Monitor > Update > Download VA image for VPN Gateways.

You will install ESXi on a server or dedicated PC. Although the CVG VM (virtual machine) is 32-bit Linux, ESXi requires hardware that is 64-bit capable (Core 2 family). Remember to enable the virtualization feature in the BIOS of the host device. Consult your hardware documentation for detailed instructions. Your virtualization host must have two physical network adapters and a minimum of 512 MB of RAM and 256 MB of disk space.

512 MB is the initial RAM setting for the CVG VM, but you can increase it. A single CVG VM uses 256 MB of disk space.

Before beginning the VM deployment, connect Ethernet cables to the physical network adapters that you intend to use. The CVG VM has two interfaces (eth0/WAN and eth1/LAN), which you assign to two networks bound to separate physical adapters. Also, to install VMware ESXi from a bootable CD, make sure the BIOS is able to boot from the CD/DVD drive. (See your hardware vendor documentation for information on changing boot order.)

You also need to install VMware vSphere Client on your computer and use it to access the ESXi hypervisor and CVG VM. Computers running Windows support vSphere Client, but Apple computers do not.

Installing ESXi

Follow these steps to install the ESXi hypervisor on a server or dedicated PC that meets the minimum requirements noted above.

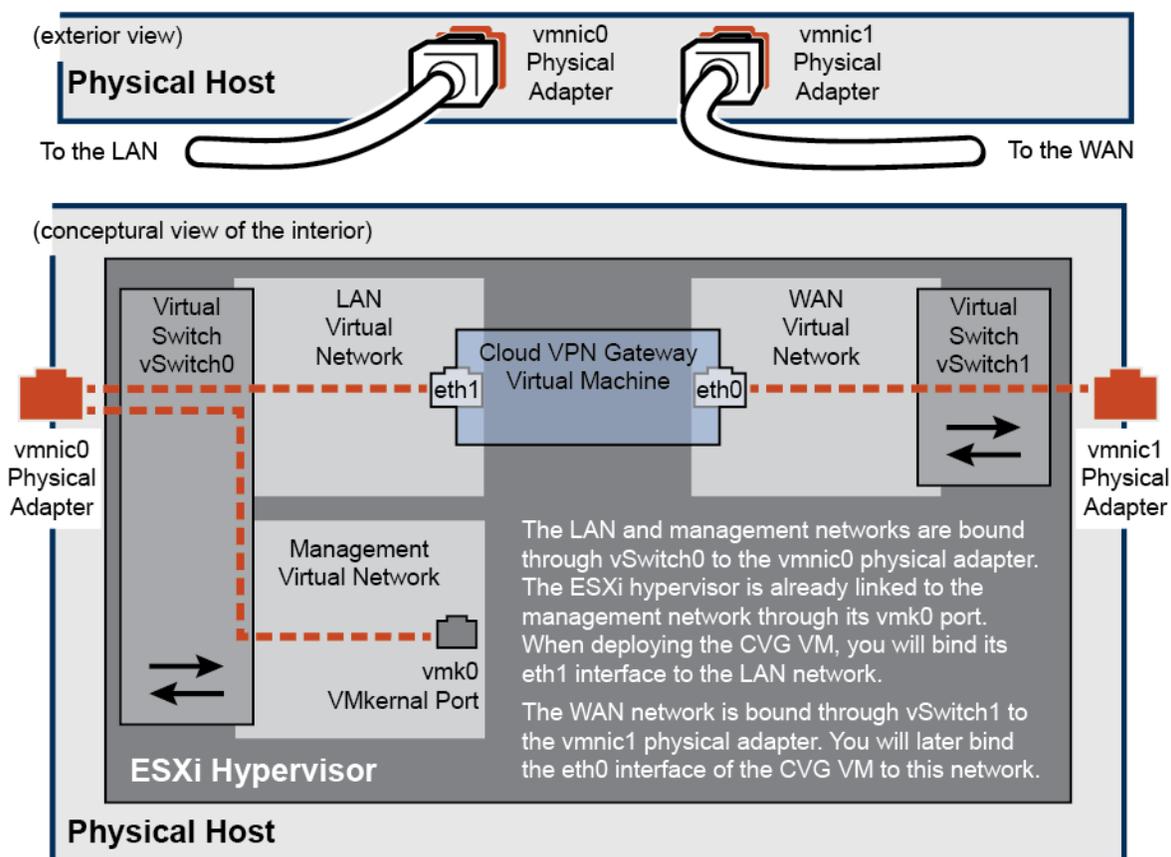
The following procedure assumes that you have a keyboard and monitor attached to the device you intend to make the ESXi host.

1. From the VMware website (see link above), register for a free account, and download ESXi 4x or later. ESXi 3 does not support the Aerohive CVG VM.
2. Burn the ESXi image to a CD or DVD. You will use this disc to install the image on the virtualization host.
3. Load the disc with the ESXi image on the host and boot it up from the disc.
4. After accepting the end user license agreement, follow the VMware ESXi installer instructions that appear onscreen to select a hard disk on which to install ESXi, set a keyboard layout preference, and define an ESXi hypervisor root admin password. When the installation is complete, remove the disc and reboot the system.

- After the system reboots, press the **F2** key to log in to the ESXi Direct Control User Interface using the root admin password that you just set. Check if the host received its network settings through DHCP. If so, note its IP address. If not, configure static network settings through the onscreen interface.
- Moving to your computer, open a browser and make an HTTP connection to the IP address of the ESXi hypervisor. Click the **Download vSphere Client** link and download and install VMware vSphere Client on your computer.

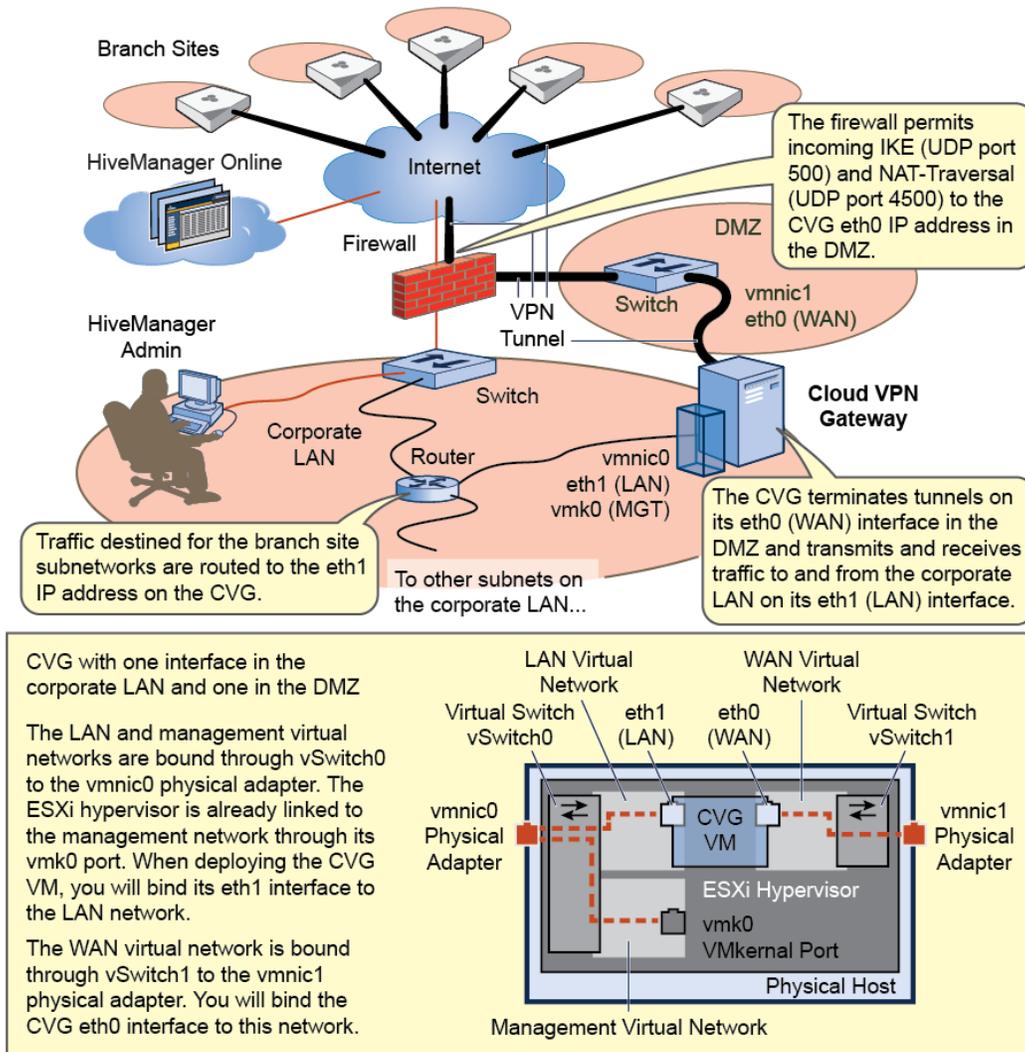
Creating and Activating Virtual Networks and Mapping Network Settings

By default, ESXi has two virtual networks: Management Network and VM Network. Both networks are bound to the vSwitch0 virtual switch, which in turn connects to the vmnic0 physical adapter. The management interface (vmk0) for the ESXi hypervisor is bound to the management virtual network. For ease of reference, you rename the VM network "LAN Network" because you cable the vmnic0 physical adapter to the LAN segment of your network. You then create a second virtual network and name it "WAN Network" and bind it to the vSwitch1 virtual switch. You connect vSwitch1 to the vmnic1 physical adapter, which in turn you cable to the WAN segment of your network. When you deploy the CVG VM, you bind its eth1 interface to the LAN virtual network and eth0 to the WAN virtual network.

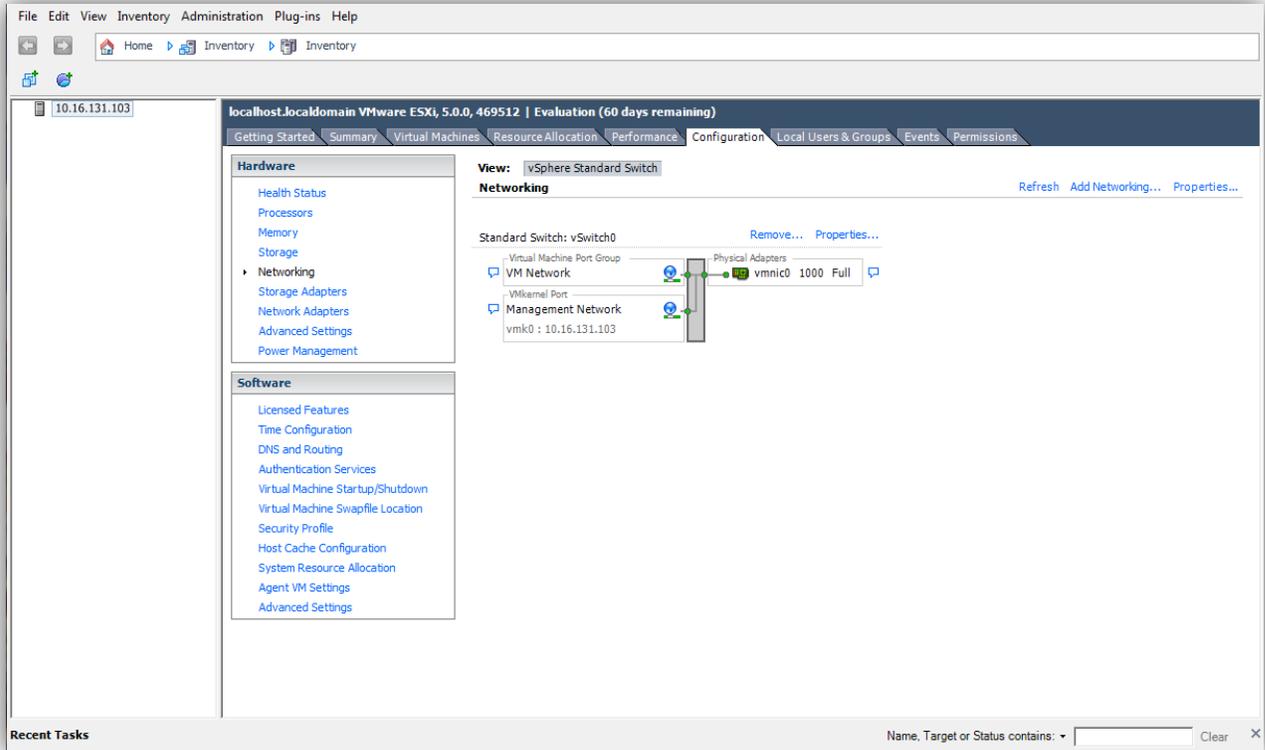


Deploying a CVG

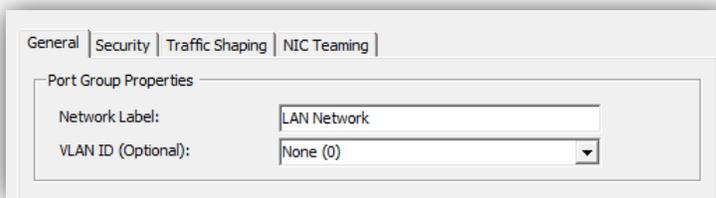
The following procedure explains how to deploy a CVG VM so that its eth0 interface connects to the DMZ network and its eth1 interface connects to the corporate LAN network. The firewall must allow inbound IKE and NAT-Traversal traffic (UDP ports 500 and 4500 respectively) to the eth0 IP address. Finally, you must either manually set static routes on the corporate LAN to send traffic destined for the branch site subnetworks to the eth1 interface or employ a dynamic routing protocol—OSPF or RIPv2—on the LAN to exchange routes with the CVG and manage the routing automatically.



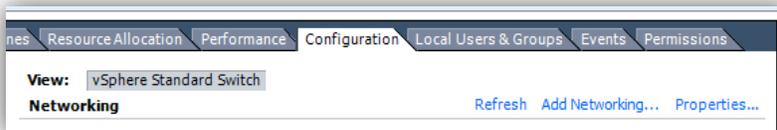
1. Launch VMware vSphere Client, enter the IP address that you defined for the ESXi hypervisor, and then log in to the ESXi hypervisor with the root admin credentials you set in the previous section.
2. Click **Configuration > Networking**.



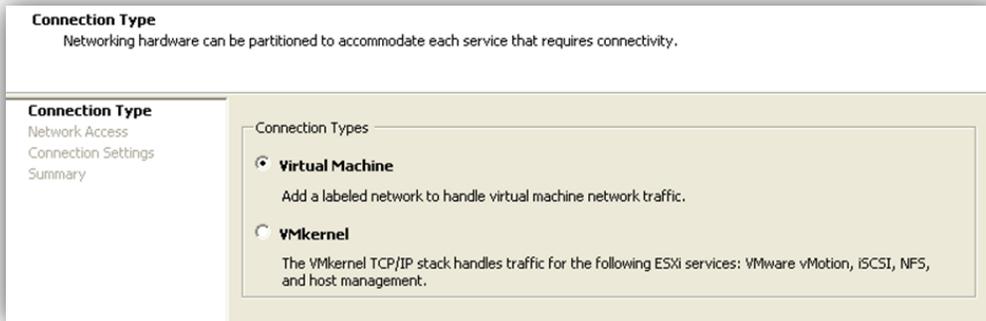
3. Click **Properties** for Standard Switch: vSwitch0. The vSwitch0 Properties dialog box appears.
4. Select **VM Network**, and then click **Edit**. The VM Network Properties dialog box appears.
5. Change the Network Label to **LAN Network**, leave the VLAN ID as **None (0)**, and then click **OK** to close the VM Network Properties dialog box. Then click **Close** to close the vSwitch0 Properties dialog box.



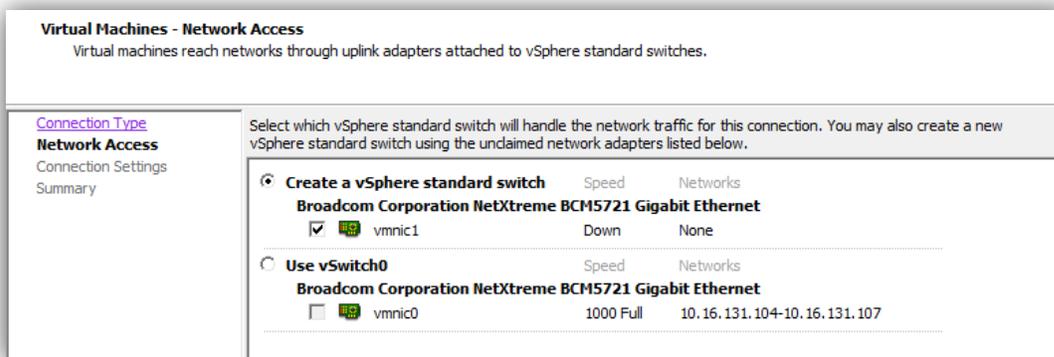
6. To create a new WAN virtual network and a virtual switch (vSwitch1) for this network, click **Add Networking**.



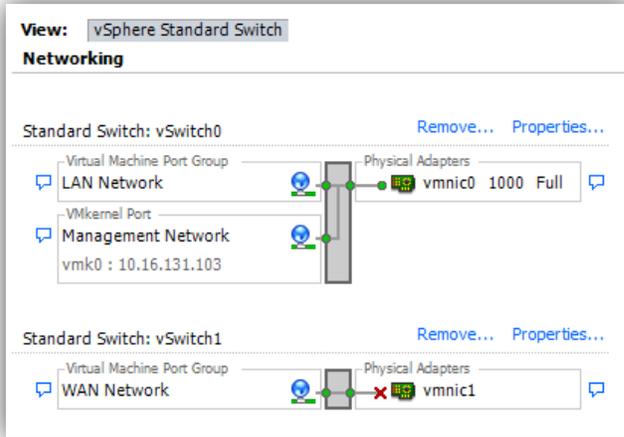
- Select **Virtual Machine** for Connection Type, and then click **Next**.



- Select **Create a vSphere standard switch**, select the **vmnic1** check box, and then click **Next**.



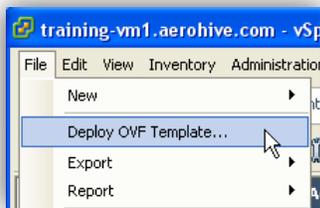
- In the Network Label field, enter **WAN Network**, leave the VLAN ID as **None (0)**, and then click **Next**. Confirm your settings and then click **Finish**. In the Configuration tab, you can now see the LAN and WAN virtual networks.



Deploying the CVG .ova Template

Use the following steps to download and deploy the .ova (Open Virtual Appliance) file on the ESXi hypervisor. An .ova file contains a virtual machine that is prepackaged and ready for deployment.

1. Log in to HiveManager, click **Monitor > Update > Download VA image for VPN Gateways**, and then save the AH_CVG.tar file to a local directory on your computer. Its file size is about 27 MB.
2. With the VMware vSphere Client, make a connection to the IP address of the ESXi hypervisor, click **File > Deploy OVF Template**. The Deploy OVF Template wizard launches.



3. Navigate to the location of the AH_CVG.tar file that you downloaded, select the file, click **Open**, and then click **Next**.
4. Verify the template details, and then click **Next**.
5. Specify a name for the .ova template, and then click **Next**.
6. Select the disk format in which you want the virtual disks to be stored. You have three choices:
 - **Thick Provision Lazy Zeroed:** When you select this option, the CVG VM claims the entire amount of configured hard disk space from the virtualization host; however, the VM does not immediately overwrite sectors with zeroes if the VM is not currently using them. As a result, any preexisting data occupying the claimed sectors might be recoverable from the host.
 - **Thick Provision Eager Zeroed:** When you select this option, the CVG VM claims the entire amount of configured hard disk space from the virtualization host and immediately overwrites all allocated—but as yet unused—sectors with zeroes. This option will take longer during initial VM deployment.

- **Thin Provision:** When you select this option, the ESXi hypervisor allocates only enough host disk space to the CVG VM for it to start, leaving the rest of the disk space for other virtual machines to use if needed. Note that one disadvantage to this approach is that the VM might run more slowly as it reclaims disk space as needed.

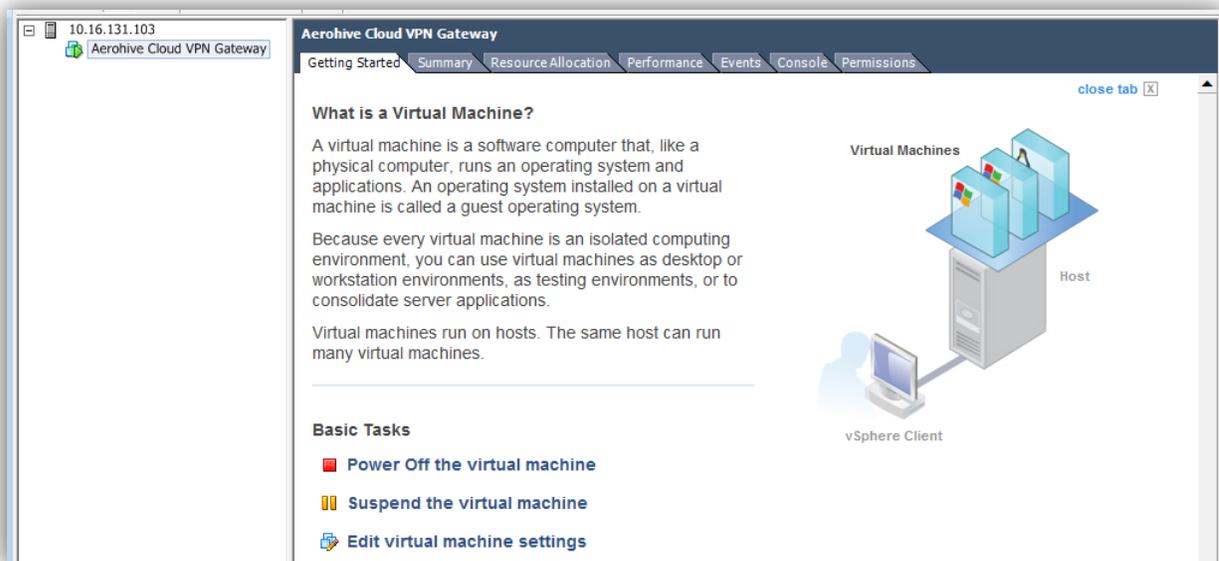
Aerohive recommends selecting either of the thick provisioning options for better performance. Although thin provisioning is useful for space-demanding VMs, the CVG requires about 100 MB of storage, so space will not typically be an issue. After you make your selection, click **Next**.

7. Check that the virtual switches you created are properly mapped to the destination networks you defined: LAN → LAN Network and WAN → WAN Network. If the mapping is correct, click **Next**.
8. Confirm your selected options, select **Power on after deployment** to start the CVG VM, and then click **Finish**.

Using the Setup Wizard to Configure CVG Network Settings

In this section, you configure network settings for the CVG using the Setup Wizard.

1. From the VMware vSphere Client, expand the ESXi icon in the left navigation panel, select the CVG icon under it, and then check in the Getting Started tab if the CVG VM is powered on. If not, click **Power on the Virtual Machine**.



2. Click the **Console** tab, and then log in by entering **admin** and **aerohive** for the login name and password.

- When the initial setup wizard appears, type **1** and press the **ENTER** key to select **1. Network Settings**.

```

Welcome to the Aerohive Cloud Virtual Gateway
Initial Setup Wizard

Select one of the following options

1. Network Settings
2. Enter Activation Code
3. Shut down

```

- Enter **2** to select **2. Manually configure interface settings**. Then define the network settings for eth0 (the WAN interface), and then apply the settings by entering **yes**. (Substitute your actual IP address settings for those shown below.)

```

Network Settings
-----

The Cloud Virtual Gateway must be able to communicate with hosts on the Internet in order
to process your activation code and be configured by HiveManager.

Choose the method for configuring the eth0 interface settings:

1. Use DHCP to set IP address, gateway, and DNS
2. Manually configure interface settings

Enter option ([1] or 2):2

Manually Configure Interface Settings
-----

Enter the IP address for Eth0:1.2.2.5
Enter the netmask length [24]: 255.255.255.0
Enter the default gateway: 1.2.2.1
Enter the DNS server IP address: 1.1.1.220
Do you want to apply the change? <[yes]:no>: yes

```

- When you enter **yes**, the CVG VM tests its connection. If all tests succeed, the following output appears:

```

Testing the connection between CVG and license server. (Press enter to start)
Checking the interface address:
OK (eth0 address = 1.2.2.5)
Checking the default gateway:
OK (IP 1.2.2.1 is alive)
Testing DNS:
OK (License server can be resolved)
Pinging the license server:
Ok (License server is alive)
Do you want to reset the networking? <yes|[no]>: no

```

(i) If the CVG cannot reach the license server and you want to return to the beginning of the wizard, press **CTRL-R**. You can also return to the wizard later by entering the following command: **wizard startup**

6. Enter the activation code that you received in an email from Aerohive. A serial number is automatically assigned to your CVG so the redirector can point it to your instance of HiveManager Online.

```

Enter Activation Code
-----

Please input the CVG Activation Code (4 to 5 chars):xxxxxx

CVG serial number 1234567892011 has been installed successfully, you can enter "show-hw-info"
to check it after reboot.

To implement the change, do you want to reboot now? <[yes]|no>: yes

```

7. After the CVG reboots, log back in by accessing its console through the vSphere Client and entering **admin** and **aerohive**. If you are managing Aerohive devices through HiveManager Online, a physical HiveManager appliance or HiveManager Virtual Appliance in the same subnet as the eth0 or eth1 interface of the CVG, or if you have configured a DNS server to resolve `hivemanager.<local_domain>` to the IP address of a physical HiveManager appliance or HiveManager Virtual Appliance, the CVG will automatically form a secure CAPWAP connection with it. To see the CAPWAP status for the CVG, enter this command:

```
show capwap client
```

If you are using a physical HiveManager appliance or HiveManager Virtual Appliance that is not in the same subnet as the CVG eth0 interface and the DNS server is not configured to resolve `hivemanager.<local_domain>` to the HiveManager IP address, enter the following command so that the CVG can send unicast CAPWAP Discovery messages to it:

```
capwap client server name <ip_addr>
```

Installing a Router

You can use a BR100 or configure an AP330 or AP350 to function as a router. Although an AP330 or AP350 eventually functions as a router, routing traffic between its LAN and wireless interfaces and its WAN interface, when it initially comes online, it functions like a Layer 2 device with only a single address on its mgt0 interface.

ⓘ If you are using a physical HiveManager appliance or HiveManager Virtual Appliance for device management, you must set the HiveManager IP address or domain name as the CAPWAP server on the BR100 or AP330 or AP350 before deploying it remotely. If HiveManager is in a network with a DHCP server, a simple approach is to connect the device to the same subnet as HiveManager so that it can get its network settings through DHCP and then broadcast CAPWAP Discovery messages to locate HiveManager. You can then configure the device with the IP address or domain name it can use to reach HiveManager when installed at a branch site. See the HiveManager Help system for further information.

To install a router at a remote site:

1. Connect the device to a power source. An AP330 or AP350 can connect to either an AC power source or a PoE switch or injector; however, if you intend to use the USB modem, you must connect it to an AC power source. The BR100 does not support PoE and must connect to an AC power source.
2. Connect the WAN/ETH0 interface on a BR100 or the ETH0 interface on an AP330 or AP350 to a modem, DSL router, or other Internet device.

The device acts as a DHCP client and automatically obtains its network settings from a DHCP server for the mgt0 interface on an AP330 or AP350 and for the ETH0/WAN interface on a BR100. After that, it automatically attempts to form a CAPWAP connection to a physical HiveManager appliance, HiveManager Virtual Appliance, or HiveManager Online. In about five minutes, the device will form a CAPWAP connection with HiveManager and appear in the HiveManager GUI on the Monitor > Devices >

All Devices page. (For information about the CAPWAP connection process, see the release notes, deployment guide, or HiveManager Help system.)

An unconfigured AP330 or AP350 does not act as a router, so any devices connected to it will be unable to access the Internet until you upload a configuration to it from HiveManager. In contrast, an unconfigured BR100 acts as a router and provides Internet access to devices connected to its LAN interfaces even before it receives a configuration from HiveManager.

3. If you want to provide Ethernet connections to devices on the LAN side, connect the ETH1 – ETH4 interfaces on a BR100 or the ETH1 interface on an AP330 or AP350 to switch or host. If you want to provide wireless connections for hosts on the LAN side of the device, you can skip this step.

Connecting the Router and the CVG

The next step is to configure and upload a network policy to the router and the CVG so that the router can build an IPsec VPN tunnel to the CVG. HiveManager contains a preconfigured network policy called *QuickStart-Wireless-Routing* that simplifies this step. If you use QuickStart-Wireless-Routing policy, you only need to configure firewall and Layer 3 IPsec settings, and then upload the configuration to your devices, as described in this section.

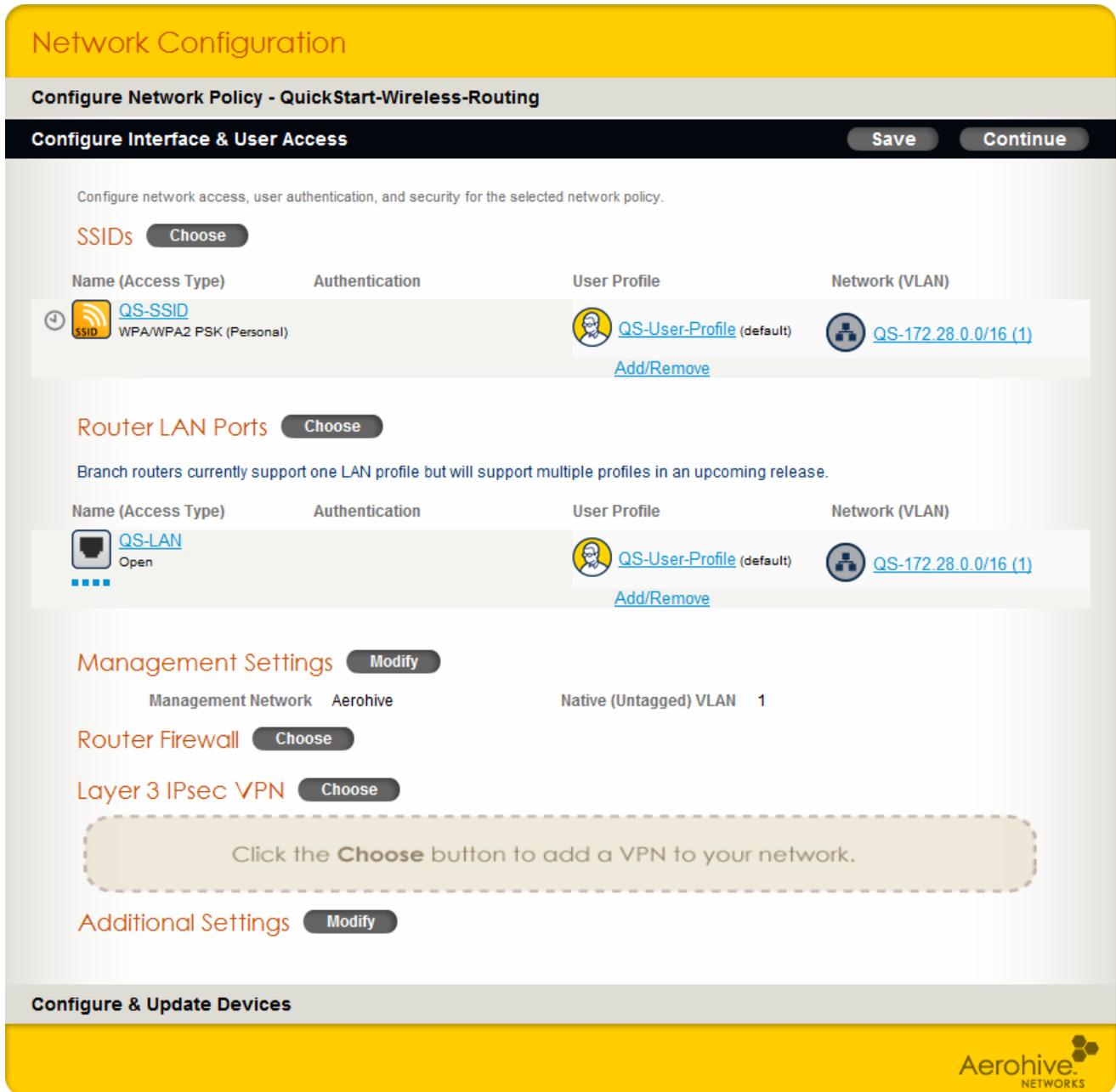
1. Log in to HiveManager, click **Monitor > Devices > All Devices** in the navigation tree, and confirm that the CVG and BR100, AP330, or AP350 appear.
2. Click **Configuration**, from the Network Policy list, choose **QuickStart-Wireless-Routing**, and then click **OK**.

The QuickStart-Wireless-Routing policy is preconfigured for a wireless and routed network. It includes an SSID with an accompanying user profile, network (172.28.0.0/16), and VLAN (1). The PSK used in the SSID is the one you set for this policy when you put HiveManager in Enterprise mode.

The policy also includes router LAN port assignments with the same accompanying user profile, network, and VLAN as those for the SSID. With these settings, the router will assign all users at the branch site to the same user profile and put them in the same subnet within the 172.28.0.0/16 network. HiveManager automatically allocates each site a subnet within the network based on the number of branches specified. For the QuickStart-Wireless-Routing policy, the 172.28.0.0/16 network is divided into 512 branches by default. It allocates the first branch site with the 172.28.0.0/25 subnet, the next with 172.28.0.128/25, the next with 172.28.1.0 /25, the one after that with 172.28.1.128/25, and so on.

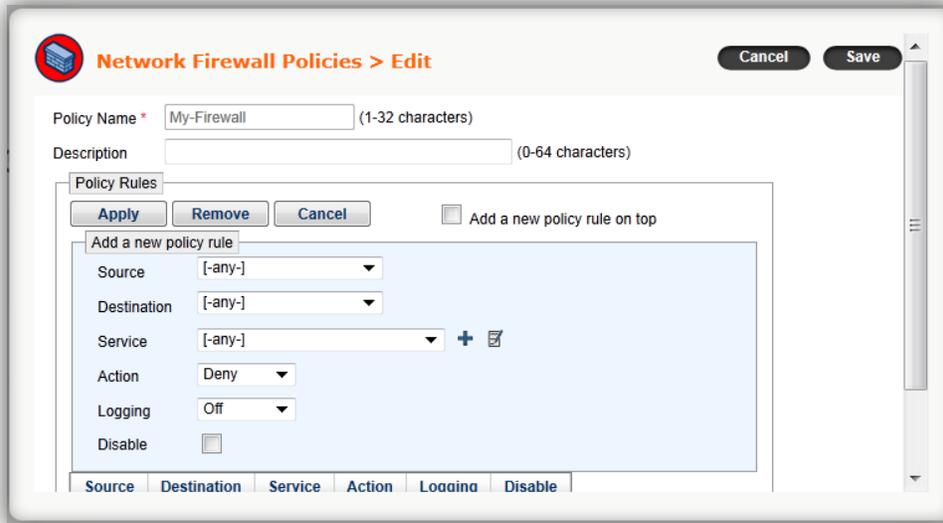
3. To add DNS server settings to the predefined network so that clients can successfully request domain name lookups, click the network object **QS-172.28.0.0/16**. From the DNS Service drop-down list in the *Edit Network* dialog box, choose the DNS service profile that HiveManager created when you first enabled Enterprise mode. By default, this DNS service profile directs clients to use their default gateway (IP address of the LAN interface or mgt0 subinterface on the SSID to which they connect) for domain name lookups, and the router than proxies them to its name servers.

If the other SSID and router LAN port settings do not suit your needs, you can modify them. However, if they are satisfactory, then you only need to configure the router firewall and Layer 3 IPsec VPN settings.



- Click **Choose** for Router Firewall, and then click **New**. Name your firewall policy, add a description, and add the rules you want the router to apply. When finished, click **Save**.

⁽ⁱ⁾ Because the router applies firewall rules in order from the top, their position in the list is important. To relocate a rule, click and drag it to different position in the policy.



- Click **Choose** for Layer 3 IPsec VPN, and then click **New**. In the *New VPN Service* configuration panel, enter the following, and then click **Save**:

Profile Name: Enter a name for the VPN profile.

Description: Enter a useful note about the VPN profile.

Layer 3 IPsec VPN: (select)

In the *VPN Gateway Settings* section, choose the name of your CVG, enter its external IP address, and then click **Apply**. The external IP address is the public-facing address that the routers can contact. If the firewall performs NAT for devices in the DMZ, then enter the external IP address that the firewall maps to the internal IP address of the eth0 interface. If the firewall does not perform NAT, then enter the eth0 IP address, which must be a public one.

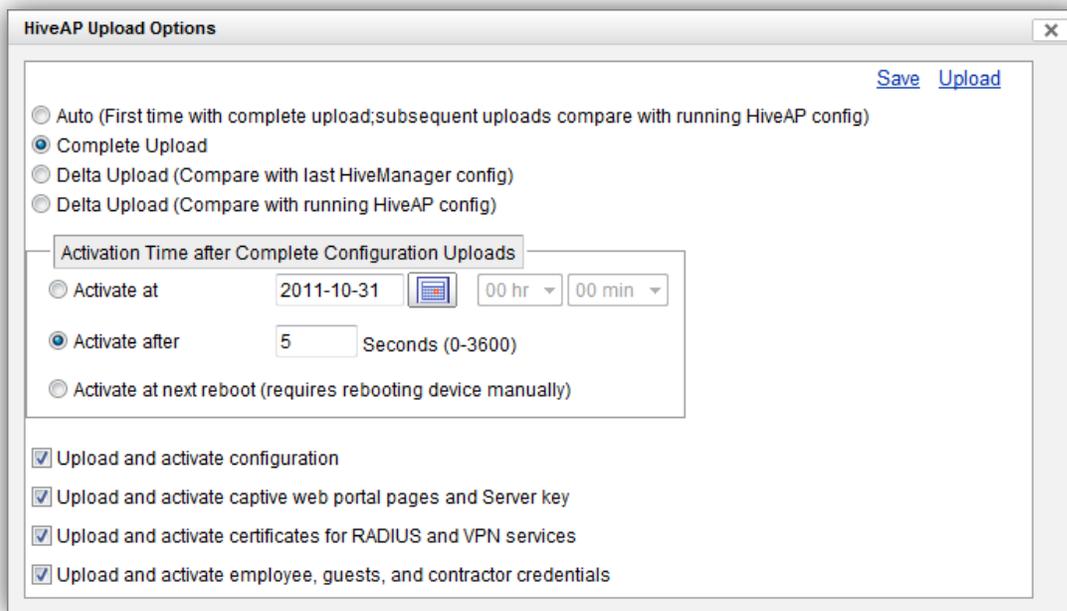
For the default tunnel policy, there are two choices for how the router processes client traffic: It can route only internal traffic through the VPN tunnel (default), or it can route all traffic through the tunnel. You can also apply routing exceptions based on user profiles and routing destinations. (For more information about VPN services, see “IPsec VPNs” elsewhere in this document.) When finished, click **Save**.

- In the *Configure Network Policy* panel, click **Continue** to save your settings and advance to the *Configure & Update Devices* panel.
- In the *Configure & Update Devices* panel, click the name of the device acting as the router and proceed as follows:

BR100 – Check that the device type is Branch Router, the network policy is QuickStart-Wireless-Routing, the DHCP client is enabled on the WAN interface (or, if not, that it has valid static network settings), and the admin state is Up on the WAN-Primary interface. If you made any changes, click **Save**. Otherwise, click **Cancel**.

AP330 or AP350 – Choose **Branch Router** from the Device Type drop-down list, which changes the available settings on the page. Check the same settings as those for the BR100, and then click **Save**.

8. In the *Configure & Update Devices* panel, select the box next to the CVG and the router to which you want to upload the QuickStart-Wireless-Routing policy and device-level configuration settings, click **Settings**, select **Complete Upload, Activate after 5 seconds**, and all of the upload-and-activate options at the bottom of the dialog box, and then click **Upload**.



9. After the devices finish loading and then rebooting to activate their new configurations, check the network settings of a client connected to the router and then test its network connectivity.
 - Check that the client received network settings through DHCP from the router. The address will be in a subnet within the 172.16.0.0/16 network, and its default gateway and DNS server will be that of either the LAN interface (for an Ethernet connection) or the mgt0.n subinterface of the QS-SSID (for a wireless connection).
 - To check routing functionality, ping an IP address, such as 206.80.44.205.
 - To test DNS functionality, ping a domain name, such as ntp1.aerohive.com. If successful, open a web browser and visit an Internet address, such as www.aerohive.com.
 - Finally, to test your VPN tunnel connection, try to reach an internal address on your corporate network, such as https://intranet-corporate-site/main.

Feature Limitations for the BR100 and AP330 and 350 as Routers

The BR100 shares many features with HiveAPs, but there are also a number of differences worth noting. Similarly, there are differences between AP330 and AP350 devices functioning as access points and as routers. The major differences are summarized in this section.

Behavioral Differences between the BR100 and HiveAPs

Mesh Links between Aerohive Routers and HiveAPs

- The recommended way for HiveAPs to communicate with a BR100 is over a wireless mesh link
- Although a HiveAP can be connected to a BR100 LAN port, this is not recommended for the following reasons:
 - The AMRP (Advanced Mesh Routing Protocol) loop prevention might not detect a routing loop if the devices are connected through both a wired and wireless backhaul link. If you cable a HiveAP to the LAN port on a BR100, disable wireless backhaul communications to ensure that there are no loops in the connections.
 - The BR100 LAN port must be configured as a trunked port to be able to process traffic from the HiveAP, and captive web portal authentication cannot be used on LAN ports in trunk mode.

Default Configuration

- HiveAPs initially act as Layer 2 access points.
 - The eth0 interface is in backhaul mode.
 - HiveAPs use DHCP to get network settings for their mgt0 interface.
- BR100 devices initially act as simple Layer 3 routers.
 - The eth0 interface is in WAN mode.
 - The mgt0 interface has static IP address: 192.168.85.1/24
 - All eth1 ports provide clients with access to the WAN and perform NAT on their source addresses.
 - DHCP and DNS servers are active on the mgt0 interface and use the following IP pool: 192.168.85.10–192.168.85.99
 - A track IP group pings 8.8.8.8 for WAN connectivity testing.
- Entering the **reset config** command or pressing the **Reset** button on a device for 10 seconds reverts it to its initial state:
 - HiveAPs have an empty configuration.
 - BR100 devices have a default configuration.

NetConfig UI

- The BR100 has a NetConfig UI with a smaller feature set than that for access points with just these settings available:
 - Local network settings for the eth0/WAN interface
 - HiveManager (CAPWAP server) and HTTP proxy settings

Wi-Fi Radio

- BR100 devices have single 2.4 GHz radio (no 5 GHz support).
- DFS and high density deployment capabilities are not supported for 2.4 GHz radio devices.
- On the device configuration page in HiveManager, the radio mode options (access, backhaul, dual mode) differ.

Behavioral Differences between Routers and HiveAPs

The routers referred to in this section include the BR100 and the AP330 and 350 configured as a router.

IP Tracking

- Routers always need a track IP group for WAN connectivity testing, which you can choose from the Track IP Group for router WAN connectivity drop-down list in the *Additional Settings* > *Service Settings* section of a network policy.
- When pushing a configuration to routers, HiveManager ignores the following track IP settings:
 - Selected track IP groups in the Track IP Groups for Remedial Actions section in Service Settings for a network policy
 - Actions to take when targets become unresponsive in the Track IP Group chosen for WAN connectivity testing

Aerohive Initial Configuration Wizard (CLI)

- The CLI Aerohive Initial Configuration Wizard is designed for HiveAPs and is not appropriate for routers, although the `wizard startup` command is not removed from the CLI on BR100s. Do not use Initial Configuration Wizard on routers.

Access Console

- The access console SSID is not available on the BR100.
 - An access console is available on HiveAPs running a default configuration.
 - An access console is not part of the default configuration on a router.
 - On routers, an access console cannot be triggered by a track IP group (see “IP Tracking” above).

802.1X Authentication not Supported on Wired LAN Ports

- You cannot configure 802.1X authentication for router LAN ports.
- You can configure captive web portal authentication for router LAN ports.

VLAN Probe

- The VLAN probe that you can set on Monitor > Tools > Diagnostics > VLAN Probe dialog box apply to the LAN interface only.

QoS

- QoS (Layer 2) classification, marking, and scheduling do not apply to eth0.

Capacity Differences for the BR100

Parameter	Maximum on the BR100	Maximum on other devices	Enforcement
Maximum number of SSIDs	8	16	HiveManager
Maximum number of associated stations (per radio)	32	100	HiveOS (internal; no configuration settings)
Maximum number of entries in the roaming cache	64	N/A	HiveOS (internal; no configuration settings)
Maximum number of network/VLAN objects	16	64	HiveManager

BR100 Feature Exclusions

Feature	Location in HiveManager	HiveManager Change
SNMP	Network Policy > Additional Settings > Management Server Settings > SNMP Server	HiveManager ignores SNMP settings when pushing a configuration to a BR100.
Location	Network Policy > Additional Settings > Management Server Settings > Server Assignment > Location Server	HiveManager ignores location server settings when pushing a configuration to a BR100.
TeacherView	Network Policy > Additional Settings > TeacherView Settings	HiveManager ignores TeacherView settings when pushing a configuration to a BR100.
OS Detection	Network Policy > Additional Settings > TeacherView Settings <i>and</i> User Profile > Client Classification Policy > Policy Rules > OS Object	HiveManager ignores client classification rules that reference OS Objects when pushing a configuration to a BR100.
WIPS	Network Policy > Additional Settings > Service Settings > WIPS Policy	HiveManager ignores WIPS settings when pushing a configuration to a BR100.
RADIUS Server/Proxy A BR100 cannot be configured as a RADIUS server or proxy.	Device Configuration > Optional Settings > Service Settings: - HiveAP RADIUS Service - HiveAP RADIUS Proxy	The <i>Service Settings</i> section has been removed from the device configuration page in the HiveManager GUI.

Feature	Location in HiveManager	HiveManager Change
Active Directory and OpenLDAP (options used with the RADIUS server feature)	(See RADIUS Server/Proxy) Active Directory and OpenLDAP authentication are used with RADIUS.	The <i>Service Settings</i> section has been removed from the device configuration page in the HiveManager GUI.
Distributing HiveOS software upgrades from HiveManager	Device Configuration > Optional Settings > Advanced Settings > Distributed HiveOS Update Image Server Preference	The setting has been removed from the device settings page. A BR100 cannot be selected as a HiveOS distribution server.

SSID Settings		
DoS (Denial of Service) prevention	SSID > Optional Settings > DoS Prevention and Filters <i>and</i> Hive Profile > Optional Settings - MAC DoS per Hive - MAC DoS per Station	HiveManager ignores DoS settings when pushing a configuration to a BR100.

Radio Profile Settings		
DFS (Dynamic Frequency Selection)	Radio Profile > Channel and Power > Enable DFS	Because DFS is only available for a 5 GHz radio and the BR100 has a 2.4 GHz radio, DFS is not applicable to a BR100.
High Density	Radio Profile > Optional Advanced Settings > High Density WLAN Settings	HiveManager ignores high density settings when pushing a configuration to a BR100.
Interference reporting	Radio Profile > Optional Advanced Settings > Interference > Enable Interface Report	HiveManager ignores interference reporting when pushing a configuration to a BR100.

Device Monitoring		
Spectrum analysis	Tools > Spectrum Analysis	If you attempt to use the tool, HiveManager displays the following error message: "Operation failed. The selected BR100 does not support this feature."
LLDP/CDP	Tools > LLDP/CDP	If you attempt to use the tool, HiveManager displays a message stating that the device was unable to execute the command.

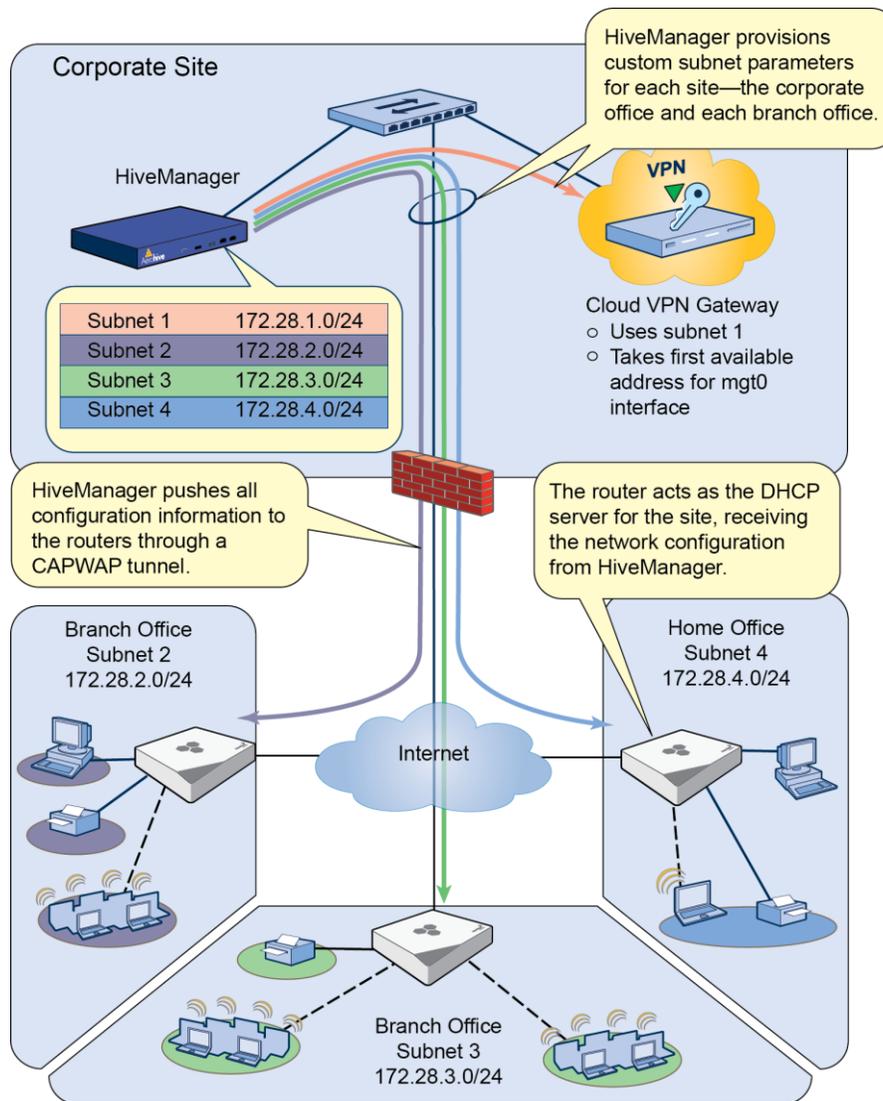
Limitations for an AP330/350 Configured as a Router

The following are unsupported features when an AP330/350 is configured as a router:

- TeacherView
- Layer 2 Firewall
- Backhaul Failover
- Layer 2 VPN
- ICMP Redirect
- Layer 2 NAT

Dynamic IP Assignment for Remote Sites

You can use HiveManager to assign IP address subnet scopes and DHCP client network settings to Aerohive routers at remote sites. When you push the configurations to the BR100 routers, the routers, acting as DHCP and DNS servers, deliver the designated network settings at the clients' request.



Centralizing the management of remote sites and distributing the services to each branch office in this way removes significant administrative overhead in maintaining branch offices and other remote users.

To apply these network settings to the routers, you must create a network object, which contains all the subnet information, and select that network object within the user profile object you plan to use.

Step 1: Configuring a Network Object

When you create a network object, it contains the VLAN, web security, DNS settings, and one or more subnetworks. You can increase the flexibility of your dynamic IP address and subnet assignments by configuring multiple subnetworks and reserving IP addresses, and then assigning them using classifiers. You can also define the network type; that is, whether the network object is used for internal (corporate) use or guest use. When you configure a network for guest use, traffic to and from the guest network cannot pass through the VPN tunnel and can only access the Internet.

To configure a network object for use by multiple branches, click **Configuration > Show Nav > Networks > New**, enter the following, and then click **Save**:

Name: Enter a name for the network object. You can later choose this name from the Network or VLAN-only Assignment drop-down list in a user profile configuration.

VLAN: Set a VLAN ID for the network.

Web Security: If you use a web security service to filter web traffic, choose either **Websense** or **Barracuda** from the drop-down list to route HTTP and HTTPS requests through the third party web security platform. In the event that the service becomes unavailable, you can choose either to permit or deny all outbound HTTP and HTTPS traffic that Websense or Barracuda would otherwise filter. For more information regarding web security, see “Web Filtering”.

DNS Service: Choose the DNS service profile from the drop-down list. If you do not see a service that you want to use, you can create a new DNS profile by clicking the **New (+)** icon.

ⓘ The DNS service profile contains information regarding DNS servers.

Description: Enter a brief description of the network object. Including such information as its purpose or location is often helpful.

Network Type: Select whether the network is for internal or guest use from the drop-down list.

In the *Subnetwork* section, click **New**, enter the following information in the *Configure Subnetwork* dialog box that appears, and then click **Save**:

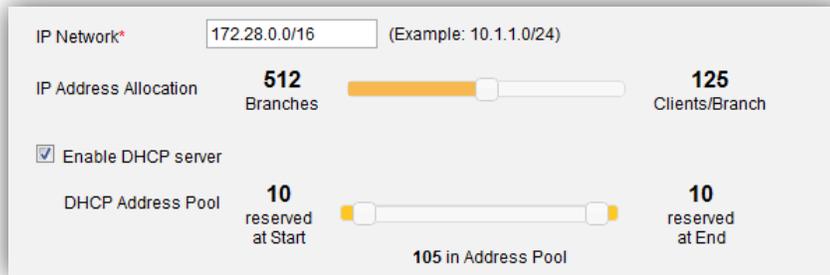
IP Network: Enter the parent IP address scope here. The parent scope is the main scope that contains the IP address scopes of all remote sites. For example, the parent scope 10.0.0.0/16 contains the subnets 10.0.1.0/24, 10.0.2.0/24, 10.0.3.0/24, and so on to 10.0.255.0/24, inclusively.

IP Address Allocation: Use the slide control to select the best match for how many branch offices you need to configure and how many clients there are at each branch. All values are displayed as powers of two, so an exact match is unlikely; however, select the maximum number of foreseeable branches and be sure the number of clients per branch exceeds the maximum foreseeable number of clients at any one branch. If you cannot fit the maximum number of clients and branches within your chosen parent scope, you must increase the parent scope.

Enable DHCP server: Enabling the DHCP server on the routers removes the necessity to have additional hardware at the remote sites provide the service. When you select Enable DHCP server, additional configuration items appear. Enter the following information, and then continue with the subnetwork configuration:

DHCP Address Pool: By default, no IP addresses are reserved. There are two slide controls to reserve IP addresses within the pool. Use the controls to select where you want your DHCP pool of addresses to begin and end. The left slide control reserves addresses at the start of the pool. The right slide control reserves addresses at the end of the pool. Below the slide control is the total number of remaining unreserved addresses in the pool.

For example, if the network configured in the illustration below, each subnet reserves ten address at the start of the pool and ten addresses at the end.



For the first subnet (172.28.0.0 – 172.28.0.127):

IP Address	Description
172.28.0.0	Network name; not used by devices.
172.28.0.1	Reserved for router; not available to client devices.
172.28.0.2 – 172.28.0.11	First ten addresses. The position of the left DHCP Address Pool slider indicates that these addresses are reserved. The DHCP service does not assign these addresses to client devices.
172.28.0.12 – 172.28.0.126	DHCP pool of addresses. The DHCP service assigns these addresses to client devices. There are 105 addresses in this pool, as noted below the DHCP Address Pool slider control.
172.28.0.127	Broadcast address; not used by devices.

Lease Time: Enter the DHCP address lease time in seconds. By default the server leases addresses for 86,400 seconds (one day). You can set the lease time from 60 seconds to 86,400,000 seconds (1000 days). Do not include commas when entering lease time values.

NTP Server IP: Enter the IP address of the NTP (Network Time Protocol) server with which you want the clients to synchronize their system clocks.

Domain Name: Enter your network domain name.

Custom Options: In this section you can enter standard (1 – 224), Aerohive (225 and 226), and custom (227 – 254) DHCP options. You can find information on using the Aerohive-specific options in the HiveManager Help system and information on specific standard DHCP options in [RFC 2132, "DHCP Options and BOOTP Vendor Extensions"](#).

Reserve subnetwork for devices by using classification rules: Select this option if you want to assign this subnet to specific HiveAPs. For example, you can set Tag1 to "Corporate" and HiveManager will apply this subnet to HiveAPs that are configured with Tag1 also set to "Corporate". HiveAPs with a different Tag1 values are assigned a different subnet.

Reserve IP addresses for devices by using classification rules: Select this option if you want to reserve a specific IP address within the subnet for a specific device. You can specify the device to receive the IP address by the device map name, HiveAP name, or by using classifier tags.

For more information regarding classifier tags, see the Help system at Configuration > Advanced Configuration > Network Objects > IP Objects/Host Names.

Step 2: Configuring a User Profile

User profiles contain settings for the levels of service and security you want to apply to users. For the configured network object to go into effect, you must select it within the user profile, save the configuration, and then upload the new configurations to the routers and access points.

To configure a user profile, click **Configuration > Show Nav > User Profiles > New**, enter the following, and then click **Save**:

Name: Enter a name for the profile. You select this profile name when configuring SSIDs and router LAN ports.

Attribute Number: The attribute number provides a means for applying returned RADIUS attributes to specific user profiles. If you use 802.1X/EAP authentication, enter a unique attribute here, otherwise leave the default value.

Network or VLAN-only Assignment: Select the network object that you just created from the drop-down list.

Description: Enter an optional description for the user profile.

Optional Settings: You can set GRE tunnels, firewalls, QoS, and so on in this section. These settings do not affect the dynamic IP address assignment. For information about them, see the HiveManager Help system.

Step 3: Applying a User Profile to SSIDs and Router LAN Ports

You can apply a user profile either to an SSID or a router LAN port. By doing so, you can assign the network settings that the user profile references to users connecting through either an SSID or LAN port.

Applying a user profile to an SSID enforces the user profile settings on any client that connects to that SSID. In past versions of HiveOS, this is the normal application of user profiles.

Applying a user profile to a specific LAN port on an Aerohive router has a similar effect, but instead of affecting only the relevant SSID, the user profile that you apply to a port affects the clients connecting through that port.

You can currently only apply one user profile to the LAN ports. In future releases, HiveOS will support the ability to apply different user profiles to different LAN ports in the same way that you can apply different user profiles to different SSIDs.

Applying a User Profile to an SSID

This section assumes that you have already created and applied an SSID to the network policy.

To apply a user profile to an SSID, click **Configuration**, select a network policy, and then click **OK** or click **Configure Interface & User Access**. In the *SSIDs* section, click the **Add/Remove** link in the User Profile column for a particular SSID, choose the user profile you want to apply to the SSID, and then click **Save**.

Applying a User Profile to a Router LAN Port

This section assumes that you have already created a LAN configuration for the routers.

To apply a user profile to a LAN port, click **Configuration**, select a network policy, and then click **OK** or click **Configure Interface & User Access**. In the *Router LAN Ports* section, click the **Add/Remove** link in the User Profile column, choose the user profile you want to apply to the LAN ports, and then click **Save**.

Step 4: Update Routers and CVG

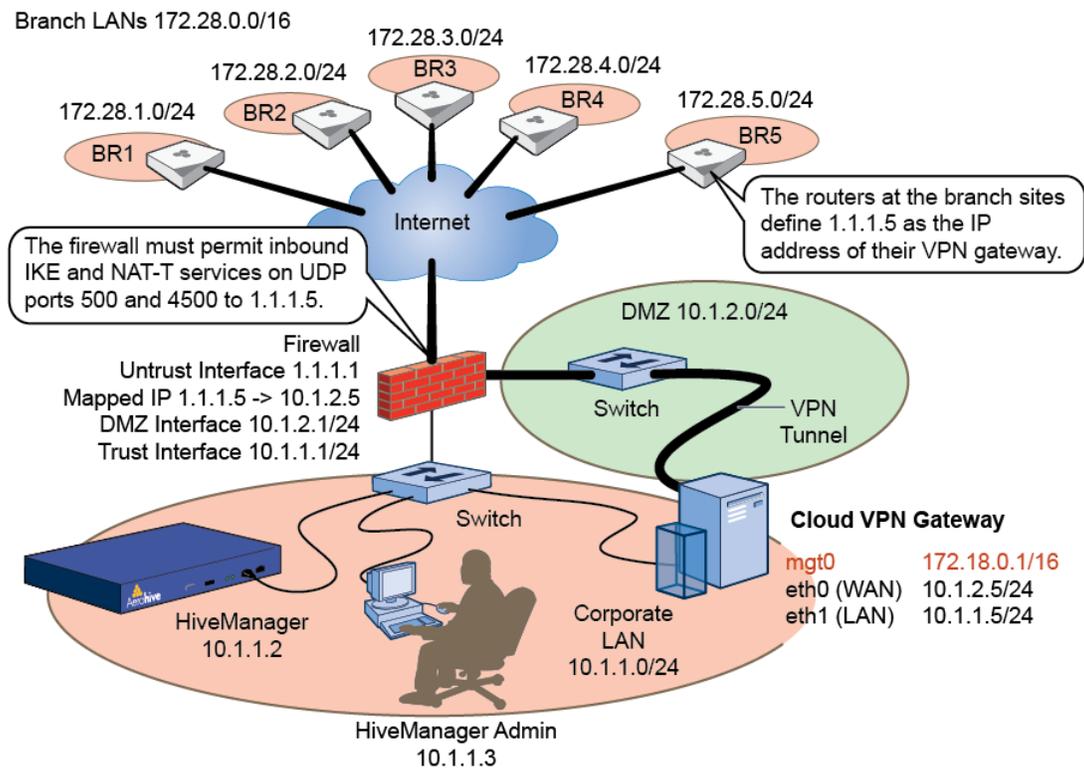
To conclude the configuration process, you must update the routers and CVG with the latest changes. To do this, click **Monitor**, select the devices you want to update, click **Update > Upload and Activate Configuration**, and then click **Upload**.

ⓘ Be sure to select the CVG for update even if you do not make explicit changes to its configuration. Updating the network object without updating the CVG configuration can cause configuration mismatches that prevent proper communication and routing.

When you complete the update, users can connect to the network, and the router automatically applies the user profile, which contains the appropriate network settings. Because the user profile is present on both the SSID and the router LAN ports, the router applies the correct network settings dynamically, whether user connects by wireless or wired LAN ports.

IPsec VPNs

Aerohive has significantly simplified the creation of IPsec VPN tunnels from routers at remote sites and a CVG (Cloud VPN Gateway) at a central corporate site. By using default configuration settings for the tunnel parameters, you merely identify the public-facing address of the WAN interface of the CVG in the configuration for the routers, and the routers build tunnels to the CVG after they receive the settings and again after each reboot. A single CVG can support up to 1000 VPN tunnels.



To configure and deploy VPN services:

1. Deploy and configure a CVG and routers as described in "Setting up a Cloud VPN Gateway and a Branch Router".
2. When you reach the point for adding VPN services to a network policy, click **Choose** for Layer 3 IPsec VPN, click **New** in the *Choose VPN Profile* dialog box, enter the following in the *New VPN Service* panel that appears, and then click **Save**:

Profile Name: Enter a name for the VPN services profile that you can reference in the network policy.

Description: Enter a useful note about the VPN profile for future reference.

Layer 3 IPsec VPN: (select)

A Layer 3 IPsec VPN is a tunnel between a router and a CVG. The router does a route lookup to determine whether to send traffic from hosts on its network to hosts on the network behind the CVG or to hosts on another site similarly connected to the CVG through a tunnel. A Layer 2 IPsec VPN creates tunnels between HiveAPs functioning as VPN clients and one or two HiveAPs functioning as VPN servers and is applied to traffic based on user profiles.

In the *VPN Gateway Settings* section, enter the following, and then click **Apply**:

Choose a previously defined CVG from the VPN Gateway drop-down list and enter the IP address that the routers can use to reach the WAN interface of the CVG. For example, the firewall protecting the corporate site might have a MIP (mapped IP) address on its Untrust interface that maps incoming IKE and NAT-T traffic to the WAN IP address on the CVG. In this case, enter the MIP address as the external IP address.

Define the default tunneling behavior by selecting one of the following two options:

Route only internal traffic through the VPN tunnel: Choose this option if you want to route traffic from branch sites destined for the corporate LAN through the VPN tunnel while routing all traffic bound for external sites to the Internet.

or

Route all traffic through the VPN tunnel: Choose this option to route all traffic from branch sites through the tunnel regardless of their destinations.

Enter the following to apply exceptions to the default tunneling behavior for specific user profiles:

User Profile: To route traffic for a specific user profile differently from the default tunneling behavior, choose a previously defined user profile, choose one of the following behaviors to apply, and then click **Apply**:

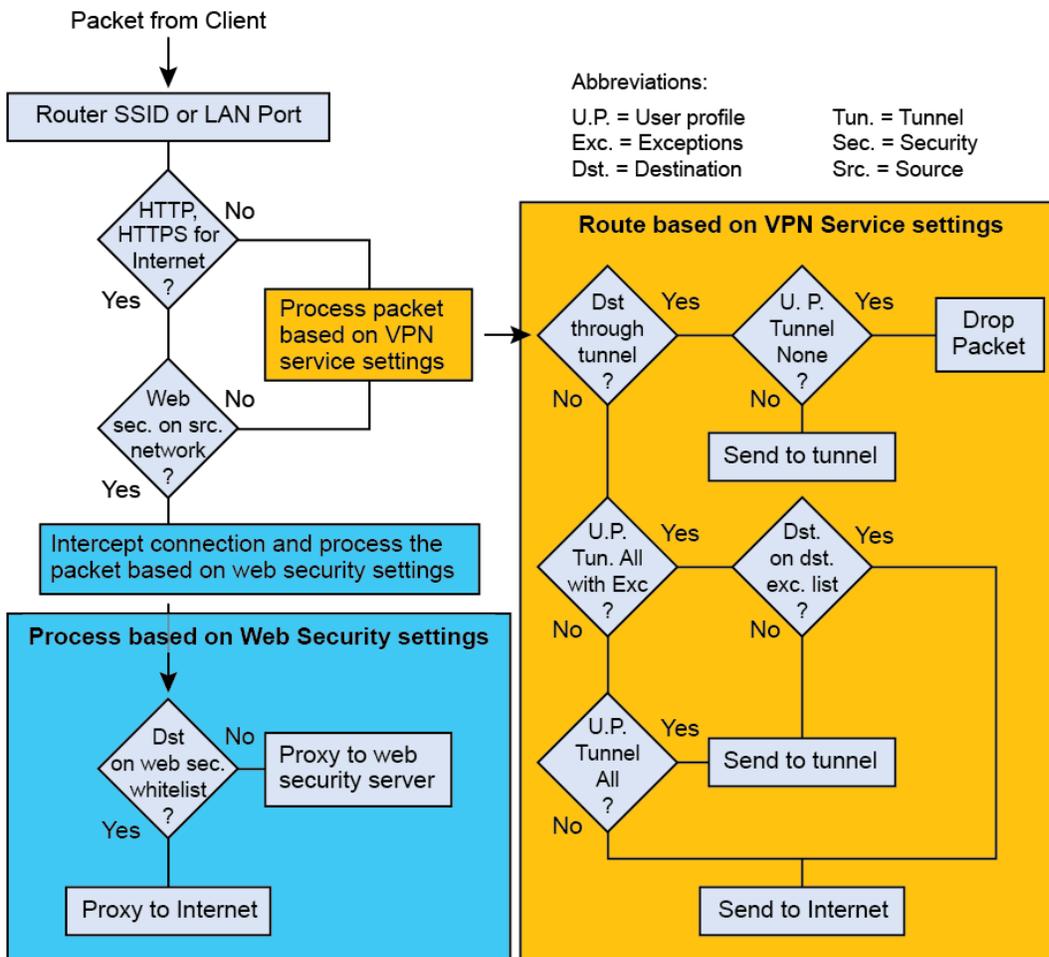
Tunnel None: Choose this option to drop any traffic from the specified user profile that would otherwise be routed through the VPN tunnel but forward all traffic routed to and from the Internet without tunneling.

Tunnel All: Choose this option to route all traffic from the specified user profile through the VPN tunnel.

Tunnel All with Exceptions: Choose this option to route all traffic from the specified user profile through the tunnel except those in the tunnel exception destination list.

Tunnel Exception Destination List: If you define the behavior for a user profile as **Tunnel All with Exceptions**, choose a list of destinations as the tunnel exceptions. The router will then tunnel all traffic except to those destinations in the list. If you do not see a list that you want to use, click the **New** icon (+), and create one.

IPsec VPN Tunnels and Web Security: If web security is enabled on a network object, it takes precedence over the tunneling behavior defined here for HTTP and HTTPS traffic bound for the Internet. Web security requires routers to redirect HTTP and HTTPS traffic to a hosted Websense or Barracuda web security server instead of routing it either to the site directly or through the tunnel. To understand how web security affects the routing of traffic through VPN tunnels, see the decision flow diagram shown below.



Based on the decision it reaches, the router takes one of the following actions:

- Proxy the packet to its destination on the Internet
- Proxy the packet to a web security server
- Drop the packet
- Tunnel the packet
- Send the packet to its destination on the Internet without proxying it

In the *Optional Settings* sections, you can modify various VPN IPsec tunnel parameters.

In the *IPsec VPN Certificate Authority Settings* section, you can change the CA and server certificates and the private key for the server certificate.

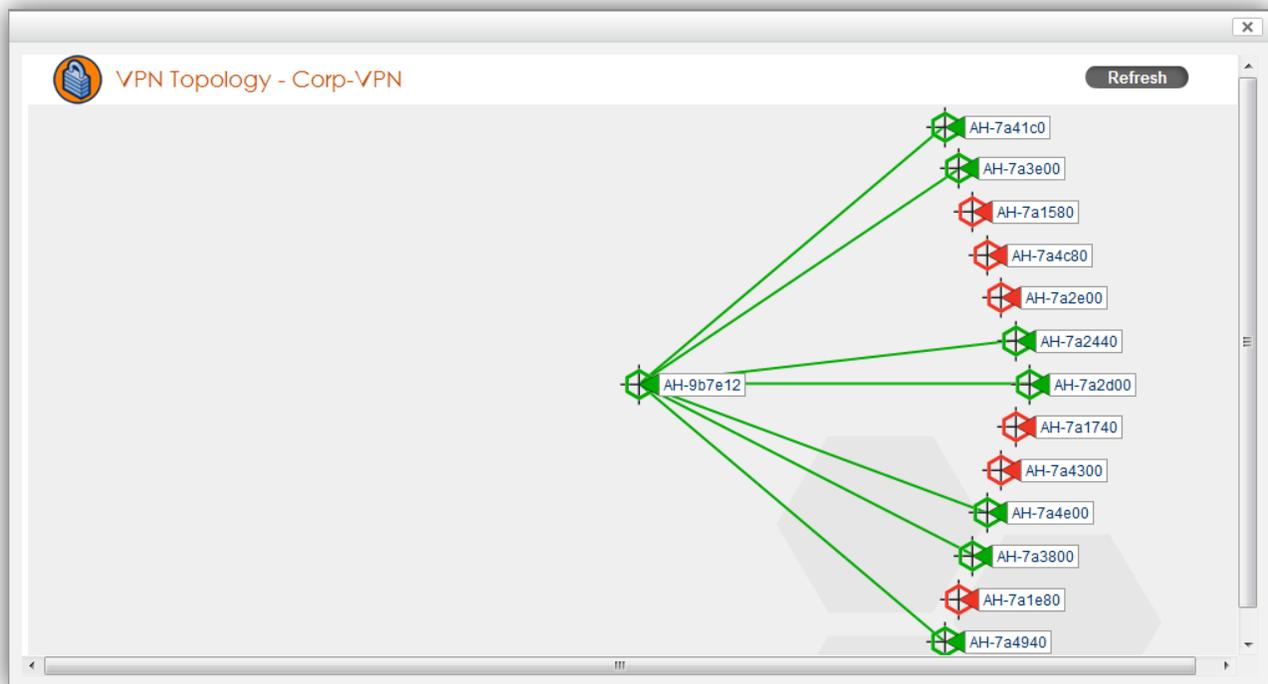
In the *Server - Client Credentials* section, HiveManager lists the randomly generated text strings that it can allocate to routers to use as passwords when identifying themselves to the CVG. When configuring the VPN services profile, this section appears empty. When you reference this VPN profile in a network policy, HiveManager automatically creates a set of credentials for distribution to routers configured to use this VPN service profile.

In the *Advanced Server Options* section, you can modify the IKE phase 1 and phase 2 security options and enable IKE ID validation so that the routers can validate the IKE ID that the CVG sends them during IKE negotiations.

In the *Advanced Client Options* section, you can disable NAT-Traversal and modify the DPD (Dead Peer Detection) settings.

3. After saving the VPN service profile, select its name in the *Choose VPN Profile* dialog box, and then click **OK**.
4. Click **Continue** at the top of the *Configure Interface & User Access* panel to save the application of the VPN profile to the network policy and advance to the *Configure & Update Devices* panel.
5. Select the CVG and all the routers that you want to build tunnels to the CVG, and click **Upload**.

To check that the routers have successfully formed tunnels to the CVG, you can see their tunnel status on the VPN topology view. There is a link to it in the *Configure Interface & User Access* panel in the network policy and another in the *System Details* section on the CVG details page that you can view by clicking **Monitor > Devices > VPN Gateways > Display Device Status Information > cvg_name**. For example, here is the VPN topology showing several routers with tunnels to a CVG. The green icons and lines indicate that their tunnels are currently up. The red icons indicate that the tunnels are currently down. (If there are redundant VPN gateways, the router icons can be orange to indicate that they are configured with redundant VPN gateways and currently have an active tunnel to one of them.)



Network Firewall

This release introduces support for network firewall policies. A network firewall policy is a set of up to 32 rules that a router uses to permit or deny traffic to and from the networks it controls. You can configure network firewall policies for BR100 routers or AP330 or AP350 devices acting as routers.

A network firewall policy rule consists of five components: three inputs (source, destination, and service) and two outputs (action and logging). For a router to perform the action specified in a rule, traffic must match all three inputs.

Source: The source of traffic this policy controls. This can be an IP network, a range of IP addresses, a network object, a user profile, a VPN, a wildcard address, or “any”.

Destination: The destination for traffic this policy controls. This can be an IP network, a range of IP addresses, a network object, a VPN, a wildcard address, a host name, or “any”.

ⓘ The use of host names for the destination is not currently supported in this release.

Service: Specify the service to which you want to apply a firewall policy, such as BGP, DHCP, DNS, FTP, HTTP, and HTTPS. The GUI provides a drop-down list of existing services, and you can add new services or modify existing services.

Action: You specify whether to permit or deny the traffic this policy controls. The default setting is Permit.

Logging: You can enable or disable logging for a policy rule. When you enable logging, the router generates a log entry whenever the policy rule applies to a new session. Note that when the rule permits the first packet in a session, subsequent packets for that session do not trigger additional log entries. For example, a new TCP connection that matches a policy rule with Permit as its action and Enable as its Logging option triggers a log entry for only the first packet of the TCP connection.

Configuring a Network Firewall Policy

The network firewall policy configuration page is located at Policy Configuration > Advanced Configuration > Security Policies > Network Firewall Policies.

To configure a network firewall policy, click **Configuration**, choose an existing network policy such as QuickStart-Wireless-Routing, and then click **OK**.

1. In the *Configure Interface & User Access* panel, click **Choose** for Router Firewall, and then click **New**.
2. In the *New Network Firewall Policy* dialog box, enter the following, and then click **Save**:

Policy Name: Enter a name for the firewall policy.

Description: Enter a useful description or note about the policy for future reference.

In the Policy Rules section, define a rule for your policy, and then click **Apply**:

Source: Choose one of the following types of objects to define the source of the traffic to which you want to apply the rule from the drop-down list. Then choose an existing object of that type or, if you do not see a particular object that you want to use, click the **New** icon (+) and create it:

[-any-]: This is the default source object. It is the equivalent of 0.0.0.0/0 and applies the rule to traffic from all IP addresses.

IP Network: Choose this to apply the rule to traffic from a particular subnet, and then choose an existing subnet (such as 10.0.0.0/255.0.0.0) from the drop-down list or create a new one.

IP Range: Choose this to apply the rule to traffic from a range of IP addresses, and then choose an existing range (such as 10.1.1.1-10.1.1.10) or create a new one.

Network Object: Choose this to apply the rule to traffic from a network object, and then choose an existing network object (such as QS-172.28.0.0/16) from the drop-down list or create a new one.

User Profile: Choose this to apply the rule to traffic from users belonging to a particular user profile, and then choose an existing user profile (such as QS-User-Profile) or create a new one.

VPN: Choose this to apply the rule to traffic coming from the VPN tunnel.

Wildcard: Choose this to apply the rule to traffic from any IP address to which the specified wildcard address applies. For example, if the wildcard is 172.28.x.1 (IP address = 172.28.1.1; wildcard = 255.255.0.255), then the rule would apply to traffic from 172.28.0.1, 172.28.1.1, 172.28.2.1, ... 172.28.254.1.

Destination: Choose one of the following types of objects to define the destination of the traffic to which you want to apply the rule from the drop-down list. Then choose an existing object of that type or, if you do not see a particular object that you want to use, click the **New** icon (+) and create it:

[-any-]: This is the default destination object. It is the equivalent of 0.0.0.0/0 and applies the rule to traffic destined for all IP addresses.

IP Network: Choose this to apply the rule to traffic to a particular subnet, and then choose an existing subnet (such as 192.168.0.0/255.255.0.0) from the drop-down list or create a new one.

IP Range: Choose this to apply the rule to traffic destined for a range of IP addresses, and then choose an existing range (such as 10.2.2.1-10.2.2.10) or create a new one.

Network Object: Choose this to apply the rule to traffic to a particular network object, and then choose an existing network object (such as QS-172.28.0.0/16) from the drop-down list or create a new one.

VPN: Choose this to apply the rule to traffic going to the VPN tunnel.

Wildcard: Choose this to apply the rule to traffic to any IP address to which the specified wildcard address applies. For example, if the wildcard is 172.x.x.1 (IP address = 172.1.1.1; wildcard = 255.0.0.255), then the rule would apply to traffic from 172.0.0.1, 172.1.0.1, 172.2.0.1, ... 172.254.254.1.

Host Name: Choose this to apply the rule to traffic destined for a particular domain name (host name), and then choose an existing host name (such as ntp1.aerohive.com) or create a new one.

Service: Choose the type of service to which you want to apply the rule. If you do not see the service that you want, click the **New** (+) icon to the right of the drop-down field to create a new one.

Action: Choose either **Permit** or **Deny** to define what the firewall does with traffic matching the source, destination, and service parameters.

Logging: Choose either **Enable** to log the start of each new permitted session or to log a denied packet, or **Disable** to refrain from logging traffic for this rule.

Disable: Select to disable the application of the rule. This is useful for troubleshooting connection issues or for temporarily delaying or suspending the rule for other purposes. Clear the check box to enable the rule.

To add another rule (you can add up to 32), click **New**, define the parameters as described above, and then click **Apply**. Each rule you add appears in the table below the previous rule. The router evaluates active firewall policy rules from top to bottom for a match. When it finds one, it either permits or denies the traffic and optionally logs the event. As you can see, the position of a rule within a policy is very important. If more than one rule in a policy matches the source or destination, the router applies the rule that is higher in the list because that is the first match it finds. To move a rule within the list, simply drag it to a new position.

ⓘ When rearranging rules, keep in mind that because the router checks rules in order from the top of the list until it finds a match, avoid placing a rule in a position that occludes (or "shadows") another rule lower than it in the list.

After defining and ordering the rules in your policy, the final rule to set is the default rule. It determines what to do to all traffic to which the other rules do not apply. You can select either **Permit all** or **Deny all**. Finally, like the other rules, you can enable or disable logging for the default rule.

3. To add the firewall policy to the network policy, select it from the Choose Firewall list, and then click **OK**. The firewall policy name now appears under Router Firewall in the *Configure Interface & User Access* panel.
4. Click **Save** at the top right of the panel to save the firewall policy as part of the network policy.
5. In the *Configure & Update Devices* panel, select the routers to which you want to apply the firewall policy, and then click **Upload**.

To configure dynamic route updates on the CVG:

1. Click **Monitor > VPN Gateways**, select the CVG, and then click **Modify**.
2. Select **Enable dynamic routing** to expand the section, enter the following, and then click **Save**:

Choose **OSPF** or **RIPv2**.

Route Advertisement: Select **LAN** if you want the CVG to advertise routes about the branch sites through its LAN interface to the corporate routers. (The routers periodically poll the CVG to learn routes at the corporate site.) By default, the LAN check box is selected.

Select **WAN** if you want the CVG to advertise routes through the WAN interface to external devices on the network or Internet. (By default, the WAN check box is cleared.)

Use MD5 authentication: Select to force the CVG to authenticate mutually with neighboring peer routers. You can use mutual authentication to restrict route updates between specified peers and prevent the malicious injection of false routes by attackers.

Password: Enter the password that the peer routers use to authenticate one another.

Area: Enter the logical area in which your CVG operates. Areas are logical groups of routers that share link state and route information. If you do not group your peer routers into areas, you can leave this field blank.

Router ID: Enter an explicit router ID in dotted decimal format (w.x.y.z). A router ID is used by a group of routers during the election of a DR (designated router) and a BDR (backup designated router), which take on central roles in maintaining peer information. If you do not specify a router ID, then the CVG uses its highest IP address as its router ID.

⁽ⁱ⁾ You can find more information on peer router authentication, areas, and using router IDs in [RFC 2328, "OSPF Version 2"](#).

Wireless USB Modem with WAN Failover

The BR100 and the AP330 and AP350 (when configured as a router) can use a wireless USB modem for a WAN connection. The typical use of the USB modem is to act as a backup to the ETH0/WAN interface; however, for locations where an Ethernet connection to the WAN is not possible, you can use the USB modem as the primary (and only) interface to the WAN.

⁽ⁱ⁾ When using a wireless USB modem on an AP330 or AP350, you must connect it to an AC power source instead of using PoE to power the device. The BR100 does not support PoE and must always use an AC power source.

In this release, Aerohive supports the following modems:

- AT&T Momentum (Sierra Wireless Aircard 313U) to connect to the 3G wireless network
- AT&T Shockwave (Sierra Wireless USBConnect 308) to connect to the 3G wireless network
- Verizon Pantech UML290 to connect to the 4G (LTE) wireless network

⁽ⁱ⁾ The international counterparts for the Momentum and Shockwave modems (the Sierra Wireless Aircard 310U, 312U and 320U) are also usable with the router.

The dialup PPP settings (APN, dialup number, user ID, and password) for both of these modems are preconfigured on HiveManager and Aerohive devices. In fact, due to the preconfigured settings, you can use a wireless USB modem for WAN connectivity (connecting as needed by default) without the need to configure anything extra as long as the following conditions are met:

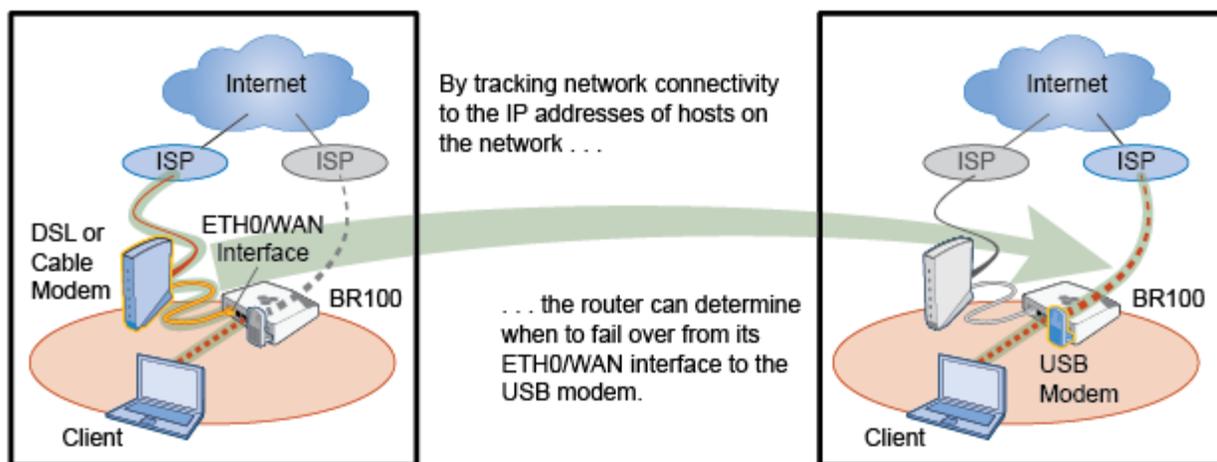
- The modem is one of the models that Aerohive supports and has been activated.
- The wireless carrier provides adequate coverage where the router is deployed.
- The network policy assigned to the Aerohive devices references a track IP group with WAN connectivity testing enabled.

Before you can use the modem with an Aerohive device, you must first have it activated. You might get this done in the store when you purchase the modem, or you might install software such as the Verizon VZAccess Manager on your computer, attach the modem to a USB port on your computer, and run the activation software yourself. In either case, try the modem first on your computer, preferably at the site where you plan on deploying the router before connecting the USB modem to the router. You can then confirm that the modem works properly and that there is adequate wireless network coverage at that location.

A WAN connectivity loss detected through IP tracking can trigger a failover. The failover from the ETH0/WAN interface to the USB modem can take anywhere from about 45 to 100 seconds for full WAN and VPN connectivity to be restored. (The range depends on the number of IP addresses being tracked and the various track IP parameters configured.) When this happens, the status LED on a BR100 changes from steady white, which indicates it has a CAPWAP connection to HiveManager through its ETH0/WAN interface, to flashing white, which indicates it is in a failover state and is using the wireless USB modem for its WAN link.

Configuring WAN Failover to the USB Modem

You can configure a router to use its Eth0 interface for its primary WAN connection and, if any issues with this connection arise, to fail over to a USB modem as its backup WAN connection.



1. Cable the WAN/ETH0 interface to a DSL or cable modem and connect one of the 3G or 4G (LTE) USB modems that Aerohive supports to the USB port.
2. In the HiveManager GUI, click **Configuration**, choose the network policy that is applied to the router, and then click **OK**.
3. In the Configure Interface & User Access panel, click **Modify** for Additional Settings, expand Service Settings, choose **QS-IP-Track-Router** from the Track IP Group for router WAN connectivity drop-down list if it is not already chosen, and then click **Save** to save the additional settings.

The QS-IP-Track-Router profile tracks the default gateway for the router and two IP addresses: 206.80.44.205 and 206.80.44.206 (the IP addresses of ntp1.aerohive.com and ntp2.aerohive.com). The track IP profile does not have any additional remedial actions enabled, so that the only action the router will take if all targets become unresponsive is to fail over to the USB modem.

ⓘ Even if remedial actions are enabled, specifying WAN connectivity testing in the track IP profile causes the router to ignore them.

4. Click **Save** to save the interface and user access configuration and advance to the *Configure & Update Devices* panel.
5. Click the host name of the router (BR100 or an AP330 or AP350 configured as a router), enter the following to configure its device settings, and then click **Save**:

Network Policy: Make sure the device is in the correct network policy

Device Type: Choose **Branch Router** from the drop-down list. If you are configuring a BR100, that is the only choice. However, if you are configuring an AP330 or AP350, you must change it from HiveAP to Branch Router.

ⓘ When you change the device type of an AP330 or AP350, you must upload a complete configuration (not a delta configuration) the next time you push settings to the HiveAP from HiveManager.

In the *Port Settings* section, make sure that the Eth0, Eth1-4, and USB ports have the following settings:

Port	Role (read-only)	Admin State	Transmission Type	Speed
Eth0	WAN-Primary	Up	Auto	Auto
Eth1-4*	LAN	Up	Auto	Auto
USB	WAN-Backup	Up	Auto	Auto

* On an AP330 or AP350, the ETH1 port acts as the LAN interface. On the BR100, four ports act as LAN interfaces.

In the *USB Modem Settings* section, select either **Connect as Needed** (the default) or **Always Connected**. When you select the first option, the router initiates a connection from its USB modem to its ISP only when there is a loss of network connectivity on its ETH0/WAN interface. When you select the second option, the router is always connected through its USB modem to its ISP in anticipation of a failover. An advantage to connecting only when needed is that you can minimize the number of minutes that the router is on the 4G or 3G network as well as the number of data bytes it transmits. An advantage to always being connected is that the failover occurs faster because the dialup PPP connection is already established.

6. Select the router, and then click **Settings** to open the *HiveAP Upload Options* dialog box. If you are converting the role of an AP330 or AP350 from HiveAP to router, select **Complete Upload, Activate after 5 seconds, and Upload and activate configuration**. (Because you are not adding a captive web portal, RADIUS or VPN services, or user accounts to the device, you can clear the other three types of objects to upload.)

If you are updating a BR100, you can upload a complete or delta configuration. If you upload a complete configuration, you must reboot the device to activate the new settings. If you upload a delta configuration, rebooting the device is unnecessary.

ⓘ If you push a complete configuration and reboot the router, wait until it regains a CAPWAP connection to HiveManager before continuing.

7. To test the failover and network connectivity through the USB modem, disconnect the Ethernet cable from the ETH0/WAN interface, and then do the following:
 - After disconnecting the cable, wait until the status LED begins flashing white.
 - Check the Monitor > Devices > Branch Routers page to see if the device has a CAPWAP connection to HiveManager. It usually takes up to five minutes for the device to re-establish a CAPWAP connection with HiveManager.
 - From a client connected to the router, ping **206.80.44.205** to see it can connect to devices on the Internet.
 - From the same client, ping **ntp1.aerohive.com** to see if can resolve DNS.
8. To return the WAN link to the ETH0/WAN interface, simply reconnect the Ethernet cable. The device fails back shortly after the ETH0/WAN interface regains network connectivity as determined by the track IP settings. Then after a few minutes, the device reforms its CAPWAP connection with HiveManager.

Configuring the USB Modem as the Only WAN Interface

For deploying a router at a site that does not have an Ethernet link to the WAN, you can use the USB modem as the primary WAN interface. The configuration steps are similar to those for defining the USB modem as a WAN backup, including the use of tracked IP addresses so that an IP tracking failover can activate the USB modem. Therefore, you can follow the instructions in the previous section. The only differences are that you do not connect an Ethernet cable to the ETH0/WAN interface, and you might also want to change the admin state for the ETH0/WAN interface from **Up** to **Down**.

DNS Proxy

The Domain Name System (DNS) is a naming system that translates human-friendly domain names into IP addresses. The BR100 provides proxy DNS services for every local network under its control. The proxy service transparently routes DNS requests and responses to and from internal or external DNS servers.

This release supports two modes of DNS proxy service; non-split and split. The default mode is split.

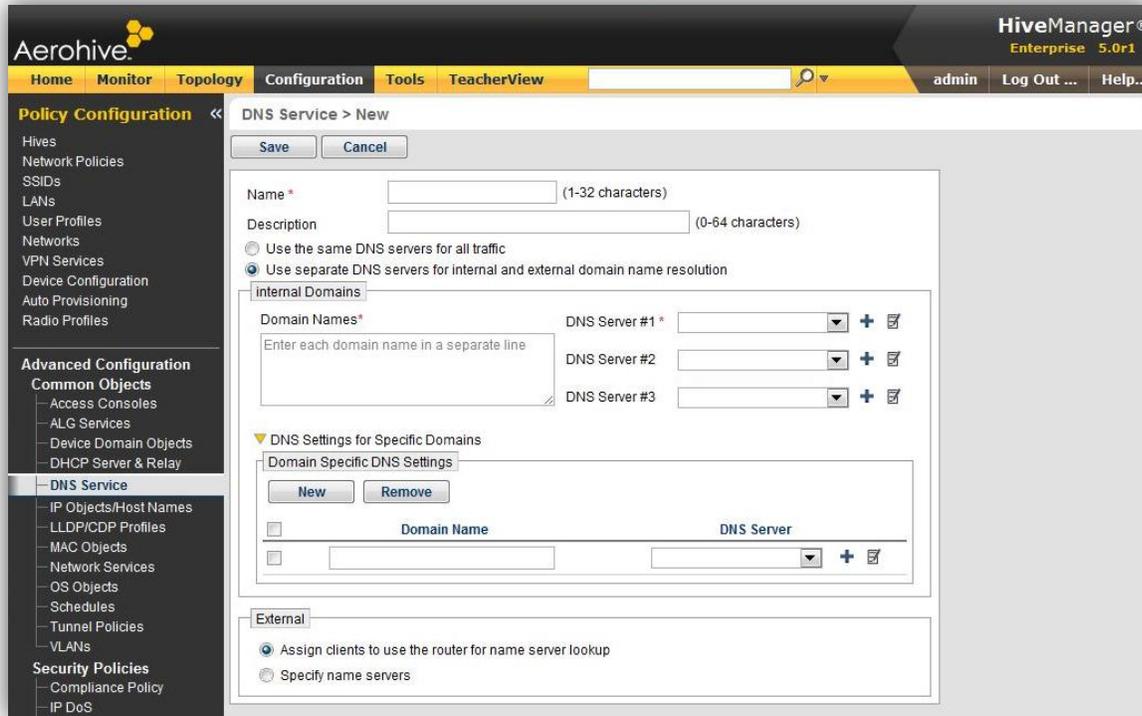
In non-split mode, the router proxies all name resolution requests to the same set of DNS servers, regardless of the name being resolved. The destination servers may reside either inside the corporate network (and accessed through the VPN tunnel) or outside the enterprise network (i.e. on the Internet). This mode is useful in the following cases:

- There are no private domain names on the corporate network, so the router proxies all requests to external DNS servers.
- There are so many private names on the corporate network that it is not feasible to list them all in a split-DNS configuration. Therefore, the router proxies to internal DNS servers.
- You want your corporate DNS server to respond to all name resolution requests proxied from routers through VPN tunnels.

In split mode, the router proxies name resolution requests for specified internal domains to internal DNS servers and proxies all other requests to external DNS servers. Split mode DNS proxy service enables a remote office to use a split-DNS scheme that may be in place on a corporate network, keeping private hostnames private. Split mode is useful in the following cases:

- You want to prevent exposure of private internal domain names to the Internet.
- You want to reduce VPN tunnel traffic by eliminating DNS lookups for domain names that external DNS servers can resolve, such as **www.aerohive.com**.

In this release, DNS service configuration appears under Policy Configuration > Advanced Configuration > Common Objects > DNS Service. From this window, you can view configured DNS services.



To configure DNS services, enter the following information, and then click **Save**:

Name: Enter a name for the DNS services profile.

Description: Enter a useful description about the DNS services profile for future reference.

Use the same DNS servers for all traffic: This is non-split mode. In this mode, the router sends all name resolution requests to the specified DNS servers, regardless of the name being resolved. You can specify up to three DNS name servers, which may be either internal DNS servers that are accessed through a VPN tunnel or DNS servers on the Internet. You can also choose **Local DNS** to make the DNS proxy use the same DNS servers that are configured for the router (typically the DNS servers the router learns through DHCP.)

Use separate DNS servers for internal and external domain name resolution: This is split-mode. The router sends DNS requests for names matching the configured internal domains to specified internal DNS servers, and sends all other requests through DHCP to external DNS servers.

For split-mode, in the *Internal Domains* panel, enter the domain names that the internal DNS servers will use for comparison and name resolution. You can configure up to 32 internal domain names for each network your BR100 supports. It is important to understand that domain names are based on patterns. The router DNS proxy uses an implicit wildcard matching scheme that matches requests such as "pc1.hr.footronix.com and my-footronix.com to the pattern footronix.com, and proxies both requests to an internal DNS server.

(ⓘ) Each name must be entered on a separate line.

Enter the IP addresses of up to three internal DNS servers. You can also restrict a domain name to a single DNS server in the *DNS Settings for Specific Domains* panel.

DNS Configuration Example

The following example describes a split-mode DNS configuration that uses a specific DNS server for specific domains.

The Footronix corporate network has internal DNS servers (IP addresses 1.2.3.4 and 1.2.3.5) that resolve private names such as files.footronix.com and hr.footronix.com for clients on the internal corporate network. These names will not be resolved for computers outside the corporate network (on the Internet). Internal domain names such as test1.qa-lab.footronix.com are resolved by the DNS server in the Footronix QA lab (IP address 5.6.7.8).

The split DNS proxy configuration for a router at a branch site with a VPN tunnel to the Footronix corporate network looks like this:

The screenshot shows the 'DNS Service > New' configuration page in the Aerohive HiveManager Enterprise 5.0r1 interface. The page is divided into several sections:

- Internal Domains:**
 - Domain Names*: A text input field with the instruction "Enter each domain name in a separate line".
 - DNS Server #1*: 1.2.3.4
 - DNS Server #2: 1.2.3.5
 - DNS Server #3: (empty)
- DNS Settings for Specific Domains:**
 - Domain Specific DNS Settings: A table with columns for Domain Name and DNS Server. One entry is visible: qa-lab.footronix.com mapped to 5.6.7.8.
- External:**
 - Assign clients to use the router for name server lookup:
 - Specify name servers:

This split-DNS configuration identifies two internal DNS servers (1.2.3.4 and 1.2.3.5) that will be used to resolve all requests for names ending with footronix.com. The domain-specific DNS setting for the Footronix QA lab specifies that all DNS requests for names ending with qa-lab.footronix.com will be sent to the server at 5.6.7.8. When you select **Assign clients to use the router for name server lookup**, clients send all external name requests to the router, which in turn proxies them to the DNS servers that the ISP provides for the remote office.

Web Filtering

You can apply web security proxy settings to a network object so that the router forwards web traffic from any user accessing the Internet through that network through a third party web filtering service—either Websense or Barracuda. Using a third party web security proxy in this way removes much of the administrative burden associated with the controlled restriction of Internet access, such as version maintenance, content categorization, and list updates.

Controlling access in this way also reduces exposure to content that can transmit malicious software, or that you must restrict for legal reasons or for reasons of propriety.

When the router sends user web traffic through a Websense or Barracuda web filtering service, the router conveys the user identity, when it is available. In this way, the web filtering service processes traffic from a user authenticated to the router using a policy configured for that user in the Websense or Barracuda administration portal. When the user identity is not available to the router (e.g., the client device is connected to a LAN port with no authentication required for access), the web filtering service applies a default policy to user web traffic.

Obtaining a Websense 30-Day Trial

Aerohive and Websense have partnered to allow you to sign up for a trial version of the service through the Websense website at www.websense.com/aerohive. When you configure HiveManager to use Websense, a link to the Websense website is available to you to obtain the 30-day trial.

ⓘ The Websense 30-day trial link is not currently live. At this time you are directed to contact Aerohive to participate in the early adopter program. When the page becomes live, you can simply fill out and submit a short form, and then receive an activation code in an email. In a later email, your account ID and security key arrive. The security key is also referred to as the encryption key in some literature because it is used to encrypt traffic between your router and the Websense proxy server.

Configuring Web Proxy Security

To use a web security proxy service, you must complete two tasks:

1. Configure HiveManager web security proxy service
2. Configure the network object to use the web security service

Step 1: Configure a web security proxy service

The configuration process for web security varies slightly depending on whether you use Websense or Barracuda as your web security provider. To configure Websense as your provider, click **Home > Administration > HiveManager Services**, select **Websense Server Settings** to expand the section, enter the following, and then click **Update**:

Service Host: By default, this text box contains the correct proxy server host name. You do not need to change this setting unless you are using Websense hybrid service (Websense cloud proxy and Websense appliance together), in which case contact Aerohive Support for configuration information.

Account ID: Enter the account ID provided by Websense.

Security Key: Enter the security key provided by Websense. HiveManager uses this key to encrypt traffic between the router and Websense proxy server. You can clear **Obscure Security Key** to view the key in plain text.

(¶) The security key is also referred to as the encryption key in some literature because it is used to encrypt traffic between your router and the Websense proxy server.

Default Domain: Enter your domain (e.g., aerohive.com). This field is optional. When the authenticated username is available to the router, the router combines the username with the domain in NTLM format (i.e., “domain\username”) in the case that the default domain is configured here, or in the case that the Windows domain is available in the authenticated identity (as part of authenticating the user to an Active Directory server).

Web Security Whitelist: Choose the whitelist object you want to use with the Websense service. The router does not route HTTP or HTTPS requests destined for domains contained in the whitelist to the proxy server.

A QS-Websense-Whitelist containing a short list of common trusted domains is the default selection. To create a new custom whitelist, click the **New (+)** icon.

To configure Barracuda as your provider, click **Home > Administration > HiveManager Services**, select **Barracuda Server Settings** to expand the section, enter the following, and then click **Update**:

Authentication Key: Enter the desired key from the Barracuda FLEX portal. You can find the authentication key by logging into the Barracuda FLEX portal at <https://webfiltering.barracudanetworks.com> and clicking **Configuration > Key Management**. Copy the key string from the Barracuda FLEX portal Key Details panel and paste it into the Authentication Key field in HiveManager. You can clear **Obscure Authentication Key** to view the key in plain text.

Service Host: By default, this text box contains the correct proxy server host name. You do not need to change this setting.

Service Port: Enter the preferred TCP port on which proxied HTTP and HTTPS requests occur. The default TCP port is 8080.

Windows Domain: Enter your domain (e.g., aerohive.com). Barracuda sends this information to the destination web server in the HTTP header. This field is optional and does not affect user policy selection by the Barracuda web service.

Default User Name: Enter a default user name that the Hiver Router provides to the Barracuda proxy server in the event that no authenticated user name is available on the router for a given web request. If no default user name is included here, or if Barracuda does not recognize the user name entered, then the Barracuda servers apply policies configured for the *Everyone* group.

Web Security Whitelist: Choose the whitelist object you want to use with the Barracuda service. The router does not route HTTP or HTTPS requests destined for domains contained in the whitelist to the proxy server.

A QS-Barracuda-Whitelist containing a short list of common trusted domains is the default selection. You can create a new custom whitelist by clicking the **New (+)** icon.

Step 2: Configure a network object to use web security

To configure the network object to use Websense or Barracuda web security proxy servers, you must have a network policy in place. This example assumes that you have no network policy currently deployed, and includes steps to create a network policy using the built-in QuickStart-Wireless-Routing network policy.

To create a network policy, click **Configuration** to display the *Network Configuration* page, choose **QuickStart-Wireless-Routing** from the list box, and then click **OK**.

By beginning with the QuickStart-Wireless-Routing policy, HiveManager automatically creates SSID, LAN, user profile, and network objects for you, each of which you can edit.

To configure the network object to use web security, click the link under the **Network (VLAN)** column in the **SSIDs** section to display the *Edit Network* popup window, choose your web security provider from the **Web Security** drop-down list, select whether you want to permit or deny all traffic if connectivity is lost, and then click **Save**.

To complete the configuration, you must repeat this process for the LAN ports. To do this, click the link under the **Network (VLAN)** column in the **Router LAN Ports** section to display the *Edit Network* popup window, choose your web security provider from the **Web Security** drop-down list, select whether you want to permit or deny all traffic if connectivity is lost, and then click **Save**.

Tunnels and Web Security

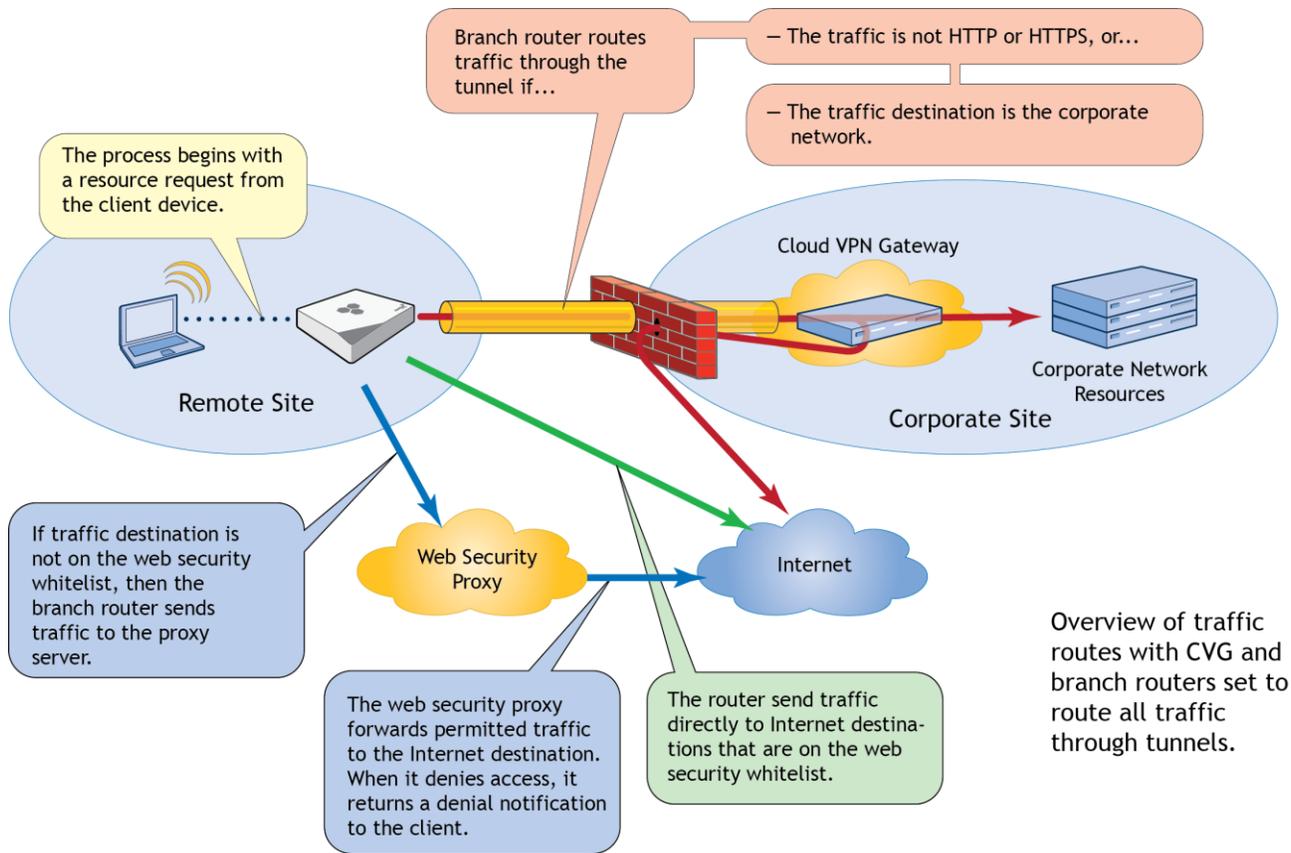
Aerohive routers are able to mitigate tunnel traffic to prevent capacity problems by making decisions regarding what traffic must travel through the tunnels when the Route all traffic through the VPN tunnel ("tunnel all") feature is active. Branch routers are able to do this by using two whitelists. The VPN whitelist exempts traffic to specified domains from passing through the VPN tunnel. The web security whitelist exempts traffic to specified domains from web filtering by a web security proxy server. Working together, these two whitelists interact predictably.

You can explicitly select which destination domains to include in a VPN whitelist. Whitelisted domains are trusted domains and the system does not require traffic destined there to pass through the tunnel.

Likewise, domains that are present in the web security whitelist are trusted domains and the system does not require traffic destined there to undergo web filtering.

ⓘ When web traffic (i.e., user traffic destined to ports 80 or 443) is destined for the Internet (as opposed to a host residing on the corporate network or behind the VPN tunnel) and it originates from a subnet corresponding to a network object that has web security enabled, then the router does not apply the Tunnel All policy to the web traffic. Instead it forwards the traffic to the web security proxy or to the destination host on the Internet.

The following illustration shows how traffic flows based on whitelist configuration.



(((The relationship of web security settings on the routing of user traffic through a VPN tunnel is also covered in "IPsec VPNs".