Configuration for Cisco ASA Series

6300-CX

Configuration for Cisco ASA Series

Overview

The Accelerated 6300-CX LTE Router provides a reliable, high-speed cellular connection that is compatible with existing wireline infrastructure. While its 4G LTE speeds are capable of operating as a primary WAN uplink, the 6300-CX can also be configured as a backup. This network redundancy solution delivers the ultimate flexibility to minimize expenses when it comes time for upgrading equipment to the latest wireless standards.

Business continuity depends on the seamless integration of failover-connectivity solutions to prevent service interruptions. Now more than ever, contingency networks play a strategic role in sustaining business operations. Unplanned outages can cost companies significant time and money, frustrating employees and clients alike, which creates a negative perception that is difficult to overcome.

Cellular data (4G LTE) bypasses wireline Internet service providers (ISPs) to facilitate the best redundancy possible. Additionally, in some situations it may be a challenge to acquire access to wired circuits or an event may call for temporary online access. Accelerated Concepts extensively tests the 6300-CX LTE router to ensure its interoperability with a wide variety of security appliances, including equipment produced by Fortinet, to best accommodate enterprise networks. Pairing the Accelerated 6300-CX with a dedicated firewall offers comprehensive security and flexibility for small business, retail, government, remote sites, and branch offices.

Cisco's Adaptive Security Appliance (ASA) series is a threat-focused line of next-generation firewalls (NGFWs) designed for multilayered network protection. The latest ASA hardware is capable of integrating its proven security capabilities with Cisco's FirePOWER service that bolsters the device's readiness to defend against advanced and zero-day attacks. This next-generation intrusion prevention system (NGIPS) incorporates comprehensive access and application control, threat prevention, routing policies, and contextual network awareness all under a single security appliance, a solution that was previously achieved by pairing an ASA firewall with a separate module dedicated to FirePOWER functionality.

For additional information, please refer to Cisco's ASA 5500 Series Configuration Guide.

Interoperability Matrix

This section covers interoperability information of the hardware tested for this solution. It includes the firmware versions of both devices as well as the date of testing.

Date	ASA Firmware	ASDM Version	6300-CX Firmware
12/2016	9.6(1)	7.6(1)	16.11.142

Caveats

The delivery of wireless services varies depending on the carrier and may lead to differences in the area of coverage, type of service (3G, 4G, LTE, etc.), available bandwidth, and IP address designation (Private or Public) among other factors. The interoperability test designed for this solution guide included LTE service, maximum coverage availability, and a public IP address assigned to each device.

Using the 6300-CX as a secondary connection assumes that a WAN Ethernet cable is plugged into the port configured for the primary uplink on the ASA device. Connect the 6300-CX's backup Ethernet cable to a port available for configuration as the secondary interface and proceed to the configuration described herein. (Compatible with all ASA series firewalls.)

Accelerated 6300-CX LTE Router Setup

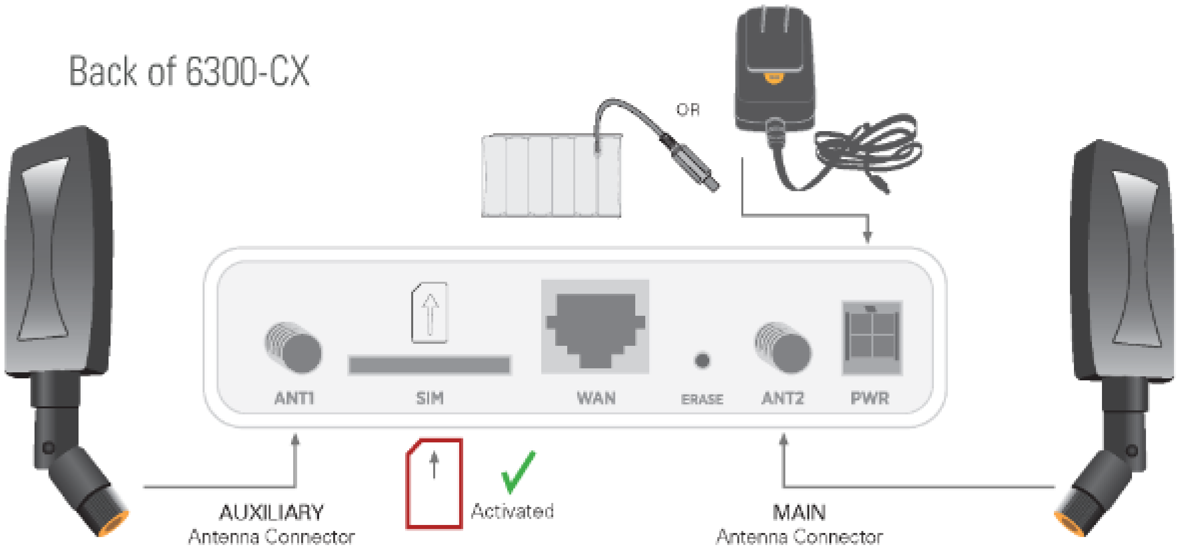
Initial Setup

Affix both antennas to the router and insert an activated SIM card before deploying the device. Be sure to select a location with optimal signal strength. For detailed instruction, refer to the tables that follow. Subsequent sections will outline site selection, powering options, and other device functionality.

Step-by-Step Guidance: Initial Setup

1. Insert the activated 2FF SIM card provided by your cellular network operator (putting the cut corner in first with metal contacts facing down). The card clicks into place when completely inserted.
2. Attach the two included antennas; both should be installed for optimal operation. Do this by gripping the metal connector section with your thumb and forefinger, tightening until secure. Do not tighten the antenna by holding any part of the plastic antenna housing.
3. To determine the optimal location for the 6300-CX, please see the "Site Survey" section.
4. Refer to the section(s) for Remote or Direct Power Installations when ready to connect the 6300-CX to the permanent power supply unit.<!--[endif]-->

5. The 6300-CX uses DHCP with IP Passthrough by default, which satisfies the setup requirements for most environments. If required, please use Accelerated View™ or the 6300-CX local GUI to configure the 6300-CX for router mode.



Site Survey

If you are unsure of the available cellular signal strength, or are choosing between several locations, please follow the instructions to identify the ideal installation site.

Step-by-Step Guidance: Site Survey

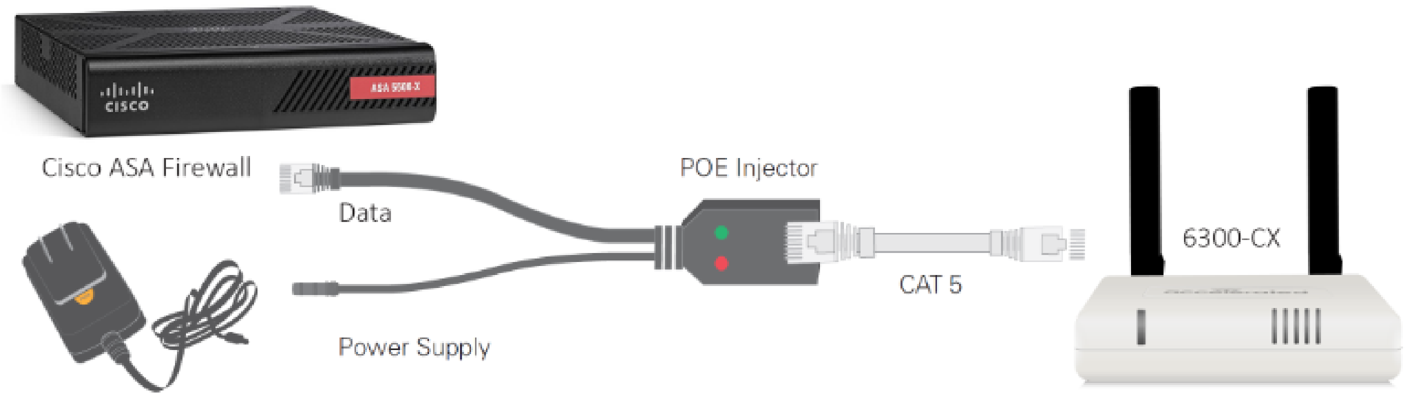
1. After following steps 1 and 2 in the "Initial Setup" section, connect the battery pack to temporarily power the Accelerated 6300-CX. The charge lasts two to four hours – it is not rechargeable and should be properly disposed of after use.
2. Move the 6300-CX to different locations within your site to determine the best compromise between signal strength and installation constraints. Since cellular signal strength may fluctuate, it is important to **wait at each location for 1 minute while observing the signal strength indicator** on the front of the device. Minimum cellular signal strength for operation is 2 bars (3+ is preferred).
3. After determining the optimal location, remove the battery pack and connect the main power supply unit or Ethernet cable connected to the PoE injector (per the power option outlined below).

Remote Power Installation – Powering Option #1

The included Power-over-Ethernet (PoE) injector allows the device to be positioned away from power outlets to simplify its installation needs. The adaptor consolidates the DC power and Ethernet connections so that both can be run to the 6300-CX via a single Ethernet cable. Distances of 300 ft have been tested on CAT6 and 250 ft on CAT5e. Note that cable conditions and the number of splices will impact actual distance.

Step-by-Step Guidance: Remote Power Installation

1. Plug the 6300-CX's power supply unit (PSU) into an AC power outlet.
2. Connect the end of the PSU into the DC input (4 pin connector) of the PoE injector.
3. Insert the male RJ45 connector of the PoE injector cable into the firewall.
4. Connect an Ethernet cable from the RJ45 socket on the PoE injector cable to the Ethernet port of the 6300-CX. (See diagram.)

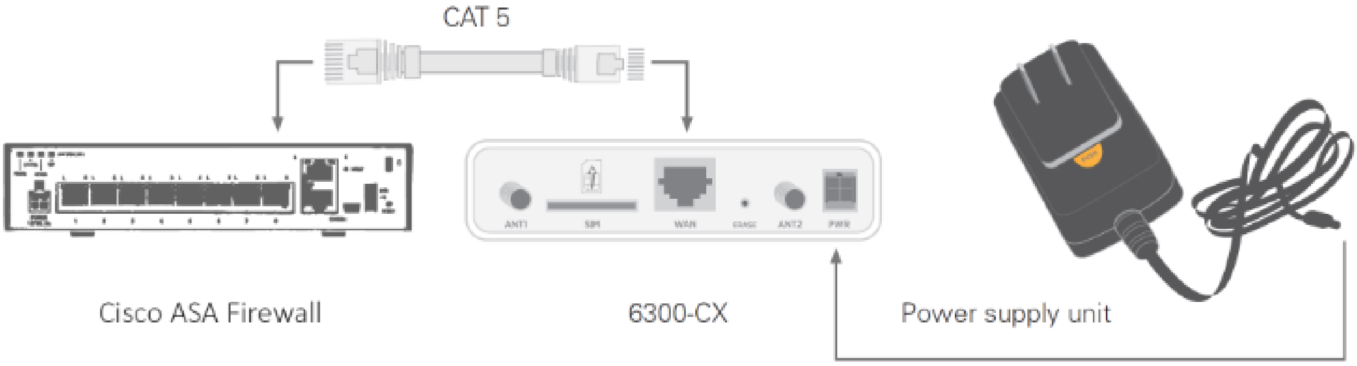


Direct Power Installation – Powering Option #2

If you plan to collocate the 6300-CX with the firewall device, you can directly power the 6300-CX without the PoE cable.

Step-by-Step Guidance: Direct Power Installation

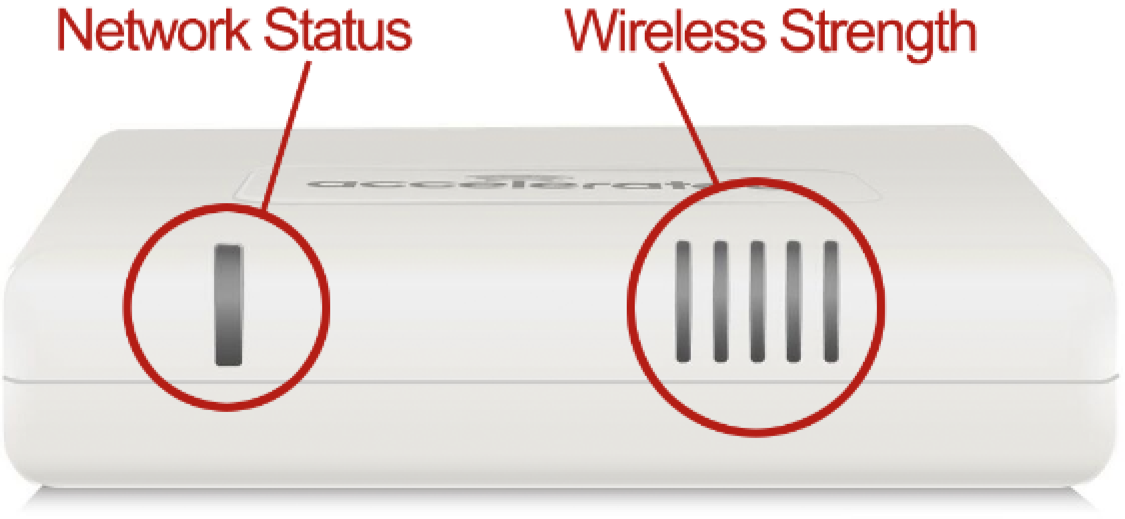
1. Use an Ethernet cable to connect the 6300-CX to the security appliance using port 1 (to use the cellular network as the primary connection) or port 3 (to configure a failover).
2. Plug the 6300-CX power supply unit (PSU) into an AC power outlet.
3. Connect the PSU into the 4-pin power connector of the 6300-CX. (See diagram.)



Understanding the 6300-CX LEDs

Once power has been established, your device will initialize and attempt to connect to the network. Device initialization may take 30-60 seconds. Indicator lights on the **Wireless Strength Indicator** show you the Cellular Network Signal Strength. The **Network Status Light** on the front left of the device displays connectivity information.

Please visit www.accelerated.com for additional information and trouble-shooting tips.



Network Status LED

🟨 **Solid Yellow**
Initializing or starting up.

🟨⬜ **Flashing Yellow**
In the process of connecting to the cellular network and to a device on its Ethernet port.

⬜▨ **Flashing White**
Has an Ethernet connection and is in the process of connecting to the cellular network.

🟩⬜ **Flashing Green**
Connected to 2G or 3G and is in the process of connecting to a device on its Ethernet port (or nothing is connected to the port).

🟩 **Solid Green**
Connected to 2G or 3G and also has an Ethernet connection.

🟦⬜ **Flashing Blue**
Connected to 4G LTE and in the process of connecting to a device on its Ethernet port.

🟦 **Solid Blue**
Connected to 4G LTE and also has an Ethernet connection.

🟥🟨 **Alternating Red/ Yellow**
Upgrading firmware. **WARNING: DO NOT POWER OFF DURING FIRMWARE UPGRADE.**

Wireless Strength LEDs

Signal Bars	Weighted dBm	Signal Strength %	Quality
▮	-113 to -99	0 - 23%	Bad
▮▮	-98 to -87	24 - 42%	Marginal
▮▮▮	-86 to -76	43 - 61%	OK
▮▮▮▮	-75 to -64	62 - 80%	Good
▮▮▮▮▮	-63 to -51	81 - 100%	Excellent

Disable IP Passthrough on the Accelerated 6300-CX LTE Router

For failover configuration with a Cisco ASA firewall, the 6300-CX must be able to provide a static IP address to the secondary WAN interface (port). It cannot do so, however, until IP Passthrough is disabled on the Accelerated device. Reconfiguring the 6300-CX in this manner places the CX in “Router Mode.” The settings outlined below should be applied from the Configuration tab of Accelerated View™ although local administration is also possible if the need arises.

The step-by-step guidance provided below assumes that default configurations, most notably the stock IP subnets, are being leveraged on both the Accelerated 6300-CX and the Cisco ASA. These values can be altered as necessary to meet any preexisting network conditions; unless otherwise indicated, assume the 192.168.0.X subnet belongs to the 6300-CX and that the 192.168.1.X subnet is assigned to the ASA.

Please refer to the 6300-CX User Manual for an in-depth walkthrough of both remote and local administration.

Step-by-Step Guidance: Disable IP Passthrough

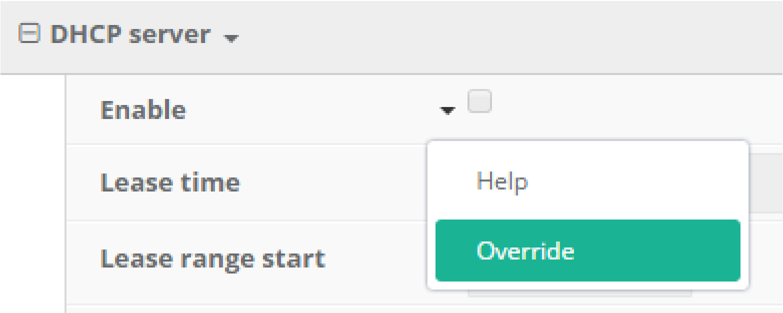
NOTE: *The MAC address is a 12-character code included on the 6300-CX’s bottom label.*

1. Sign in to Accelerated View and locate the 6300-CX by entering its **MAC address** in the **Search** field.
2. Click on the link in the **MAC** column to bring up the device’s profile.
3. Navigate to the **Configuration** tab.<!--[endif]-->
4. When configuring Accelerated devices, it is best to utilize new or existing **Group Configuration** profiles so that settings can be centrally stored and later applied to additional devices. Click the **Edit group configuration** link to proceed with the device setup.
5. **Settings** in Accelerated View are categorized and nested according to their scope of configuration:
6. Modem ? Passthrough: deselect the Enable checkbox
   Network ? Interfaces ? LAN ? IPv4: confirm the Interface type is set to Static IP address
   Network ? Interfaces ? LAN ? IPv4: confirm the Address is 192.168.0.1/24
   Network ? Interfaces ? LAN ? IPv4 ? DHCP server: select Enable
   (The “?” symbol denotes nested categories. Network ? Interfaces ? LAN, for example, points to the LAN menu nested inside the Interfaces section within the Network category.) points to the **LAN** menu nested inside the **Interfaces** section within the **Network** category.)

7. Click **Update** to finalize the new settings.
8. To apply the new settings immediately, reboot the CX or reference the step-by-step guidance for issuing remote commands.

NOTE:*Changes made to a group configuration are applied to ALL devices assigned to that group. To adjust settings for individual devices, select the* **Override** *button from the pull-down menu situated next to each field/ setting in question and make any necessary changes without editing the group config.*

NOTE:*Devices sync with Accelerated View once a day by default; pending configuration updates will apply at this time.*



ASA Configuration with the Accelerated 6300-CX

Failover Interface Settings

IP Policies and Static Routes serve as the foundation for how firewalls control and shape the flow of data through the networks they safeguard. Cisco ASA devices come preconfigured with security settings in place, though these routes and policies assume a traditional, single-WAN setup. The first Ethernet port, labeled "1," is designated for the primary WAN uplink with the remaining ports relegated to LAN access. An interface must be configured for the secondary WAN uplink to establish failover functionality. More importantly, both uplink interfaces must be configured to use a static IP address.

NOTE: Device administration is best handled using the Cisco ASDM desktop application, which connects a computer to the firewall's GUI without having to enable http server access. Initialize the ASDM-IDM Launcher and connect to the default gateway address provided by the ASA firewall: 192.168.1.1; the username and password are blank by default.

For an in-depth walkthrough of how to manage your ASA device via ASDM, please refer to Cisco's Configuration Guide.

Step-by-Step Guidance: Interface Settings

NOTE: *If the primary Internet connection routes traffic using either the 192.168.1.X or 192.168.0.X subnet, an alternative subnet will need to be used for the ASA and 6300-CX respectively.*

1. After connecting to the firewall via Cisco ASDM, navigate to the **Configuration** tab and select **Interfaces.**

2. ASA devices have two default interface configurations: GigabitEthernet1/1, allocated for the “outside” route, and GigabitEthernet1/2, allocated for the “inside” route.
3. Double click GigabitEthernet1/1 to edit the interface – rename it to “Primary” and select **Use Static IP**.
4. Specify the **IP Address** and **Subnet Mask** for the static IP assignment associated with the primary Internet connection. Contact your network administrator if these values are unknown.
5. Enter a **Description** for tracking purposes if desired. “FiOS Broadband,” for example.
6. Click **OK** to finalize any changes. ASDM may display a warning about static routes being altered – click **OK**.
7. Double click GigabitEthernet1/3 to edit the secondary WAN uplink.
8. Select **Enable Interface**, assign an **Interface Name** (and optional **Description**), and toggle to **Use Static IP**.
9. Specify the static IP Address and Subnet Mask. If the 6300-CX is configured to use its default IP range, feel free to use the following values: 192.168.0.120 (IP Address) and 255.255.255.0 (Subnet Mask).
10. There should now be 3 interfaces configured: Primary, inside, and Secondary.

! NOTE: Changes made to the ASA configuration via ASDM are inactive until the **Apply** button is clicked.

Static Routes and Tracking

The Cisco ASA device is ready for dual-WAN configuration once its two WAN connections are properly set (per the guidance from page 7 of this document). Any active interface must have a static route defined in order authorize traffic over the network. The firewall can then leverage advanced prioritization options to further reinforce the failover redundancy provided by the 6300-CX’s backup LTE connection.

Failover itself is accomplished by the simultaneous application of interface metrics, which allows the network to establish a primary (the shorter/ smaller metric) and secondary (the longer/ larger metric) uplink, coupled with the tracking options configurable via static routes. With tracking enabled, the firewall actively verifies whether or not its primary WAN interface is online.

For an in-depth walkthrough of how to manage your ASA device via ASDM, please refer to Cisco’s Configuration Guide.

Step-by-Step Guidance: Static Routes and Tracking

NOTE:*Please refer to Cisco’s guidance on how to perform a configuration backup if there is concern over being able to recreate any policies or routes.*

1. After connecting to the firewall via Cisco ASDM, navigate to the **Configuration** tab and select **Static Routes from the Routing menu (found under Device Setup).**
2. Delete any existing static routes. These will need to be recreated with dual-WAN failover taken into consideration.
3. Click **Add** to create a new static route for each interface. Unless otherwise specified by the network administrator, use the following values:

Primary	Secondary
IP Address Type: IPv4 **Interface:** Primary **Network:** any4 **Gateway IP:** Use the corresponding Gateway IP established on page 7, step 4 **Metric:** 1	**IP Address Type:** IPv4 **Interface:** Secondary **Network:** any4 **Gateway IP:** Use the corresponding Gateway IP established on page 6, step 5 **Metric:** 120

1. For the **Primary** route, under **Options**, select **Tracked**. The **Track ID** and **SLA ID** are used to distinguish this configuration within ASDM. The **Track IP** Address can be set to any valid address used for connectivity testing (8.8.8.8 is a safe bet) and the **Target Interface** should remain "Primary."
2. Select Monitoring Options and set the **Frequency** to establish how often the ASA firewall should verify the connectivity of the primary WAN uplink. (10 seconds, for example.) Other settings can be adjusted as needed.

NOTE:*Set the **Number of Packets** to 3 unless otherwise specified.*

NAT Rules

The Cisco ASA comes with a default NAT rule for its primary interface to ensure the proper flow of traffic as packets travel across static routes. Once configured for two WAN interfaces, a second NAT rule should be defined for the failover connection. Note that any additional preexisting rules will need to be recreated for the secondary interface to maintain security continuity during failover.

For an in-depth walkthrough of how to manage your ASA device via ASDM, please refer to Cisco's Configuration Guide.

Step-by-Step Guidance: NAT Rules

1. After connecting to the firewall via Cisco ASDM, navigate to the Configuration tab and select the Firewall menu. Click on NAT Rules.
2. Click the Add button to generate a new rule.
3. Unless otherwise specified by your network administrator, apply the new rule as follows: **Match Criteria (Source Interface, Source Address, Destination Address, Service)** – any **Action: Translated Packet – Source NAT Type:** Dynamic PAT (Hide); **Source Address:** Secondary; **Destination Address** and **Service:** Original
4. Be sure "Enable rule" is selected under **Options**.
5. Click **OK** to finalize the new rule.

DHCP and DNS Configuration

To ensure seamless failover, it is best to specify DHCP and DNS settings so that the internal interface is used to provide consistency no matter whether the primary or failover WAN is leveraged for connectivity.

Step-by-Step Guidance: DHCP and DNS Configuration

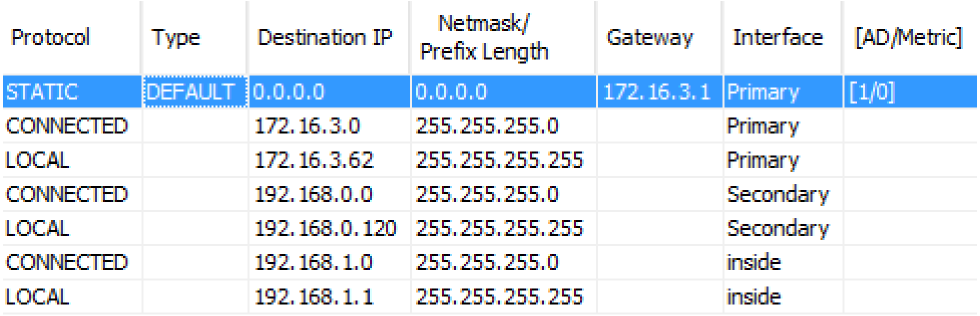
1. From the **Configuration** tab, select the **Device Management** menu. Expand **DNS** and click on **DNS Client**.
2. Using the pull-down menus in the **DNS Lookup** table, set the WAN **Interfaces** to “False” so that their DNS is disabled. Set the “inside” interface to “True.”
3. Ensure **Enable DNS Guard on all interfaces** is selected.
4. Expand the **DHCP** menu and select **DHCP Server**. Double click on “inside.”
5. Select **Enable DHCP server** and utilize the predefined **DHCP Address Pool** unless otherwise notified by your network administrator.
6. Specify any DNS preferences using the **Optional Parameters**.
7. Click **OK** to finalize the configuration.

NOTE: Changes made to the ASA configuration via ASDM are inactive until the **Apply** button is clicked.

Verification/ Monitoring

Cisco ASDM provides real-time monitoring of traffic flowing through ASA devices. After completing the Accelerated 6300-CX configuration to establish backup connectivity, route monitoring can confirm that both the failover and failback mechanisms are functioning as intended.

Look for the line currently selected as the **DEFAULT**. This will change from the primary to secondary interface as soon as the failover condition is triggered (per the tracking parameters established during static route configuration), and revert back to primary once the connection is reestablished.



Protocol	Type	Destination IP	Netmask/ Prefix Length	Gateway	Interface	[AD/Metric]
STATIC	DEFAULT	0.0.0.0	0.0.0.0	172.16.3.1	Primary	[1/0]
CONNECTED		172.16.3.0	255.255.255.0		Primary	
LOCAL		172.16.3.62	255.255.255.255		Primary	
CONNECTED		192.168.0.0	255.255.255.0		Secondary	
LOCAL		192.168.0.120	255.255.255.255		Secondary	
CONNECTED		192.168.1.0	255.255.255.0		inside	
LOCAL		192.168.1.1	255.255.255.255		inside	

For an in-depth walkthrough of how to manage your ASA device via ASDM, please refer to Cisco’s Configuration Guide.

Step-by-Step Guidance: Verification/ Monitoring

1. After connecting to the firewall via Cisco ASDM, navigate to the **Monitoring** tab and select the **Routing** menu. Click on **Routes**.
2. The **Type** column indicates which route is serving traffic currently by indicating the **DEFAULT** route.
3. Disconnect the primary interface by unplugging the Ethernet cable and click **Refresh**. The new default should be associated with the secondary connection.
4. Reconnect the primary interface and wait 10 to 30 seconds. Click **Refresh** and verify that the default route has reverted back to the primary WAN uplink.

NOTE: Changes made to the ASA configuration via ASDM are inactive until the **Apply** button is clicked.