WAN Failover Configuration for Palo Alto PA Series

6310-DX

WAN Failover Configuration for Palo Alto PA Series

Overview

Integrating cellular Internet access into a traditional, wireline data network is typically accomplished through one of three interfaces: USB aircards, embedded radios, or a dedicated cellular networking appliance. Of these methods, only the dedicated appliance provides a solution that can overcome the challenges of deploying reliable LTE connectivity.

Both USB aircards and embedded radios only capture cell signals as they are received from the equipment closet or server rack where the edge appliance resides (since both must integrate directly in/ on a host device). This is rarely where coverage is optimal. Aircards in particular present significant challenges due to their need for driver support, their lack of external antennas, and the short lifespan of these consumer-grade dongles.

LTE networking appliances are ideal for wireless WAN failover because they integrate with networks via Ethernet (or WiFi). To streamline cellular deployments, Digi's Cellular Extenders are optimized from the point of installation all the way through to data plan management. Setup is simplified when using a Remote Mounting Kit (RMK) -- the included (passive) PoE injector and temporary battery pack for site survey -- and Digi Cellular Extenders are set for IP passthrough by default to ensure the backup (cellular) WAN connection is completely controlled by the network's existing edge.

This document covers how to install a Digi Cellular Extender and configure it for failover with a third-party networking appliance. Since all Digi Cellular Extenders, the 6300-CX and 6310-DX, default to IP passthrough, most of the software settings described below apply to the third-party device referenced in this article. Requirements for dual-WAN configuration will vary depending on the make and firmware version of the edge appliance controlling the failover parameters.

Interoperability Matrix

When configuring dual-ISP failover within the Palo Alto Networks Operating System (PAN-OS), it is required that both WAN uplinks are assigned a static address (private or public).

See below for 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	PAN-OS Firmware	Cellular Extender Firmware
11/2018	5.0.6	18.4.54.41

Caveats

Good signal strength is required to maintain reliable cellular Internet access. A site survey should be performed prior to installing the Digi Cellular Extender. While network performance varies depending on the carrier and location, all deployments can be optimized to minimize the challenges presented by building materials, RF interferene, and other environmental constraints.

Using a Digi Celluler Extender for WAN failover assumes that an active Internet connection is available from another network interface set as the primary connection for the edge appliance. It is recommended that the Cellular Extender runs in IP passthrough mode to integrate seamlessly with existing IT infrastructure.

NOTE: *The third-party appliance tested in this document was running its default configuration. If the steps outlined in this document interfere with existing customizations, or vice versa, consider backing up the edge appliance's current settings and testing failover functionality after temporarily erasing the third-party device's configuration.*

Accelerated 6310-DX Setup

Initial Setup

Digi Cellular Extenders have a socket that houses the CORE 1002-CM Plug-In Modem in order to provide LTE connectivity. Prior to plugging in the modem, insert an active 2FF SIM card into either (or both) of the 1002-CM's two SIM slots.

After securing the plug-in module, cover the exposed side of the main appliance using the included faceplate and affix both antennas. The unit is now assembled for cellular network access.

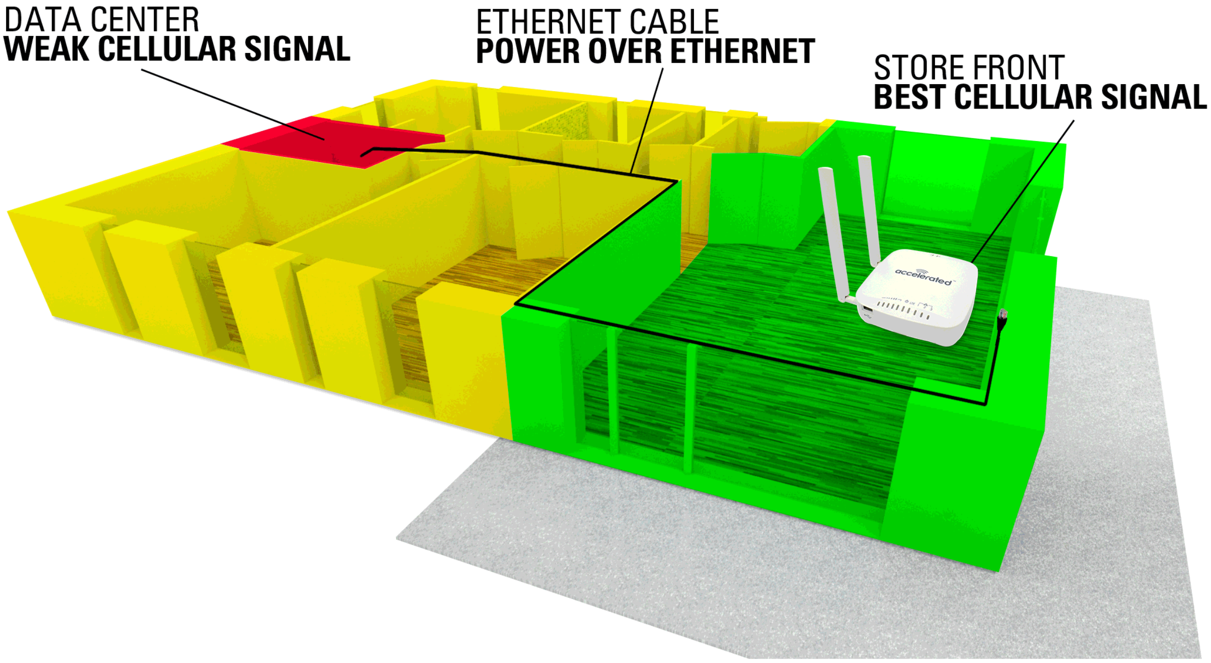
Step-by-Step Guidance: Initial Setup

1. Open the gift box and identify the following components:
   - Cellular Extender appliance
   - CORE 1002-CM module
   - Active SIM card (2FF)
   - Faceplate
   - Cellular antennas (2x)
2. Insert the 2FF SIM card(s) into the 1002-CM. The card clicks into place when completely inserted.
3. Slide the 1002-CM into the Cellular Extender's socket
4. Clip the faceplate into place so the cellular SMA connectors are exposed.
5. Affix the 2 antennas.
6. Refer to the Remote or Direct Power installation instructions when ready to connect power.
   - *NOTE: It is strongly recommended that a site survey is preformed prior to installation.*

Site Survey

The mounting bracket that comes with Digi Cellular Extenders presents multiple options for device placement. Perform a site survey to make an informed decision as to where the ideal on-site location for cellular services might be, based off of reception and proximity to the edge appliance.

Using the temporary battery pack, power up the unit and wait for it to establish a cellular connection before moving around to potential install locations -- see the LEDs section of this document for more information on the Digi Cellular Extender's various status indicators.

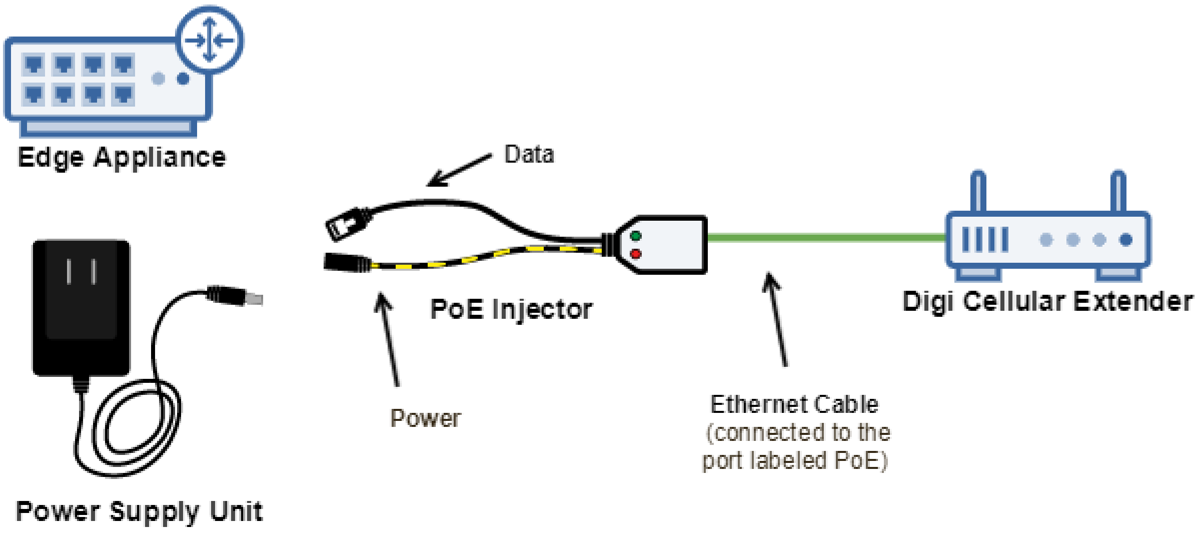


NOTE: If the Cellular Extender is having difficulties connecting to its LTE network, please refer to the article that covers Staging for Initial Connectivity.

Step-by-Step Guidance: Site Survey

1. Use the Remote Mounting Kit's battery pack to power the device.
2. Wait for the blue, blinking LED to confirm LTE connectivity.
3. Step outside, away from any obstructions/ building materials if possible, and wait at a single location for 60 to 90 seconds.
    - Refer to this signal strength reading, as indicated by the onboard LEDs, as the baseline signal quality.
4. Return inside and find a location for the Cellular Extender to be mounted – the goal is to find a spot with reception equal to the baseline (outdoor) signal.
    - Situate the device as close as possible to an exterior wall, with higher elevations being ideal.

Power Option 1: Remote Installation



Digi offers a Remote Mounting Kit (RMK) that includes 3 key components:

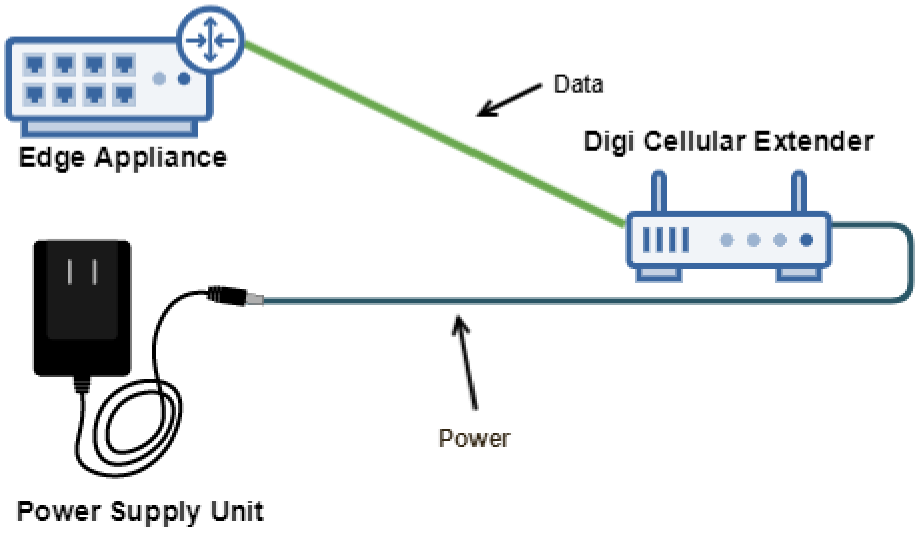
- Passive Power-over-Ethernet (PoE) Injector
- Temporary Battery Pack
- Install Accessories

Using the PoE injector, the Digi Cellular Extender can be powered up to 300 ft away from the unit's power supply using only the (Cat 5 or Cat 6) Ethernet cable that also integrates LTE data access into the network.

Step-by-Step Guidance: Remote Installation

1. Plug the included power supply unit (PSU) into an AC power outlet.
2. Connect the barrel jack of the PSU into the DC input of the PoE injector.
3. Insert the male RJ45 connector of the PoE injector cable into the WAN port getting configured for failover (on the edge appliance).
4. Run an Ethernet cable from the RJ45 socket on the PoE injector to the Ethernet port of the Digi Cellular Extender labeled PoE.

Power Option 2: Direct Installation



If optimal signal is readily available within range of a power outlet, Digi's Cellular Extenders can be connected directly to the included power supply and then integrated into the network using a standard Ethernet cable.

Step-by-Step Guidance: Direct Installation

1. Plug the included power supply unit (PSU) into an AC power outlet.
2. Connect the barrel jack of the PSU into the DC input of the Digi Cellular Extender.
3. Use an Ethernet cable to connect the Cellular Extender from its LAN port to the WAN port being configured for failover on the edge appliance.

LEDs

Once power has been established, the Digi Cellular Extender will initialize and attempt to connect to a cellular network per the settings provisioned to its inserted SIM card. Device initialization may take several minutes as it joins an LTE network for the first time.

❗ *NOTE: Click here for troubleshooting assistance with initial connectivity.*

Indicator lights on the ***Wireless Strength Indicator*** update every 30 seconds to show the currently observed signal strength, while the ***Network Status Light*** updates to display the type of cellular connectivity available. Please refer to the following table for more information:

Network Status LED

🟨	**Solid Yellow** Initializing or starting up.	🟩	**Solid Green** Connected to 2G or 3G and also has a device linked to a LAN port.
🟨⬜	**Flashing Yellow** In the process of connecting to the cellular network and to any device on its LAN port(s).	🟦⬜	**Flashing Blue** Connected to 4G LTE and in the process of connecting to a device on its LAN port(s).
⬜▨	**Flashing White** Established LAN connection(s) and is in the process of connecting to the cellular network.	🟦	**Solid Blue** Connected to 4G LTE and also has a LAN connection.
🟩⬜	**Flashing Green** Connected to 2G or 3G and is in the process of connecting to any device on its LAN port(s), or nothing is connected to the port.	🟥🟨	**Alternating Red/ Yellow** Upgrading firmware. **WARNING: DO NOT POWER OFF DURING FIRMWARE UPGRADE.**

Signal 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

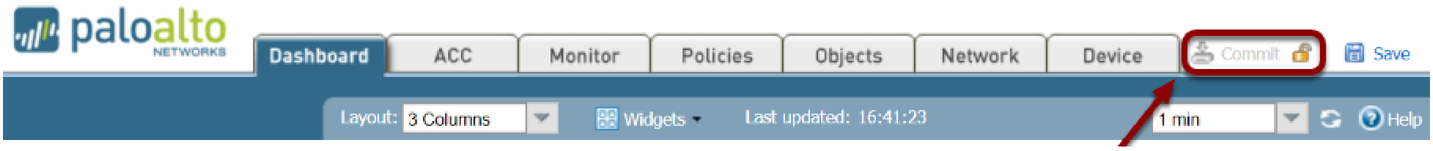
IP Passthrough

Digi Cellular Extenders are set by default with IP passthrough configured for the PoE-enabled Ethernet port, meaning any client device connected to the passthrough interface will receive the IP address directly assigned to the Cellular Extender's LTE radio.

It is suggested that IP passthrough is used when deploying a backup WAN connection into an edge appliance to ensure seamless network integration. With passthrough enabled the Cellular Extender will not directly control the routing of packets going to or from its LTE radio interface, instead deferring to the logic (routing tables and firewall policies) of the edge appliance.

To toggle IP passthrough on or off, please refer to the following configuration example: LAN port with IP passthrough. Note that this is only required for devices running non-standard configs.

Palo Alto Configuration



Refer to the steps outlined below for details on how to set PA Series firewalls for dual-WAN failover. Changes must be ***Committed*** before they are live on the appliance.

*NOTE: Digi Support will assist in troubleshooting interoperability between the Digi Cellular Extender and a third-party appliance. However, support is limited to a *stock* configuration of the third-party device.*

This means that the current (non-Digi) config will need to be backed up, either through a formal “export” feature or by taking notes/ screenshots of non-standard settings, leaving technicians in a position to configure the device as if it were brand new (therefore being able to rely on third-party vendor documentation).

If failover settings are validated but then break using the third-party appliance's non-standard production config, troubleshooting with third-party support may be required.

Removing the Default Virtual Wire

PA-Series firewalls come preconfigured with a default virtual wire interface between ports Ethernet 1/1 and Ethernet 1/2 (as well as a corresponding default sucrity policy and zone), used to effectively "bridge" two Ethernet ports. Delete these settings to prevent them from interfering with the dual-WAN configuraiton.

Step-by-Step Guidance: Removing the Default Virtual Wire

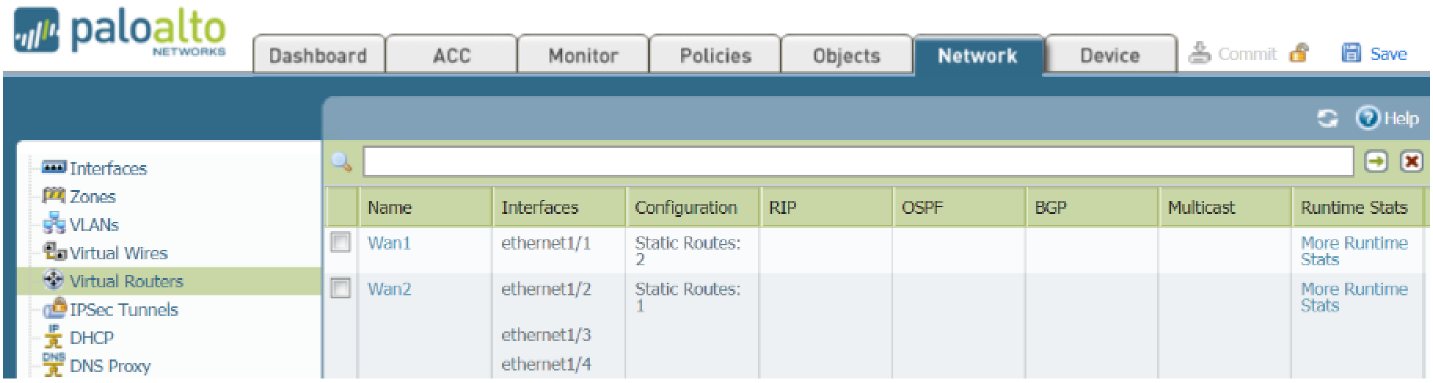
You must delete the configuration in the following order:

1. Navigate to *Policies > Security*, select the default rule and click *Delete*.
2. Browse to *Network > Virtual Wires*, choose the virtual wire and click *Delete*.
3. From *Network > Zones*, select each zone and click *Delete*.
4. Under *Network > Interfaces*, select each interface (ethernet1/1 and ethernet1/2) and click *Delete*.
5. Finalize these changes by selecting *Commit* from the top-right of the GUI.

Creating Virtual Routers

Next, set interfaces that correspond to the intended Ethernet ports and functionality. This document assumes the primary ISP is connected to Ethernet 1/1 and that the LTE connection provided by the Digi Cellular Extender terminates to Ethernet 1/2. The remaining ports -- Ethernet 1/3 and Ethernet 1/4 -- are reserved for LAN access. WAN failover is accomplished on the Palo Alto Networks OS by setting up 2 "Virtual Routers" with varying priority, and then setting up static routes that dictate when available WAN uplinks are utilized based off of metric values associated with each route.

For this sample configuration, the primary ISP is associated with its own virtual router as the default WAN route so long as it is available. A second virtual router hosts the cellular ISP as well as the LAN ports. There are static routes associated with each virtual router that dynamically point oubtound traffic to the intended WAN interface depending on an available connection ince routes with metric values closer to (but greater than) 0 are honored first, and are prioritized accordingly across virtual routers.



	Name	Interfaces	Configuration	RIP	OSPF	BGP	Multicast	Runtime Stats
☐	Wan1	ethernet1/1	Static Routes: 2					More Runtime Stats
☐	Wan2	ethernet1/2 ethernet1/3 ethernet1/4	Static Routes: 1					More Runtime Stats

Step-by-Step Guidance: Creating Virtual Routers

Creating the first virtual router:

1. Navigate to *Network > Virtual Routers* to edit an existing entry or click *Add* to create a new one.
2. From the *General* tab, click *Add* under *Interfaces* and select *ethernet1/1*.
3. Unless otherwise specified, leave the remaining values set to defaults and select the *Static Routes* tab.
4. Click *Add* to create a route with the following information:
   - Name: the label used to identify this route.
     - Enter *Next_Hop,* or another desired naming convention.
   - Destination: the intended path for the route to take.
     - Enter *0.0.0.0/0* to specify "any" destination address.
   - Interface: the Ethernet port associated with the route.
     - Select *ethernet1/1* to select the primary Internet connection.
   - Next Hop: where data heads to next after reaching the designated interface.
     - Set for *IP Address* and enter the *Gateway IP* address of the primary Internet connection.
   - Admin Distance: a relative value used to prioritize routes with the same metric.
     - Leave this blank unless otherwise specified.
   - Metric: Routes with lower metric values are prioritized first.
     - Leave this set to *10* unless otherwise specified.
5. Select *OK* to finalize the first static route.
6. Select *OK* again to create the first virtual router.

Creating the second virtual router:

1. Create a second virtual router by selecting *Add* from *Network > Virtual Routers*.
2. From the *General* tab, click *Add* under *Interfaces* and select the remaining Ethernet ports.
3. Unless otherwise specified, leave the remaining values set to defaults and select *Static Routes* tab.
4. Click *Add* to create a route with the following information:
   - Name: *Next_Hop2*, or another desired naming convention.
   - Destination: *0.0.0.0/0*
   - Interface: *ethernet1/2*
   - Next Hop (set for *IP Address*): *Gateway IP* of the cellular Internet connection
   - Admin Distance: blank unless otherwise specified
   - Metric: *20*
5. Select *OK* to finalize the second static route.
6. Select *OK* again to create the second virtual router.

Adding a "return" route to the first virtual router:

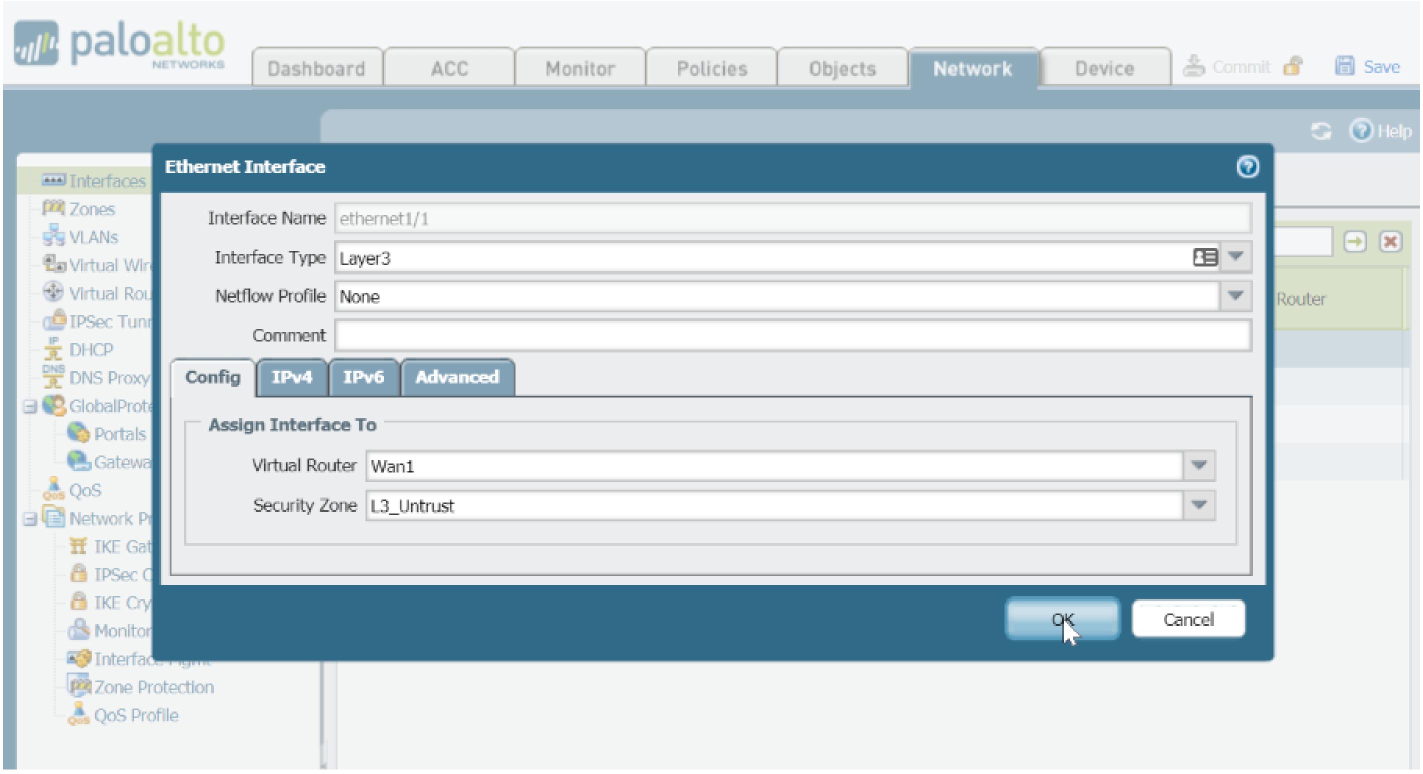
1. Click on the name of the first virtual router.
2. Select the *Static Routes* tab.
3. Click *Add* to create a second route with the following information:

- **Name:** *Return*, or another desired naming convention.
- **Destination:** *192.168.0.0/16*, or whatever poolcorresponds to the firewall's LAN
- **Interface:** *ethernet1/2*
- **Next Hop** (set for **Next VR**): Select the second virtual router created in the previous section
- **Admin Distance:** blank unless otherwise specified
- **Metric:** *10*

4. Select *OK* to finalize the second return route.
5. Select *OK* again to finalize changes.

Security Settings

Additional steps are required to ensure seamless, secure routing regardless of which WAN is currently active (primary broadband or cellular failover). Notably, each interface needs to be assigned to its intended firewall zone and access to relevant services, policies and protocols must be set.



Ethernet Interface

Interface Name: ethernet1/1

Interface Type: Layer3

Netflow Profile: None

Comment:

Assign Interface To

Virtual Router: Wan1

Security Zone: L3_Untrust

Step-by-Step Guidance: Security Settings

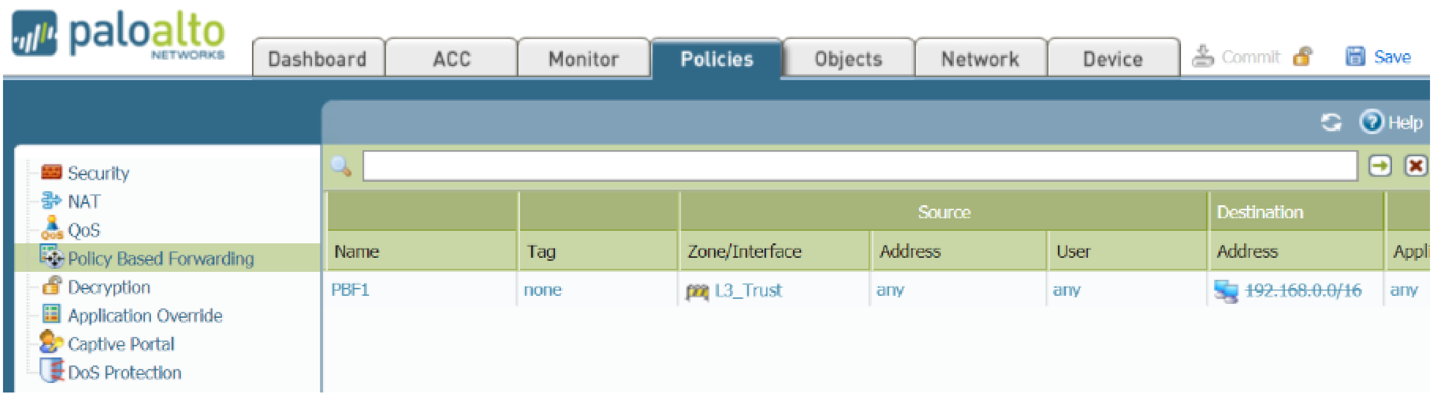
1. Navigate to *Network* > *Interfaces* and select *ethernet1/1*.
2. From the *Security Zone* pulldown menu under the *Config* tab, select the entry intended for the WAN-facing, "untrusted," or "external" zone.
    - This may need to be created if it doesn't exist already by selecting *New Zone*.
3. Click on the *IPv4* tab and select *Add.*

4. Enter the IP address and network mask associated with the WAN connection.
5. Click on *Advanced* and browse to the *Other Info* tab.
6. Choose to apply an existing *Management Profile* or select *New Management Profile* to specify new list of permitted services for the interface.
7. Click *OK* to finalize the interface changes.
8. Repeat these steps for *ethernet1/2*, replacing the entry in step #4 above with the IP and netmask associated with the cellular WAN.
9. Steps 1 through 7 must also be repeated for the *LAN interfaces*, however they should instead be added to a *"trusted" or "internal" firewall zone.*
10. Navigate to *Policies > Security* and select *Add.*
11. Create a *Security Policy Rule* with an accurate *Name* and *Description.*
    - For this example, a rule to "allow all traffic" from the internal zone to the external zone is described.

12. On the *Source* tab, add the zone selected in step #9.
13. On the *Destination* tab, add the zone selected in step #2.
14. Click *OK* to finalize the policy rule.

Failover Monitor

To dynamically route to either the primary ISP or cellular backup based off of the availability of the primary ISP, a policy-based forwarding (PBF) rule must be created to specify when the firewall should use its failover connection.



		Source			Destination	
Name	Tag	Zone/Interface	Address	User	Address	Appl
PBF1	none	L3_Trust	any	any	~~192.168.0.0/16~~	any

Step-by-Step Guidance: Failover Monitor

1. Navigate to *Policies > Policy Based Forwarding.*
2. Click *Add* to create a new PBF rule.
3. From the *General* tab, enter a *Name* and *Description* to identify the rule.
4. Switch to the *Source* tab and *Add* the LAN/ trusted zone to the Zone table.
    - This is the same zone created in step #9 of the previous section.

5. On the *Destination* tab, *Add* the *internal* address pool.
6. Select the *Negate* checkbox.
7. From the *Forwarding* tab, set the following options:

- *Action:* Forward
- *Egress Interface:* ethernet1/1
- *Next Hop:* Gateway IP of primary ISP
- *Monitor:* Enabled *(checked)*
- *Profile:* Create a *New Monitor Profile*
    - Next to *Action*, select *Fail Over*
    - Adjust the *Interval* and *Threshold* as desired.
- *IP Address:* Enter a test target IP (such as 8.8.8.8)

8. Click *OK* to finalize the PBF rule.

Testing the Backup WAN

Failover configuration is complete after working through the steps outlined above. Per this setup, the PA-Series firewall will route traffic out of its primary Ethernet WAN so long as it is online. The cellular connection becomes the primary outbound route should the primary WAN fail.

When simulating the loss of network connectivity, it is best to keep all Ethernet cables connected and simply remove the Internet connection to the ISP (e.g. the coax terminating to a broadband cable modem). This is to more closely emulate the conditions of a real-word network outage rather than a broken cable link.