Enabling Dual ISP Redundancy on a Palo Alto Firewall

For access to live Palo Alto Networks lab boxes, go to:
https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab

Overview

Sun Management is a Palo Alto Networks Partner, Palo Alto Networks Certified Services Partner, and Palo Alto Networks Authorized Training Center. Our Engineers have designed and installed over $100M in Palo Alto Firewall Security since 2009. As a Palo Alto Networks Authorized Training Center, we have trained over 2000 students on effective utilization of the Palo Alto Networks Firewall. As such, we aim to provide continuous access to on-going training for our existing clients, potential clients and any other individual interested in further developing their engineering skills with Palo Alto Networks Firewalls.

Organizations need to be resilient to occasional outages and issues with their internet service provider. Many choose to have two internet service providers to ensure that their network and business operations don't suffer for no fault of their own. The Palo Alto Firewall can instantly detect an internet outage on the primary ISP and switch to the secondary ISP with minimal issue.

The Scenario

We need to ensure that an outage at our primary ISP will not significantly disrupt our organization's productivity. We can configure Path Monitoring that continuously monitors the availability of the routes out of our primary ISP. If a ping fails to return, we can automatically failover our traffic to using the secondary ISP with only slight disruption to existing sessions.

On the Palo Alto Networks Firewall

High level steps on the firewall for ISP redundancy and traffic failover:

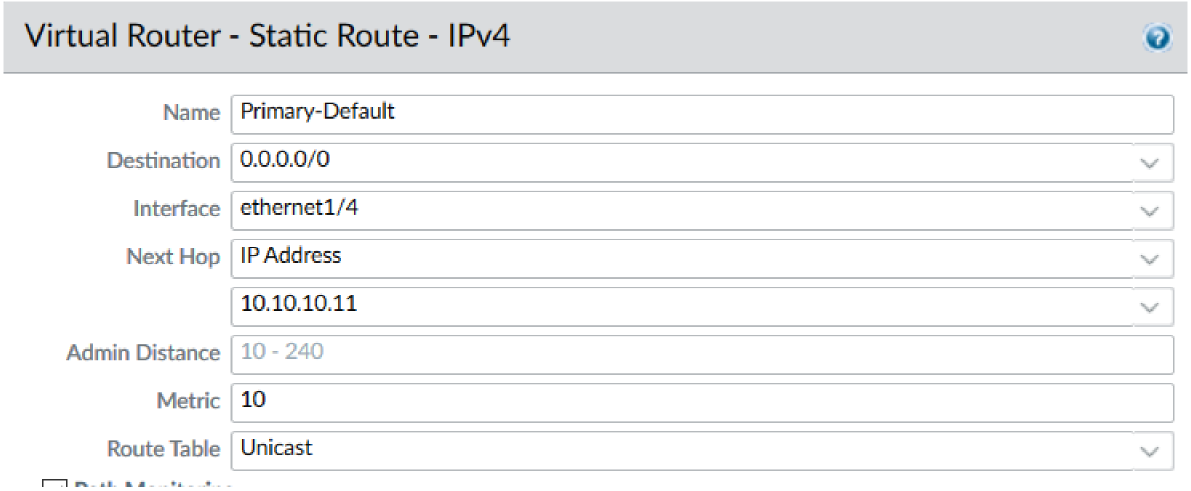
1. Setup default routes for each ISP and Path Monitoring for the primary ISP
2. Configure NAT policy rules
3. Commit and Verify Configuration

For demonstration purposes, let's assume that:

Primary ISP – Ethernet 1/4 - 10.10.10.78/24
Secondary ISP – Ethernet 1/5 - 10.10.20.99/24
Primary Default Gateway - 10.10.10.11
Secondary Default Gateway - 10.10.20.22

1. Default Routes and Path Monitoring

Let's start by setting up our primary default route and path monitoring.
Name: Primary-Default
Destination: 0.0.0.0/0
Interface: ethernet1/4
Next Hop: IP Address 10.10.10.11



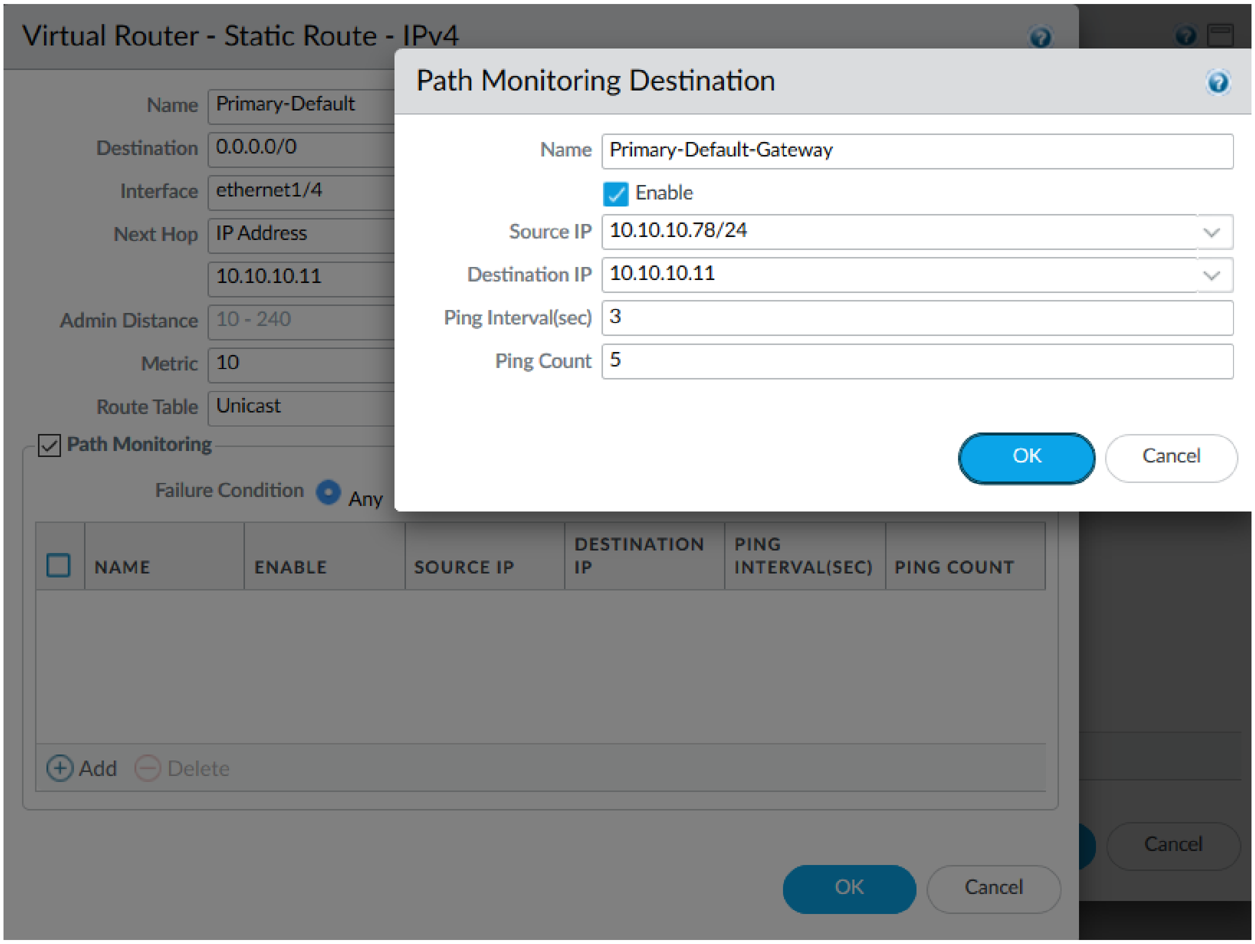
Virtual Router - Static Route - IPv4

Name	Primary-Default
Destination	0.0.0.0/0
Interface	ethernet1/4
Next Hop	IP Address
	10.10.10.11
Admin Distance	10 - 240
Metric	10
Route Table	Unicast

□ Path Monitoring

Now that we have the default route, let's configure path monitoring for this route.

Name: Primary-Default-Gateway
Source IP: 10.10.10.78/24 – (The address block we have for our Primary ISP)
Destination: 10.10.10.11 – (Our default gateway)
We can hypothetically ping anything on the internet to monitor this path, but let's stick to the default gateway.



Virtual Router - Static Route - IPv4

Name	Primary-Default
Destination	0.0.0.0/0
Interface	ethernet1/4
Next Hop	IP Address
	10.10.10.11
Admin Distance	10 - 240
Metric	10
Route Table	Unicast

☑ Path Monitoring

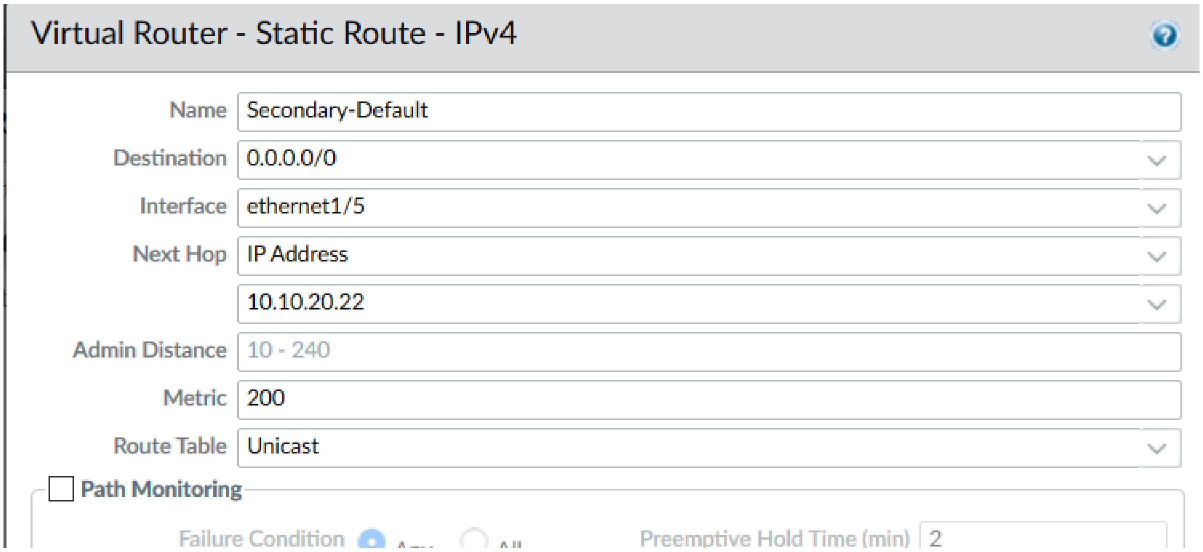
Failure Condition ● Any

□	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT

Path Monitoring Destination

Name	Primary-Default-Gateway
	☑ Enable
Source IP	10.10.10.78/24
Destination IP	10.10.10.11
Ping Interval(sec)	3
Ping Count	5

Let’s configure our secondary route. We’ll make sure to give this route a higher metric so that it’s only used if the primary route is deemed inaccessible.



Virtual Router - Static Route - IPv4

Name	Secondary-Default
Destination	0.0.0.0/0
Interface	ethernet1/5
Next Hop	IP Address
	10.10.20.22
Admin Distance	10 - 240
Metric	200
Route Table	Unicast

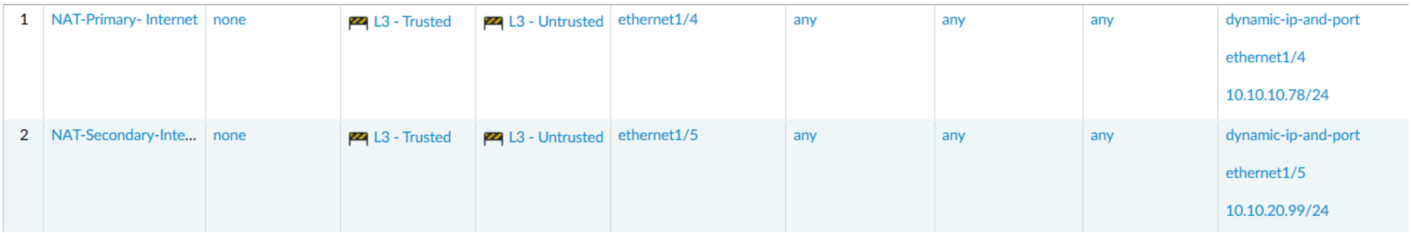
□ Path Monitoring

Failure Condition ● Any ○ All   Preemptive Hold Time (min) 2

Now that this is configured, if a ping fails to return, the primary route will be removed from the routing table and the secondary route will be active. If the firewall finds that the primary path has returned pings for 60 seconds, it will once again become the active route.

2. NAT Configuration

We want to ensure that we are translating to the correct public IP based on which interface and ISP we are using. Both internet providers have been placed in the same security zone, for further network segmentation, we could create a zone for each provider.

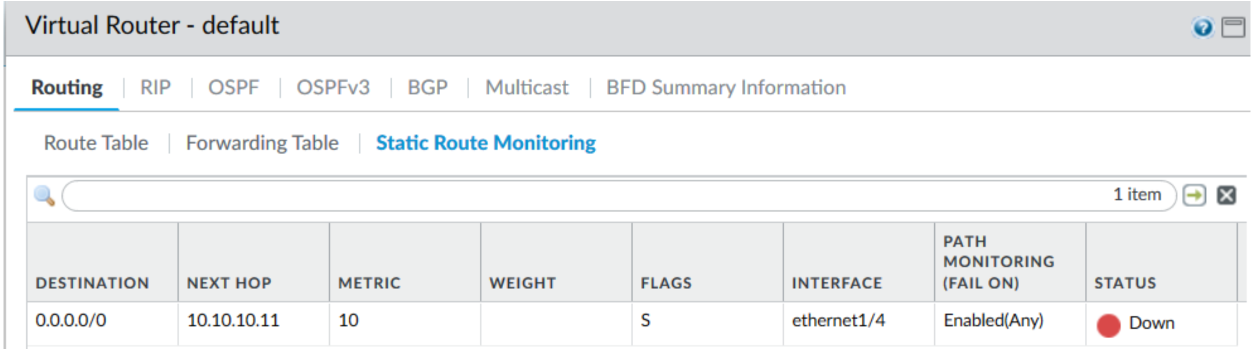


1	NAT-Primary- Internet	none	L3 - Trusted	L3 - Untrusted	ethernet1/4	any	any	any	dynamic-ip-and-port ethernet1/4 10.10.10.78/24
2	NAT-Secondary-Inte...	none	L3 - Trusted	L3 - Untrusted	ethernet1/5	any	any	any	dynamic-ip-and-port ethernet1/5 10.10.20.99/24

3. Commit and Verify

Now, we'll commit our changes. In the top right, we'll hit "Commit to Device"

Once that is complete, we can go to our routing table and verify the path monitoring. The Static Route Monitoring tab will tell us that status of our monitored route. Below is the instance in which the path is down and the primary route has been taken out of the routing table so that the secondary route may be used.



DESTINATION	NEXT HOP	METRIC	WEIGHT	FLAGS	INTERFACE	PATH MONITORING (FAIL ON)	STATUS
0.0.0.0/0	10.10.10.11	10		S	ethernet1/4	Enabled(Any)	● Down

Next Steps

If you want to implement this in your environment and would be more comfortable having someone with experience help you in the process, contact your Sun Management account rep to schedule one of our certified Palo Alto Networks engineers to assist with setting up ISP redundancy on the firewall.

If you want to test this on your own and do not have access to a lab environment to do so, contact your Sun Management account rep to get pricing on a lab bundle. The PA-220 and VM-50 appliances are excellent platforms for testing things such as this and there are specific part numbers for lab equipment that are more heavily discounted than the same appliance for use in production.

Sun Management

Sun Management is a Value Added Reseller (VAR) focusing on Network and Internetwork Security Requirements. We work primarily in the Mid Atlantic area: Maryland (MD), Virginia (VA), District of Columbia (DC), West Virginia (WV), Delaware (DE) and Pennsylvania (PA). Our credentials include Palo Alto Networks Services Provider, Palo Alto Networks Certified Training Partner, and Palo Alto Networks Certified Managed Security Service Provider (MSSP) using CORTEX XSOAR in a multi-tenant environment.

We address requirements concerning Network Detection and Response (NDR); internal and external TLS and SSL requirements for complete data visibility; End Point Detection and Response (EDR); Gramm Leach Bliley Act, HIPPA, Sarbanes Oaxley and PCI DSS; penetration testing and firewall optimization; and Data Protection by tracking all Data Flows within the network, across applications, between users/servers and in the cloud. Contact us at (888) 773-9422 to setup a POC or if you just want more

Resource Links:

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PLL8CAO

https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/networking/static-routes/configure-path-monitoring-for-a-static-route.html