Configuring Policy-Based Routing (PBR) with IP SLA Tracking - Auto Redirecting Traffic

Written by: Administrator. Posted in: Cisco Routers - Configuring Cisco Routers (Cisco-technical-knowledgebase/cisco-routers.html)

What is Policy-Based Routing?

Policy-Based Routing (PBR) is a very popular feature in Cisco routers, it allows the creation of policies that can selectively alter the path that packets take within the network. Policy-Based Routing can be used to mark packets so that certain types of traffic are prioritized over the rest, sent to a different destination or exist via a different physical interface on the router.

Classification of interesting traffic is performed using Access-Control Lists (ACLs). These can be standard, extended or named access lists as we know them.

Once the interesting traffic is 'matched' with the use of ACLs, the router will perform the configured 'set' function which is defined by the Administrator. This 'set' function essentially tells the router what to do with the matched traffic and can include sending it to another gateway, dropping it, prioritizing it over other traffic, and much more.

Policy-Based Routing with IP SLA Monitoring for Automatic Fail-Over

This article will show how to use Policy-Based Routing to mark a specific type of traffic, for example http, and redirect it to a web proxy (usually Linux Squid) so all network web traffic is automatically filtered through the proxy.

In such setups, network users have no knowledge of the proxy’s existence as they are not required to configure their web browser to use the proxy. All user traffic is forwarded to a single gateway (Cisco ASA Firewall) and from there to router R1. This example is good solution for creating a transparent proxy with automatic failover.
Router R1, with the help of Policy-Based Routing, ‘marks’ all http traffic and then performs the appropriate ‘set’ function, which is to redirect the selected traffic to the Linux proxy with IP address 192.168.150.2.

The Linux proxy accepts the traffic, makes the necessary checks defined by the Administrator and forwards it to the Internet via R2 router.

To complement our solution we’ve added IP SLA tracking so that R1 will continuously monitor the Linux proxy to ensure it has not failed or gone offline. If for any reason router R1 loses connectivity with the Linux proxy, the IP SLA & Policy-Based Routing mechanism will stop redirecting http traffic to it and forward it directly to the Internet via R2, effectively bypassing the failed proxy.

The next diagram shows how router R1 will respond to a failure of the Linux proxy as described above:

This solution smartly combines Cisco’s Policy-Based Routing with IP SLA tracking and provides a number of benefits, some of which are:

- Automatic redirection of selected (http) traffic to the Linux Proxy.
- Transparent web proxy to all network users, with web filtering according to company policy.
- Continuous monitoring of proxy after failure – automatic recovery if proxy is back online.

Note: More examples of IP SLA Tracking can be found in our Configuring Static Route Tracking using IP SLA (Basic) ([cisco-technical-knowledgebase/cisco-routers/813-cisco-router-ipsla-basic.html](http://www.firewall.cx/cisco-technical-knowledgebase/cisco-routers/813-cisco-router-ipsla-basic.html)) article.

**HOW TO CONFIGURE IP SLA TRACKING FOR A HOST**

First step is to configure IP SLA tracking for the desired host. This will ensure R1 router will continuously monitor the Linux proxy and stop redirecting http traffic to it in the event it fails:

```
R1(config)# ip sla 1
R1(config-ip-sla)# icmp-echo 192.168.150.2
R1(config-ip-sla)# frequency 4
R1(config-ip-sla)# timeout 2000
R1(config-ip-sla)# threshold 100
R1(config-ip-sla)# ip sla schedule 1 life forever start-time now
```

The above configuration defines and starts an IP SLA probe on router R1.

The ICMP Echo probe sends an ICMP Echo (ping) packet to IP 192.168.150.2 every 4 seconds, as defined by the frequency parameter. Timeout sets the amount of time (in milliseconds) the Cisco IOS IP SLAs operation waits for a response from its request packet. This has been set to 2000 milliseconds, or 2 seconds which gives the host ample time to respond. Threshold sets the rising threshold that generates a reaction event and stores history information for the Cisco IOS IP SLAs operation.

After defining the IP SLA operation, our next step is to define an object that tracks the SLA probe. This can be accomplished by using the IOS Track Object as shown below:

```
R1(config)# track 1 ip sla 1 reachability
```

The above command will track the state of the IP SLA operation. If there are no ping responses from the monitored IP address (192.168.150.2), the track will go down and it will come back up when the IP SLA operation starts receiving ping responses once again.

To verify the track status, use the “show track” command as shown below:
Configuring Policy-Based Routing (PBR) with IP SLA Tracking - Aut...

HOW TO CONFIGURE POLICY-BASED ROUTING TO REDIRECT SELECTED (HTTP) TRAFFIC

Once we have IP SLA up and running the next step is to configure PBR so we can redirect http traffic.

First, we need to use Access-Control Lists to select the traffic we want to redirect. Keep in mind that PBR does not limit the type of ACL that can be used. This means you can use IP named ACLs, standard ACLs, extended ACLs, time-based ACLs and others. In our example we are going to use IP named ACLs:

```
R1(config)# ip access-list extended http-traffic
R1(config)# permit tcp 192.168.5.0 0.0.0.255 any eq www
```

We've decided to name our IP-named ACL 'http-traffic'. This unique ACL name will be used later in our route-map. By making the appropriate changes in the ACLs we can define different types of traffic that will be redirected. In our example all http traffic from the 192.168.5.0 network that is destined to the Internet (any) is selected.

Now we must create a route-map that will use the above defined ACLs and instruct the router to redirect the traffic to the Linux proxy:

```
R1(config)# route-map linux-proxy permit 1
R1(config-route-map)# match ip address http-traffic
R1(config-route-map)# set ip next-hop verify-availability 192.168.150.2 1 track 1
```

The above command creates a permissive route-map named linux-proxy. The match IP address parameter within the route-map informs the router which set of ACLs defines the traffic we are interested in. Since we've defined our interesting traffic using IP named ACLs, all we need to do is reference the name of our ACL previously created.

The last command configures the route map to verify the reachability of the tracked object (192.168.150.2). If the tracked object is reachable (IP SLA reports it is reachable, then our policy-based route will redirect the defined traffic to it). If the tracked object is not reachable, (IP SLA reports the host is not reachable - down) then our policy-based route will stop redirecting traffic.

APPLYING THE POLICY-BASED ROUTE

We are almost done. The very last step is to enable and identify the route-map to be use for policy routing. This is performed by selecting the router interface for which the policy routing will be enabled, and applying the policy-route:

```
R1(config-if)# interface Vlan1
R1(config-if)# ip policy route-map linux-proxy
```

In our scenario, R1's VLAN1 interface is connected to the 192.168.150.0/24 network where our ASA and Linux proxy reside so we apply the policy routing to that.

ROUTE-MAP & IP SLA STATISTICS

Keeping a close eye on the router's route-map & IP SLA performance can be achieved with the use of a few simple commands. Monitoring your route-map's performance the first couple of days is a very good idea as it will help verify that traffic is still being redirected to the host.

On the other hand, looking at IP SLA statistics will help identify possible failures or changes of state which were not noticed by anyone.

The `show route-map` command is a favourite as it combines enough information to help verify everything is working as it should:

```
R1# show route-map
route-map linux-proxy, permit, sequence 1
Match clauses:
ip address (access-lists): http-traffic
Set clauses:
ip next-hop verify-availability 192.168.150.10 1 track 1 [up]
Policy routing matches: 3864291 packets, 511957007 bytes
```

The numbers shown here verify immediately that our host is reachable (up) and that R1 has redirected more than 510MB of traffic through the Linux proxy!

The `show IP SLA statistics` command provides in a similar way useful information that helps verify the object tracking is working correctly and the tracked host is up:

```
R1# show ip sla statistics
```

The command output verifies that the tracked object is UP and has a response time of 1ms. A closer look shows that for the duration of the tracking, the state has changed 30 times and the last change was 1 day and 8 hours ago. This information is extremely important should it be necessary to troubleshoot intermittent problems that might be reported by the users.
Configuring Policy-Based Routing (PBR) with IP SLA Tracking - Aut...
Configuring Policy-Based Routing (PBR) with IP SLA Tracking - Aut...

http://www.firewall.cx/cisco-technical-knowledgebase/cisco-routers/8...