How do I configure Policy Based Routing (PBR) on a Cisco Multilayer Switch or Router to forward traffic to the WSA?

Document ID: 118156

Contributed by Vladimir Sousa and Siddharth Rajpathak, Cisco TAC
Engineers.

Aug 05, 2014

Contents

Question:

Question:

How do I configure Policy Based Routing (PBR) on a Cisco Multilayer Switch or Router to forward traffic to the WSA?

Environment: Cisco Web Security appliance (WSA), transparent mode − L4 switch

When WSA is configured in transparent mode using a L4 switch, no configuration is needed on the WSA. The redirection is controlled by the L4 switch (or router).

It is possible to use Policy Based Routing (PBR) to redirect web traffic to the WSA. This is achieved by matching the correct traffic (based on tcp ports) and instructing the router/switch to redirect this traffic to the WSA.

In the following example, WSA's data/proxy interface (either M1 or P1 depending on configuration) is on a dedicated VLAN interface of the multilayer switch/router (Vlan 3) and the Internet router is on a dedicated VLAN interface as well (Vlan4). Clients are on Vlan1 and Vlan2.

Initial Configuration (only relevant parts displayed)

```
interface Vlan1
desc User VLAN 1
ip address 10.1.1.1 255.255.255.0
!
interface Vlan2
desc User VLAN 2
ip address 10.1.2.1 255.255.255.0
!
interface Vlan3
desc Cisco WSA dedicated VLAN
ip address 192.168.1.1 255.255.255.252
!
```

```
interface Vlan4
desc Internet Router dedicated VLAN
ip address 192.168.2.1 255.255.255.252
!
ip route 0.0.0.0 0.0.0.0 192.168.2.2
```

Given the above example, and Cisco WSA having an IP address of 192.168.1.2, you would add the following commands to set up Policy Based Routing (PBR):

Step 1: Define Web traffic

```
! Match HTTP traffic
access−list 100 permit tcp 10.1.1.0 0.0.0.255 any eq 80
access−list 100 permit tcp 10.1.2.0 0.0.0.255 any eq 80
! Match HTTPS traffic
access−list 100 permit tcp 10.1.1.0 0.0.0.255 any eq 443
access−list 100 permit tcp 10.1.2.0 0.0.0.255 any eq 443
```

Step 2: Define a route map to control where packets are output.

```
 route−map ForwardWeb permit 10
 match ip address 100
 set ip next−hop 192.168.1.2
```

Step 3: Apply the route map to the correct interface.

```
!Note that this should be applied to the source interface (client side)
interface Vlan1
ip policy route−map ForwardWeb
!
interface Vlan2
ip policy route−map ForwardWeb
```

Note: This method of traffic redirection (PBR) has some limitations. The main problem with this method is that traffic will always be redirected to the WSA even if the appliance is not reachable (due to network problems for instance). So, there is no fail over option.

To workaround this deficiency, you may configure either of the following:

1. ***PBR with tracking options*** when using Cisco Routers. This feature is used to verify the availability of the next hop before redirecting traffic.

   More details on the following article:
   Policy Based Routing with the Multiple Tracking Options Feature Configuration Example
2. Tracking options are not available for Cisco Catalyst Switches. However, there's an advanced workaround available to achieve the same behavior.

   Details can be found on the following Cisco Wiki:
   Policy−based Routing (PBR) with tracking for Catalyst 3xxx switches − A workaround using EEM