
Policy Based Routing

Advanced Routing

daniel.juarez@iteso.mx, enrique.rios@iteso.mx, TEAM: 5

2024-10-06

Contents

1	Contextualization	1
1.1	Network Topology	1
1.2	Objectives	2
2	Methodology	3
3	PoC	5
3.1	Access lists	5
3.2	Route maps	6
3.3	Trace from each pc to the file server	7
4	Team Findings and Member's conclusions	11
5	References	12

1 Contextualization

Policy Based Routing is defined as a series of prewritten rules on a router in a way that overrides its routing table to satisfy the routing rules defined on a policy. PBR rules set packets to a route map based on the packet's metadata, rules can be applied to certain protocol, port or address, then based on a policy, the packet will be sent through a certain route overriding the routing table.

This report covers the configuration steps and implementation of Policy Based Routing. It is assumed there is an IPv4 WAN already configured working with the EIGRP routing protocol. The topology where PBR concepts will be applied illustrates that there are two departments connected to Guadalajara's gateway, where this router is directly connected to 4 WAN providers. The objective is to redirect each department's traffic to its corresponding WAN provider.

1.1 Network Topology

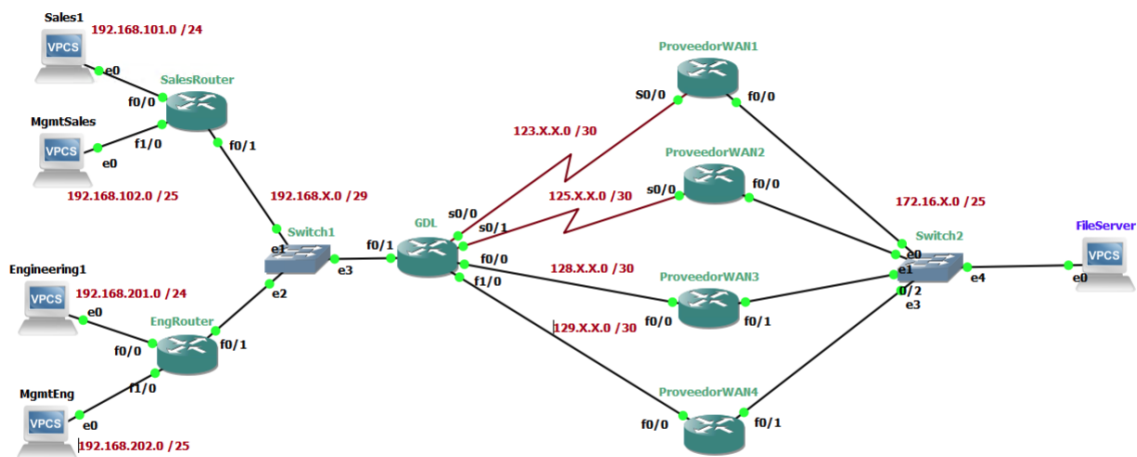


Figure 1.1: PBR topology

1.2 Objectives

- To configure and apply policy based routing.
- Redirect traffic for each department through its corresponding WAN provider.

2 Methodology

The selection of the router that will redirect network traffic must be done based on the objective, in this case, certain traffic must be redirected to a certain WAN route, the only router with such capability within the topology is GDL's router, since it is directly connected to all WAN providers.

To configure a PBR on a cisco router, it is required to set up access lists to target traffic of interest, then create a route map that will be configured to redirect to a certain hop all traffic that matches the access lists' criteria[1].

- Create an access list (or a set of them):

```
access-list {id} permit ip {ipv4} any
```

In the topology's case on GDL router:

```
access-list 101 permit ip 192.168.101.0 0.0.0.255 any
access-list 102 permit ip 192.168.102.0 0.0.0.127 any
access-list 103 permit ip 192.168.201.0 0.0.0.255 any
access-list 104 permit ip 192.168.202.0 0.0.0.127 any
```

- Set up a route map and name it:

```
route-map {name}
```

- The router's CLI will change its mode, match a certain access list and set a hop to send the target traffic:

```
match ip address {access-list id}
set ip next-hop {next gateway}
```

A cisco router only supports one route map per port, so it is needed to set up a single route map with different rules, the router will automatically detect that route maps are different

```
route-map PBR-Sales-Eng
match ip address 101
set ip next-hop 123.5.5.2

route-map PBR-Sales-Eng
match ip address 102
set ip next-hop 125.5.5.2

route-map PBR-Sales-Eng
match ip address 103
set ip next-hop 128.5.5.2

route-map PBR-Sales-Eng
match ip address 104
set ip next-hop 129.5.5.2
```

- Apply the created policies to the desired interfaces:

```
in {interface}
ip policy route-map {policy name}
```

Applied to our case:

```
ip policy route-map PBR-Sales-Eng
```

3 PoC

3.1 Access lists

```
File Edit Tabs Help
GDL#
GDL#
GDL#
GDL#
GDL#
GDL#
GDL#
GDL#
GDL#
GDL#
GDL#
GDL#
GDL#
GDL#
GDL#
GDL#
GDL#
GDL#
GDL#
GDL#
GDL#
GDL#
GDL#
GDL#sh acc
GDL#sh acce
GDL#sh access-
GDL#sh access-1
GDL#sh access-lists
Extended IP access list 101
    10 permit ip 192.168.101.0 0.0.0.255 any
Extended IP access list 102
    10 permit ip 192.168.102.0 0.0.0.127 any
Extended IP access list 103
    10 permit ip 192.168.201.0 0.0.0.255 any
Extended IP access list 104
    10 permit ip 192.168.202.0 0.0.0.127 any
GDL#
GDL#
GDL#
GDL#
GDL#
GDL#
GDL#
GDL#
GDL#
```

Figure 3.1: access list on GDL

3.2 Route maps

```
File Edit Tabs Help
GDL(config-if)#
GDL(config-if)#
GDL(config-if)#
GDL(config-if)#
GDL(config-if)#
GDL(config-if)#
GDL(config-if)#
GDL(config-if)#
GDL(config-if)#
GDL(config-if)#
GDL(config-if)#
GDL(config-if)#
GDL(config-if)#
GDL(config-if)#
GDL(config-if)#
GDL(config-if)#
GDL(config-if)#
GDL(config-if)#
*Mar  1 00:14:27.495: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
GDL(config-if)#do sh route-map
route-map PBR-Sales-Eng, permit, sequence 10
  Match clauses:
    ip address (access-lists): 101
  Set clauses:
    ip next-hop 123.5.5.2
  Policy routing matches: 0 packets, 0 bytes
route-map PBR-Sales-Eng, permit, sequence 20
  Match clauses:
    ip address (access-lists): 102
  Set clauses:
    ip next-hop 125.5.5.2
  Policy routing matches: 0 packets, 0 bytes
route-map PBR-Sales-Eng, permit, sequence 30
  Match clauses:
    ip address (access-lists): 103
  Set clauses:
    ip next-hop 128.5.5.2
  Policy routing matches: 0 packets, 0 bytes
route-map PBR-Sales-Eng, permit, sequence 40
  Match clauses:
    ip address (access-lists): 104
  Set clauses:
    ip next-hop 129.5.5.2
  Policy routing matches: 0 packets, 0 bytes
GDL(config-if)#
```

Figure 3.2: route maps on GD

3.3 Trace from each pc to the file server

```
File Edit Tabs Help
Trying 100.88.96.25...
Connected to 100.88.96.25.
Escape character is '^['.

Welcome to Virtual PC Simulator, version 1.3 (0.8.1)
Dedicated to Daling.
Build time: Feb 22 2024 06:25:41
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
Copyright (c) 2021, Alain Degreffe (alain.degreffe@eve-ng.net)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Modified version for EVE-NG.

Press '?' to get help.

Executing the startup file

Checking for duplicate address...
VPCS : 192.168.101.2 255.255.255.0 gateway 192.168.101.1

VPCS> trace 172.16.5.5
trace to 172.16.5.5, 8 hops max, press Ctrl+C to stop
 1  192.168.101.1   9.540 ms  9.562 ms  9.295 ms
 2  192.168.5.3   29.534 ms 29.930 ms 30.178 ms
 3  123.5.5.2    50.276 ms 50.427 ms 50.435 ms
 4  **172.16.5.5  35.736 ms (ICMP type:3, code:3, Destination port unreachable)

VPCS> █
```

Figure 3.3: Sales

```
File Edit Tabs Help
Trying 100.88.96.25...
Connected to 100.88.96.25.
Escape character is '^]'.

Welcome to Virtual PC Simulator, version 1.3 (0.8.1)
Dedicated to Daling.
Build time: Feb 22 2024 06:25:41
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
Copyright (c) 2021, Alain Degreffe (alain.degreffe@eve-ng.net)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Modified version for EVE-NG.

Press '?' to get help.

Executing the startup file

Checking for duplicate address...
VPCS : 192.168.102.2 255.255.255.128 gateway 192.168.102.1

VPCS> trace 172.16.5.5
trace to 172.16.5.5, 8 hops max, press Ctrl+C to stop
 1  192.168.102.1   9.145 ms  10.058 ms  9.605 ms
 2  192.168.5.3   30.128 ms  30.014 ms  19.726 ms
 3  125.5.5.2    39.775 ms  50.423 ms  39.649 ms
 4  **172.16.5.5  65.058 ms (ICMP type:3, code:3, Destination port unreachable)

VPCS> █
```

Figure 3.4: MgmSales

```
File Edit Tabs Help
Trying 100.88.96.25...
Connected to 100.88.96.25.
Escape character is '^]'.

Welcome to Virtual PC Simulator, version 1.3 (0.8.1)
Dedicated to Daling.
Build time: Feb 22 2024 06:25:41
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
Copyright (c) 2021, Alain Degreffe (alain.degreffe@eve-ng.net)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.co.cn.
Modified version for EVE-NG.

Press '?' to get help.

Executing the startup file

Checking for duplicate address...
VPCS : 192.168.201.2 255.255.255.0 gateway 192.168.201.1

VPCS> trace 172.16.5.5
trace to 172.16.5.5, 8 hops max, press Ctrl+C to stop
 1  192.168.201.1   9.777 ms  9.484 ms  9.631 ms
 2  192.168.5.3   19.618 ms  19.315 ms  19.215 ms
 3  128.5.5.2    30.323 ms  29.819 ms  29.342 ms
 4  **172.16.5.5  36.827 ms (ICMP type:3, code:3, Destination port unreachable)

VPCS> █
```

Figure 3.5: Engineering

```
File Edit Tabs Help
Trying 100.88.96.25...
Connected to 100.88.96.25.
Escape character is '^['.

Welcome to Virtual PC Simulator, version 1.3 (0.8.1)
Dedicated to Daling.
Build time: Feb 22 2024 06:25:41
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
Copyright (c) 2021, Alain Degreffe (alain.degreffe@eve-ng.net)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Modified version for EVE-NG.

Press '?' to get help.

Executing the startup file

Checking for duplicate address...
VPCS : 192.168.202.2 255.255.255.128 gateway 192.168.202.1

VPCS> trace 172.16.5.5
trace to 172.16.5.5, 8 hops max, press Ctrl+C to stop
 1  192.168.202.1   8.922 ms  9.851 ms  8.987 ms
 2  192.168.5.3   29.713 ms 30.300 ms 30.038 ms
 3  129.5.5.2    49.760 ms 50.568 ms 50.488 ms
 4  **172.16.5.5  55.015 ms (ICMP type:3, code:3, Destination port unreachable)

VPCS> █
```

Figure 3.6: MgmEngineering

4 Team Findings and Member's conclusions

Juarez Mota Daniel Alejandro: Policy Based Routing was not only a difficult concept to learn but also to apply, given its simplicity, yet it was necessary in the real world. One of the applications I found is the smart selection of traffic. It could, for instance, be applied in a VPN scenario where certain traffic must be encrypted, but for some other type, encryption might not be required. I did not have complications with theoretical concepts or with their implementation, given that PBR is also intuitive.

Jose Enrique Rios Gomez: Policy-Based Routing is not a particularly complex topic, but it was challenging to apply. Even though I knew the commands and the theory, I struggled with where to implement them. I initially thought that the PBR commands should be applied near the VPCs, but I was mistaken. Instead, they needed to be applied closer to the providers, as PBR redirects packets based on route maps.

5 References

[1]

“Policy-Based Routing (PBR) Explained,” CBT Nuggets. <https://www.cbtnuggets.com/blog/technology/networking/policy-based-routing-pbr-explained>