Policy Based Routing

This chapter describes how to configure FTD to support policy based routing (PBR) through FMC's Policy based Routing page. The following sections describe policy based routing, guidelines for PBR, and configuration for PBR.

About Policy Based Routing

In traditional routing, packets are routed based on the destination IP address. However, it is difficult to change the routing of specific traffic in a destination-based routing system. Policy Based Routing (PBR) gives you more control over routing by extending and complementing the existing mechanisms provided by routing protocols.

PBR allows you to set the IP precedence. It also allows you to specify a path for certain traffic, such as priority traffic over a high-cost link. With PBR, you can define routing that is based on criteria other than destination network such as source port, destination address, destination port, protocol, applications, or a combination of these objects.

You can use PBR to classify the network traffic based on applications. This routing method is applicable in scenarios where, numerous devices access applications and data in a large network deployment. Traditionally, large deployments have topologies that backhaul all the network traffic to a hub as encrypted traffic in a route-based VPN. These topologies often result in issues such as packet latency, reduced bandwidth, and packet drop. Overcoming these issues involves high-cost complex deployments and management.

PBR policy enables you to securely breakout traffic for specified applications. You can configure PBR policy in the Firepower Management Center user interface to allow the applications to be directly accessed.

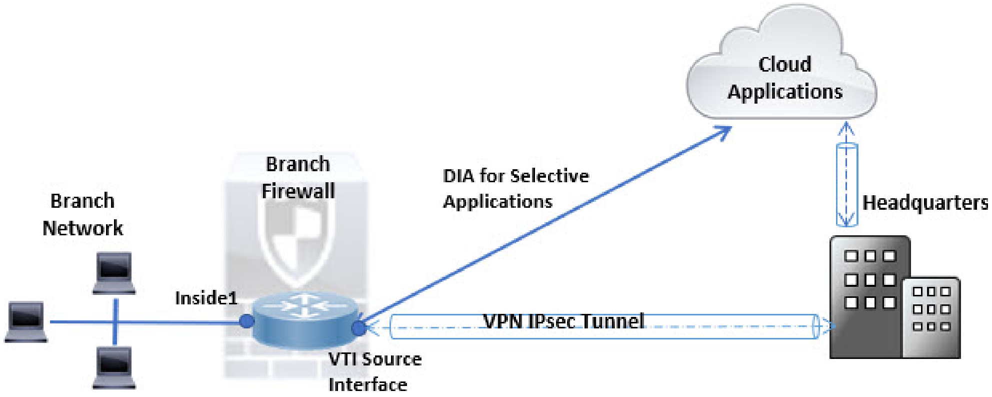
Why Use Policy Based Routing

Consider a company that has two links between locations: one a high-bandwidth, low-delay expensive link, and the other a low-bandwidth, higher-delay, less-expensive link. While using traditional routing protocols, the higher-bandwidth link gets most, if not all, of the traffic sent across it based on the metric savings obtained by the bandwidth, delay, or both (using EIGRP or OSPF) characteristics of the link. With PBR, you can route higher priority traffic over the high-bandwidth/low-delay link, while sending all other traffic over the low-bandwidth/high-delay link.

Following are a few scenarios where you can use Policy Based Routing:

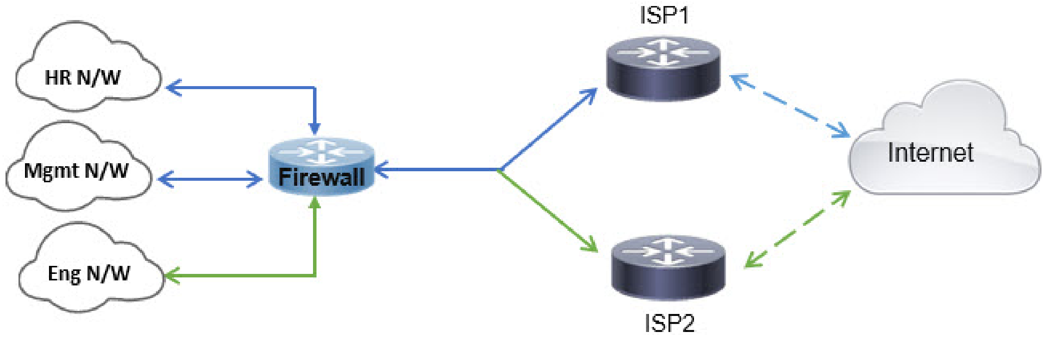
Direct Internet Access

In this topology, application traffic from the branch office can be routed directly to the internet instead of through the VPN tunnel connecting to the headquarters. The branch FTD is configured with an internet exit point and the PBR policy is applied on the ingress interface (*Inside 1*) to identify the traffic based on the applications defined in the ACL. Correspondingly, the traffic is forwarded through the egress interfaces directly to the internet or to the IPsec VPN tunnel.



Equal-Access and Source-Sensitive Routing

In this topology, traffic from the HR and Mgmt networks can be configured to go through ISP1 and traffic from Eng network can be configured to go through ISP2. Thus, policy based routing enables the network administrators to provide equal-access and source-sensitive routing, as shown here.



Load Sharing

In addition to the dynamic load-sharing capabilities offered by ECMP load balancing, network administrators can now implement policies to distribute traffic among multiple paths based on the traffic characteristics.

As an example, in the topology depicted in the Equal-Access Source Sensitive Routing scenario, an administrator can configure policy based routing to route the traffic from HR network through ISP1 and traffic from Eng network through ISP2 and thus share the load.

Guidelines and Limitations for Policy Based Routing

Firewall Mode Guidelines

PBR is supported only on routed firewall mode.

Device Guidelines

- PBR through FMC's Policy Based Routing page is supported only from Version 7.1+ on both the FMC and the device.
- When you upgrade FMC or Firepower Threat Defense to version 7.1 and higher, the PBR configuration in the device is removed. You must configure PBR again using the Policy Based Routing page. If the managed device is lower than version 7.1, you must configure PBR again using FlexConfig with deploy option set to "every time."
- Configuring application based PBR policy on cluster devices is not supported.

Interface Guidelines

- Only routed interfaces and non management-only interfaces belonging to the Global virtual router can be configured as ingress or egress interface.
- PBR is not supported on user-defined virtual routers.
- Only interfaces that have a logical name can be defined in the policy.
- Static VTIs can be configured only as egress interfaces.
- Before proceeding with configuration, ensure that the ingress and egress traffic of each session flows through the same ISP-facing interface to avoid unexpected behavior caused by asymmetric routing, specifically when NAT and VPN are in use.

IPv6 Support

PBR supports IPv6.

Application-Based PBR and DNS Configuration

- Application-based PBR uses DNS snooping for application detection. Application detection succeeds only if the DNS requests pass through FTD in a clear-text format; the DNS traffic is not encrypted.
- You must configure trusted DNS servers.

For more information on configuring DNS servers, see DNS.

PBR Policies Not Applied for Output Route Look-up

Policy Based Routing is an ingress-only feature; that is, it is applied only to the first packet of a new incoming connection, at which time the egress interface for the forward leg of the connection is selected. Note that PBR will not be triggered if the incoming packet belongs to an existing connection, or if NAT is applied and NAT chooses the egress interface.

PBR Policies Not Applied for Embryonic Traffic

Note An embryonic connection is where the necessary handshake between source and destination has not been made.

When a new internal interface is added and a new VPN policy is created using a unique address pool, PBR is applied to the outside interface matching the source of the new client pool. Thus, PBR sends traffic from the client to the next hop on the new interface. However, PBR is not involved in the return traffic from a host that has not yet established a connection with the new internal interface routes to the client. Thus, the return traffic from the host to the VPN client, specifically, the VPN client response is dropped as there is no valid route. You must configure a weighted static route with a higher metric on the internal interface.

Additional Guidelines

- All existing configuration restrictions and limitations of route map will be carried forward.
- While defining the ACL for the policy match criteria, you can select multiple applications from a list of predefined applications to form an Access Control Entry (ACE). In FTD, the predefined applications are stored as Network Service objects and the group of applications as Network Service Groups (NSG). The application or network service group is detected through first-packet classification. Currently, you cannot add to or modify the predefined applications list.
- Unicast Reverse Path Forwarding (uRPF) validates the source IP address of packets received on an interface against the routing table and not against the PBR route map. When uRPF is enabled, packets received on an interface through PBR are dropped as they are without the specific route entry. Hence, when using PBR, ensure to disable uRPF.

Configure Policy-Based Routing Policy

You can configure the PBR policy on the Policy Based Routing page by specifying the ingress interfaces, match criteria (Extended Access Control List), and egress interfaces.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the FTD device.

Step 2 Click **Routing**.

Step 3 Click **Policy Based Routing**.

The Policy Based Routing page displays the configured policy. The grid displays the list of ingress interfaces and a combination of the policy-based route access list, and egress interfaces.

Step 4 To configure the policy, click **Add**.

Step 5 In the **Add Policy Based Route** dialog box, select the **Ingress Interface** from the drop-down list.

Note Only interfaces that have logical names and that belong to a global virtual router are listed in the drop-down.

Step 6 To specify the match criteria and the forward action in the policy, click **Add**.

Step 7 In the **Add Forwarding Actions** dialog box, do the following:

a) From the **Match ACL** drop-down, choose the extended access control list object. You can predefine the ACL object (see Configure Extended ACL Objects) or click the **Add** (+) icon to create the object. In the **New Extended Access List Object** box, enter a name, click **Add** to open the **Add Extended Access List Entry** dialog box, where you can define the network, port, or application match criteria for the PBR policy.

Note You cannot have both application and destination address defined in an ACE.

To selectively apply PBR on the incoming interface, you can define *Block* criteria in the ACE. When the traffic matches the block rule of the ACE, the traffic is forwarded to the egress interface based on the routing table.

b) From the **Send To** drop-down list:

- To select the configured interfaces, choose **Egress Interfaces**.
- To specify the IPv4/IPv6 next hop addresses, choose **IP Address**. Proceed to Step 7.e, on page 5

c) If you have selected **Egress Interfaces**, from the **Interface Ordering** drop-down, choose the relevant option:

- By **Interface Priority**—The traffic is forwarded based on the priority of the interfaces. Traffic is routed to the interface with the least priority value first. When the interface is not available, the traffic is then forwarded to the interface with the next lowest priority value. For example, let us assume that *Gig0/1*, *Gig0/2*, and *Gig0/3* are configured with priority values *0*,*1*, and *2* respectively. The traffic is forwarded to *Gig0/1*. If *Gig0/1* becomes unavailable, the traffic is then forwarded to *Gig0/2*.

  Note To configure the priority for the interfaces, click **Configure Interface Priority** on the Policy Based Routing page. In the dialog box, provide the priority number against the interfaces, and then click **Save**. You can also configure the priority for an interface in the Interface Settings.

  When the priority value is the same for all the interfaces, the traffic is balanced among the interfaces.

- By **Order**—The traffic is forwarded based on the sequence of the interfaces specified here. For example, let us assume that *Gig0/1*, *Gig0/2*, and *Gig0/3* are selected in the following order, *Gig0/2*, *Gig0/3*, *Gig0/1*. The traffic is forwarded to *Gig0/2* first, then to *Gig0/3*, irrespective of their priority values.

d) In the **Available Interfaces** box, all the interfaces with their priority values are listed. From the list of interfaces, click the **Add** (⊕) button to add to the selected egress interfaces. Proceed to Step 7.f, on page 5

e) If you have selected **IP Address**, enter the IP addresses separated by commas in the **IPv4 Addresses** or **IPv6 Addresses** fields. The traffic is forwarded as per the sequence of the specified IP addresses.

f) Click **Save**.

Step 8 To save the policy, click **Save** and **Deploy**.

The FTD uses ACLs to match traffic and perform routing actions on the traffic. Typically, you configure a route map that specifies an ACL against which traffic is matched, and then you specify one or more actions for that traffic. Finally, you associate the route map with an interface on which you want to apply PBR on all incoming traffic.

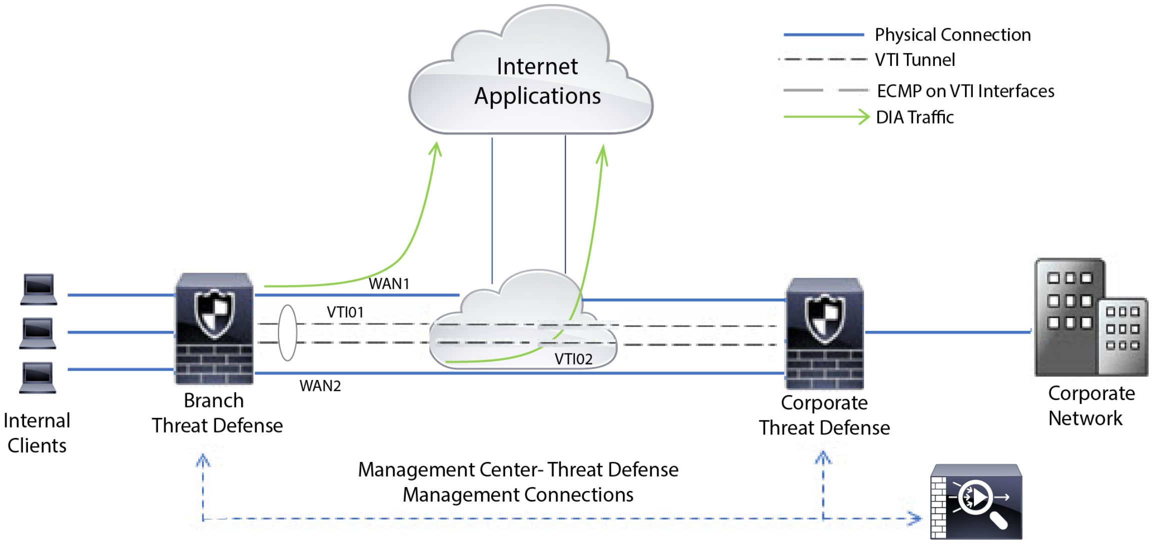
Configuration Example for Policy Based Routing

Consider a typical corporate network scenario where all the branch network traffic passes through a route-based VPN of the corporate network and diverges to the extranet, when required. Accessing the web-based applications that address day-to-day operations through the corporate network results in huge network expansion and maintenance costs. This example illustrates the PBR configuration procedure for direct internet access.

The following figure depicts the topology of a corporate network. The branch network is connected to the corporate network through a route-based VPN. Traditionally, the corporate FTD is configured to handle both the internal and external traffic of the branch office. With the PBR policy, the branch FTD is configured with a policy that routes specific traffic to the WAN network instead of the virtual tunnels. The rest of the traffic flows through the route-based VPN, as usual.

This example also illustrates the configuring of the WAN and the VTI interfaces with ECMP zones to achieve load balancing.

Figure 1: Configuring Policy Based Routing on Branch FTD in FMC



Before you begin

This example assumes that you have already configured WAN and VTI interfaces for the branch FTD in FMC.

Procedure

Step 1 Configure policy based routing for the branch FTD, select the ingress interfaces:

a) Choose **Devices** > **Device Management**, and edit the FTD device.

b) Choose **Routing** > **Policy Based Routing**, and on the **Policy Based Routing** page, click **Add**.

c) In the **Add Policy Based Route** dialog box, select the interfaces (say, *Inside 1*, and *Inside 2*) from the **Ingress Interface** drop-down list.

Step 2 Specify the match criteria:

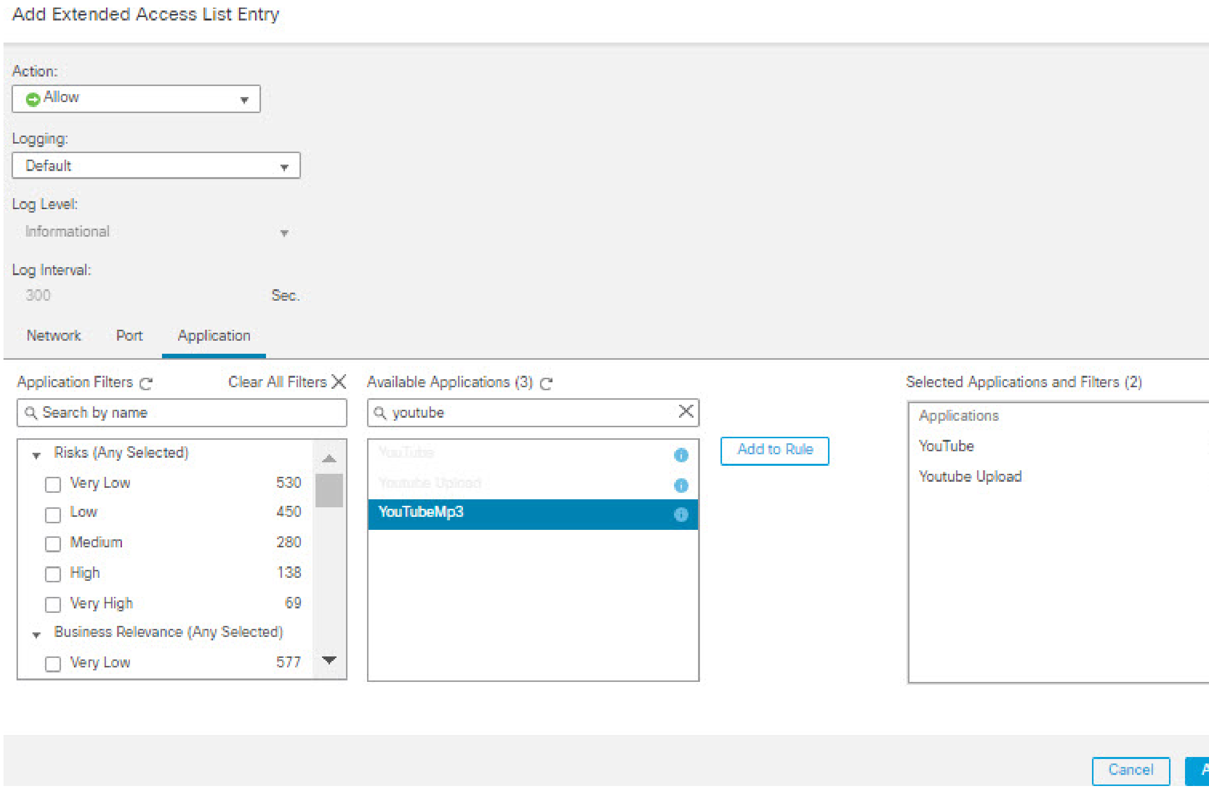
a) Click **Add**.

b) To define the match criteria, click the **Add** (+) button.

c) In **New Extended Access List Object**, enter the name for the ACL (say, *DIA-FTD-Branch*), and click **Add**.

d) In the **Add Extended Access List Entry** dialog box, choose the required web-based applications from the **Application** tab:

Figure 2: Applications Tab



Add Extended Access List Entry

Action: Allow

Logging: Default

Log Level: Informational

Log Interval: 300 Sec.

Application Filters: Search by name

Risks (Any Selected)	
□ Very Low	530
□ Low	450
□ Medium	280
□ High	138
□ Very High	69
Business Relevance (Any Selected)	
□ Very Low	577

Available Applications (3): youtube

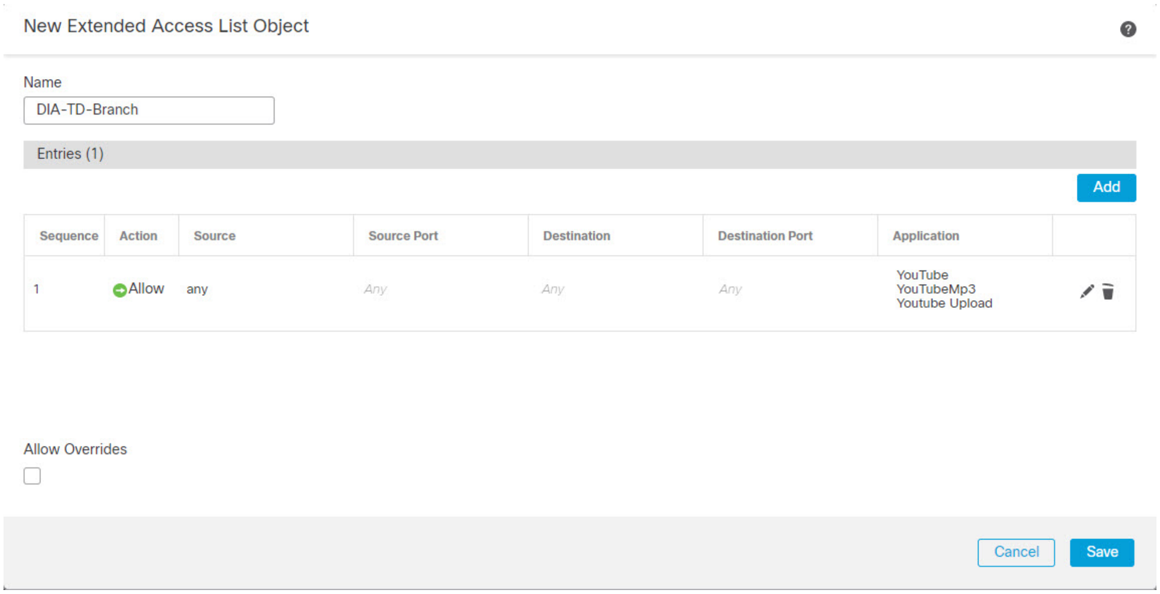
- YouTube
- Youtube Upload
- YouTubeMp3

Selected Applications and Filters (2)

Applications
- YouTube
- Youtube Upload

On the FTD, the application group in an ACL is configured as a network service group and each of the applications as a network service object.

Figure 3: Extended ACL



New Extended Access List Object

Name: DIA-TD-Branch

Entries (1)

Sequence	Action	Source	Source Port	Destination	Destination Port	Application
1	Allow	any	Any	Any	Any	YouTube YouTubeMp3 Youtube Upload

Allow Overrides

□

e) Click **Save**.

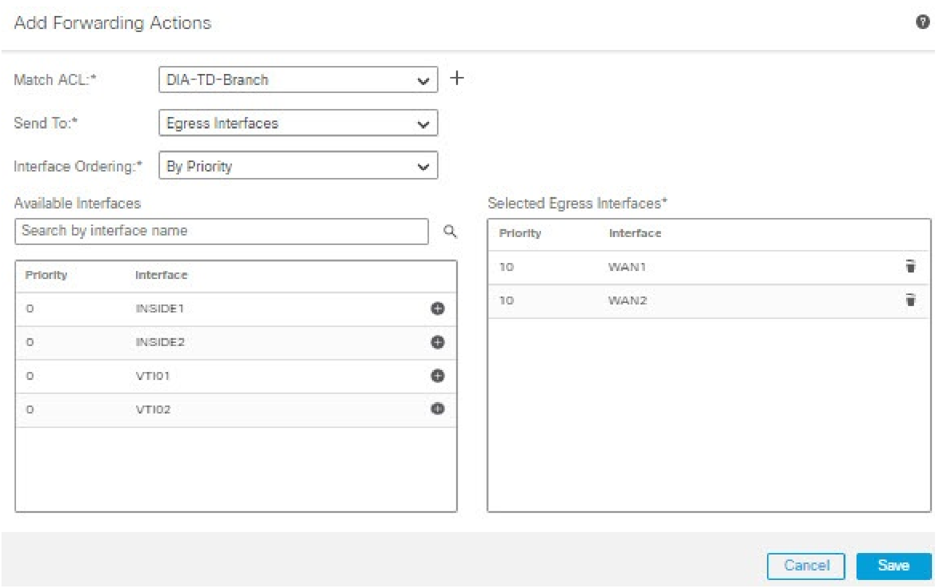
f) Select *DIA-FTD-Branch* from the **Match ACL** drop-down list.

Step 3 Specify the egress interfaces:

a) From the **Send To** and **Interface Ordering** drop-down lists, choose Egress Interfaces, and By Priority respectively.

b) Under **Available Interfaces**, click the ⊕ button against the respective interface names to add *WAN1* and *WAN2*:

Figure 4: Configuring Policy Based Routing



Add Forwarding Actions

Match ACL:* DIA-TD-Branch

Send To:* Egress Interfaces

Interface Ordering:* By Priority

Available Interfaces

Search by interface name

Priority	Interface
0	INSIDE1
0	INSIDE2
0	VTI01
0	VTI02

Selected Egress Interfaces*

Priority	Interface
10	WAN1
10	WAN2

c) Click **Save**.

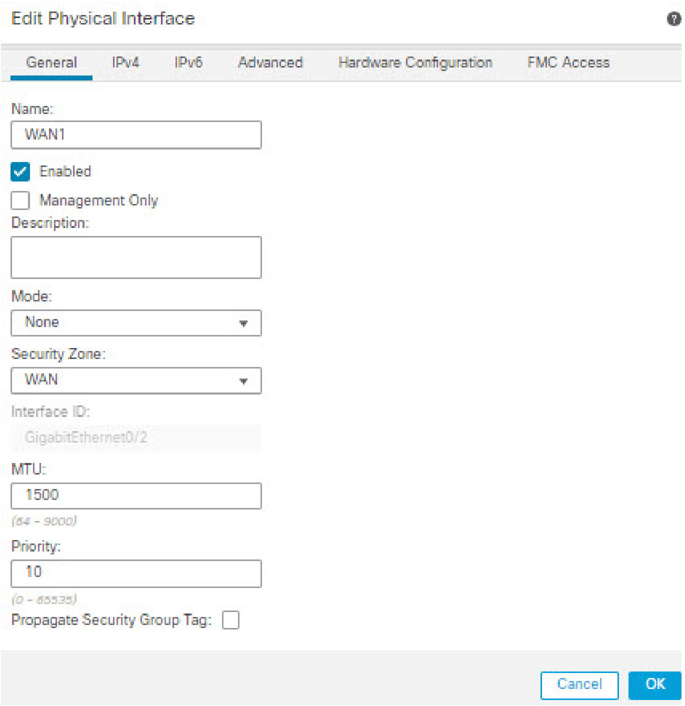
Step 4 Interface priority configuration:

You can set the priority value for the interfaces either in the **Edit Physical Interface** page, or in the **Policy Based Routing** page (**Configure Interface Priority**). In this example, the Edit Physical Interface method is described.

a) Choose **Devices** > **Device Management**, and edit the branch FTD.

b) Set the priority for the interfaces. Click **Edit** against the interface and enter the priority value:

Figure 5: Setting Interface Priority



Name: WAN1

☑ Enabled

□ Management Only

Description:

Mode: None

Security Zone: WAN

Interface ID: GigabitEthernet0/2

MTU: 1500

(64 - 9000)

Priority: 10

(0 - 65535)

Propagate Security Group Tag: □

c) Click **Ok** and **Save**.

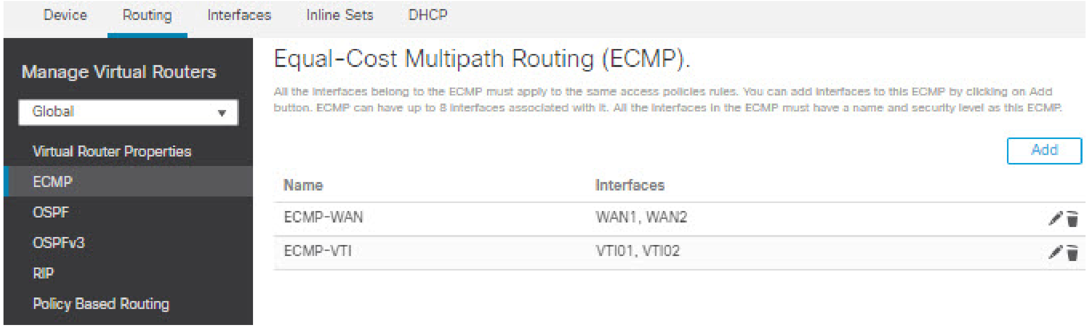
Step 5 Create ECMP zones for load balancing:

a) In the **Routing** page, click **ECMP**.

b) To associate interfaces to the ECMP zone, click **Add**.

c) Select *WAN1* and *WAN 2* and create an ECMP zone—*ECMP-WAN*. Similarly, add *VTI01* and *VTI02* and create an ECMP zone—*ECMP-VTI*:

Figure 6: Associating Interfaces with ECMP Zone



Equal-Cost Multipath Routing (ECMP).

All the interfaces belong to the ECMP must apply to the same access policies rules. You can add interfaces to this ECMP by clicking on Add button. ECMP can have up to 8 interfaces associated with it. All the interfaces in the ECMP must have a name and security level as this ECMP.

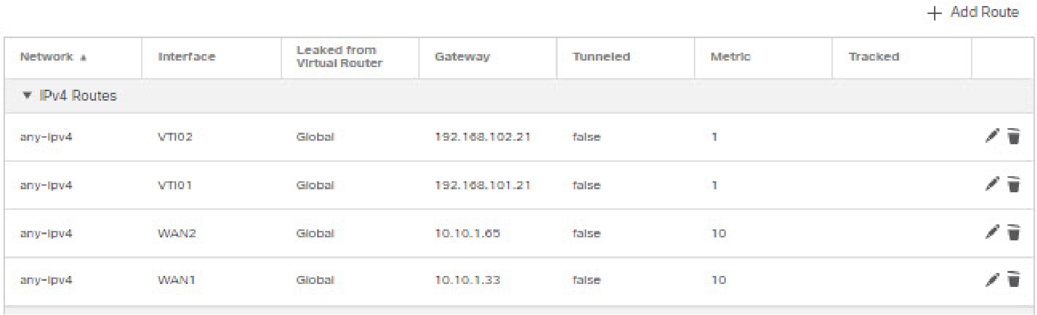
Name	Interfaces
ECMP-WAN	WAN1, WAN2
ECMP-VTI	VTI01, VTI02

Step 6 Configure static routes for the zone interfaces for load balancing:

a) In the **Routing** page, click **Static Route**.

b) Click **Add** and specify the static routes for *WAN1*, *WAN2*, *VTI01*, and *VTI02*. Ensure that you specify the same metric value for the interfaces belonging to the same ECMP zones (Step 5):

Figure 7: Configuring Static Routes for ECMP Zone Interfaces



Network ▲	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
any-ipv4	VTI02	Global	192.168.102.21	false	1	
any-ipv4	VTI01	Global	192.168.101.21	false	1	
any-ipv4	WAN2	Global	10.10.1.65	false	10	
any-ipv4	WAN1	Global	10.10.1.33	false	10	

Note Ensure that the zone interfaces have the same destination address and metric, but different gateway addresses.

Step 7 Configure trusted DNS on the WAN objects of the branch FTD to ensure secured flow of traffic to the internet:

a) Choose **Devices** > **Platform Settings**, and create a DNS policy on the branch FTD.

b) To specify the trusted DNS, **Edit** the policy and click **DNS**.

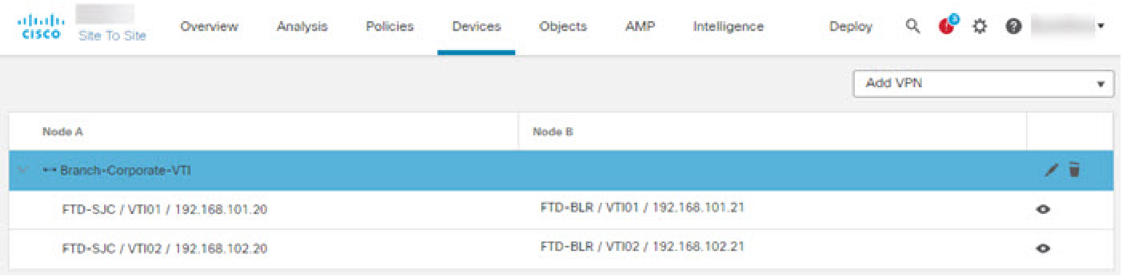
c) To specify the DNS servers for the DNS resolution to be used by WAN objects, in the **DNS Settings** tab, provide the DNS server group details and select WAN from the interface objects.

d) Use the **Trusted DNS Servers** tab to provide specific DNS servers that you trust for the DNS resolution.

Step 8 **Save** and **Deploy**.

Any *YouTube* related access requests from the branch inside network *INSIDE1* or *INSIDE2* are routed to *WAN1* or *WAN2* as they would match the *DIA-FTD-Branch* ACL. Any other request, say *google.com*, are routed through *VTI01* or *VTI02* as configured in the Site to Site VPN Settings:

Figure 8: Site to Site VPN Settings



Node A	Node B
Branch-Corporate-VTI	
FTD-SJC / VTI01 / 192.168.101.20	FTD-BLR / VTI01 / 192.168.101.21
FTD-SJC / VTI02 / 192.168.102.20	FTD-BLR / VTI02 / 192.168.102.21

With the ECMP configured, the network traffic is seamlessly balanced.

History for Policy Based Routing

Table 1:

Feature	Minimum FMC	Minimum FTD	Details
Configure policy based routing from the FMC web interface.	7.1.0	7.1.0	**Upgrade impact. Redo FlexConfigs after upgrade.** You can now configure policy based routing (PBR) from the FMC web interface. This allows you to classify network traffic based on applications and to implement direct internet access (DIA) to send traffic to the internet from a branch deployment. You can define a PBR policy and configure it on ingress interfaces, specifying match criteria and egress interfaces. Network traffic that matches the access control policy is forwarded through the egress interface based on priority or the order as configured in the policy. This feature requires Version 7.1+ on both the FMC and the device. When you upgrade the FMC to Version 7.1+, existing policy based routing FlexConfigs are removed. After you upgrade your devices to Version 7.1+, redo your policy based routing configurations in the FMC web interface. For devices that you do not upgrade to Version 7.1+, redo the FlexConfigs and configure them to deploy "every time." New/modified screens: **Devices** > **Device Management** > **Routing** > **Policy Based Routing**