Enhanced Policy-Based Routing and Site Manager

As network-based applications start being hosted on private or public cloud, network appliances forward network traffic based on configured policies. The enhanced Policy-based Routing (ePBR) routing enables application-based routing. Application-based routing provides a flexible, device-agnostic policy routing solution without impacting application performance.

- Information About Enhanced Policy-Based Routing and Site Manager, on page 1
- Configure Enhanced Policy-Based and Site Manager, on page 4

Information About Enhanced Policy-Based Routing and Site Manager

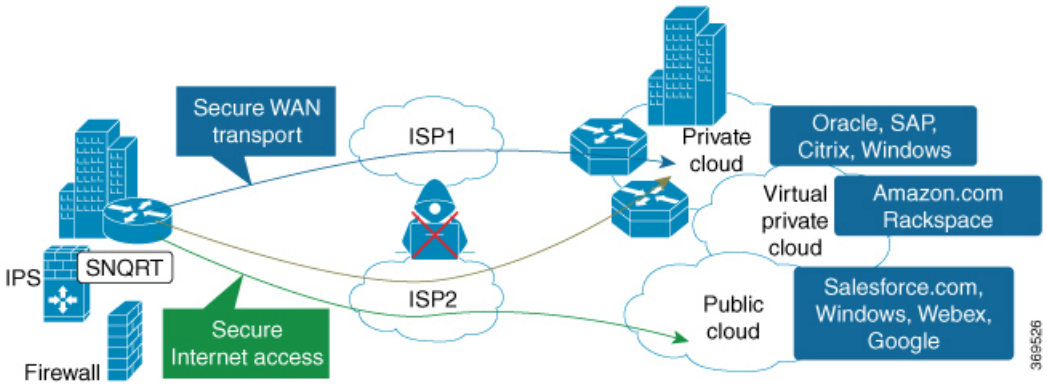
About Enhanced Policy-Based Routing and Site Manager

With central Internet access, all traffic traverses the Dynamic Multipoint VPN (DMVPN) tunnel and is routed to headquarters. This feature allows trusted SaaS traffic to be forwarded out over the optimized path (directly local break out) while other traffic still back-haul to headquarter over VPN.

Network-based Application Recognition version 2 (NBAR2) and Policy-Based Routing (PBR) solution first configures QoS to mark the SaaS application traffic to Differentiated Services Code Point (DSCP) 2, then configures PBR to redirect DSCP 2 traffic to Internet branch router DIA interface. However, this solution does not support flow stickness.

In the Enhanced Policy-Based Routing and Site Manager feature, using Site Manager Direct Cloud Access (DCA) and Direct Internet Access (DIA) you can selectively route cloud services applications such as Google, Salesforce, and Microsoft Office 365 through an Internet path that is specified in the path preference. Non-SaaS traffic can still be back-hauled to data center for further inspection.

Figure 1: Direct Cloud Access (DCA) / Direct Internet Access (DIA)



Site Manager

Site Manager and Border Router

- Site Manager—Site manager is a logical entity that implements specific policies on all border devices in a site. The site manager is also responsible for all policy-based routing and the path performance reported by border devices.

  This site manager has network connections to border routers and may connect to the centralized controller, if configured. You can define policies for the site manager or define policies in a centralized controller and publish to each site. Site-manager use default route as its nexthop address.

- Border Router—A border router is an enterprise WAN edge or internet edge device that connects to the site manager and gets routing information and reports path status. The border router forwards packets according to policy decision. Multiple border routers can be configured on one site and can be connected to the site controller.

The site manager is responsible for all policy-based routing and the path performance reported by a branch router.

Note NBAR classifcation occurs at branch router LAN ingress.

To achieve location proximity and to achieve better application performance, the SaaS server must be close to the branch router. Site Manager DCA uses cisco Umbrella branch to change DNS request from enterprise DNS resolver to a public DNS resolver, such as OpenDNS resolver or Google DNS resolver, which helps in placing the SaaS server closer to the branch router. OpenDNS account and registration is not manadatory. DNS request must be unencrypted traffic from the endpoint to the DNS server.

Prerequisites for Configuring Site Manager

- Cisco Umbrella branch must be enabled. Site Manager DCA uses a default route to determine the next-hop address, Cisco Umbrella is automatically enabled. For Site Manager DIA Cisco Umbrella branch must be enabled to intercept DNS to public DNS resolver.

Restrictions for Configuring Site Manager

- Site Manger does not support IPv6 addresses
- Site manager and Enhanced PBR may not work properly if NBAR does not classify packet properly.
- NBAR may not classify application properly in one of the following scenarios:
  - Proxy server is configured, or the DNS traffic does not pass through the router.
  - DNS request has encrypted traffic from the endpoint to the DNS server.

Feature Comparison

Feature/PBR	Application-Based Routing	Site Manager	Enhanced PBR
Flow Stickiness	Not Supported	Supported	Supported
Fallback Routing	EEM script to control the fallback routing	Path preference	
Symmetric	Asymmetric routing for dual branch scenario	Symmetric routing for dual branch scenario	

Benefits of ePBR – Application-Based Routing

- Directed Internet Access (DIA) – DIA routes Internet-bound traffic or public cloud traffic from the branch directly to the Internet. The ePBR-Application-based Routing feature allows you to local breakout guest Internet traffic and apply local security policies like Zone-based Firewall to the guest traffic.
- Directed Cloud Access (DCA) - To achieve improved Software as a Service (SaaS) application experience, you can define SaaS and its policy at the site manager. You can specify the DCA interfaces so that DCA path performance can be monitored and the best policy path can be selected. To achieve local proximity, the destination of the DNS request is modified to a public DNS resolver. The DNS request is then forwarded through a DCA interface to an SaaS server close to the branch site, therefore achieving local breakout.
  - DNS request from end host is usually to an enterprise internal DNS server, in order to achieve location proximity, we modify the destination of the DNS request to a well-known public DNS resolver (like OpenDNS resolver, Google DNS resolver) and forward this DNS request through DCA interface, the DNS resolver gives a SaaS server close to the branch site, with this we usually can get a better SaaS application experience. You can also define local policy to merge with the global policy defined by the network hub, if IWAN is configured, or take precedence over the policy defined by hub, if IWAN is not configured.
- Internet Edge with Multihoming - On the internet edge with multiple ISP links, you can define a policy to forward specific traffic to one ISP or load balance among the existing ISP links.
- Flow-Stickness—Flow-stickness can provide first packet stickiness when NABR is applied. When the border router has multiple paths and a switch to a different path is triggered due to an event like performance downgrade, flow-stickness can keep the original path of traffic request stable connection.

Configure Enhanced Policy-Based and Site Manager

Configuring a Single Border Router

```
enable
configure terminal
 class-map match-any whitelist
    match protocol attribute application-group ms-cloud-group
    match protocol amazon-wen-services
 policy-map trype epbr SaaS-list
    class whitelist
       set ip vrf fvrf next-hop 10.20.1.1
       exit
     exit
  interface GigabitEthernet3.30
    description B1MCBR-LAN
    encapsulation dot1q 30
    ip address 10.20.0.1 255.255.255.0
    service-policy type epbr input SaaS-list
    exit

  interface GigabitEthernet2.30
    encapsulation dot1q 30
    ip vrf forwarding fvrf
    ip address 10.20.1.1. 255.255.255.0
```

Configuring Redirect for Single Border Router

```
enable
configure terminal
ip nat inside source route-map LAN interface GigabitEthernet2.30 vrf BR-LAN overload
!
interface GigabitEthernet3.30
description B1MCBR-LAN
encapsulation dot1Q 30
vrf forwarding BR-LAN
ip address 10.20.0.1 255.255.255.0
ip nbar protocol-discovery ipv4
ip nat inside
service-policy type epbr input REDIRECT
exit
!
!
interface GigabitEthernet2.30
 description B1MCBR-WAN
 encapsulation dot1q 30
 vrf forwarding fvrf
 ip address 10.20.1.1 255.255.255.0
 ip nat outside
exit
!
!
configure terminal
policy-map type epbr REDIRECT
 class AppMatchMulti
  set {ipv4 | ipv6} vrf fvrf [next-hop 10.20.1.2]
class AclMatchMulti
```

```
  set interface Dialer1
!
!
!
class-map match-all AppMatchMulti
 match protocol skype
class-map match-all AclMatchMulti
 match access-group name AclMatchMulti
end
```

Configuring Flow Stickness for Single Border Router

Use the following commands to configure flow stickness for single border router

```
enable
configure terminal
interface GigabitEthernet3.30
 description B1MCBR-LAN
 encapsulation dot1Q 30
 vrf forwarding BR-LAN
 ip address 10.20.0.1 255.255.255.0
 ip nbar protocol-discovery ipv4
 service-policy type epbr input FLOWSTICKNESS
exit
!
!
interface GigabitEthernet2.30
 description B1MCBR-WAN
 encapsulation dot1q 30
 vrf forwarding fvrf
 ip address 10.20.1.1 255.255.255.0
exit
!
!
configure terminal
 policy-map type epbr FLOWSTICKNESS
 parameter default flow-stickness
  class AppMatchMulti
   set {ipv4 | ipv6} vrf fvrf [next-hop 10.20.1.2]
  class AclMatchMulti
   set {ipv4 | ipv6} global [next-hop 10.75.1.15]
!
!
!
class-map match-all AppMatchMulti
 match protocol skype
class-map match-all AclMatchMulti
 match access-group name AclMatchMulti
end
```

Configuring Site Manager with DCA (Local Policy)

Configuration on Branch (BR1) and Master Controller (MC)

```
enable
configure terminal
    site-manager default
      vrf default
        border
```

```
      master local
     master branch
      source-interface loopback0
      policy local type dca
        class DCA sequence 1
            match application google-group policy saas-dca
            path-preference DIA1 fallback DIA2
            exit
        exit
       exit
     exit
    interface gigabitethernet3.30
      description B1MCBR-LAN
      encapsulation dot1q 30
      ip address 10.20.0.1 255.255.255.0
      site-manager inside
      exit
     exit
    interface gigabitethernet2.30
      encapsulation dot1q 30
      ip vrf forwarding fvrf
      ip address 10.20.0.1 255.255.255.0
      site-manager path DIA1 direct-internet-access
      exit
     exit
```

Configuration on Branch, BR2

```
enable
configure terminal
    site-manager default
      vrf default
        border
         source-interface loopback0
         master 192.168.3.22
        exit
       exit
      exit
     interface gigabitethernet3.30
        description B1MCBR-LAN
        encapsulation dot1q 30
        ip address 10.20.0.1 255.255.255.0
        site-manager inside
        exit
       exit
      interface gigabitethernet2.30
        encapsulation dot1q 30
        ip vrf forwarding fvrf
        ip address 10.20.0.1 255.255.255.0
        site-manager path DIA2 direct-internet-access
        exit
       exit
```

Configure Site Manager with DCA (Global Policy)

Use the following commands to configure Site Manager with DCA (Global Policy). Use the following commands to configure Site Manager with DIA (Customized local Policy). If there are many branch sites requiring similar DCA policies, you can configure the policy in a central place (For example, DMVPN hub site) and the policy is published to all branch sites that have connectivity to the hub site

Configuration on Hub Master Controller

```
enable
configure terminal
    site-manager default
      vrf default
        master hub
       policy group default type DCA
        class DCA sequence 1
          match application ms-cloud-group policy saas-dca
          path-preference DIA1 fallback DIA2
        exit
       exit
      exit
```

Configuration on Branch, BR1 and Master Controller, MC

```
enable
configure terminal
    site-manager default
      vrf default
        border
          master local
        master branch
          source-interface loopback0
          hub 10.200.1.1
          exit
         exit
        exit

      interface gigabitethernet3.30
        description B1MCBR-LAN
        encapsulation dot1q 30
        ip address 10.20.0.1 255.255.255.0
        site-manager inside
        exit
       exit
      interface gigabitethernet2.30
        encapsulation dot1q 30
        ip vrf forwarding fvrf
        ip address 10.20.0.1 255.255.255.0
        site-manager path DIA1 direct-internet-access
        exit
       exit
```

Configuration on Branch, BR2

```
enable
configure terminal
    site-manager default
      vrf default
        border
         source-interface loopback0
         master 192.168.3.22
        exit
       exit
      exit
  interface gigabitethernet3.30
        description B1MCBR-LAN
        encapsulation dot1q 30
        ip address 10.20.0.1 255.255.255.0
        site-manager inside
```

```
  exit
 exit
interface gigabitethernet2.30
  encapsulation dot1q 30
  ip vrf forwarding fvrf
  ip address 10.20.0.1 255.255.255.0
  site-manager path DIA2 direct-internet-access
  exit
 exit
```

Configure Site Manager With DIA (Local Policy)

Use the following commands to configure Site Manager with DIA (Customized local Policy). If there are many branch sites requiring similar DCA policies, you can configure the policy in a central place (For example, DMVPN hub site) and the policy is published to all branch sites that have connectivity to the hub site.

Configuration on Branch, BR1 and Master Controller, MC

```
enable
configure terminal
    ip access-list extended DIA-traffic
      deny ip 10.20.0.0 0.0.255.255
      permit ip any any
    class-map type site-manager match-any DIA-class
      match access-group DIA-traffic

    site-manager default
      vrf default
        border
          master local
        master branch
          source-interface loopback0

          policy local type DIA
           class DIA-class
           path-prefernce DIA1 fallback DIA2
          exit
         exit
        exit

      interface gigabitethernet3.30
        description B1MCBR-LAN
        encapsulation dot1q 30
        ip address 10.20.0.1 255.255.255.0
        site-manager inside
        exit
       exit
      interface gigabitethernet2.30
        encapsulation dot1q 30
        ip vrf forwarding fvrf
        ip address 10.20.0.1 255.255.255.0
        site-manager path DIA1 direct-internet-access
        exit
       exit
```

Configuration on Branch, BR2

```
enable
configure terminal
    site-manager default
      vrf default
```

```
        border
         source-interface loopback0
         master 192.168.3.22
        exit
       exit

  interface gigabitethernet3.30
        description B1MCBR-LAN
        encapsulation dot1q 30
        ip address 10.20.0.1 255.255.255.0
        site-manager inside
        exit

   interface gigabitethernet2.30
        encapsulation dot1q 30
        ip vrf forwarding fvrf
        ip address 10.20.0.1 255.255.255.0
        site-manager path DIA2 direct-internet-access
        exit
```

Configure Site Manager With DIA (Global Policy)

Use the following commands to configure Site Manager with DIA (customized global policy)

Configuration on Branch, BR1 and Master Controller, MC

```
enable
  configure terminal
    site-manager default
      vrf default
        border
          master local
        master branch
          source-interface loopback0
          hub 10.200.1.1

         exit
        exit

      interface gigabitethernet3.30
        description B1MCBR-LAN
        encapsulation dot1q 30
        ip address 10.20.0.1 255.255.255.0
        ip nat inside
        site-manager inside
        exit
       exit
      interface gigabitethernet2.30
        encapsulation dot1q 30
        ip vrf forwarding fvrf
        ip address 10.20.0.1 255.255.255.0
        ip nat outside
        site-manager path DIA1 direct-internet-access
        exit
       exit
```

Configuration on Hub Master Controller

```
enable
configure terminal
    ip access-list extended DIA-traffic
```

```
    deny ip 10.20.0.0 0.0.255.255.
    permit ip any any
  class-map type site-manager match-any DIA-class
    match access-group DIA-traffic
 site-manager default
    vrf default
      master hub
     policy group default type DIA
      class DCA sequence 1
        match application ms-cloud-group policy saas-dca
        path-preference DIA1 fallback DIA2
      exit
     exit
    exit
```

Configuration on Branch, BR2

```
enable
configure terminal
    site-manager default
      vrf default
        border
         source-interface loopback0
         master 192.168.3.22
        exit
       exit

  interface gigabitethernet3.30
        description B1MCBR-LAN
        encapsulation dot1q 30
        ip address 10.20.0.1 255.255.255.0
        ip nat inside
        site-manager inside
        exit

   interface gigabitethernet2.30
        encapsulation dot1q 30
        ip vrf forwarding fvrf
        ip address 10.20.0.1 255.255.255.0
        ip nat outside
        site-manager path DIA2 direct-internet-access
        exit
```

Feature Information for ePBR - Application-Based Routing

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 1: Feature Information for Overview of Cisco TrustSec

Feature Name	Releases	Feature Information
ePBR-Application-Based Routing	Cisco IOS XE Gibraltar 16.11.1	As network-based applications start being hosted on private or public cloud, network appliances need to forward network traffic based on configured policies. The enhanced Policy-based Routing (ePBR) routing enables application-based routing. Application-based routing provides a flexible, device-agnostic policy routing solution, while also ensuring application performance.