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.

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 ePBR - Application-Based Routing

Information About Enhanced Policy-Based Routing and Site Manager

Restrictions for Enhanced Policy-Based Routing and Site Manager

- IPv6 is supported by enhanced policy-based routing but not supported by site manager
- Support is added only for ICMP probe, TCP probe is not supported

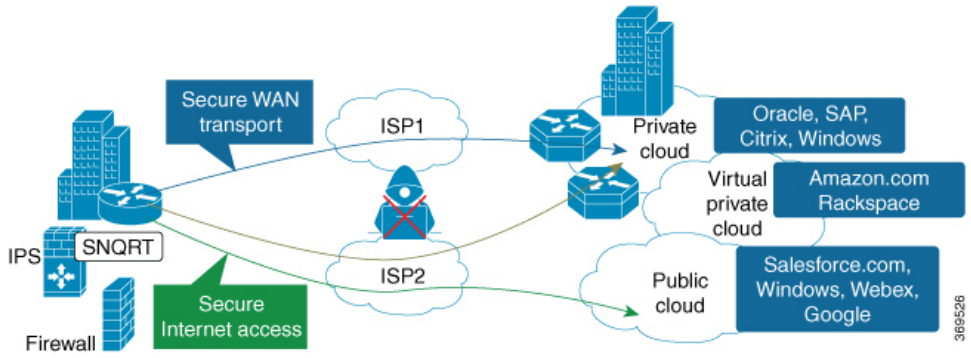
About Enhanced Policy-Based Routing and Site Manager

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.

- 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.
- Outlook365 traffic category - Outlook365 endpoints are classified into optimize/allow/default by Microsoft based priority order and published externally. Network and security devices can apply its forwarding and security decision based on the traffic category information. Starting from IOS XE Amsterdam 17.3.1, SD-AVC gets traffic category information from Outlook365 and pushes to routing devices, ePBR can match this new traffic category attribute and policy routing to a certain path, for eg, bypass Firewall or local break out. This helps to improve Outlook365 application experience to avoid unnecessary latency due to security devices or backhaul path.
- Internet Edge Load Balancing - On the internet edge with multiple ISP links, you can use advanced load balance algorithms, such as static weight, and dynamic link bandwidth per packet to forward specific traffic to one ISP or load balance among the existing ISP links. This helps to fully utilize all the available links instead of only the active or backup links. On the internet edge with multiple ISP links, you can define apolicy to forward specific traffic to one ISP or load balance among the existing ISP links.

Configure Enhanced PBR to Allow and Optimize Office365 Traffic

Enable SD-AVC on the devices to get the traffic category information from Office365 cloud, you can then enable Enhanced Policy-based Routing (ePBR) to steer Office365 traffic to the expected path.

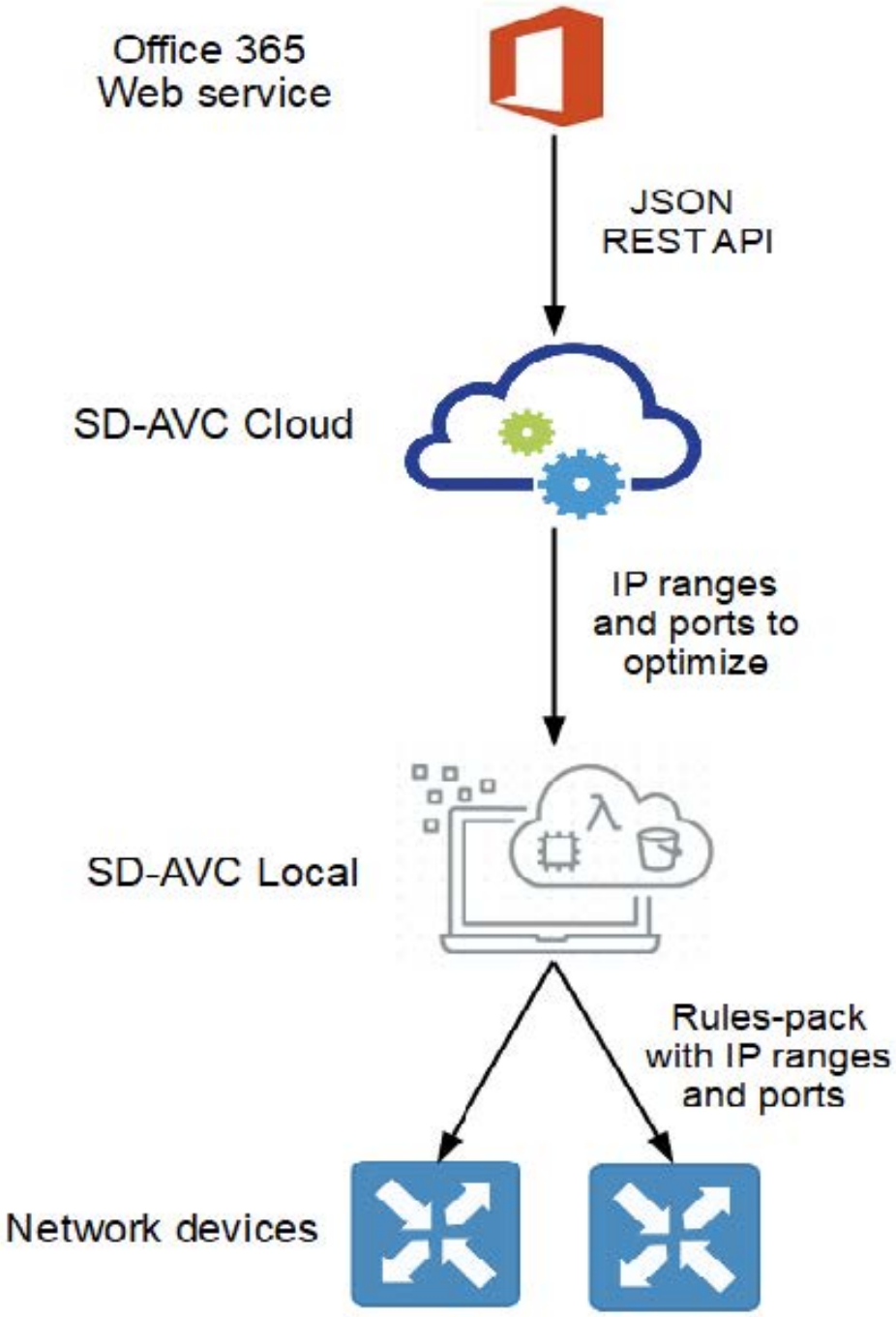


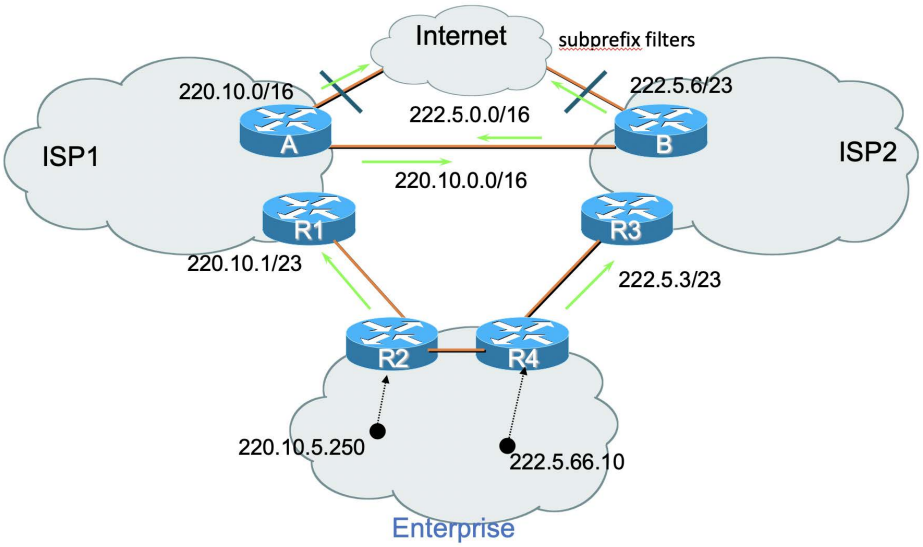
Figure 2:

Define a class map to match all the optimized category Office365 traffic, apply the ePBR policy and redirect these optimize traffic to another device, which is specified by the nexthop. You can add multiple nexthops such that if there is no route to the first nexthop, you can switch the second nexthop.

SD-AVC, which procures the traffic category information from Office365, pushes this information to specific routing devices in the network. Enhanced-PBR then matches this Office365 traffic category attribute and policy routing to a certain path, for example - bypass Firewall or local breakout.

Configure Internet Edge Load Balancing

Enterprise internet edge has multiple ISP links connected to one or multiple edge routers - R2 and R4. In order to fully utilize all the ISP links, the site-manager load balance feature is enabled on these edge devices to load



balanceinternettraffic.

Specify the LAN interfaces with “site-manager inside” and the WAN interfaces with “site-manager path”, then define the load balance policy in the site-manager primary controller to balance the load of traffic across all the WAN interfaces. You can define the DIA-class and specify the load balance method to be used - static weight, based on WAN dynamic bandwidth, and the load balance algorithm. The DIA-class is defined to specify the kind of traffic that needs to be load balanced, for example, if you require all internet traffic, you can specify this in the class so that all enterprise internal traffic is filtered by destination.

Configure Enhanced Policy-Based and Site Manager

Configure ePBR to Optimize Office 365 traffic

```
Enable
Configure terminal
class-map match-any optimize class
match traffic-category optimize
policy-map type epbr traffic-category-policy
class optimize class
set ipv4 vrf test next-hop 2.2.2.2 1.1.1.1
set ipv6 vrf test next-hop 2003::1 2002::1 2005::1
interface GigabitEthernet2
ip address 192.168.1.1 255.255.255.0
ip nbar protocol-discovery
negotiation auto
ipv6 address 2004::1/64
no mop enabled
no mop sysid
service-policy type epbr input traffic-category-policy
```

Configure Internet Edge Load Balancing

```
Enable
Configure terminal
site-manager
vrf default
master branch
source-interface Loopback0
policy local type dia
class DIA-class sequence 10
path-preference ISP1 ISP2 fallback routing
```

Border

```
site-manager
vrf default
border local
source-interface Loopback0
master 10.10.0.0
```

LAN Interface

```
interface GigabitEthernet3.30
description B1MCBR-LAN
encapsulation dot1Q 30
ip address 10.10.10.1 255.0.0.1
site-manager inside
```

WAN Interface

```
interface GigabitEthernet2.30
encapsulation dot1Q 30
ip address 10.10.10.0
site-manager path ISP1 direct-internet-access
interface GigabitEthernet3.30
encapsulation dot1Q 30
ip address 10.20.1.1
site-manager path ISP2 direct-internet-access
```

Verify the Configuration of Master traffic-classes on Primary Controller

```
Device# show site-manager master traffic-classes
Classmap: DIA-class DSCP: * [255] Traffic classid:41 classmap_id:8984
Clock Time: 17:31:04 (CST) 04/22/2020 TC Created: 00:10:48 ago
Present State: CONTROLLED
Channel1: 10 #mC30m (Gi0/0/0, LG:DIA2, BW:1000000 Kb/s, Used:752072 Kb/s, Util: 75%,
Weight:144)
Channel2: 16 #W820Z (Gi0/0/0, LG:DIA1, BW:1000000 Kb/s, Used:584202 Kb/s, Util: 58%,
Weight:255)
Load-sharing Algorithm: include-ports source destination(0x6)
Stickiness: Disabled
ICMP Probe: IP 8.8.8.8 DSCP default
Match App: No
Class-Sequence in use: 10
Class Name: DIA-class using policy best-effort
Reason for Latest Route Change: uncontrolled to Controlled Transition
Route Change History:
Date and Time Previous Exit Current Exit Reason
1:17:24:41 CST)04/22/20 None/0.0.0.0/None (Ch:0)#mC30m/3.3.3.3/Gi0/0/0Ch:10) Uncontrolled
to Controlled..
```

Verify the status of the Border Router at Branch

```
Device# show site-manager border status
Instance Status: UP
Present status last updated: 1w4d ago
Loopback: Configured Loopback0 UP (3.3.3.3)
Master: 1.1.1.1
Master version: 2
Connection Status with Master: UP
MC connection info: CONNECTION SUCCESSFUL
Connected for: 00:22:12
Connection Keepalive: 10 seconds
External Wan interfaces:
Name: GigabitEthernet0/0/0 Interface Index: 8 SNMP Index: 1 SP: #mC30m Status: UP
Auto Tunnel information:
Name:Tunnel1 if_index: 24
Virtual Template: Not Configured
Borders reachable via this tunnel: 2.2.2.2
--------------------------------------------------
```

Debug Commands

- **debug site-manager master route-control**
- **debug site-manager border dia**
- **debug site-manager border route-control**
- **debug site-manager master pdp path-preference**
- **debug site-manager master pdp path-selection**

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
```