Site-Local Failover for NAT DIA

Site-Local Failover for NAT DIA

Table 1: Feature History

Feature Name	Release Information	Description
Support for Site-Local Failover for NAT DIA	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	Support for NAT DIA traffic failover in sites with more than one edge device. The support for same-site NAT DIA local failover works with NAT44 and NAT66 by tunneling the traffic from one edge device to another edge device that has NAT DIA access within a site.

Information About Site-Local Failover for NAT DIA

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.16.1a and Cisco Catalyst SD-WAN Manager Release 20.16.1

In Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and earlier, NAT DIA was managed by directing specific types of network traffic directly to the internet from a local branch or site through configured exit DIA interfaces. In the absence of a local exit DIA interface, the NAT DIA traffic was routed through a central data center.

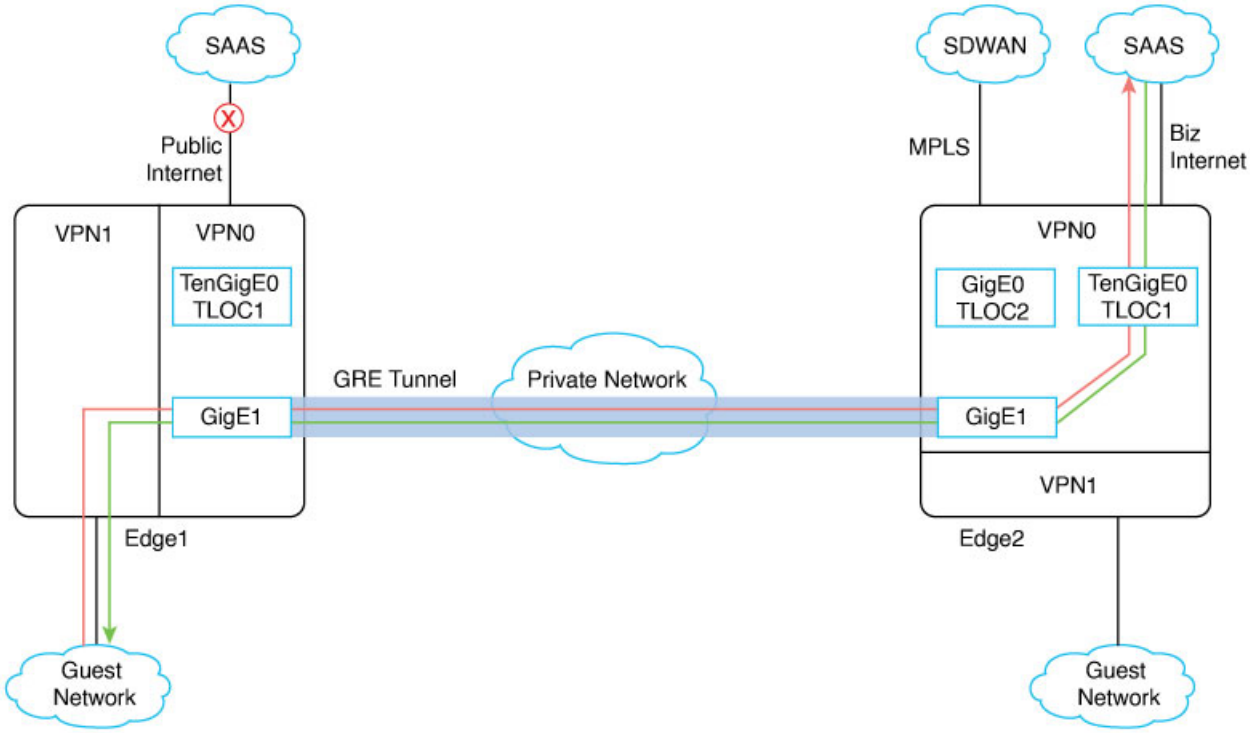
Starting from Cisco IOS XE Catalyst SD-WAN Release 17.16.1a, site-local failover for NAT DIA introduces a method for NAT (NAT44 and NAT66) DIA traffic to failover to other edges within the same site that are

configured for NAT DIA in the event that the primary NAT DIA circuit goes down. This feature supports NAT DIA traffic failover in sites with multiple edge devices using dedicated Layer 3 standard GRE tunnels.

With this release, you can enable site-local redundancy for NAT DIA, which also works with existing Layer 2 and Layer 3 TLOC extension-based deployments. The DIA traffic initially fails over via a GRE Tunnel interface to the site-local redundant router to check for an available TLOC that is capable of DIA. If TLOC is not available, the DIA traffic uses NAT fallback as backup. The edge device detects the existence of a DIA interface based on endpoint trackers.

To enable the NAT-DIA site-local redundancy solution, use a standard dedicated GRE tunnel interface, which carries only the NAT DIA traffic to the site-local redundant Cisco Catalyst SD-WAN edge devices. The source interface of the tunnel on either edge device can be a physical interface or a subinterface on the transport VPN. NAT DIA traffic is routed between the two edges in the same site. We recommend that you use port-channels as the traffic is diverted via the GRE tunnel even for flows redirected to hub sites. Consider the link bandwidth while choosing the underlay interface for the GRE Tunnel. Routing is not required in the GRE tunnel overlay.

Figure 1: Workflow of Site-Local Failover for NAT DIA



For example, when NAT DIA from Edge1 is unavailable, the traffic is transported over the Layer 3 standard GRE tunnel interface to Edge2. Edge2, which is configured as the router for site-local failover, decapsulates the incoming traffic and forwards it to the interface enabled with NAT DIA, *TenGigE0 TLOC1*. Similarly, return traffic from *TenGigE0 TLOC1* which is identified as the NAT DIA traffic which arrived over the GRE tunnel, is translated and forwarded, over the Layer 3 standard GRE tunnel interface to Edge1. Edge1 then decapsulates the incoming traffic and forwards it to the source interface in service VPN.

Benefits of Site-Local Failover for NAT DIA

- Site-local failover for NAT DIA with TLOC extension: You can configure site-local failover for NAT DIA with existing Layer 2 and Layer 3 TLOC extension-based deployments.
- Improved performance in application SLAs: Implementing site-local failover for NAT DIA leads to reduced latency, jitter, drops, and decreased cost.

Restrictions for Site-Local Failover for NAT DIA

- Overlapping subnets: Subnets originating from different VPNs during failover must be unique and cannot have the same host IP.
- GRE tunnel: In Cisco IOS XE Catalyst SD-WAN Release 17.16.1a, only one GRE tunnel is supported currently irrespective of number of TLOC extensions between the edges devices in the same site.
- Packets from transport VPN 0: Site-local failover does not support packets originating from transport VPN 0.
- Centralized data policy: Site-local failover is supported only with NAT DIA centralized data policy.

Configure Site-Local Failover for NAT DIA

You can configure site-local failover for NAT DIA by using the **site-local-redundancy** command in the centralized data policy by using CLI commands.

Before You Begin

- Create a GRE tunnel interface between the edge devices. For information about configuring GRE tunnels, see GRE Over IPsec Tunnels.
- Configure the centralized data policy to enable NAT DIA. For more information, see NAT Fallback on Cisco IOS XE Catalyst SD-WAN Devices.

Configure Site-Local Failover for NAT DIA using CLI

For more information about using CLI templates, see CLI Templates.

Note By default, CLI templates execute commands in global config mode.

This section provides example CLI configurations to configure site-local failover for NAT DIA:

1. Configure the GRE Tunnel interface using the **site-local-redundancy** command. For more information about this command, see the action (centralized policy) command in the *Cisco Catalyst SD-WAN Qualified Command Reference* guide.

- Configure Edge1 for site-local redundancy. To configure NAT DIA failover for NAT44, use an IPv4 address, and for NAT66, use an IPv6 address.

```
interface GRE-tunnel-name
 description variable-name
 ip address ip-address-of-edge1
 ip mtu mtu-size
 site-local-redundancy
 keepalive keepalive-value
 tunnel source source-interface-name
 tunnel destination interface-ip-address-of-edge2
end
!
```

- Configure Edge2 for site-local redundancy. To configure NAT DIA failover for NAT44, use an IPv4 address, or for NAT66, use an IPv6 address.

```
interface GRE-tunnel-name
 description variable-name
 ip address ip-address-of-edge2
 ip mtu mtu-size
 site-local-redundancy
 keepalive keepalive-value
 tunnel source source-interface-name
 tunnel destination interface-ip-address-of-edge1
end
!
```

2. Configure the centralized data policy for NAT DIA by using the **site-local-redundancy** command

```
policy
 data-policy data-policy-name
  vpn-list list-name
   sequence sequence-number
    match source-data-prefix-list data-prefix list-name
    !
    action accept
     count vpn-list-name
     nat use-vpn 0
     nat fallback
     nat site-local-redundancy     !
   !
   default-action accept
  !
 !
```

Here's the complete example to configure the edge devices in the same site and the centralized data policy for NAT44:

Configure Edge1. To configure NAT DIA failover for NAT44, use an IPv4 address, or for NAT66, use an IPv6 address.

```
interface Tunnel15000561
 description GRE Tunnel Interface for NAT-DIA fallback
```

```
 ip address 192.0.2.1
 ip mtu 1500
 site-local-redundancy
 keepalive 6 3
 tunnel source GigabitEthernet6
 tunnel destination 192.0.2.2
end
!
```

Configure Edge2. To configure NAT DIA failover for NAT44, use an IPv4 address, and for NAT66, use an IPv6 address.

```
interface Tunnel15000561
 ip address 192.0.2.2
 ip mtu 1500
 site-local-redundancy
 keepalive 6 3
 tunnel source GigabitEthernet6
 tunnel destination 192.0.2.1
end
!
```

Configure the centralized data policy to enable site-local failover by using the **site-local-redundancy** command.

```
policy
 data-policy same-site-nat-dia-fallback-site-1
  vpn-list nat-dia-vpn-1
   sequence 1
    match
     source-data-prefix-list same-site-nat-dia-site-1
    !
    action accept
     count ss-nat-dia-s1
     nat use-vpn 0
     nat fallback
     nat site-local-redundancy
    !
   !default-action accept
  !
 !
```

Verify Site Local Failover For NAT DIA

```
#show platform hardware qfp active feature nat datapath basecfg | inc DIA

NAT DIA enabled
NAT DIA mutliple methods disabled
#show platform software sdwan slr database
Status : True
-------------------------------------------------------------
Index Ifname Ifindex Valid Status
-------------------------------------------------------------
0 Tunnel15000561 26 True True
```

Verify Configuration for Edge1

```
#show platform hardware qfp active feature nat datapath basecfg | inc DIA
NAT DIA enabled
NAT DIA mutliple methods disabled
```

```
#show platform software sdwan slr database
Status : True
------------------------------------------------------------
Index  Ifname          Ifindex   Valid   Status
------------------------------------------------------------
0     Tunnel15000561    26      True    True

#show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
tcp  172.25.12.1:5062      172.25.12.1:48670     4.2.2.2:80            4.2.2.2:80
icmp 172.25.12.1:197       198.51.100.4:197         8.8.8.8:197           8.8.8.8:197
Total number of translations: 2
```

After the local breakout from edge1 device goes down:

```
#show ip nat translations
Total number of translations: 0

#show platform software sdwan slr database
Status : True
------------------------------------------------------------
Index  Ifname          Ifindex   Valid   Status
------------------------------------------------------------
0     Tunnel15000561    25      True    True
```

Verify Configuration for Edge2 (Site-Local Failover Device)

```
#show platform hardware qfp active feature sdwan datapath slr table hosts
VPN_IDX Host_IP Flags Tun_idx IFNAME Tx_encap_Pr Rx_decap_Pr Tx_encap_Sec Rx_decap_Sec
-------------------------------------------------------------------------------------------------------
1        198.51.100.3          0x0     65519      Tunnel15000561   0          0
0          0
1        198.51.100.4          0x1     65519      Tunnel15000561   0          0
0          0


#show ip nat translations
Pro Inside global         Inside local          Outside local         Outside global
<snip>
udp  172.21.11.1:5062      10.10.92.1:12346      172.21.20.1:12346     172.21.20.1:12346
icmp 172.21.11.1:199       10.10.1.4:199         8.8.8.8:199           8.8.8.8:199
<snip>Total number of translations: 10

#show ip nat translations
Pro Inside global         Inside local          Outside local         Outside global
<snip>
udp  172.21.11.1:5062      10.10.92.1:12346      172.21.20.1:12346     172.21.20.1:12346
icmp 172.21.11.1:199       198.51.100.4:199         8.8.8.8:199           8.8.8.8:199
<snip>
Total number of translations: 10

#show platform hardware qfp active feature sdwan datapath statistics | sec SLR
SDWAN SLR:
Total SLR policy : 0
Total SLR policy fail : 0
Total SLR Down : 0
Total SLR Tunnel adj not found : 0
Total SLR SB not Init : 0
Total SLR Host mem req : 0
Total SLR Host mem req : 0
Total SLR Dst Changed : 0
Total SLR Dia Down Fallback : 0
Total SLR Dia Down Restrict Drop Pkt : 0
Total SLR v4 Host Entry add failed : 0
Total SLR v6 Host Entry add failed : 0
```

```
Total SLR mdata encap        : 20
Total SLR mdata decap        : 44
```