Cisco Catalyst SD-WAN Firewall High Availability

Table 1: Feature History

Feature	Release Information	Description
Cisco Catalyst SD-WAN Firewall High Availability	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	By implementing High Availability in Cisco Catalyst SD-WAN, you can set up two Cisco IOS XE Catalyst SD-WAN devices in either active-active or active-standby configurations. When high availability is enabled, features like the Zone Based Firewall (ZBF) and Network Address Translation (NAT) synchronize their states between the devices, whether in active-standby or active-active modes. In the event of a failure of the active device, the standby device seamlessly takes over operations without interrupting session flows, thus eliminating the need for reconnection.

Information About Cisco Catalyst SD-WAN Firewall High Availability

High availability ensures the continuous operation of essential services such as Zone Based Firewall (ZBF) and Network Address Translation (NAT). High availability provides a seamless switchover of these services in the event of a device failure.

In a high-availability environment, firewall and NAT functionalities synchronize their operational states between two Cisco IOS XE Catalyst SD-WAN devices through redundancy groups. A redundancy group is a pairing of two Cisco IOS XE Catalyst SD-WAN devices where one is designated as the active device and the other as the standby. VPNs are associated with these redundancy groups. Cisco Catalyst SD-WAN supports two redundancy groups, allowing one set of traffic to be active on one device and another set of traffic to be active on the peer device.

The synchronization of stateful features such as firewall sessions and NAT mappings from the active device to the standby device ensures that the standby device has all the necessary information to maintain service continuity if the active device fails. This seamless transition prevents service disruption and ensures high availability.

Note While high availability aims to provide seamless operation, certain features may not transition traffic as smoothly during failover scenarios. Support for Application Layer Gateway (ALG) and Application Inspection and Control (AIC) is on a best-effort basis, and the traffic switchover might not be seamless. Similarly, traffic flows involving TCP/TLS proxy (Unified Threat Defense) and Network-Based Application Recognition (NBAR)/Deep Packet Inspection (DPI) may experience disruptions during failover.

Redundancy Groups

A redundancy group is a pairing of devices in a high-availability configuration in Cisco Catalyst SD-WAN that ensures continuous service. The devices in the redundancy group can operate either in an active or standby state. VPNs are associated with the redundancy groups, and the VPN traffic is processed by the active device in the redundancy group. Cisco Catalyst SD-WAN supports a maximum of two redundancy groups.

In an active-active configuration, both devices in the two redundancy groups simultaneously process traffic, providing load balancing and redundancy. In this setup, VPNs are distributed across two Cisco IOS XE Catalyst SD-WAN devices, resulting in the creation of two redundancy groups. Redundancy group configuration should have the **preempt** option configured for active-active (two redundancy groups) mode.

In an active-standby configuration, all the VPNs are assigned to a single Cisco IOS XE Catalyst SD-WAN device, creating one redundancy group. For active-standby (only one redundancy group configured) mode, the **preempt** option is not recommended

By correctly configuring redundancy groups, you can ensure high availability and continuous service in your Cisco Catalyst SD-WAN environment. VPNs that are not associated with a redundancy group do not have their traffic protected by high availability.

VPN Associations

You can associate VPNs with redundancy groups in Cisco Catalyst SD-WAN. To do this, you must manually assign each VPN to its redundancy group. If you configure route leaking between VPNs, it is contained within the same redundancy groups, and this is enforced by Cisco SD-WAN Manager for proper traffic management and high availability.

Redundancy Group Init Roles

Init roles are used while configuring redundancy groups on Cisco IOS XE Catalyst SD-WAN devices. These roles determine the initial state of a device within a redundancy group, specifying whether it should start as the active or standby device. Proper configuration of init roles ensures that one device takes on the responsibility of handling traffic (active) while the other remains in a ready state (standby) to take over in case of a failure.

The **`init-role active`** within redundancy groups helps you to select between active and standby options when both redundancy groups have equal priority. You must configure this role appropriately for each redundancy group. Designate one device as **`init-role active`**, and configure the other as **`init-role standby`**.

When **`preempt`** is set, the redundancy group with **`init-role active`** become actives if the redundancy group priorities of the peer devices are equal. This allows for automatic switchover to their initial state after faults have been addressed.

Implicit and Explicit Tracking

Redundancy groups use object tracking to determine their state. Examples of this include Cisco Catalyst SD-WAN session tracking, NAT endpoint tracking, and interface state tracking.

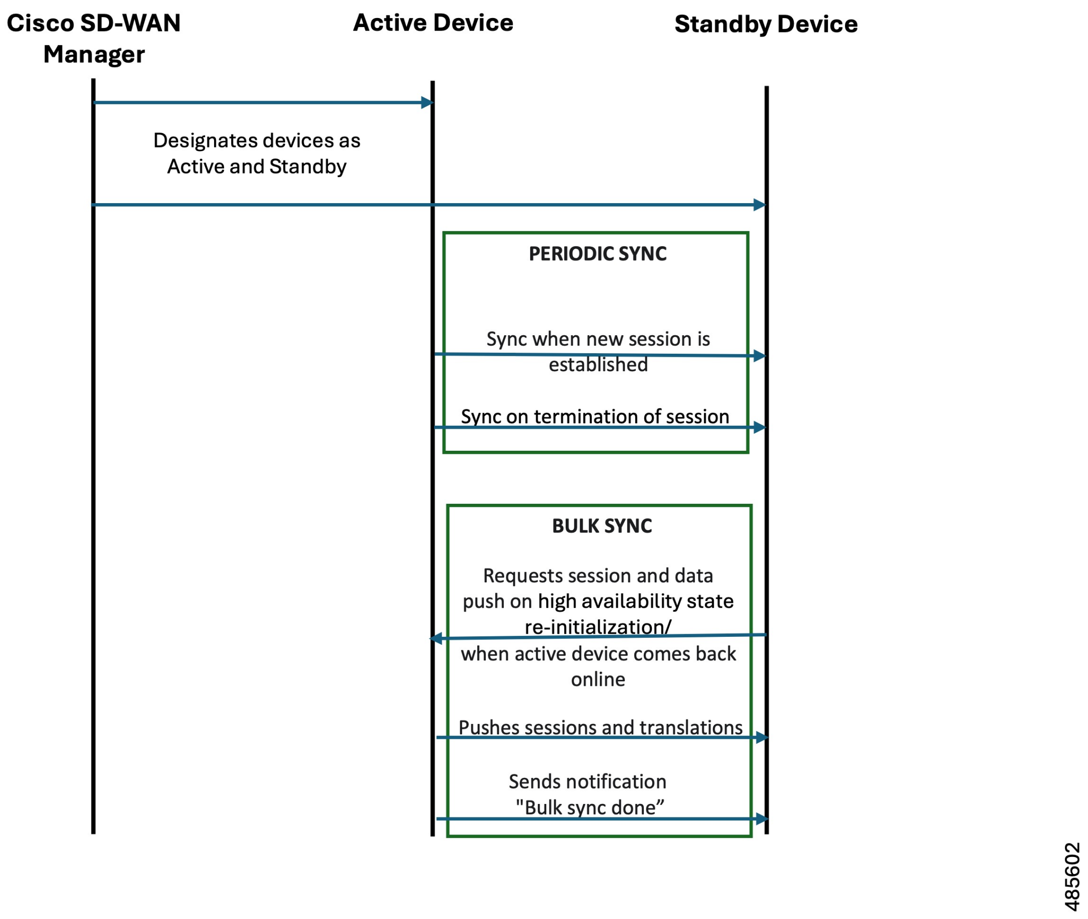
The redundancy groups can also be configured to create an object. Virtual Router Redundancy Protocol (VRRP) tracks the redundancy group object so that it can follow the redundancy group state. For example, if the redundancy group state is active, the VRRP state is primary; if the redundancy group state is standby, the VRRP state is backup.

State Synchronization

There are two types of state synchronization between the active and standby devices:

- Periodic Sync: This occurs as soon as a session is established. For example, when a NAT entry is created or a firewall session is established, the state is immediately synchronized. Similarly, when a session is deleted, the corresponding state is also removed.
- Bulk Sync: This occurs whenever the high availability state is re-initialized, or when a Cisco IOS XE Catalyst SD-WAN device is reloaded or comes back online. During this process, the standby device requests the active device to push the sessions and translations to it. After this synchronization is complete, the active device issues a **`bulk sync done`** notification to the standby device. At this point, standby device transitions to hot standby. When the bulk sync is fully completed, the standby device is considered to be in a hot standby state.

Figure 1: State Synchronization


Cisco SD-WAN Manager
Active Device
Standby Device
Designates devices as Active and Standby
PERIODIC SYNC
Sync when new session is established
Sync on termination of session
BULK SYNC
Requests session and data push on high availability state re-initialization/ when active device comes back online
Pushes sessions and translations
Sends notification "Bulk sync done"
485602

Path Optimization

Path optimization in Cisco Catalyst SD-WAN ensures that WAN traffic is always directed to the active Cisco IOS XE Catalyst SD-WAN device, thereby avoiding traffic redirection, also known as peer diversion, and ensuring efficient traffic flow. When you enable path optimization, WAN traffic consistently flows to the active Cisco IOS XE Catalyst SD-WAN device, eliminating the need for peer diversion, where traffic would otherwise be redirected from the standby device to the active device.

For LAN traffic, you can direct traffic to the active Cisco IOS XE Catalyst SD-WAN device using Interior Gateway Protocol (IGP) rewrite or Virtual Router Redundancy Protocol (VRRP) following the redundancy group.

For WAN traffic, path optimization directs the traffic to the active device, preventing it from reaching the standby device.

IGP Rewrite

IGP Rewrite is a technique used to ensure that LAN-side traffic is directed to the active Cisco IOS XE Catalyst SD-WAN device within a redundancy group. Interior Gateway Protocols (IGPs) such as Open Shortest Path First (OSPF) or Border Gateway Protocol (BGP) dynamically route traffic within a network.

By adjusting the IGP metrics or routes, you can configure the network to prefer the active Cisco IOS XE Catalyst SD-WAN device for routing LAN traffic. This ensures that the active device handles the majority of the traffic, providing efficient traffic flow and minimizing the chances of traffic being redirected to the standby device.

VRRP Following Redundancy Group State

In the context of a redundancy group, you can configure VRRP to follow the state of the redundancy group. This means that the VRRP primary role is assigned to the Cisco IOS XE Catalyst SD-WAN device with the active redundancy group, ensuring that LAN-side traffic is directed to the active redundancy group. If the active redundancy group fails, VRRP reassigns the primary role to the device with the new active redundancy group, ensuring continuous service.

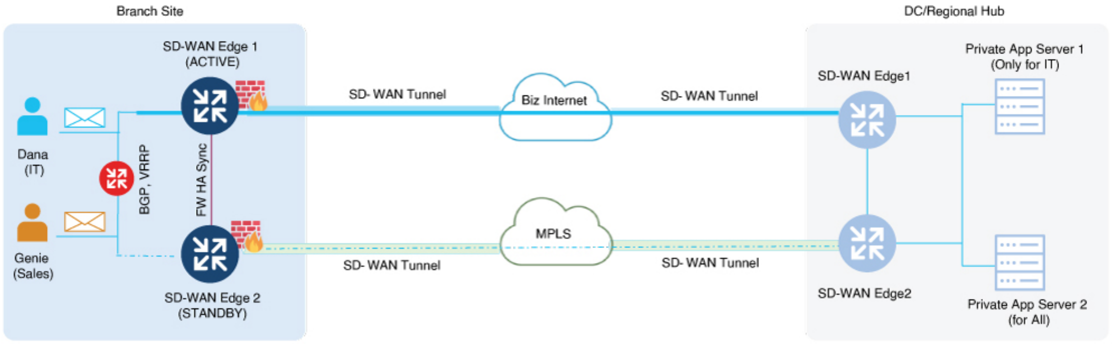
You can assign only one VPN to an interface, and the VRRP for that interface must follow the redundancy group associated with the same VPN. You can configure both VRRP and the redundancy group on the same Cisco IOS XE Catalyst SD-WAN device.

IGP Rewrite and VRRP following the redundancy group state are techniques used to attract LAN-side traffic to the device with the active redundancy group. By using these techniques, you can ensure that LAN-side traffic is consistently directed to the active redundancy group associated with the Cisco IOS XE Catalyst SD-WAN device. Combined with path optimization for WAN traffic, this ensures that all traffic is efficiently routed to the active redundancy group associated with the Cisco IOS XE Catalyst SD-WAN device until it fails. In such a setup, the states of firewall and NAT services are continuously synchronized between the two Cisco IOS XE Catalyst SD-WAN devices. In the event of a failover, the standby redundancy group associated with the Cisco IOS XE Catalyst SD-WAN device takes over, and these services will continue to run seamlessly, maintaining high availability and continuous service.

In this sample topology for path optimization, VPN traffic flows through the active device, SD-WAN Edge 1, in both directions—from LAN to WAN and from WAN to LAN.

SD-WAN Edge 1, as the active device, modifies the routing parameters for LAN traffic and the OMP affinity for WAN traffic to attract traffic in both directions (LAN to WAN and WAN to LAN).

Figure 2: Path Optimization



Peer Diversion

Peer diversion is a mechanism where traffic arriving on a Cisco IOS XE Catalyst SD-WAN device with an associated redundancy group in a standby state is diverted to the peer device in the redundancy group. The peer device refers to the other device in the redundancy group.

Redundancy group configuration should include the **asymmetric-routing always-divert enable** command when setting up high availability in a redundancy group. This option ensures that when traffic reaches the standby device, it is diverted to the active device regardless of the type of traffic.

There are two methods of Peer diversion:

- LAN Divert
- WAN Divert

LAN Diversion

For the LAN traffic, based on VPN-to-redundancy group mapping, if the device is in the standby state for the traffic in a specific VPN, the traffic is diverted to the active device.

WAN Diversion

For the WAN traffic, if traffic is directed to a device in a standby state, Peer diversion uses session information from Cisco Catalyst SD-WAN to identify and redirect the traffic to the active device in the redundancy group.

Peer diversion efficiently manages traffic by diverting it to the active redundancy group associated with the Cisco IOS XE Catalyst SD-WAN device when it arrives at a standby device. This mechanism is crucial for maintaining seamless traffic management and high availability in Cisco Catalyst SD-WAN environments. It ensures that features like Application Aware Routing and stateful services, such as firewall and NAT, are processed only on the active redundancy group.

VPN Homing

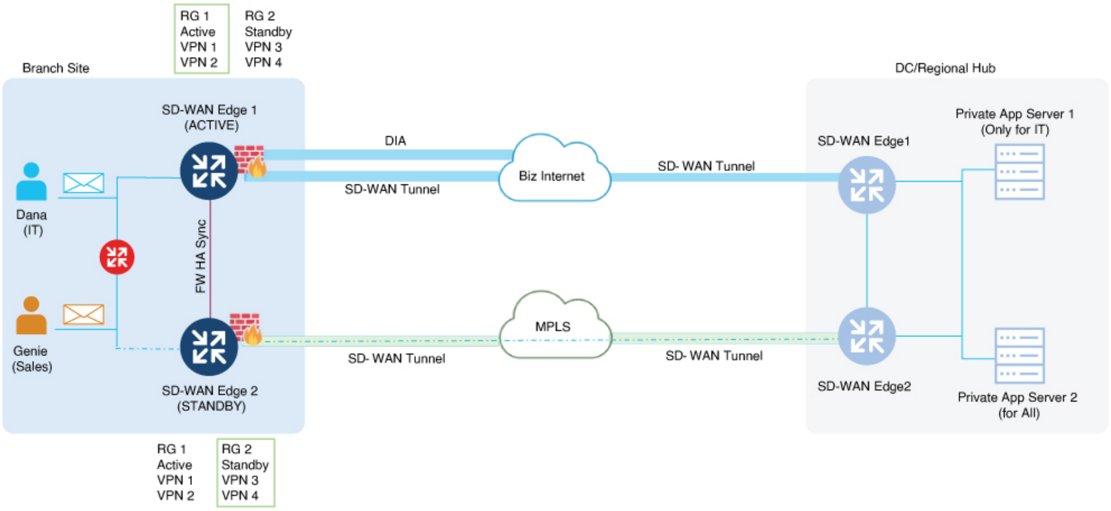
VPN homing is a technique used to manage and optimize the routing of VPN traffic through specific Cisco IOS XE Catalyst SD-WAN devices. This involves mapping VPNs to redundancy groups to determine which Cisco IOS XE Catalyst SD-WAN device will be active for the corresponding VPN traffic. Multiple VPNs can be mapped to a single redundancy group, allowing for flexible and efficient traffic management.

For seamless failover and consistent traffic routing, both the active and standby Cisco IOS XE Catalyst SD-WAN devices must have the same VPN to redundancy group mapping. This ensures that the network can maintain high availability and continuous service.

In this sample topology for VPN homing, two redundancy groups are configured for devices SD-WAN Edge 1 and SD-WAN Edge 2 in an active-active setup. As part of VPN homing, Service Side VPNs, VPN 1 and VPN 2, are associated with RG1, while VPN 3 and VPN 4 are associated with RG2.

As a result of this active-active setup, traffic is load-balanced across both devices, with SD-WAN Edge 1 handling traffic for VPN 1 and VPN 2, and SD-WAN Edge 2 handling traffic for VPN 3 and VPN 4. This configuration ensures efficient traffic management and high availability.

Figure 3: VPN homing



High Availability Interconnect

An interconnect is a dedicated connection between peer Cisco IOS XE Catalyst SD-WAN devices. It facilitates communication and synchronization between devices, allowing the high availability infrastructure to determine which redundancy group is active or standby. The interconnect also enables the transfer of session data to the standby redundancy group and provides a path for peer-diverted traffic.

In a high availability set up, the interconnect interface enables synchronization of services, such as Firewall and NAT, between two Cisco IOS XE Catalyst SD-WAN devices. This setup enables features to synchronize their state, such as sessions and translations, which is essential for seamless failover and high availability.

High Availability Configuration Options

When configuring the interconnect for high availability, you have the following options:

- Single Interface: A single physical interface or a subinterface can be used as the interconnect.
- Port Channel: A port channel can be used to provide redundancy and increased bandwidth for the interconnect.

Only a single interconnect interface may be configured. If multiple interfaces are required to meet throughput requirements, use a port channel.

On interconnect interfaces, default Quality of Service (QoS) configurations are applied to prioritize traffic. These QoS policies ensure that critical synchronization and management traffic is handled efficiently and without delay. High availability protocol traffic receives the highest precedence, followed by session management traffic, while peer divert traffic utilizes the remaining bandwidth.

Redundant Interface IDs

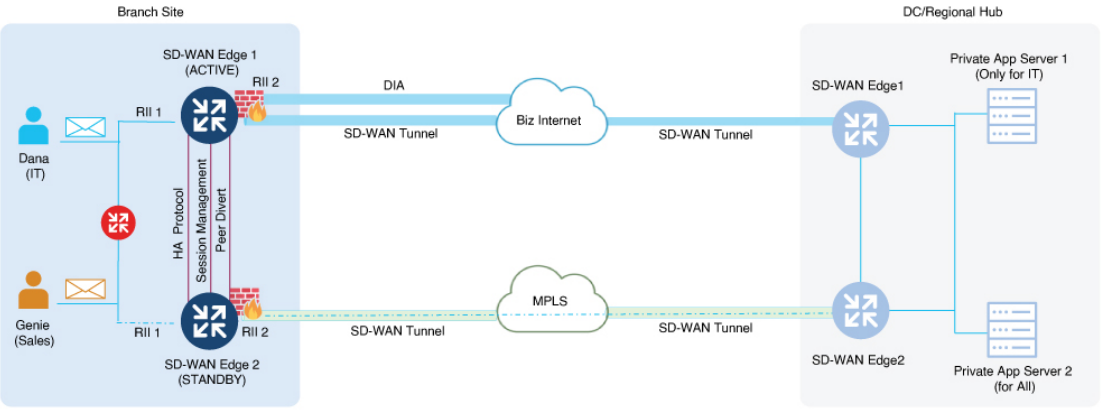
Redundant Interface IDs (RII) enable high-availability peer Cisco IOS XE Catalyst SD-WAN devices to be mapped and associated with each other. Cisco SD-WAN Manager automatically generates a unique RII for each interface on a Cisco IOS XE Catalyst SD-WAN device, and this RII must be replicated on the peer device. LAN and WAN interfaces must be configured with RII to ensure that each interface on one device corresponds to the redundant interface on another device. This includes configuring RII for the SD-WAN tunnel for service-side NAT.

By assigning matching RIIs to interfaces on both the active and standby Cisco IOS XE Catalyst SD-WAN devices, we logically pair the interfaces, forming a singular interface.

In a sample high availability interconnect topology, interconnect links (logical links) are set up between the active device (SD-WAN Edge 1) and the standby device (SD-WAN Edge 2). The high availability protocol uses keepalive messages to determine which device is active and which is standby. The state synchronization mechanism synchronizes the states of high availability features such as firewall and NAT between the active and standby devices. The peer diversion link ensures that traffic arriving on the standby device is diverted to the active device. The RII is essential to identify and manage of interfaces across active and standby devices.

Note Interfaces that do not have an RII assigned will not support high availability.

Figure 4: High Availability Interconnect and State Synchronization



NAT Pool Assignments

In Cisco Catalyst SD-WAN, NAT pools can be associated with redundancy groups to ensure high availability and efficient traffic management.

For NAT Direct Internet Access (DIA) configuration in active-active mode, two redundancy groups are configured, and NAT pools are assigned in a round-robin manner across these groups.You can use the CLI Add-on profile to assign a specific a redundancy group to a NAT pool. The mapping of NAT pools to redundancy groups should be the same as the mapping of VPNs to redundancy groups. For NAT translations to be synchronized, NAT mapping must belong to a redundancy group.

For NAT DIA configuration in active-standby mode, only one redundancy group is configured. When you associate a redundancy group with a NAT pool, the configured redundancy group is assigned to the NAT pool.

For service-side NAT configuration, NAT pools can be assigned to a VPN using service-side NAT mapping. Cisco SD-WAN Manager ensures that the redundancy group associated with the NAT pool matches the redundancy group the VPN is mapped to in the redundancy group configuration.

For more information, see NAT Deployment Models, on page 9.

NAT Deployment Models

Cisco Catalyst SD-WAN includes the following types of NAT configurations:

- NAT DIA: Allows remote sites to route traffic directly to the internet rather than routing the traffic to a central site or data center.
- Service-Side NAT: Allows you to configure internal NAT on data traffic traveling to and from the service hosts of the network overlay. Service-Side NAT translates data traffic of internal host addresses that match a configured centralized data policy.

NAT DIA

You can configure NAT DIA to allow direct internet access in high availability setups, ensuring continuous service and efficient traffic management. In a NAT DIA high availability configuration, policies must be configured, and NAT mapping must be associated with redundancy groups to ensure high availability.

Configure a pair of Cisco IOS XE Catalyst SD-WAN devices with a redundancy group. Both devices must be connected to the same set of hosts on the LAN side. When you configure one redundancy group, one device operates as the active device while the other remains in standby mode. You can connect the WAN interfaces of each device to the same or different internet service providers (ISPs) and place them on different subnets. Despite subnet differences, you can successfully divert stateful traffic because you configure the same RII on both interfaces. For more information about RII, see the section **Redundant Interface IDs** in High Availability Interconnect, on page 7.

Configure the WAN interfaces of both Cisco IOS XE Catalyst SD-WAN devices with an IGP routing protocol such as Internal Border Gateway Protocol (iBGP) or OSPF to install the NAT pool subnet into the ISP router along with other routes. During a switchover, the standby router becomes active and traffic is diverted to it as the sessions were previously synchronized.

For NAT DIA, match the reduncy group ID in the NAT mapping to the VPN traffic. Multiple VPNs belonging to the same redundancy group can share the same DIA mapping. NAT mappings configured without a redundancy group ID are used by control traffic on the device, and sessions created through this mapping are not synchronized.

You can configure NAT DIA for high availablility in Cisco SD-WAN Manager using configuration groups or by using the CLI Add-On Profile. For information see, Configure NAT DIA for Cisco Catalyst SD-WAN Firewall High Availability, on page 17, CLI Add-On Profile.

Service-Side NAT

A Service-Side NAT configuration is a used in high availability setups to ensure continuous service and efficient traffic management for overlay traffic.

In a service-side NAT for high availability configuration, configure policies and associate VPNs to redundancy group for high availability. In a Service-Side NAT high availability configuration set up, Cisco SD-WAN Manager checks whether a VPN is associated with any redundancy group and if NAT pools are configured as part of the VPN configuration. If the VPN is already associated with an redundancy group, the configured NAT pools for that VPN is considered for high availability. For information on configuring service-side NAT in Cisco SD-WAN Manager, see Configure Service-Side NAT.

Alarms and Notifications

Cisco SD-WAN Manager provides a way to monitor and log events related to redundancy group roles. When you navigate to **Monitor** > **Logs** in Cisco SD-WAN Manager, the page displays device-generated events, including those triggered by the toggling of redundancy group roles during a high availability failover.

Toggling of redundancy group roles occurs when the state of an redundancy group changes from active to standby or vice versa. This ensures continuous service during an high availability failover. The **Logs** page in Cisco SD-WAN Manager allows you to monitor and track these changes, displaying any failover events so that you can take appropriate action if necessary.

Restrictions for Cisco Catalyst SD-WAN Firewall High Availability

Device Compatibility

- Cisco IOS XE Catalyst SD-WAN devices used as active and standby devices must be of the same platform model.
- Among the Cisco Catalyst 8500 Series Edge platforms, flow-based platforms such as C8500L-8S4X platform do not support high availability.

VPN and Redundancy Group Configuration

- VPNs with route leaking must be associated with the same redundancy group.
- To maintain consistency between VRRP state and redundancy group state, each VRRP group must track the redundancy group associated with the same VPN (that is, VRRP group state follows redundancy group state).
- Both the active and standby devices must have identical NAT, firewall, and redundancy configurations. This is essential to ensure seamless failover and high availability.

Protocol and Interface Limitations

- Redundancy groups cannot be configured or managed at the individual interface level on the device

  IPv6 cannot be configured on peer interconnect interfaces.
- Because VPN0 is not part of the redundancy group, its NAT translations are not synchronized to the standby device. Control traffic of VPN 0 can be translated using NAT mapping without a redundancy group, as the traffic of VPN 0 is not required to be protected.

NAT DIA

- NAT DIA is supported only in a full mesh topology.
- NAT DIA is supported only with NAT pools; interface or loopback overload is not supported.
- Asymmetric routing in NAT DIA can be addressed by sending influenced routes to attract traffic toward the active redundancy group.
- For NAT DIA configuration in an active-active redundancy group, use the add-on CLI profile.

- For NAT DIA configuration using the add-on CLI profile, multiple NAT methods must be used to configure NAT mappings associated with the redundancy group.
- In an active-active setup with two redundancy groups, the mapping of NAT DIA pools to redundancy groups should be the same as the mapping of VPNs to redundancy groups.

High Availability Features

- Cisco Catalyst SD-WAN firewall high availability configuration and NAT DIA fallback are two ways to ensure high availability. Both features must not be used concurrently.
- The high availability link is expected to be up at all times to handle asymmetric paths.

Configure Cisco Catalyst SD-WAN Firewall High Availability

Configure Cisco Catalyst SD-WAN Firewall High Availability Using Configuration Groups Workflows

The configuration group workflow in Cisco SD-WAN Manager provides a guided method to create configuration groups and feature profiles. For more information see, Overview of Configuration Group Workflows.

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Create Configuration Group**.
2. Enter a name for your configuration group.
3. Enter the description.
4. Click **Next**
5. Define the site settings and WAN circuits using the **Site Configurations** step.

Field	Description
Site Type	The configuration group type is **Single Router** by default. Choose **Dual Router**. Choose a role for the site: **Edge Site**: Used for branch offices or remote locations. **Border Site**: Used for data centers or central hubs.
Site Settings	Enter site specific values that may be common to other devices in Cisco SD-WAN Manager. **Local Device Access**: Enter a password for local device access. **Message of the Day:** Enter the message content to display important information to users upon login. This can include network policies, maintenance notifications, or security warnings. **Login**: Enter a login banner to display a legal notice or welcome message before the login prompt.

Field	Description
WAN Interfaces	Configure the WAN interfaces for the two Cisco IOS XE Catalyst SD-WAN devices. • **Full Mesh**: Choose this option to configure high availability with NAT DIA. • **Transport Extension**: Choose this option to extend the transport network to additional sites or devices. Choose the IP addressing method for each WAN interface: • **DHCP**: Choose this option for the WAN interface to automatically obtain an IP address from a DHCP server. • **Static IP**: Choose this option to configure the IP address, subnet mask, and gateway for the WAN interface. • **Transport Sharing to Edge Device**: Click tthis option to share the transport network with edge devices for better resource utilization. • **Transport Name**: Enter a name for the transport network. • **Interface Color**: Assign a color to each transport network to visually differentiate them in the Cisco SD-WAN Manager interface. • **Use for Secondary Login**: Choose this option if the WAN interface should be used as a secondary login path for redundancy. This applies when a secondary region is configured in the Network Hierarchy Management. • **Shared with Access Region**: Click this option if the WAN interface should be shared with an access region. • **Exclusive to Secondary Region**: Click this option if the WAN interface should be exclusive to a secondary region. • **Show Advanced**: Configure additional settings for the WAN interface.
WAN Routing	Include WAN routing details with BGP routes, OSPF routes, or multiple static IPv4 routes for your WAN transport VPN. **Note** In the case of NAT, the WAN routing selected here is used to advertise the NAT pool to the ISP
LAN and Service VPN Profile	Enable or disable VRRP settings. **Add Multiple VPNs at Once**: Use the option to add multiple VPNs. **VPN**: Enter a number for the VPN. **Number of Interfaces**: Choose the number of interfaces that will be used for each VPN segment. **Add Routing**: Configure routing protocols and static routes, or both, for each LAN segment. **Show Advanced**: Configure additional settings for the VPN segments.

6. Click **Next**.

7. On the **Additional Features** page, click **Dual Router High Availability** to create a redundancy group using the service VPNs.

   The service VPNs previously created are listed here.

8. Click the VPNs that will participate in high availability.

9. Click on a Cisco IOS XE Catalyst SD-WAN device to designate it as the active device for that VPN. This configures VPN homing, which determines which VPNs will participate in high availability. The following combinations are possible:

   a. **Active-Active**: Distribute the VPNs across two Cisco IOS XE Catalyst SD-WAN devices, resulting in the creation of two redundancy groups.

   b. **Active-Standby**: Assign all VPNs to a single Cisco IOS XE Catalyst SD-WAN device creating one redundancy group.

   c. **None**: Exclude VPNs from participating in high availability by setting their option to None. This means that traffic will be dropped if the active Cisco IOS XE Catalyst SD-WAN device fails.

10. Choose an high availability Interconnect option. The default selection is **Port-Channel** with a single member link, supporting up to two member links. Alternatively, you can choose a standalone interface.

11. Click **Next**.

12. In the **Summary** page, review the high availability configuration, and click **Create Configuration Group**.

Configure Cisco Catalyst SD-WAN Firewall High Availability Using Configuration Groups Feature Profiles

Create Configuration Group for High Availability

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

2. Click **Create Configuration Groups**

3. Enter a name for the configuration group.

4. Enter description for the configuration group.

5. From the **SiteType** drop-down list, choose **Dual Router**.

6. In the **Tag for Edge Device 01** field, enter a name for the first Cisco IOS XE Catalyst SD-WAN device.

   Tag names to identify the devices are displayed by default as **EdgeDevice_01** and **EdgeDevice_02**. To rename the tag names for the devices, click **Edit**.

7. In the **Tag for Edge Device 02** field, enter a name for the second Cisco IOS XE Catalyst SD-WAN device.

8. Click **Create** to create a new configuration group for two Cisco IOS XE Catalyst SD-WAN devices.

Create an Interconnect Interface for High Availability

1. From the **Transport and Management Profile** drop-down list, configure VPN 0 or the WAN VPN.

2. Click + icon next to a transport VPN, and click **Add New Feature**, and then click **Ethernet Interface**.

3. From the **Ethernet Interface** drop-down list, click **Add New** to create a Ethernet interface, which is the interconnect interface.

   The interconnect interface enables synchronization of services, such as firewall and NAT, between the two Cisco IOS XE Catalyst SD-WAN devices. It can be configured as either a physical interface or a port channel interface.

   To create a port channel interface for interconnection, click the **EtherChannel** tab.

4. From the **Ethernet Interface** page, in the **Basic Configuration** tab, enter an interface name.

5. Click the toggle **Use as Dual Router High Availability Interconnect** to enable interconnect on an interface. The interconnect only supports IPv4 addresses.

Note Only one interconnect interface can be created. To create a different interconnect interface, click **Use as Dual Router High Availability Interconnect** to disable the current interconnect. If multiple interconnect interfaces are needed, create a port-channel. For more information on creating a port-channel, see Configure a Transport Side EtherChannel Using a CLI Template.

6. Under **IPv4 Settings**, click to choose an option between **Dynamic** and **Static**.

7. Click **Save on Both Devices**.

Add a Service Profile for High Availability

The Service Profile helps you configure a VPN at LAN level. Add a Service Profile to the configuration group, and then create VPNs for the service profile. For more information about creating VPNs in the Service Profile, see Service VPN.

Configure High Availability

After you have created a service profile with VPNs, do the following:

1. From the Service Profile page, click **Add New Feature**.

2. Choose **Dual Router High Availability** to create a redundancy group using the VPNs from the Service Profile.

3. From the **Dual Router High Availability** drop-down list, click **Add New**.

4. Enter a name and description for the Dual Router High Availability profile.

   The VPNs that you created under the service profile will be listed here. Choose which VPNs will participate in high availability.

5. Click on a Cisco IOS XE Catalyst SD-WAN device to designate it as the active device for that VPN. This configures VPN homing, which determines which VPNs will participate in high availability. The following combinations are possible:

   a. **Active-Active**: Distribute the VPNs across two Cisco Catalyst IOS-XE SD-WAN devices, resulting in the creation of two redundancy groups.

   b. **Active-Standby**: Assign all VPNs to a single Cisco Catalyst IOS-XE SD-WAN device, creating one redundancy group.

   c. **None**: Exclude VPNs from participating in high availability by setting their option to None. This means that traffic will be dropped if the active Cisco IOS XE Catalyst SD-WAN device fails.

6. Click **WAN symmetry after switchover** to enable traffic from the WAN side to always be directed to the activeCisco IOS XE Catalyst SD-WAN device. This means that peer divert is not necessary, as the traffic will be routed to the active Cisco IOS XE Catalyst SD-WAN device, ensuring efficient and seamless traffic management.

Configure VRRP for Cisco Catalyst SD-WAN Firewall High Availability

To configure VRRP to follow the state of the redundancy group, enable **Follow Dual Router High Availability** in Cisco SD-WAN Manager. This configuration ensures that the VRRP primary role is assigned to the Cisco IOS XE Catalyst SD-WAN device with the active redundancy group, directing LAN-side traffic to the active redundancy group. If the active redundancy group fails, VRRP automatically reassigns the primary role to the device with the new active redundancy group, ensuring continuous service.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **…** adjacent to the configuration group name and choose **Edit**.
3. Edit the **Service Profile**.
4. Edit an Ethernet interface.
5. Click **VRRP**.
6. Click **Add VRRP IPv4** , and enter the following NAT pool parameters:

Table 2: VRRP Configuration

Parameter Name	Description
Group ID	Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups. Range: 1 through 255
Priority	Enter the priority level of the router. There router with the highest priority is elected as primary VRRP router. If two Cisco IOS XE Catalyst SD-WAN devices have the same priority, the one with the higher IP address is elected as primary VRRP router. Range: 1 through 254 Default: 100

Parameter Name	Description
Timer (milliseconds)	Specify how often the primary VRRP router sends VRRP advertisement messages. If subordinate routers miss three consecutive VRRP advertisements, they elect a new primary VRRP router. Range: 100 through 40950 milliseconds Default: 100 milliseconds **Note** When the timer is 100 ms for the VRRP feature template on Cisco IOS XE Catalyst SD-WAN devices, the VRRP fails if the traffic is high on LAN interface.
Track OMP Track Prefix List	By default, VRRP uses of the state of the service (LAN) interface on which it is running to determine which Cisco IOS XE Catalyst SD-WAN device is the primary virtual router. if a Cisco IOS XE Catalyst SD-WAN device loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, configure one of the following: **Track OMP**: Click **On** for VRRP to track the Overlay Management Protocol (OMP) session running on the WAN connection. If the primary VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session. **Track Prefix List**: Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the Track OMP option. In addition, if reachability to all of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the Cisco IOS XE Catalyst SD-WAN devices determine the primary VRRP router.
IP Address	Enter the IP address of the virtual router. This address must be different from the configured interface IP addresses of both the local Cisco IOS XE Catalyst SD-WAN device and the peer running VRRP.
Follow Dual Router High Availability	Click to enable VRRP to follow the state of the redundancy group.
VRRP Tracking Object	Enable an object to be tracked and perform an action, either **`decrement`** or **`shutdown`** based on the object's status. The Object number represents the interface to be tracked. Range: 1 through 100

7. Click **Add**.

Configure NAT DIA for Cisco Catalyst SD-WAN Firewall High Availability

To configure NAT DIA for high availability, do the following:

1. Create a configuration group with full mesh topology. For more information, see Create Configuration Group for NAT DIA, on page 17.
2. Create NAT Pools for high availability. For more information, see Create NAT Pools for High Availability, on page 19.

Create Configuration Group for NAT DIA

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Create Configuration Group**.
2. Enter a name for your configuration group.
3. Enter the description.
4. Click **Next**
5. Define the site settings and WAN circuits using the **Site Configurations** step.

Field	Description
Site Type	The configuration group type is **Single Router** by default. Choose **Dual Router**. Choose a role for the site: **Edge Site**: Used for branch offices or remote locations. **Border Site**: Used for data centers or central hubs.
Site Settings	Enter site specific values that may be common to other devices in Cisco SD-WAN Manager. **Local Device Access**: Enter a password for local device access. **Message of the Day:** Enter the message content to display important information to users upon login. This can include network policies, maintenance notifications, or security warnings. **Login**: Enter a login banner to display a legal notice or welcome message before the login prompt.

Field	Description
WAN Interfaces	Configure the WAN interfaces for the two Cisco IOS XE Catalyst SD-WAN devices. • **Full Mesh**: Click full mesh to configure DIA NAT. • **DHCP**: Click DHCP if the WAN interface should obtain an IP address automatically from a DHCP server. • **Static IP**: Click Static IP if you want to manually configure the IP address, subnet mask, and gateway for the WAN interface. • **Transport Name**: Enter a name to the transport network. • **Interface Color**: Assign a color to each transport network to visually differentiate them in the Cisco SD-WAN Manager interface. • **Use for Secondary Login**: Choose this option if the WAN interface should be used as a secondary login path for redundancy. This applies when a secondary region is configured in the Network Hierarchy Management. • **Shared with Access Region**: Click this option if the WAN interface should be shared with an access region. • **Exclusive to Secondary Region**: Click this option if the WAN interface should be exclusive to a secondary region. • **Show Advanced**: Click to configure additional settings for the WAN interface.
WAN Routing	Click **Add Routing** to include WAN routing details with BGP routes, OSPF routes, or multiple static IPv4 routes for your WAN transport VPN. The option you select here is used to advertise the NAT pool to the ISP.
LAN and Service VPN Profile	**Redundancy Protocol**: Click to enable or disable VRRP settings. **Add Multiple VPNs at Once**: Use the option to add multiple VPNs. **VPN**: Enter a number for the VPN. **Number of Interfaces**: Choose the number of interfaces that will be used for each VPN segment. **Add Routing**: Configure routing protocols and static routes for each VPN segment. **Show Advanced**: Click to configure additional settings for the VPN segments.

6. Click **Next**.

7. In the **Additional Features** page, click **Dual Router High Availability** to create a redundancy group using the VPNs.

   The Service VPNs that you created before will be listed here.

8. Click the VPNs that will participate in high availability

9. Click on a Cisco IOS XE Catalyst SD-WAN device to designate it as the active device for that VPN. This configures VPN homing, which determines which VPNs will participate in high availability. The following combinations are possible:

a. **Active-Active**: Distribute the VPNs across two Cisco IOS XE Catalyst SD-WAN devices, resulting in the creation of two redundancy groups.

b. **Active-Standby**: Assign all VPNs to a single Cisco IOS XE Catalyst SD-WAN device creating one redundancy group.

c. **None**: Exclude VPNs from participating in high availability by setting their option to None. This means that traffic will be dropped if the active Cisco IOS XE Catalyst SD-WAN device fails.

10. Choose an high availability Interconnect option. The default selection is **Port Channel** with a single member link, supporting up to two member links. Alternatively, you can choose a standalone interface.
11. Click **Next**.
12. On the **Summary** page, review the high availability configuration, and click **Create Configuration Group**.

Create NAT Pools for High Availability

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **…** adjacent to the configuration group name and choose **Edit**.
3. Edit the **Transport & Management Profile**.
4. Edit an Ethernet interface.
5. Click **NAT**.
6. In the **NAT** drop-down list, change the scope from **Default** to **Global**, and click **On** to enable NAT.
7. Click **Add Multiple NAT** to configure NAT pools.
8. Choose **Pool** as the NAT Type, and enter the following NAT pool parameters:

Table 3: NAT Pool Parameters

Parameter Name	Description
Pool ID	Enter a NAT pool ID.
Range Start	Enter a starting IP address for the NAT pool. a. Change the scope from **Default** to **Global** to enable the field. b. Enter the starting IP address for the NAT pool.
Range End	Enter a closing IP address for the NAT pool. a. Change the scope from **Default** to **Global** to enable the field. b. Enter the last IP address for the NAT pool.
Prefix Length	Enter the NAT pool prefix length.

Parameter Name	Description
Overload	Click to enable per-port translation. The default is **On**. **Note** If **Overload** is set to **Off**, only dynamic NAT is configured on the end device. Per-port NAT is not configured.
Dual Router High Availability Mapping	Click to enable dual router high availability mapping for the NAT pool. Enabling this ensures that traffic using this pool will be translated and protected.

9. Click **Add**.

   Similarly, you can configure high availability for NAT pools for static NAT and port forwarding.

Configure Service-Side NAT for Cisco Catalyst SD-WAN Firewall High Availability

In a service-side NAT for high availability configuration, policies must be configured and VPNs should be associated to redundancy group for high availability. Cisco SD-WAN Manager checks whether a VPN is associated with any redundancy group and if NAT pools are configured as part of the VPN configuration. If the VPN is already associated with an redundancy group, the configured NAT pools for the VPN will be considered. For information on configuring service-side NAT in Cisco SD-WAN Manager, see Configure Service-Side NAT.

Configure Cisco Catalyst SD-WAN Firewall High Availability Using CLI Commands

For information about using the CLI Profile in a configuration group, see CLI Add-On Profile.

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

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

This section provides example CLI configurations to configure Cisco Catalyst SD-WAN firewall high availability in an active-active redundancy group or in an active-standby redundancy group.

Configure High Availability in an Active-Active Redundancy Group

```
redundancy
 application redundancy
  group group-id
```

```
preempt
control interface-name protocol protocol-id data interface-name
asymmetric-routing interface interface-name
asymetric-routing always-divert enable
track object-number tracker-name
vpn vpn-id
track-enable track-number
init-role {active|standby}
path-optimization
```

Here’s the complete configuration example for configuring high availability in an active-active redundancy group. The Cisco IOS XE Catalyst SD-WAN device with this configuration defaults to the redundancy group being in standby when both devices come up.

```
redundancy
 application redundancy
  group 1
   preempt
   control GigabitEthernet6 protocol 1
   data GigabitEthernet6
   asymmetric-routing interface GigabitEthernet6
   asymetric-routing always-divert enable
   track 950 ha-wan-tracker
   vpn 3
   vpn 4
   vpn 5
   track-enable 32763
   init-role active
   path-optimization
  group 2
   preempt
   control GigabitEthernet6 protocol 1
   data GigabitEthernet6
   asymmetric-routing interface GigabitEthernet6
   asymetric-routing always-divert enable
   track 950 ha-wan-tracker
   vpn 1
   vpn 2
   track-enable 32764
   init-role standby
   path-optimization
```

Here's a sample configuration on the peer Cisco IOS XE Catalyst SD-WAN device.

```
redundancy
 application redundancy
  group 1
   preempt
   control GigabitEthernet6 protocol 1
   data GigabitEthernet6
   asymmetric-routing interface GigabitEthernet6
   asymetric-routing always-divert enable
   track 950 ha-wan-tracker
   vpn 3
   vpn 4
   vpn 5
   track-enable 32763
   init-role standby
   path-optimization
  group 2
   preempt
   control GigabitEthernet6 protocol 1
   data GigabitEthernet6
   asymmetric-routing interface GigabitEthernet6
   asymetric-routing always-divert enable
   track 950 ha-wan-tracker
   vpn 1
   vpn 2
   track-enable 32764
   init-role active
   path-optimization
```

Configure High Availability in an Active-Standby Redundancy Group

```
redundancy
 application redundancy
  group group-id
   preempt
   control interface-name protocol protocol-id data interface-name
   asymmetric-routing interface interface-name
   asymmetric-routing interface interface-name
   track object-number tracker-name
   vpn vpn-id
   track-enable track-number
   init-role {active|standby}
   path-optimization
```

Here’s the complete configuration example for configuring high availability in an active-standby redundancy group. This Cisco IOS XE Catalyst SD-WAN device is configured to be in the standby state.

```
redundancy
 application redundancy
  group 1
   preempt
   control GigabitEthernet6 protocol 1
   data GigabitEthernet6
   asymmetric-routing interface GigabitEthernet6
   asymetric-routing always-divert enable
   track 950 ha-wan-tracker
   vpn 3
   vpn 4
   vpn 5
   track-enable 32763
   init-role standby
   path-optimization
```

Here’s a sample configuration for the peer Cisco IOS XE Catalyst SD-WAN device in the active state .

```
redundancy
 application redundancy
  group 1
   preempt
   control GigabitEthernet6 protocol 1
   data GigabitEthernet6
   asymmetric-routing interface GigabitEthernet6
   asymetric-routing always-divert enable
   track 950 ha-wan-tracker
   vpn 3
   vpn 4
   vpn 5
   track-enable 32763
   init-role active
   path-optimization
```

Configure VRRP for High Availability Using CLI Commands

This section provides example CLI configuration to configure VRRP for high availability.

```
interface interface-name
 vrf forwarding vrf-id
 ip address ipv4-address subnet-mask
 no ip redirects
 ip mtu mtu-size
 load-interval interval
 negotiation auto
 ipv6 address ipv6-address
 no ipv6 redirects
 arp timeout timeout-value
 vrrp vrrp-group-id address-family ipv4
  vrrpv2
  track object-number decrement value
  address ipv4-address primary
 exit
 vrrp vrrp-group-id address-family ipv6
  track object-number decrement value
  address ipv6-address primary
  address ipv6-address
 exit
 redundancy rii rii-value
```

Here’s a complete configuration example for configuring VRRP for high availability.

```
interface GigabitEthernet7
 vrf forwarding 5
 ip address 12.168.51.15 255.255.255.0
 no ip redirects
 ip mtu 1496
 load-interval 30
 negotiation auto
 ipv6 address 2001:DB8:1:51::15/64
 no ipv6 redirects
 arp timeout 1200
 vrrp 45 address-family ipv4
  vrrpv2
  track 32763 decrement 10
  address 12.168.51.1 primary
 exit
 vrrp 54 address-family ipv6
  track 32763 decrement 10
  address FE80::1 primary
  address 2001:DB8:51:51::1/64
 exit
 redundancy rii 2053
```

Configure NAT for High Availability Using CLI Commands

Configure NAT DIA for High Availability

1. Configure NAT pool and redundancy.

```
ip nat pool pool-name start-ip end-ip prefix-length prefix-length
ip nat inside source list access-list pool pool-name redundancy
redundancy-group-id mapping-id mapping-id overload match-interface interface-name
ip nat inside source static inside-local-ip inside-global-ip vrf vrf-id
egress-interface interface-name redundancy redundancy-group-id mapping-id
mapping-id
ip nat inside source list access-list interface interface-name overload
```

Here’s the complete configuration example for configuring NAT pool and redundancy.

```
ip nat pool natpool1 15.1.1.1 15.1.1.10 prefix-length 24
ip nat inside source list dia-list-1 pool natpool1 redundancy 1 mapping-id 8194 overload
 match-interface GigabitEthernet3
ip nat inside source static 201.201.201.12 15.1.1.11 vrf 1 egress-interface
GigabitEthernet3 redundancy 1 mapping-id 7
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet3 overload
```

2. Configure NAT pool and port-forwarding redundancy.

```
ip nat pool pool-name start-ipaddress end-ipaddress prefix-length prefix-length
ip nat inside source list access-list pool pool-name redundancy redundancy-group
 mapping-id mapping-id overload match-interface interface
ip nat inside source static inside-local-ip inside-global-ip vrf vrf-name
egress-interface interface redundancy redundancy-group mapping-id mapping-id
ip nat inside source list access-list interface interface overload
```

Here’s the complete configuration example for configuring NAT pool and redundancy.

```
ip nat pool natpool1 15.1.1.1 15.1.1.10 prefix-length 24
ip nat inside source list dia-list-1 pool natpool1 redundancy 1 mapping-id 8194 overload
 match-interface GigabitEthernet3
ip nat inside source static 201.201.201.12 15.1.1.11 vrf 1 egress-interface
GigabitEthernet3 redundancy 1 mapping-id 7
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet3 overload
```

3. Policy configuration for NAT DIA and high availability.

```
policy
 data-policy policy-name
  vpn-list vpn-list-name
   sequence sequence-number
    match
     source-ip source-ip-address
     protocol protocol-numbers
    !
    action accept
     nat pool nat-pool-id
    !
   !
   default-action accept
  !
 !
 lists
  vpn-list vpn-list-name
   vpn vpn-id
  !
  site-list site-list-name
   site-id site-id
  !
 !
!apply-policy
 site-list site-list-name
  data-policy policy-name from-service
!
```

Here’s the complete configuration example for policy configuration on Cisco SD-WAN Controller for NAT and high availability.

```
policy
 data-policy b2b-vm1
  vpn-list b2b-vm1
   sequence 101
    match
     source-ip 12.201.201.0/24
     destination-ip 10.0.5.0/24
     protocol 1 6 17
    !
    action accept
     nat use-vpn 0
     nat source-dia-pool 1
    !
   !
  default-action accept
 !
!
lists
 vpn-list b2b-vm1
  vpn 1
 !
 site-list site100
  site-id 100
 !
!
apply-policy
 site-list site100
  data-policy b2b-vm1 all
!
!
```

4. NAT DIA interface configuration.

```
interface interface-name
 ip address ip-address subnet-mask
 ip nat outside
 negotiation auto
 ipv6 address ipv6-address
 ipv6 enable
 ipv6 nd ra suppress all
 redundancy rii rii-id
```

Here's a complete configuration about interface setup with NAT and redundancy.

```
interface GigabitEthernet3
 ip address 10.0.5.11 255.255.255.0
 ip nat outside
 negotiation auto
 ipv6 address 2001:A0:5::B/64
 ipv6 enable
 ipv6 nd ra suppress all
 redundancy rii 350
```

Configure Service-Side NAT for High Availability

1. Configure NAT pool and redundancy.

   ```
   ip nat pool pool-name start-ip end-ip prefix-length prefix-length
   ip nat inside source static inside-local-ip inside-global-ip vrf vrf-id
   match-in-vrf redundancy redundancy-group-id mapping-id mapping-id pool pool-name
   ip nat inside source list access-list pool pool-name redundancy
   redundancy-group-id mapping-id mapping-id vrf vrf-id match-in-vrf overload
   ```

   Here’s the complete configuration example for configuring service-side NAT for high availability.

   ```
   ip nat pool natpool1 15.1.1.1 15.1.1.10 prefix-length 24
   ip nat inside source static 192.168.11.2 15.1.1.5 vrf 1 match-in-vrf redundancy 1
   mapping-id 11 pool natpool1
   ip nat inside source list global-list pool natpool1 redundancy 1 mapping-id 5 vrf 1
   match-in-vrf overload
   ```

2. Configure NAT pool and port-forwarding redundancy.

   ```
   ip nat pool pool-name start-ipaddress end-ip prefix-length prefix-length
   ip nat inside source static protocol inside-local-ip local-port inside-global-ip
   global-port vrf vrf-id match-in-vrf redundancy redundancy-group-id mapping-id
   mapping-id pool pool-name
   ip nat inside source list access-list pool pool-name redundancy
   redundancy-group-id mapping-id mapping-id vrf vrf-id match-in-vrf overload
   ```

   Here’s the complete configuration example for configuring NAT pool and redundancy.

   ```
   ip nat pool natpool1 15.1.1.1 15.1.1.10 prefix-length 24
   ip nat inside source static udp 192.168.11.2 2558 15.1.1.11 2558 vrf 1 match-in-vrf
   redundancy 1 mapping-id 87 pool natpool1
   ip nat inside source list global-list pool natpool1 redundancy 1 mapping-id 5 vrf 1
   match-in-vrf overload
   ```

3. Policy configuration for service-side NAT and high availability.

   ```
   policy
    data-policy policy-name
     vpn-list vpn-list-name
      sequence sequence-number
       match
        source-ip source-ip-address
        protocol protocol-numbers
       !
       action accept
        nat pool nat-pool-id
       !
      !
      default-action accept
     !
   ```

```
 !
 lists
  vpn-list vpn-list-name
   vpn vpn-id
  !
  site-list site-list-name
   site-id site-id
  !
 !
!apply-policy
 site-list site-list-name
  data-policy policy-name from-service
!
```

Here’s the complete configuration example for policy configuration on Cisco SD-WAN Controller for NAT and high availability.

```
policy
 data-policy vm1
  vpn-list vm1
   sequence 20
    match
     source-ip 20.201.201.0/24
     protocol 1 6 17
    !
    action accept
     nat pool 1
    !
   !
   default-action accept
  !
 !
 lists
  vpn-list vm1
   vpn 1
  !
  site-list vm1
   site-id 100
  !
 !
!
apply-policy
 site-list vm1
  data-policy vm1 from-service
!
```

Note If you want to disable the application redundancy feature, and there are existing NAT configurations that rely on this redundancy, you must remove those NAT configurations first. Only after removing the NAT configurations can you proceed to disable the application redundancy.

Verify High Availability

Verify Redundacy Groups

The following is a sample output from the **show redundancy application group** command. This command provides detailed information about the redundancy groups configured on a Cisco IOS XE Catalyst SD-WAN device, showing their redundancy group IDs, redundancy group names, and current states (active or standby). This information helps to monitor and manage high availability and failover configurations effectively.

```
Device# show redundancy application group
Group ID Group Name      State

1   Generic-Redundancy-1 STANDBY
2   Generic-Redundancy2 ACTIVE
```

The following is a sample output from the **show redundancy application group** command with group id. This command provides information about the specified redundancy application group on a Cisco IOS XE Catalyst SD-WAN device. It includes the administrative and operational states, roles of the current and peer devices, communication status, path optimization, and redundancy framework states.

```
Device# show redundancy application group 1
Group ID:1
Group Name:

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: STANDBY
Peer Role: ACTIVE
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes
Path Optimization: Enabled
TLOC Pref Change: 0

RF Domain: btob-one
RF state: STANDBY HOT
Peer RF state: ACTIVE

Device# show redundancy application group 2
Group ID:2
Group Name:

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: STANDBY
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes
Path Optimization: Enabled
TLOC Pref Change: 0

RF Domain: btob-two
RF state: ACTIVE
Peer RF state: STANDBY HOT
```

The following is a sample output from the **show redundancy application group all** command. This command provides information about all redundancy application groups configured on a Cisco IOS XE Catalyst SD-WAN device.

```
Device# show redundancy application group all
Faults states Group 1 info:
Runtime priority: [100]
RG Faults RG State: Up.
Total # of switchovers due to faults:           0
Total # of down/up state changes due to faults: 0

RG Protocol RG 1

Role: Standby
    Init Role: Standby
    Negotiation Flags 0x1
    Tunnel: UP, DIA: DOWN
    Negotiation: Enabled
    Priority: 100
    Protocol state: Standby-hot
    Ctrl Intf(s) state: Up
    Active Peer: address 10.1.55.15, priority 100, intf Po1
    Standby Peer: Local
    Log counters:
            role change to active: 1
            role change to standby: 1
            disable events: rg down state 0, rg shut 0
            ctrl intf events: up 2, down 1, admin_down 0
            reload events: local request 0, peer request 0


RG Media Context for RG 1
Ctx State: Standby
    Protocol ID: 1
    Media type: Default
    Control Interface: Port-channel1
    Current Hello timer: 3000
    Configured Hello timer: 3000, Hold timer: 10000
    Peer Hello timer: 3000, Peer Hold timer: 10000
    Stats:
            Pkts 10, Bytes 620, HA Seq 0, Seq Number 10, Pkt Loss 0
            Authentication not configured
            Authentication Failure: 0
            Reload Peer: TX 0, RX 0
            Resign: TX 1, RX 0
    Active Peer: Present. Hold Timer: 10000
            Pkts 3, Bytes 102, HA Seq 0, Seq Number 7, Pkt Loss 0


Group ID:1
Group Name:

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: STANDBY
Peer Role: ACTIVE
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes
Path Optimization: Enabled
TLOC Pref Change: 0

RF Domain: btob-one
RF state: STANDBY HOT
Peer RF state: ACTIVE

Faults states Group 2 info:
Runtime priority: [100]
```

```
RG Faults RG State: Up.
Total # of switchovers due to faults:           0
Total # of down/up state changes due to faults: 0


RG Protocol RG 2
Role: Active
    Init Role: Active
    Negotiation Flags 0x1
    Tunnel: UP, DIA: DOWN
    Negotiation: Enabled
    Priority: 100
    Protocol state: Active
    Ctrl Intf(s) state: Up
    Active Peer: Local
    Standby Peer: address 10.1.55.15, priority 100, intf Po1
    Log counters:
            role change to active: 1
            role change to standby: 0
            disable events: rg down state 0, rg shut 0
            ctrl intf events: up 2, down 1, admin_down 0
            reload events: local request 0, peer request 0



RG Media Context for RG 2
Ctx State: Active
    Protocol ID: 1
    Media type: Default
    Control Interface: Port-channel1
    Current Hello timer: 3000
    Configured Hello timer: 3000, Hold timer: 10000
    Peer Hello timer: 3000, Peer Hold timer: 10000
    Stats:
            Pkts 8, Bytes 496, HA Seq 0, Seq Number 8, Pkt Loss 0
            Authentication not configured
            Authentication Failure: 0
            Reload Peer: TX 0, RX 0
            Resign: TX 0, RX 1
    Standby Peer: Present. Hold Timer: 10000
            Pkts 4, Bytes 136, HA Seq 0, Seq Number 9, Pkt Loss 0


Group ID:2
Group Name:

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: STANDBY
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes
Path Optimization: Enabled
TLOC Pref Change: 0

RF Domain: btob-two
RF state: ACTIVE
Peer RF state: STANDBY HOT
```

Verify Protocol Details of Redundancy Groups

Examples

The following is sample output from the **show redundancy application group protocol** command.

```
Device# show redundancy application group protocol

RG Protocol RG 1
------------------
        Role: Active
        Init Role: Active
        Negotiation Flags 0x1
        Tunnel: UP, DIA: DOWN
        Negotiation: Enabled
        Priority: 100
        Protocol state: Active
        Ctrl Intf(s) state: Up
        Active Peer: Local
        Standby Peer: address 10.1.55.14, priority 100, intf Po1
        Log counters:
                role change to active: 11
                role change to standby: 7
                disable events: rg down state 3, rg shut 0
                ctrl intf events: up 5, down 2, admin_down 1
                reload events: local request 1, peer request 0

RG Media Context for RG 1
--------------------------
        Ctx State: Active
        Protocol ID: 1
        Media type: Default
        Control Interface: Port-channel1
        Current Hello timer: 3000
        Configured Hello timer: 3000, Hold timer: 10000
        Peer Hello timer: 3000, Peer Hold timer: 10000
        Stats:
                Pkts 10001, Bytes 620062, HA Seq 0, Seq Number 10001, Pkt Loss 0
                Authentication not configured
                Authentication Failure: 0
                Reload Peer: TX 0, RX 0
                Resign: TX 3, RX 4
        Standby Peer: Present. Hold Timer: 10000
                Pkts 7385, Bytes 251090, HA Seq 0, Seq Number 10004, Pkt Loss 0



RG Protocol RG 2
------------------
        Role: Standby
        Init Role: Standby
        Negotiation Flags 0x1
        Tunnel: UP, DIA: DOWN
        Negotiation: Enabled
        Priority: 100
        Protocol state: Standby-hot
        Ctrl Intf(s) state: Up
        Active Peer: address 10.1.55.14, priority 100, intf Po1
        Standby Peer: Local
        Log counters:
                role change to active: 3
                role change to standby: 3
                disable events: rg down state 0, rg shut 0
                ctrl intf events: up 1, down 0, admin_down 0
                reload events: local request 0, peer request 0
```

```
RG Media Context for RG 2
--------------------------
        Ctx State: Standby
        Protocol ID: 1
        Media type: Default
        Control Interface: Port-channel1
        Current Hello timer: 3000
        Configured Hello timer: 3000, Hold timer: 10000
        Peer Hello timer: 3000, Peer Hold timer: 10000
        Stats:
                Pkts 7396, Bytes 458552, HA Seq 0, Seq Number 7396, Pkt Loss 0
                Authentication not configured
                Authentication Failure: 0
                Reload Peer: TX 0, RX 0
                Resign: TX 3, RX 2
        Active Peer: Present. Hold Timer: 10000
                Pkts 7177, Bytes 244018, HA Seq 0, Seq Number 7394, Pkt Loss 0
```

This example verifies the protocol-specific details of application redundancy groups such as the current role (active or standby), status of control interfaces, negotiation flags, priorities, and peer details. The example also verifies the status of tunnels and Direct Internet Access (DIA), log counters for various events, and media context settings, including hello and hold timers. Additionally, it provides statistics on packet and byte counts, sequence numbers, packet loss, and authentication status.

Verify Redundancy Group Interfaces

The following is sample output from the **show redundancy application control-interface group** command.

```
Device# show redundancy application control-interface group 1

The control interface for rg[1] is Port-channel1
Interface is Control interface associated with the following protocols: 1
BFD Enabled
Interface Neighbors:
Peer: 10.1.55.14 Active RGs: 2 Standby RGs: 1 BFD handle: 0

The control interface for rg[2] is Port-channel1
Interface is Control interface associated with the following protocols: 1
BFD Enabled
Interface Neighbors:
Peer: 10.1.55.14 Active RGs: 2 Standby RGs: 1 BFD handle: 0
```

This example shows **`Port-channel1`** is the control interface for redundancy groups 1 **`(rg[1])`** and 2 **`(rg[2])`**. The interface is associated with protocol ID 1 and has BFD enabled.

The following is sample output from the **show redundancy application data-interface group** command.

```
Device# show redundancy application data-interface group

The data interface for rg[1] is Port-channel1
The data interface for rg[2] is Port-channel1
```

In this example, the command output indicates that the data interface for both redundancy group 1 (rg[1]) and redundancy group 2 (rg[2]) is Port-channel1. This setup ensures that Port-channel1 is used to handle the data traffic for both redundancy groups, facilitating efficient traffic management and high availability.

Verify Redundancy Interface Identifiers Configuration

The following is sample output from the **show redundancy rii** command.

```
Device# show redundancy rii
No. of RIIs in database: 10
 Interface                         RII Id     decrement
  GigabitEthernet3.104          :   2049         0
  GigabitEthernet3.103          :   2050         0
  GigabitEthernet3.102          :   2051         0
  GigabitEthernet7              :   2053         0
  GigabitEthernet3.105          :   2054         0
  Tunnel2                       :   513          0
  Tunnel1                       :   514          0
  GigabitEthernet3.101          :   2052         0
  GigabitEthernet2              :   1            0
  GigabitEthernet1              :   2            0
```

In this example, there are 10 RIIs in the database. The table lists each interface along with its associated RII ID and decrement value, which is 0 for all entries. The interfaces include various GigabitEthernet ports and Tunnel interfaces, each uniquely identified by an RII. This information helps in managing high availability by mapping and associating interfaces accurately within redundancy groups.

Verify Firewall Datapath in Redundancy Groups

The following is sample output from the **show platform hardware qfp active feature firewall datapath rg** command.

```
Device# show platform hardware qfp active feature firewall datapath rg 1

rg 1, rg_state 0x00030035 (Active, Transport Up, Flow On, AR Transport UP, Allow New Sessions,
 Update Peer)
11 (RG Active) ha_handle 0x00020102 rg_flags 0x0 session id 0x5

==== HA general stat ====
Initial bulksync retry count 0
Allocated retry entries 0
Current retry queue depth 0
Maximum queued retries 0
Max retries queued ever 0
Stats were all zero

==== HA active stat ====
Total received messages 1
Session create requests 5
Session delete requests 5
Bulksync requests received 1
Bulksync complete 1
Session sync attempt: create 5
Session sync attempt: delete 5

==== HA standby stat ====
Stats were all zero
```

In this example, the command output shows that redundancy group 1 is active, with all transport and flow mechanisms operational. The high availability general statistics indicate no retries were necessary, suggesting stable synchronization. The active statistics reveal that session creation and deletion requests are being processed efficiently, and bulksync operations are functioning correctly. The standby statistics show no activity, which is typical in a stable high availability setup. This detailed information helps ensure seamless failover and maintain high availability in the network.

The following is sample output from the **show platform hardware qfp active feature firewall datapath rg 1 all** command.

```
Device#  show platform hardware qfp active feature firewall datapath rg 1 all
rg 1, rg_state 0x00030035 (Active, Transport Up, Flow On, AR Transport UP, Allow New Sessions,
 Update Peer)
11 (RG Active) ha_handle 0x00020102 rg_flags 0x0 session id 0x5

==== HA general stat ====
Initial bulksync retry count 0
Allocated retry entries 0
Current retry queue depth 0
Maximum queued retries 0
Max retries queued ever 0
Total retry allocations 0
Retry allocation failures 0
Total retry entries queued 0
Flow on 0
Flow off 0
Retry timeout 0

==== HA active stat ====
Total received messages 1
Missing RII 0
Session create requests 5
Session delete requests 5
Session update requests 0
Bulksync requests received 1
Bulksync complete 1
L7 buffers allocated 0
L7 buf alloc failure 0
Failed to send L7 data 0
L7 data sent 0
Invalid opcode recvd 0
Message too short 0
Bad version number 0
Bad magic number 0
Create NAKs received 0
No HA buffer 0
No buffer false positive 0
Session sync attempt: create 5
Session sync attempt: update 0
Session sync attempt: delete 5
Session sync attempt: l7 data 0
vrf mapping failures 0
Invalid protocol 0
PAM classificaiton failure 0
Classificaiton failure 0
Could not find parent flow 0
Asymmetric routing injection 0
Data transport down 0
Bad bulk sync feature id 0
Bad bulk sync message length 0
Bulk sync error: init not complete 0
Bulk sync - active now standby 0
Bulk sync - Standby not read 0
Transport Down 0
Attempt to initiate bulk sync on active 0
Invalid no response bulk sync timer on active 0
Bulk sync request retry re-queued 0
Bulk sync request retry re-queue failed 0
Bulk sync done re-queued 0
Bulk sync done re-queue failed 0

==== HA standby stat ====
Total received messages 0
Session create requests 0
Session delete requests 0
Session update requests 0
```

```
Create NAK sent 0
Inspection policy not found 0
Could not create session 0
Could not create subordinate session 0
New sessions not allowed 0
Could not locate ingress uidb RII 0
Could not locate egress uidb RII 0
RG not configured 0
Could not locate uidb sub-block 0
Invalid zone - no inspection 0
Invalid zone - drop 0
Invalid zone pair 0
Classification failed 0
Classification results missing stats 0
Subflow RG mismatch 0
RG mismatch on create/flow exists 0
Could not find session 0
Session RG mismatch 0
Session delete miss 0
Session delete RG mismatch 0
Layer 7 data 0
Rcvd bad opcode 0
Msg too short 0
Unsupported msg version 0
Bulk sync requested 0
Bulk sync requested timeout 0
Bulk sync requested failed 0
Bulk Sync msg sent 0
Bulk sync complete 0
Peer not identified 0
Could not allocate msg buffer 0
Could not find VRF 0
Asymmetric routing redirect 0
Asymmetric routing redirect failed - no uidb_sb 0
Asymmetric routing redirect failed - no AR 0
Transport Down 0
Bulk sync failed : no response 0
Existing session removed/replaced 0
Invalid message magic number 0
```

In this example, the output displays all statistics using the `all` option in the command, providing detailed insights into the current state and performance metrics of both the active and standby components of the High Availability system. The high availability system is functioning correctly, with the active component efficiently handling requests and synchronization processes, while the standby component remains prepared without any errors or issues.

Verify Firewall Session Information in High Availability Environments

The following is sample output from the **show policy-firewall session platform detail** command.

```
Device# show policy-firewall session platform detail

[s=session  i=imprecise channel c=control channel  d=data channel u=utd inspect A/D=appfw
action allow/deny]
Session ID:0x100000B7 192.168.11.10 34157 10.0.12.131 80 proto 6 (1:1:1:1) (3:0x3000050:http)
 [sc]
 pscb : 0x156da640,  key1_flags: 0x00000000
 bucket : 34590, prev 0x0, next 0x0    fw_flags: 0x01800000 0x20c06a21,
  Flattened-AVC HA-AVC
  Root Protocol-TCP Initiator Alert Proto-State:Timewait Session-db HA-create Max-session
    icmp_error count 0 ureachable arrived: no
    scb state: active, nxt_timeout: 100, refcnt: 1 NBAR verdict count 0
    ha nak cnt: 0, rg: 1
    hostdb: 0x0, L7: 0x0, stats: 0x160ebfc0, child: 0x0
    isn:        1826966309 last ack:       987459709 next seq:         1826966394 wnd_size:
          2169783926
 wnd_scale:         29200
    isn:         987459708    last ack:        987459708    next ack:        987459708
wnd_size:          2169783926
 wnd_scale:         65535
    tcp flags:     0x00000000 :  : proto: 0018: l7 ooo drop 0x010 l7_prot 0x12 - http
    root scb: 0x0 act_blk: 0x160e3f00
    ingress/egress intf: GigabitEthernet3.101 (65530), GigabitEthernet1 (65530)
    current time 284036397554511 create tstamp: 283915721110241 last access: 284035994128283
 now 284036397556361 csec left
    nat_out_local_addr:port: 10.0.12.131:80
    nat_in_global_addr:port: 101.101.101.101:34157
    ip6: addr1 :: addr2 ::
    key ip4: addr1 10.0.12.131:80 addr2 192.168.11.10:34157
    syncookie fixup: 0x0,  halfopen linkage: 0x0 0x0
    cxsc_cft_fid: 0x00000000
    tw timer: 0x00000000 0x00000000 0x00000000 0x14f53101
    domain_ab1 0x0 14 per filter stats 0x0 avc class id 0x3 http SGT: 0 DGT: 0
    NAT handles 0x11194110 0x00000000
    FlowDB in2out 0x00000000 alloc_epoch 0 out2in 0x00000000 alloc_epoch 0 ppe tid 0
    icmp_err_time 0 utd_context_id 0, classification epoch scb: 0x1 actblk :0x1 avc class
stats 0x0
    VPN id src 1, dst 0
    zone pair ZP_ZONE_1_untrusted_ZON_47132514 class
ZONE_1_TO_UNTRUSTED-seq-SEQUENCE-829881385-cm_
```

In this example, the command **show policy-firewall session platform detail** provides detailed information about firewall sessions on the device, particularly when high availability is involved. This command is used to gather comprehensive data about active firewall sessions, including session states, counters, and other important metrics.

Monitor Firewall High Availability

You can monitor the traffic or applications using Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Locate the device that you want to view the status for. You can either scroll through the list of devices in the device table or enter a keyword in the search bar.
3. Choose the device by clicking its name in the **Hostname** column.
4. In the left pane, click **Real Time**.
5. From the **Device Options** drop-down list in the right pane, choose **Redundancy Group App Group**. This option allows you to view detailed information about the redundancy groups configured on the selected device.

View Network Site Topology

Cisco SD-WAN Manager provides a visual representation of the network topology for each site, featuring the Cisco IOS XE Catalyst SD-WAN devices deployed in a high-availability configuration. Cisco SD-WAN Manager displays the topology of the chosen site, illustrating the interconnected devices and their roles within the high-availability configuration. For more information, see View Network Site Topology.