MX Warm Spare - High Availability Pair

MX Warm Spare Overview

This page describes how to set up a High availability (HA) pair using the VRRP protocol between two MX Security Appliances in either one-arm Concentrator mode or NAT mode, as well as the expected behavior of configured HA pairs. High availability can be used to minimize downtime in the event of a hardware failure.

Only one license is required for an HA pair. The warm spare unit does not require a separate license. Alerts for Warm spare failover can be configured on the Alerts and Administration page.

Note: The secondary MX must be the same MX model as the primary. Warm spare functionality is not supported between different MX models (e.g. MX80 & MX100).
Use Case

In most customer deployments, network downtime has a direct impact on the business and should be avoided at all costs. Warm Spare functionality prevents the network from having a single point of failure at the edge and allows for fast, automatic recovery in the event of device failure, reducing the negative impact on end-user services.

Benefits

- In the event of hardware failure, network downtime will be greatly reduced or eliminated entirely depending on the architecture being used.
- No manual intervention by the network administration team will be required to facilitate recovery from a hardware failure.

Terminology

For purposes of this document, it is important to understand the following terms and their meaning:

**Primary**: The MX that is configured as the "main" MX for the network. If both MXes are online, this is the MX that traffic should be flowing through. This is a static designation, meaning that regardless of the current state of the network the Primary will always be the Primary.

**Spare**: The MX that is configured as the "secondary" MX for the network. If both MXes are online, this is the MX that is the inactive warm spare. This is a static designation, meaning that regardless of the current state of the network the Secondary will always be the Secondary.

**Active (Master)**: The MX that is currently acting as the edge firewall/security appliance for the network. This is a dynamic designation.

**Passive**: The MX that is currently acting as an inactive warm spare with no traffic passing through it. This is a dynamic designation.

**Dual Master**: Dual Master describes a scenario in which both the Primary and the Spare are in the Active state. This occurs when both MXes are online and communicating with the cloud, but the Secondary is not receiving heartbeat packets (see VRRP heartbeats in the next section) from the Primary. This can cause several issues with Dynamic DNS, VPN, and traffic processing in general and should be avoided at all costs. The Physical Architectures section of this document describes how to deploy an MX Warm Spare pair in order to minimize the chances of a Dual Master scenario occurring.
Underlying Concepts and Technologies

**VRRP Heartbeats**

Failure detection for an MX Warm Spare pair uses VRRP heartbeat packets. These heartbeat packets are sent from the Primary MX to the Secondary MX on all configured VLANs in order to indicate that the Primary is online and functioning properly. As long as the Secondary is receiving these heartbeat packets, it functions in the spare state. If the Secondary stops receiving these heartbeat packets, it will assume that the Primary is offline and will transition into the master state. When the MX is in NAT mode, VRRP heartbeats are not sent over the WAN; there is no guarantee that the WAN interfaces can communicate with each other. Instead, we use a mechanism called "connection monitor" to determine the WAN state of the device.

For more in-depth information regarding the VRRP Mechanics on the MX, please see the [NAT HA Failover Behavior](#) documentation.

**Connection Monitor**

Connection monitor is an uplink monitoring engine built into every MX Security Appliance. The mechanics of the engine are described in [this article](#). When all uplinks of a Primary MX are marked as failed by connection monitor, that MX will stop sending VRRP heartbeat packets, which will initiate a Warm Spare failover. Once at least one uplink on the Primary returns to a working state, the Primary resumes sending heartbeat packets and the Secondary relinquishes the Active role back to the Primary.

**DHCP Synchronization**

To prevent a scenario in which an IP address is assigned by the Primary via DHCP and then that same address is assigned to another client by the Secondary after a failover, the DHCP lease table is synchronized regularly between the Primary and Secondary over UDP port 3483.

**Dashboard Configuration**

To configure warm spare failover for an existing Dashboard network, navigate to the [Security & SD-WAN > Monitor > Appliance status](#), and select [Configure warm spare](#) near the upper-left side of the page, below the device name. In the window that appears, select **Enabled**. Enter the serial number of the Secondary MX and select the desired Uplink IP configuration, then select **Update** to enable Warm Spare.

### Warm spare

![Configure warm spare](#)

**Use MX uplink IPs:** When using this option, the current Active MX will use its distinct uplink IP or IPs when sending traffic out to the Internet. This option does not require additional public IPs for Internet-facing MXes, but also results in more disruptive failover because the source IP of outbound flows will change.
**Use virtual uplink IPs:** When using this option, both MXes will use a shared virtual IP (VIP) when sending traffic out to the Internet. This option requires an additional public IP per uplink but allows for seamless failover because the IP address the network is using to communicate with the Internet will be consistent. The VIP for each uplink must be in the same subnet as the IPs of the MXes themselves for that uplink, and the VIP must be different from both MX uplink IPs.

To configure a new network with warm spare failover, create the network as you would normally and add the Primary MX. Then add the Secondary MX using the process described above.

Regardless of which option is selected, both MX devices will need their own uplink IP addresses for Dashboard connectivity.

Dashboard configuration should always be performed before the Secondary MX is physically connected to the network.

Note that when an MX is added to a network that already contains an MX of the same model from the Organization > Inventory page, the MX will automatically be added to that network in warm spare mode.

**MX Mode Options for Warm Spare Configuration**

MX devices can be configured in a warm spare, high-availability pair using one of two MX addressing options:

- VPN Concentrator/Passthrough Mode
- NAT Mode

Note that while the mode is reflected in Dashboard as a **VPN Concentrator/Passthrough Mode** the MX only supports a One-Armed concentrator topology for this mode. Additional information regarding this can be found in the Connecting the MXes in a “One-Armed” VPN Concentrator Pair section.

Each mode will result in having two MXs on the same network, with a primary able to fail over to a secondary. However, each mode requires a slightly different configuration. The different configuration methods and considerations are detailed here. If you need more information about the MX addressing modes, or how to select which one is best for your deployment, refer to our **MX Addressing and VLANs article**.

**VPN Concentrator Warm Spare**

Concentrator warm spare is used to provide high availability for a Meraki AutoVPN head-end appliance.

**Network Setup**

Each concentrator has its own IP address to exchange management traffic with the Meraki Cloud Controller. However, the concentrators also share a virtual IP address that is used for non-management communication.
Connecting the MXes in a “One-Armed” VPN Concentrator Pair

Before deploying MXs as one-arm VPN concentrators, place them into **Passthrough or VPN Concentrator** mode on the **Addressing and VLANs** page. In one-armed VPN concentrator mode, the units in the pair are connected to the network **only** via their respective **Internet** ports. **Make sure they are not connected directly via their LAN ports.** They must be within the same IP subnet and able to communicate with each other, as well as with the Cisco Meraki Dashboard. Only VPN traffic is routed to the MX, and both ingress and egress packets are sent through the same interface.

**Virtual IP**

The virtual IP address (VIP) is shared by both the primary and warm spare VPN concentrator. VPN traffic is sent to the VIP rather than the physical IP addresses of the individual concentrators. The virtual IP is configured by navigating to **Security & SD-WAN > Monitor > Appliance status** when a warm spare is configured. It must be in the same subnet as the IP addresses of both appliances, and it must be unique. In particular, it cannot be the same as either the primary or warm spare's IP address.

**Failure Detection**

The two concentrators share health information over the network via the VRRP protocol. Failure detection does not depend on connectivity to the Internet / Meraki dashboard.

In the event that the primary unit fails, the warm spare will assume the primary role until the original primary is back online. When the primary VPN concentrator is back online and the spare begins receiving VRRP heartbeats again, the warm spare concentrator will relinquish the active role back to the primary concentrator.

The total time for failure detection, failover to the warm spare concentrator, and ability to start processing VPN packets is typically less than 30 seconds.

**NAT Warm Spare**

NAT Warm Spare is used to provide redundancy for internet connectivity and appliance services when an MX Security Appliance is being used as a NAT gateway.

**WAN Virtual IPs**

Virtual IP addresses (VIPs) are shared by both the primary and warm spare appliance. Inbound and outbound traffic uses this address to maintain the same IP address during a failover and reduce disruption. The virtual IPs are configured on the **Security & SD-WAN > Monitor > Appliance status** page, under the **SPARE** section in the upper-left corner of the page. If two uplinks are configured, a VIP can be configured for each uplink. Each VIP must be in the same subnet as the IP addresses of both appliances for the uplink it is configured for, and it must be unique. In particular, it cannot be the same as either the primary or warm spare's IP address.
LAN IP addresses are configured based on the Appliance IPs in any configured VLANs. No virtual IPs are required on the LAN.

**Failure Detection**

There are two failure detection methods for NAT mode warm spare.

**WAN Failover:** WAN monitoring is performed using the same internet connectivity tests that are used for uplink failover. For more data on these checks, see the Cisco Meraki Knowledge Base. If the primary appliance does not have a valid internet connection based on these tests, it will stop sending VRRP heartbeats which will result in a failover. When uplink connectivity on the original primary appliance is restored and the warm spare begins receiving VRRP heartbeats again, it will relinquish the active role back to the primary appliance.

**LAN Failover:** The two appliances share health information over the network via the VRRP protocol. These VRRP heartbeats occur at layer 2 and are performed on all configured VLANs. If no advertisements reach the spare on any VLAN, it will trigger a failover. When the warm spare begins receiving VRRP heartbeats again, it will relinquish the active role back to the primary appliance.
DHCP Synchronization

The MXes in a NAT mode high availability pair exchange DHCP state information over the LAN on UDP port 3483. This prevents a DHCP IP address from being handed out to a client after a failover if it has already been assigned to another client prior to the failover.

Requirements and Best Practices

When configuring NAT HA, it is critical that both MXs have a reliable connection to each other on the LAN, so the Primary MX's VRRP heartbeats can be seen reliably by the Spare. To ensure this connection is reliable:

- The two MXs should be connected to each other through a downstream switch (or, ideally, multiple switches) on the LAN to allow for passing VRRP heartbeats.
  - There should be no more than one additional hop between them, and they must be able to communicate on all VLANs.
  - Make sure STP is enabled on the downstream switching infrastructure, as a properly-configured HA topology will introduce a loop on the network.
- When first configuring NAT HA, the Spare should be added and configured in Dashboard before the device is physically deployed, so it will immediately fetch its configuration and behave appropriately.

Additionally, the following other considerations should be kept in mind:

- Both MXs must share the same number of uplinks. That is, if the Primary MX has dual uplinks, then the Spare must have dual uplinks as well.
- If a virtual IP is being used, then each uplink of the two MXs must share the same broadcast domain on the WAN side.

Cellular Failover Behavior

Meraki does not currently support any cellular failover with a high availability (HA) pair; as we do not perform connection monitoring on cellular uplinks (as of MX 10.X+), which is necessary for HA uplink failover. At this time, if a cellular uplink is used in an HA pair, the following will occur in order:

1. Primary MX WAN 1+2 fails > fails over to Secondary MX
2. Secondary MX WAN 1+2 fails > fails over to Primary MX Cellular
3. Primary MX cellular fails > fails over to Secondary MX Cellular

While it is possible to use cellular failover as described above, it is not officially supported by Meraki.

Recommended Topologies

There are two physical architectures available for NAT Warm Spare deployments.

Fully Redundant (Multiple Switches)

In this architecture, the Primary and Secondary MXs are not directly connected, and VRRP Heartbeats are carried...
between the downstream switches. This is the recommended architecture for most deployments, as there is no single point of failure in this topology.

Fully Redundant (Switch Stack)

In this architecture, the Primary and Secondary MXs are connected via a downstream switch stack. Each switch has at least one uplink to each MX. This ensures that there is no single point of failure in the topology.
Troubleshooting NAT Warm Spare

If there is a problem with the NAT HA configuration, there may be various symptoms that will affect the network, and it may not be obvious that the root cause is NAT HA. This section outlines what issues with HA typically look like, as well as recommended troubleshooting steps.

**Dual Master Issue**

The most common sign of a problem with NAT HA is a Dual Master scenario, where both the Primary and Spare MX report in Dashboard as being Active (master). This can be observed in Dashboard under Security & SD-WAN > Monitor > Appliance status and comparing the current state of each appliance.

This will occur if the Primary MX is online and sending heartbeats that aren't seen by the Spare, resulting in the Spare thinking that the Primary is down. If both the Primary and Spare are in the master state, this will cause various issues with the network, affecting DHCP, routing, VPN, etc.
Recommended Troubleshooting Steps

If network issues are occurring that appear to be related to NAT HA, the following troubleshooting steps should be taken to identify the root cause:

1. Check both appliances in Dashboard (under Security & SD-WAN > Monitor > Appliance status) to check if there is a Dual Master scenario as outlined above.
   a. If both appliances are consistently reporting in the "active" state, check their LAN connection and make sure they can communicate with each other.
   b. If the Spare MX is intermittently reporting as active while the Primary remains online and active, check that both MXes can communicate with each other on all VLANs. Additionally, ensure there are no bad cables connecting the two devices or any other physical issue that could result in unreliable communication.
   c. In any case, it is strongly recommended to take a packet capture on the LAN side of each MX, to get a clear picture of where the VRRP heartbeats are being lost.

2. If the HA pair is configured to use a virtual IP on the uplink, make sure that each pair of WAN connections (WAN 1 on each MX, for example) share the same broadcast domain, so they can both be seen by the upstream device. See the image below for an example topology with dual uplinks/ISPs.