Passthrough Mode on the MX Security Appliance and Z-series Teleworker Gateway

The MX Series Security Appliance and Z-series Teleworker Gateway can be deployed in Passthrough or VPN Concentrator mode. In this mode, it will not perform address translation and acts as a layer 2 bridge between the Internet and LAN ports.

When in passthrough mode, the MX is best used for in-line:

- Layer 3/7 firewall rules, traffic shaping, and analysis
- Network asset discovery and reporting
- Intrusion detection
- Security and content filtering
- Client and site-to-site VPN

Configuration Differences

There are a number of differences in configuration between Routed and passthrough modes on the MX:

- Secondary uplinks cannot be used for Internet connectivity. Thus Security & SD-WAN > Configure > SD-WAN & traffic shaping > Uplink configuration only has the option for limiting bandwidth on WAN 1.
- Site-to-site VPN can only operate in split-tunnel mode when configured as a hub. Traffic bound to VPN subnets must be directed to the MX.
- DHCP is no longer available. DHCP requests will simply pass through the MX.
- Cellular uplink is no longer available.
- VLANs cannot be configured. The MX/Z1 will act as a bridge between the Internet and LAN ports.

Considerations for VPN and Other Features

When using an MX as a site-to-site VPN peer, it will only be able to send client traffic over the VPN tunnel if that traffic has been directed to it. As such, a router or L3 switch on the network will need to have static routes configured, such that VPN-bound traffic is sent to the MX. This traffic will then be encrypted and sent through the site-to-site VPN tunnel. Traffic bound to the Internet or other destinations will simply pass through the appliance:
An MX in passthrough mode can be configured to perform a number of functions like when in Routed mode. However, the appliance acts as an invisible third party, only touching traffic when required by a configured function. It can passively perform intrusion detection and collect statistics about traffic passing through it without taking action. It can also perform traffic shaping and content/security filtering functions to intercept and manipulate traffic as needed:

**Additional Resources**

For details on how to configure IDS, traffic shaping, content filtering, security filtering, warm spare, and other MX functions, please visit the [MX Series Configuration Guide](#).