

Meraki MX is an enterprise security & SD-WAN appliance designed for distributed deployments. Ideal for admins who demand both ease of deployment and a state-of-the-art feature set one would expect out of a next-gen firewall: intrusion prevention, content filtering, anti-malware, geo-based firewalling, remote access and more.

Key Features:

Auto VPN: The fastest site-to-site VPN set up with just 3 clicks. The dashboard features tools which give administrators a real-time view of VPN site performance.

Cloud Management: Remotely manage and monitor all Meraki devices from anywhere.

Identity-based Firewall: Easily control access to your network with the MX identity-based firewall, using user and device identity to enforce granular security policies.

SD-WAN: Improve the reliability and performance of your WAN with SD-WAN technology, seamlessly connecting branch locations and optimizing traffic routing.

Talos Content Filtering¹: Block inappropriate websites and control access to content.

IDS/IPS¹: Protect your network against cyber threats with advanced intrusion prevention capabilities, which continuously monitor network traffic and alert on any potential threats.

Malware Protection¹: Cisco's Advanced Malware Protection is integrated into MX devices to ensure all files coming into the network are classified as clean, malicious, or unknown.

Cloud Integration: Extend SD-WAN to public cloud providers including AWS, Azure, Alibaba Cloud, GCP and private cloud environments using Cisco NFVIS.

High availability and failover: Ensure the continuous availability of your network with configuration options supporting high availability and failover features.

Cisco Secure Client VPN: Using Secure Client ([AnyConnect](#)) with Meraki MX for remote access can enable users secure and seamless connectivity between different locations.

Umbrella Integrations (DNS /SIG¹): Link Meraki dashboard with the Cisco Umbrella dashboard and easily assign Umbrella content filtering and security policies.

PCI Compliance: PCI 3.2 certified cloud management backend.

ThousandEyes: Deploy Agents to get insight into how apps and networks are performing.

¹ Advanced Security license required

FAQs:

Q: Can the MX form IPsec VPN tunnels to non-Meraki devices?

A: Yes, the MX supports standard IPsec VPN in addition to Meraki Auto VPN.

Q: Does my network traffic flow through the Cisco Meraki cloud infrastructure?

A: User data (network traffic, web browsing etc.) does not flow through the Meraki cloud, and instead flows directly to the destination on the LAN or across the WAN.

Q: What happens if the devices can't access the Cisco Meraki cloud?

A: If your MX loses connectivity, it will operate with the last known configuration. All data flows will operate assuming the service provider link is still up. The MX will attempt to reconnect and failover to other Meraki data centers for reporting and analytics.

License Comparisons:

(All Meraki products require a license)

| | Enterprise | Adv Security | SD-WAN Plus |
|---|------------|--------------|-------------|
| 3-click secure SD-WAN connectivity (Auto VPN) | ✓ | ✓ | ✓ |
| L7 stateful firewall | ✓ | ✓ | ✓ |
| Site-to-Site and Client VPN | ✓ | ✓ | ✓ |
| Application Visibility and Control | ✓ | ✓ | ✓ |
| Malware Protection (AMP) | | ✓ | ✓ |
| Secure Malware Analytics Support (requires license) | | ✓ | ✓ |
| Intrusion Detection & Prevention (IDS/IPS) | | ✓ | ✓ |
| Talos URL Content filtering (CIPA Compliant) | | ✓ | ✓ |
| Layer 7 Geo-IP Firewall Rules | | ✓ | ✓ |
| Google SafeSearch & YouTube EDU enforcement | | ✓ | ✓ |
| Internet Outages from ThousandEyes | | | ✓ |
| Smart L7 local internet breakout | | | ✓ |
| Performance-based internet routing | | | ✓ |
| ML-powered SD-WAN analytics | | | ✓ |

Enterprise license for all products:

- Access to Cloud Portal
- Warranty (varies by product, lifetime for MX)
- 24x7 Enterprise Support
- Feature and software upgrades
- Group Policies can be applied across multiple Meraki platforms

Discovery:

- How many branches do you have and how do you manage them?
- How are you currently managing VPN between your branches?
- Do you control internet access and web applications? If so, how do you accomplish that today?

Resources:

[SalesConnect](#)

[Data Sheet](#)

[MX Sizing Guide](#)

[MX Announcements](#)

[AnyConnect on MX](#)

[Meraki Community](#)

[Webinars](#)

[Learning](#)

[Auto-VPN](#)

[Documentation](#)

[Meraki Blog](#)

[Public page](#)