



MX Sizing Principles

July 2023

This document provides information to supplement the selection of suitable Cisco Meraki MX security and SD-WAN appliances based on industry standard benchmarks and in-depth feature descriptions. It is highly recommended the information in this document be used in conjunction with a proof-of-concept trial to finalize model selections.

Overview

Cisco Meraki MX security and SD-WAN appliances provide unified threat management (UTM) and SD-WAN in a powerful all-in-one device.

Given the broad range of configurations an MX can be deployed in, device performance will vary depending on the use case. Choosing the right MX depends on the use case and the deployment characteristics. For detailed sizing and capabilities of vMX devices please review the [vMX specific data sheet](#).

The technical information contained in this document is designed to help answer the following questions:

- How do I decide which MX model(s) I should evaluate?
- How does device performance vary by features enabled?
- How do MX models compare against other vendors?

MX portfolio capabilities

	Z3/C	Z4	MX67 (C/W)	MX68 (W/CW)	MX75	MX85	MX95	MX105	MX250	MX450	vMX Small	vMX Medium	vMX Large			
																
Dual WAN ¹			✓	✓	✓	✓	✓	✓	✓	✓						
3G/4G/5G failover ²	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓						
Built-in LTE modem model available	✓		✓	✓												
Built-in wireless available	✓	✓	✓	✓										N/A		
Built-in PoE+ model available ³	✓	✓		✓	✓	✓	✓	✓								
WAN fiber connectivity					SFP	SFP	SFP+	SFP+	SFP, SFP+	SFP, SFP+						
Dual power supply								✓	✓	✓						
Form factor	Desktop	Desktop	Desktop	Desktop	Desktop	1U	1U	1U	1U	1U	Virtual	Virtual	Virtual			
HTTPS inspection ⁴	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	N/A					
Advanced Malware Protection		✓	✓	✓	✓	✓	✓	✓	✓	✓	N/A					
Intrusion detection and prevention			✓	✓	✓	✓	✓	✓	✓	✓	N/A					

¹ For MX67(C/W) devices, dual WAN is available via a convertible LAN interface.

² For models without integrated cellular, cellular failover is available when leveraging a MG cellular gateway.

³ Z3; Z4, MX68, and MX75 have PoE+ capabilities for LAN ports. MX85; MX95, and MX105 have PoE capabilities for WAN ports. Please refer to product-specific data sheets for additional details.

⁴ Available natively on indicated platforms, via Cisco Umbrella SD-WAN extension, or a third-party provider reachable via VPN.

Network performance benchmarks

Industry-standard benchmarks are designed to help you compare MX appliances to those from other vendors. These tests assume perfect network conditions with ideal traffic patterns. When measuring maximum throughput for a certain feature, all other features are disabled. All throughput performance results below are achieved by running MX firmware version 18.107. Actual results in production networks will vary.

	Z3/C	Z4	MX67/68	MX75	MX85	MX95	MX105	MX250	MX450	vMX Small	vMX Medium	vMX Large
Max stateful (Layer 3) firewall throughput in NAT mode with large payload file transfers	100 Mbps	500 Mbps	600 Mbps	1 Gbps	1 Gbps	2 Gbps	3 Gbps	4 Gbps	5 Gbps			
Max Stateful (Layer 3) Firewall Throughput in NAT mode (EMIX)¹	100 Mbps	500 Mbps	600 Mbps	1 Gbps	1 Gbps	2 Gbps	3 Gbps	4 Gbps	4 Gbps			
Max VPN throughput with large payload files transfers	50 Mbps	250 Mbps	300 Mbps	500 Mbps	500 Mbps	800 Mbps	1 Gbps	1 Gbps	2 Gbps	250 Mbps	500 Mbps	1 Gbps
Max VPN throughput (EMIX)²	50 Mbps	250 Mbps	300 Mbps	500 Mbps	500 Mbps	800 Mbps	1 Gbps	1 Gbps	1.5 Gbps	250 Mbps	500 Mbps	1 Gbps
Max throughput with all security features enabled³	N/A	300 Mbps	300 Mbps	700 Mbps	700 Mbps	2 Gbps	2.5 Gbps	2 Gbps	2.5 Gbps			
Max site-to-site VPN tunnels⁴	10	25	50	75	200	500	1,000	3,000	5,000	50	250	1,000
Recommended maximum site-to-site VPN tunnels⁵	4	8	50	75	100	250	500	1,000	1,500	50	250	1,000
Recommended maximum client VPN tunnels	1	2	50	75	100	250	250	500 ⁶	500 ⁶	50	250	500 ⁶
WAN failover⁷	<5 seconds											
Auto VPN tunnel failover⁷	Sub-second											
Dynamic path selection⁷	Sub-second											

Testing includes use of industry standard IXIA breakpoint RFC-2544 benchmark testing and enterprise mix (EMIX) testing.

¹ Max stateful (L3) firewall throughput in NAT mode, or simply NAT throughput, uses the EMIX performance test with no features enabled other than a L3 firewall rule.

² Max site-to-site VPN throughput, or VPN throughput, uses the EMIX performance test with no features as we do in NAT throughput, but over a single Auto VPN tunnel.

³ Max "throughput" is based on IPS in detection mode using the "connectivity" rule set with the exception of Z4. Z4 Security features testing is performed only with AMP enabled.

⁴ Max site-to-site VPN tunnels are based on lab-testing scenarios where no client traffic is transferring over the VPN tunnels.

⁵ Recommended max site-to-site VPN tunnels are based on lab-testing scenarios with client traffic transferring over VPN tunnels.

⁶ [Load balancing](#) for client VPN can be utilized if more than 500 connections are required.

⁷ Times for failover after failover criteria has been met.

Features, benefits, and performance impact

Unified Threat Management (UTM) products come with a variety of security and networking features. Understanding the benefits and trade-offs of these features is crucial to getting the maximum security benefit without unnecessary performance degradation.

	Benefits	Performance impact	Recommendations
Cisco Advanced Malware Protection (AMP)	Blocks HTTP-based file downloads based on the disposition received from the Cisco AMP cloud.	Low	Consider disabling for guest VLANs and using firewall rules to isolate those VLANs. Also consider disabling if you run a full malware client like AMP for endpoints on host devices.
Content filtering	Category-based URL filtering	Low	Consider blocking only necessary categories while aligning with your security guidelines.
Web-safe Search	Turning Google/Bing SafeSearch option on	Low	Must be deployed in tandem with "disable encrypted search" option to be effective.
Cisco IDS/IPS (SNORT)	Provides alerts / prevention for suspicious network traffic	Medium	Rulesets other than "connectivity" have a larger performance impact. Additionally, consider not sending IDP/IPS syslog data over VPN in low-bandwidth networks.
HTTPS inspection	Allows advanced security features on the MX to inspect and act on HTTPS traffic	High	Use of Cisco Umbrella SD-WAN extensions to offload processing from edge or concentrator devices will reduce performance impacts to MX devices.
Number of VPN tunnels	Secure, encrypted traffic between locations	High	Use split-tunnel VPN and deploy security services at the edge.
FIPS mode	FIPS Compliant security levels for dashboard connectivity; device storage, and VPN transmissions.	High	Consider engaging your account specialist for appropriate sizing and network architecture when using this feature.

Use case recommendations

Although there is no hard limit on the number of users that can be deployed on MX appliances, for purposes of this document, all tests were performed with the user counts shown in the table below. Exceeding these user counts may result in performance that varies from the sizing data contained in this guide.

Recommended use cases

Z3/C	Z4	MX67/68 series	MX75	MX85	MX95	MX105	MX250	MX450	vMX
Teleworker gateway with up to 5 devices	Teleworker gateway with up to 5 devices	Small branch with up to 50 users	Small branch with up to 200 users	Small to medium branch with up to 250 users	Medium to large branch with up to 500 users	Large branch with up to 750 users	Campus or VPN concentrator with up to 2,000 users	Campus or VPN concentrator with up to 10,000 users	Cloud VPN concentrator with up to 2,000 users

Built-in MX device utilization

This document aims to provide guidance on the expected utilization and load levels for specific MX models with certain features enabled. However, to accurately predict the load on the device, it must be tested in its designated environment under expected conditions. This means that device utilization in certain situations could be high even before reaching the recommended numbers in the previous tables.

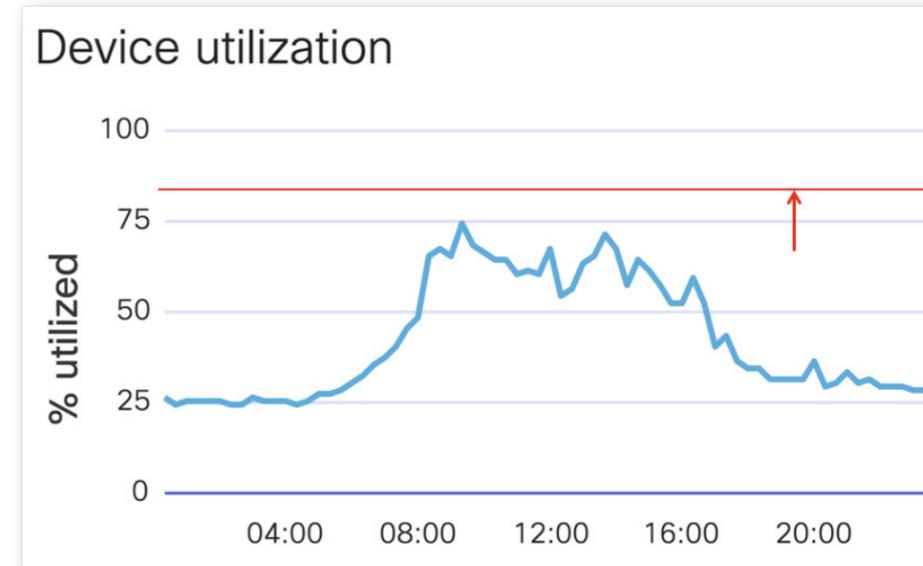
MX [device utilization](#) helps provide a better understanding of the device's load over time and can be used to assess the utilization level and whether a higher end device or a load reduction is required. If an MX device is consistently over 85% utilization during normal operation*, upgrading to a higher throughput model or reducing the per device load should be considered. The MX device utilization tool is available through an API endpoint or as a graph shown on the Summary Report page.

MX device utilization calculation

The device utilization data reported to the Meraki dashboard is based on a load average measured over a period of one minute. The load value is returned in numeric value ranging from 1 through 100. A lower value indicates a lower load and a higher value indicates a more intense workload. Currently, the device utilization value is calculated based on the CPU utilization of the MX as well as its traffic load.

Due to load averaging, it's possible for transient load spikes to occur without being visible in the utilization metric. For example, a device load that is consistently shown as less than 85% may still be experiencing transient load spikes. These transient load spikes may cause packets received in excess of the device's forwarding capacity to be dropped.

* With all the desired features turned on, the expected number of clients connected and/or the expected traffic mix traversing the device.



Conclusion

While every network will have a unique traffic pattern, this highlights a few common scenarios to help you choose the right Cisco Meraki MX product for your environment. Consider planning for future growth by allocating buffer room in your firewall selection (i.e., if you currently have 550 users, choose an MX that supports 1,000 users). This will ensure that you can continue enabling additional security and network features as they become available. Also, considering ISP speeds are increasing year over year, it's important to choose a firewall that will serve you well over time.

