Meraki

MX Sizing Principles

March 2021

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

Overview

Cisco Meraki MX Security & SD-WAN Appliances deliver are Unified Threat Management (UTM) and SD-WAN from 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.

This 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

	MX64(W)	MX67(W/C)	MX68(W/CW)	MX84	MX100	MX250	MX450	vMX Small	vMX Medium	vMX Large
										
Dual Links	✓	✓	✓	✓	✓	✓	✓			
3G / 4G Failover	✓	✓	✓	✓	✓	✓	✓			
Built-In LTE Modem Model Available		✓	✓							
Built-In Wireless Available	✓	✓	✓						N/A	
Built-In PoE+ Model Available			✓							
Hard Drive				1TB	1TB	128GB (SSD)	128GB (SSD)			
WAN Fiber Connectivity				SFP	SFP	SFP, SFP+	SFP, SFP+			
Dual Power Supply						✓	✓			
Form Factor	Desktop	Desktop	Desktop	1U	1U	1U	1U	Virtual	Virtual	Virtual
HTTPS Inspection*	✓	✓	✓	✓	✓	✓	✓		N/A	

*Available via built-in third-party VPN to Umbrella SIG or Zscaler.

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. Actual results in production networks will vary.

	MX64 series	MX67/68 series	MX84	MX100	MX250	MX450	vMX Small	vMX Medium	vMX Large
Max throughput with all security features enabled	200 Mbps	300 Mbps	320 Mbps	650 Mbps	2 Gbps	4 Gbps	N/A		
Max Stateful (L3) firewall throughput in passthrough mode	250 Mbps	450 Mbps	500 Mbps	750 Mbps	4 Gbps	6 Gbps			
Max Stateful (L3) firewall throughput in NAT mode	200 Mbps	450 Mbps	500 Mbps	750 Mbps	4 Gbps	6 Gbps			
Max site-to-site VPN throughput	100 Mbps	200 Mbps	250 Mbps	500 Mbps	1 Gbps	2 Gbps	200 Mbps	500 Mbps	1 Gbps
Max concurrent site-to-site VPN tunnels [1]	50	50	100	250	3,000	5,000	50	250	1,000
Recommended maximum concurrent site-to-site VPN tunnels [2]	50	50	100	250	1,000	1,500	50	250	1,000
Recommended maximum concurrent client VPN tunnels	50	50	100	250	500[3]	500[3]	50	250	500
Max AMP throughput	250 Mbps	300 Mbps	500 Mbps	750 Mbps	2 Gbps	4 Gbps	N/A		
Max IDS throughput	200 Mbps	300 Mbps	320 Mbps	650 Mbps	2 Gbps	4 Gbps			
WAN failover[4]	<5 seconds	<5 seconds	<5 seconds	<5 seconds	<5 seconds	<5 seconds			
Auto VPN tunnel failover[4]	Sub-second	Sub-second	Sub-second	Sub-second	Sub-second	Sub-second	Sub-second	Sub-second	Sub-second
Dynamic Path Selection[4]	Sub-second	Sub-second	Sub-second	Sub-second	Sub-second	Sub-second	Sub-second	Sub-second	Sub-second

All throughout performance results above are achieved running MX 14.39 firmware using the recognized, industry-standard IXIA BreakingPoint testing software.

[1] The maximum concurrent site-to-site VPN tunnels are based on lab testing scenarios where no client traffic is transferring over the VPN tunnels.

[2] Recommended concurrent site-to-site VPN tunnels are based on lab testing scenarios with client traffic transferring over VPN tunnels.

[3] More than 500 client VPN connections can be achieved, please refer to **this guide**.

[4] Times for failover after failover criteria has been met.

Features, benefits, and performance impact

UTM products come with a variety of security and networking features. Understanding the benefits and tradeoffs 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 filed 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.
Cisco IDS / IPS (SNORT)	Provides alerts / prevention for suspicious network traffic	Medium	Consider not sending IDS/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	The performance impact of HTTPS inspection will be high on any appliance on the market. An alternative could be to consider moving the HTTPS inspection workload to the cloud with Cisco Umbella SIG.
Number of VPN tunnels	Secure, encrypted traffic between locations	High	Use split-tunnel VPN and deploy security services at the edge.
Content filtering (top sites)	Category based URL filtering using locally downloaded database	Low	Choose this option if your priority is speed over coverage.
Content filtering (full list)	Category based URL filtering using the full database hosted at Brightcloud.com	Low	Choose this option if your priority is 100% coverage and security. Web browsing will be slightly slower at the beginning but will improve as more and more URL categories are cached.
Web safe-search	Turning Google / Bing safe-search option on	Low	Must be deployed in tandem with “disable encrypted search” option to be effective.

Client recommendations

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

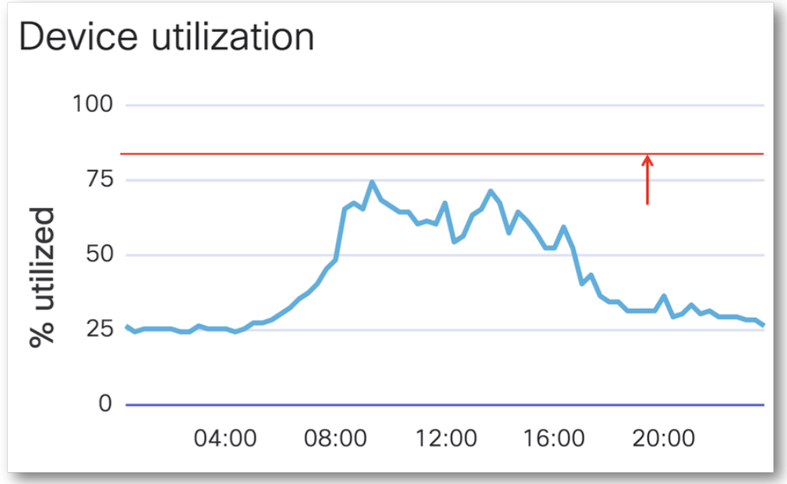
Recommended number of client devices

	MX64 series	MX67/68 series	MX84	MX100	MX250	MX450
Recommended client devices	50	50	200	500	2,000	10,000

Built-in MX device utilization

This document aims to educate users 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 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 upon 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 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 (e.g., if you currently have 550 users, choose an MX that supports 1000 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 is important to choose a firewall that will serve you well over many years.