Cisco Meraki

MX Sizing Guide

SEPTEMBER 2018

This technical document provides guidelines for choosing the right Cisco Meraki security appliance based on real-world deployments, industry standard benchmarks and in-depth feature descriptions.

Overview

Cisco Meraki MX Security Appliances are Unified Threat Management (UTM) products. UTM products offer multiple security features in a simple-to-deploy, consolidated form factor. Given the number of security features that can be deployed in any given MX, device performance will vary depending on the use-case. Choosing the right MX depends on the use-case and the deployment characteristics.

This technical guide is designed to help answer the following questions:

- How do I decide which MX model I need?
- Which features should I turn on?
- How do MX models compare against the competition?

Choosing the right hardware

Cisco Meraki MX products come in 8 product families. The chart below outlines MX hardware properties available under each family:

	MX64(W) 	MX65(W) 	MX67(W/C) 	MX68(W/CW) 	MX84 	MX100 	MX250 	MX450
Dual Wan Links	✓	✓	✓	✓	✓	✓	✓	✓
3G / 4G Failover	✓	✓	✓	✓	✓	✓	✓	✓
Built-In LTE Modem Model Available			✓	✓				
Built-In Wireless Available	✓	✓	✓	✓				
Built-In PoE+ Model Available		✓		✓				
Hard Drive					1TB	1TB	128GB (SSD)	128GB (SSD)
Fiber Connectivity					SFP	SFP	SFP, SFP+	SFP, SFP+
Dual Power Supply							✓	✓
Form Factor	Desktop	Desktop	Desktop	Desktop	1U	1U	1U	1U

Network performance benchmarks

Industry standard benchmarks are designed to help you compare MX security appliances to firewalls 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.

	MX64/65 series	MX67/68 series	MX84	MX100	MX250	MX450
Max throughput with all security features enabled	200 Mbps	300 Mbps	320 Mbps	650 Mbps	2 Gbps	4 Gbps
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 VPN throughput	100 Mbps	200 Mbps	250 Mbps	500 Mbps	1 Gbps	2 Gbps
Max concurrent VPN tunnels [1] (site-to-site or client VPN)	50	50	100	250	3,000	5,000
Recommended maximum concurrent VPN tunnels [2] (site-to-site or client VPN)	50	50	100	250	1,000	1,500
Max AMP throughput	250 Mbps	300 Mbps	500 Mbps	750 Mbps	2 Gbps	4 Gbps
Max IDS throughput	200 Mbps	300 Mbps	320 Mbps	650 Mbps	2 Gbps	4 Gbps

The SD-WAN feature set for the MX includes active-active VPN, which creates VPN tunnels between peers on all available uplinks in order to make the most efficient possible use of available WAN bandwidth. A connection between two peers can therefore contain up to four tunnels, depending on the number of MX uplinks at each site. This should be taken into consideration when making VPN sizing decisions.

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

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

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
Malware protection	Blocks HTTP-based filed downloads based on the disposition received from the Cisco AMP cloud.	High	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.
IDS / IPS	Provides alerts / prevention for suspicious network traffic	High	Consider not sending IDS/IPS syslog data over VPN in low-bandwidth networks.
VPN	Secure, encrypted traffic between locations	Medium	Use split-tunnel VPN and deploy security services at the edge.
Web caching	Accelerating access to Web content by caching locally	Medium	Ideal for repetitively accessing heavy multimedia content frequently for low bandwidth networks. Not recommended for high bandwidth networks. Please note that YouTube doesn't support web caching.
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	Medium	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.
Blocking encrypted search	Disabling Google / Bing searches via https (port 443), allowing Web safe-search enforcement	Low	Must be deployed in tandem with "Web safe-search" to be effective. Requires a DNS setting modification, otherwise will also break Google apps. Check Meraki knowledge base for further information.

Client recommendations

Although there is no hard limit on the number of client devices that can be deployed below MX Security 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.

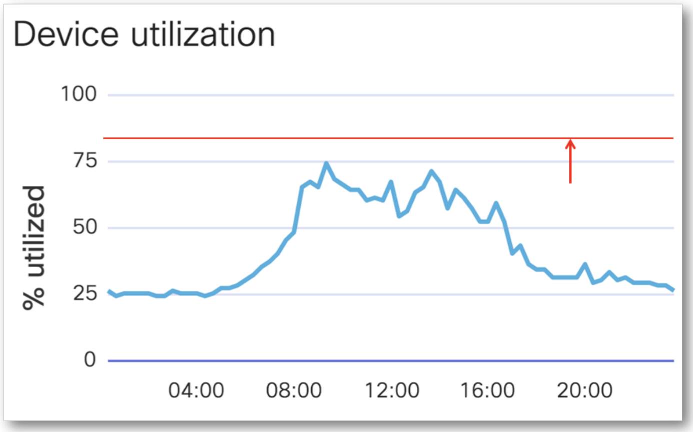
RECOMMENDED NUMBER OF CLIENT DEVICES

	MX64/65 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 guide aims to educate the user 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. There are a large number of variables in each individual network that will affect real-world performance, such as the unique traffic blend and the features in use.

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 guide 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.