MX Sizing Guide & Principles

This document serves as a guide for the architecture and design of networks incorporating MX firewall appliances. This document aims to help determine the appropriate MX model to evaluate, understand how the performance of devices can vary with different features enabled, and compare MX models with those from other vendors.

Click 日本語 for Japanese

Use of This Document

Current Firmware Version: MX 18.2x

This document is to be used to assist in the architecture and design of networks in which MX firewall appliances will be present. Key questions which this document is designed to help answer are:

- 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?

It is highly recommended to leverage this document with a proof of concept for further validation of design and implementation as each network environment is unique.

With the release of each major MX firmware version throughput; feature specific data, or flow and session specific data may change. This document will provide guidance on these MX performance metrics in a variety of scenarios and environments.

> Note that each network environment and traffic profile is unique. It should be taken into account that the numbers presented in this document are obtained during testing in a vacuum where no detrimental network or traffic profile behavior is present.

> The Performance metrics detailed in this document are based on the **Current Firmware Version** listed above. It should be noted not all platforms can support MX 18.2x, more details surrounding this can be found here.

Portfolio Capabilities

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

Choosing the right MX depends on the use case and deployment characteristics.
For detailed sizing and capabilities of vMX devices please review the vMX specific data sheet.

Below is a breakdown of the MX; Z-Series, and vMX Portfolio's hardware capabilities.

MX-Series

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

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

Dual power supply models have an active/standby redundant power supply and do not provide combined power.

MX68 and MX75 PoE+ capabilities are available for LAN ports. MX85, MX95, and MX105 PoE+ capabilities are available for WAN ports. PoE/PoE+ is provided to an MG via these ports is supported. Please refer to product-specific data sheets for additional details.

HTTPS Inspection is available natively on indicated platforms via Cisco Umbrella SD-WAN extension, or via a third-party provider reachable via VPN.

	MX67 (C/W)	MX68 (W/ CW)	MX75	MX85	MX95	MX105	MX250	MX450
Dual Active WAN	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
3G/4G Failover	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Built-in LTE Modem*	Yes	Yes	No	No	No	No	No	No
Built-in Wi-Fi**	Yes	Yes	No	No	No	No	No	No
Built-in PoE+	No	Yes	Yes	Yes	Yes	Yes	No	No
WAN Fiber Connectivity	No	No	SFP	SFP	SFP+	SFP+	SFP, SFP+	SFP, SFP+
Dual Power Supply	No	No	No	No	No	Yes	Yes	Yes
Form Factor	Desktop	Desktop	Desktop	1U	1U	1U	1U	1U
HTTPS Inspection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Advanced Malware Protection (AMP)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Intrusion Detection and Prevention (SNORT IPS/ IDS)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

* - Only if the MX model has a C. Ex: MX67C, MX68C

** - Only if the MX model has a W. Ex: MX67W, MX68W

Z-Series

	Z3 (C)	Z4 (C)
Dual Active WAN	No	No
3G/4G Failover Model Available	Yes	Yes

Built-in LTE Modem Model Available	Yes	Yes
Built-in Wi-Fi Available	Yes	Yes
Built-in PoE (LAN Port) Model Available	Yes (802.3af, PoE)	Yes (802.3at, PoE+)
WAN Fiber Connectivity	No	No
Dual Power Supply	No	No
Form Factor	Desktop	Desktop
HTTPS Inspection	Yes	Yes
Advanced Malware Protection (AMP)	No	Yes
Intrusion Detection and Prevention (SNORT IPS/IDS)	No	No

vMX-Series

	vMX-Small	**vMX-Medium**	**vMX-Large**	**vMX-Extra Large**
Dual WAN	N/A	N/A	N/A	N/A
3G/4G/5G Failover	N/A	N/A	N/A	N/A
Built-in LTE Modem Model Available	N/A	N/A	N/A	N/A
Built-in Wireless Available	N/A	N/A	N/A	N/A
Built-in PoE+ Model Available	N/A	N/A	N/A	N/A
WAN Fiber Connectivity	N/A	N/A	N/A	N/A
Dual Power Supply	N/A	N/A	N/A	N/A
Form Factor	Virtual	Virtual	Virtual	Virtual
HTTPS Inspection	N/A	N/A	N/A	N/A
Advanced Malware Protection (AMP)	N/A	N/A	N/A	N/A
Intrusion Detection and Prevention (SNORT IPS/IDS)	N/A	N/A	N/A	N/A

Use Case Recommendations

A use case recommendation is based off of the device throughput; available feature set, and maximum flow table capacity. In this calculation, each client is considered to consume up to 50 flows.

MX-Series

	MX67	MX68	MX75	MX85	MX95	MX105	MX250	MX450
Recommended Maximum Device Count	50	50	200	250	500	750	2,000	10,000

Z-Series

	Z3 (C)	Z4 (C)
Recommended Maximum Device Count	5	15

vMX-Series

	vMX-Small	vMX-Medium	vMX-Large	vMX-Extra Large
Recommended Maximum Device Count	500	2,500	10,000	20,000

Feature Specific Data

The following items should be noted:

- Max site-to-site VPN tunnels are based on lab-testing scenarios where no client traffic is transferring over the VPN tunnels.
- Recommended max site-to-site VPN tunnels are based on lab-testing scenarios with client traffic transferring over VPN tunnels.
- Load balancing for client VPN can be utilized if more than 500 connections are required.
- Criteria must be met prior to WAN; dynamic path selection, or tunnel failover times occurring.

MX-Series

	MX67	MX68	MX75	MX85	MX95	MX105	MX250	MX450
Maximum Site to Site VPN Tunnel Count	50	50	75	200	500	1,000	3,000	5,000
Recommended Maximum Site to Site VPN Tunnel Count	50	50	75	100	250	500	1,000	1,500
Maximum Number of Client VPN Tunnels	50	50	75	100	250	250	500	500
Maximum Number of AnyConnect Sessions	100	100	250	250	500	750	1000	1500

WAN Failover	< 5 Sec	< 5 Sec	< 5 Sec	< 5 Sec	< 5 Sec	< 5 Sec	< 5 Sec	< 5 Sec
Auto VPN Tunnel Failover	Sub-second	Sub-second	Sub-second	Sub-second	Sub-second	Sub-second	Sub-second	Sub-second
Dynamic Path Selection	Sub-second	Sub-second	Sub-second	Sub-second	Sub-second	Sub-second	Sub-second	Sub-second

Z-Series

	Z3 (C)	**Z4 (C)**
Maximum Site to Site VPN Tunnel Count	10	10
Recommended Maximum Site to Site VPN Tunnel Count	4	8
Maximum Number of Client VPN Tunnels	1	2
WAN Failover	< 5 Sec	< 5 Sec
Auto VPN Tunnel Failover	Sub-second	Sub-second
Dynamic Path Selection	Sub-second	Sub-second

vMX-Series

	vMX-Small	**vMX-Medium**	**vMX-Large**	**vMX-Extra Large**
Maximum Site to Site VPN Tunnel Count	50	250	1,000	10,000
Recommended Maximum Site to Site VPN Tunnel Count	50	250	1,000	10,000
Maximum Number of Client VPN Tunnels	50	250	500	To be announced
WAN Failover	N/A	N/A	N/A	N/A
Auto VPN Tunnel Failover	Sub-second	Sub-second	Sub-second	Sub-second
Dynamic Path Selection	Sub-second	Sub-second	Sub-second	Sub-second

Flow and Session Data

It is important to understand the number of flows, or open sessions, supported by each appliance. For purposes of sizing, a flow is any transmission on an open socket within the last 5 minutes. Note that this is not a recommended flow capacity number, but instead these values are to be maximums.

MX-Series

	MX67	**MX68**	**MX75**	**MX85**	**MX95**	**MX105**	**MX250**	**MX450**

Maximum Concurrent Sessions	25,000	25,000	50,000	125,000	200,000	250,000	500,000	1,000,000

Z-Series

	Z3 (C)	**Z4 (C)**
Maximum Concurrent Sessions	5,000	10,000

vMX-Series

	vMX-Small	**vMX-Medium**	**vMX-Large**	**vMX-Extra Large**
Maximum Concurrent Sessions	25,000	125,000	1,000,000	1,000,000

Performance Data

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 features unless otherwise noted below are disabled. Actual results will vary.

The following items should be noted during review:

- Firewall Throughput tests have the following configuration applied:
  - Layer 3 Firewall enabled
  - QoS
  - DPI (NBAR)
- Advanced Security Throughput Tests are performed for MX-Series devices with the following configuration:
  - QoS
  - DPI (NBAR)
  - IPS Ruleset: 'Connectivity'
  - AMP enabled
  - Content Filtering enabled
  - IPS Mode in Detection or Prevention configuration
- Single & Multi-Tunnel VPN Throughput tests have the following configuration applied:
  - QoS
  - DPI (NBAR)
  - Layer 3 Firewall enabled
- Secure Teleworker Throughput Tests are performed for Z-Series devices with the following configuration:

- QoS
- DPI (NBAR)
- AMP Enabled

MX-Series

	MX67	MX68	MX75	MX85	MX95	MX105	MX250	MX450
Firewall Throughput **RFC2544 - 1518 Byte**	700 Mbps	700 Mbps	1 Gbps	1 Gbps	2.5 Gbps	5 Gbps	7.5 Gbps	10 Gbps
Firewall Throughput **EMIX**	700 Mbps	700 Mbps	1 Gbps	1 Gbps	2.5 Gbps	5 Gbps	7 Gbps	10 Gbps
NGFW Throughput (Advanced Security - Prevention) **EMIX**	300 Mbps	300 Mbps	500 Mbps	500 Mbps	1.5 Gbps	2 Gbps	1.5 Gbps	3.5 Gbps
NGFW Throughput (Advanced Security - Detection) **EMIX**	400 Mbps	400 Mbps	1 Gbps	1 Gbps	2 Gbps	2.5 Gbps	3.5 Gbps	7 Gbps
Single Tunnel VPN Throughput RFC2544 1400 Byte	400 Mbps	400 Mbps	1 Gbps	1 Gbps	2.0 Gbps	2.5 Gbps	3 Gbps	3.5 Gbps
Multi-Tunnel VPN Throughput RFC2544 1400 Byte	≤ 400 Mbps	≤ 400 Mbps	1 Gbps	1 Gbps	2.5 Gbps	3 Gbps	3.5 Gbps	4.5 Gbps
Single Tunnel VPN Throughput EMIX	300 Mbps	300 Mbps	1 Gbps	1 Gbps	1.5 Gbps	2 Gbps	2 Gbps	3 Gbps
Multi-Tunnel VPN Throughput EMIX	≤ 300 Mbps	≤300 Mbps	≤ 1 Gbps	≤ 1 Gbps	≤ 1.5 Gbps	≤ 2 Gbps	≤ 2 Gbps	4.5 Gbps

Note: NGFW = next generation firewall, EMIX = enterprise mix

Z-Series

	Z3 (C)	Z4 (C)
Secure Teleworker Throughput	NA	300 Mbps

Firewall Throughput **RFC2544 - 1518 Byte**	200 Mbps	500 Mbps
Firewall Throughput **EMIX**	200 Mbps	500 Mbps
Single Tunnel VPN Throughput RFC2544 1400 Byte	75 Mbps	250 Mbps
Single Tunnel VPN Throughput EMIX	50 Mbps	250 Mbps

vMX-Series

	vMX-Small	**vMX-Medium**	**vMX-Large**	**vMX-Extra Large**
vMX VPN Throughput **iPerf**	250 Mbps	500 Mbps	1 Gbps	10 Gbps

Features, benefits, and performance impact

Features and Benefits

Each feature provides advanced benefits tailored to specific use cases. Below is an elaboration on a feature; its use case, and a recommendation for sizing appropriately for deployment or implementation.

Cisco Advanced Malware Protection (AMP)

Cisco Advanced Malware Protection (AMP) is an industry-leading anti-malware technology, integrated into MX Security Appliances.
Consider disabling this feature for guest VLANs and leveraging firewall rules to isolate guest VLANs. Also consider disabling if clients within the network are secured via a full malware client, such as AMP for endpoints.

Content Filtering

Content filtering, powered by Cisco TALOS, allows you to block certain categories of websites based on your organizational policies.
Consider blocking only necessary categories while aligning with your organization's security guidelines.

Web-Safe Search

MX Security Appliances have the option to force all web searches to use Web search filtering.
Must be deployed in tandem with "disable encrypted search" option to be effective.

Cisco IPS/IDS (SNORT)

Intrusion Detection and Prevention, powered by Snort, monitors and protects your network from malicious activity.
Rulesets other than 'Connecitvity' have a larger performance impact. Additionally, consider not sending IDS/IPS syslog data over VPN in low-bandwidth environments.

HTTPS Inspection

HTTPS Inspection enhances Advanced Security features by enabling them to inspect and act on HTTPS traffic.
Use of Cisco Umbrella SD-WAN extensions to offload processing from edge or concetrator devices will reduce performance impacts to MX devices.

Number of VPN Tunnels

Auto VPN creates VPN tunnels between sites in an automated, seamless fashion.
Consider using split tunnel VPN while deplyoying security services at the edge of your network environments.

FIPS Mode

FIPS Mode enables the use of only FIPS compliant mechanisms for MX devices.
Consider engaging your account specialist for appropriate sizing and network architecture when planning to leverage this feature.

Performance Impact Breakdown

Feature Name	Performance Impact
Cisco Advanced Malware Protection (AMP)	Low
Content Filtering	Low
Web-Safe Search	Low
FIPS Mode (Non-VPN Services)	Low
Cisco IDS/IPS (SNORT)	Medium
HTTPS Inspection (On device, not offloaded)	High
Number of VPN Tunnels	High
FIPS Mode (VPN Services)	High