



# MX Sizing Guide

**DECEMBER 2017**

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 6 models. The chart below outlines MX hardware properties for each model:

	MX64	MX64W	MX65	MX65W	MX84	MX100	MX400	MX600
								
<b>Dual Wan Links</b>	✓	✓	✓	✓	✓	✓	✓	✓
<b>3G / 4G Failover</b>	✓	✓	✓	✓	✓	✓	✓	✓
<b>Built-In Wireless</b>		✓		✓				
<b>Built-In PoE+</b>			✓	✓				
<b>Hard Drive (TB)</b>					1	1	1	4
<b>Fiber Connectivity</b>					SFP	SFP	SFP, SFP+	SFP, SFP+
<b>Dual Power Supply</b>							✓	✓
<b>Form Factor</b>	Desktop	Desktop	Desktop	Desktop	1U	1U	1U	2U

# 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(W)	MX65(W)	MX84	MX100	MX400	MX600
<b>Max throughput with all security features enabled</b>	200 Mbps	200 Mbps	300 Mbps	650 Mbps	1 Gbps	1 Gbps
<b>Max Stateful (L3) firewall throughput in passthrough mode</b>	250 Mbps	250 Mbps	500 Mbps	750 Mbps	1 Gbps	1 Gbps
<b>Max Stateful (L3) firewall throughput in NAT mode</b>	200 Mbps	200 Mbps	500 Mbps	750 Mbps	1 Gbps	1 Gbps
<b>Max connections</b>	100,000	100,000	250,000	500,000	1,000,000	2,000,000
<b>Max connections per second</b>	5,000	5,000	8,000	12,000	30,000	30,000
<b>Max VPN throughput</b>	100 Mbps	100 Mbps	250 Mbps	500 Mbps	↑ 1 Gbps	1 Gbps
<b>Max concurrent VPN tunnels</b> (site-to-site or client VPN)	50	50	100	250	1,000	5,000
<b>Max AV throughput</b>	250 Mbps	250 Mbps	500 Mbps	750 Mbps	1 Gbps	1 Gbps
<b>Max IDS throughput</b>	200 Mbps	200 Mbps	300 Mbps	650 Mbps	1 Gbps	1 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.

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

	<b>BENEFITS</b>	<b>PERFORMANCE IMPACT</b>	<b>RECOMMENDATIONS</b>
<b>Anti-virus / anti-phishing</b>	Provides flow based protection for Web traffic (port 80).	High	Consider disabling for guest VLANs and using firewall rules to isolate those VLANs. Also consider disabling AV/anti-phishing if you run a full AV client on host devices.
<b>IDS / IPS</b>	Provides alerts / prevention for suspicious network traffic	High	Consider not sending IDS/IPS syslog data over VPN in low-bandwidth networks.
<b>VPN</b>	Secure, encrypted traffic between locations	Medium	Use split-tunnel VPN and deploy security services at the edge.
<b>Web caching</b>	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.
<b>Content filtering (top sites)</b>	Category based URL filtering using locally downloaded database	Low	Choose this option if your priority is speed over coverage.
<b>Content filtering (full list)</b>	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.
<b>Web safe-search</b>	Turning Google / Bing safe-search option on	Low	Must be deployed in tandem with "disable encrypted search" option to be effective.
<b>Blocking encrypted search</b>	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.

# Real-world use cases

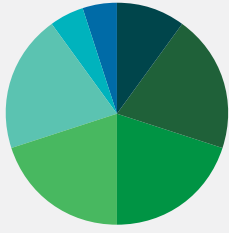
In this section, we'll cover the most common deployment use cases for the Meraki MX:

- **“Everything on”**
- **K-12 school with limited bandwidth**
- **K-12 school with high bandwidth**
- **College / higher education institution**
- **Retail branch**
- **Head-end concentrator for retail branches**

For each case, we'll articulate which features should be turned on and measure the maximum throughput achieved with each MX model.


## USE CASE: “Everything On”

Often, administrators would like to know what network throughput would look like if they turned on all of the features of their MX security appliance (worst-case scenario). Please refer to the “Features, benefits, and the performance impact” table in this document when fine-tuning the firewall configuration to achieve maximum security without unnecessary performance degradation.

FIREWALL CONFIGURATION	TEST TRAFFIC PATTERN					
<p>Security features enabled:</p> <ul style="list-style-type: none"> <li>• NAT mode</li> <li>• Split-tunnel VPN</li> <li>• Content filtering</li> <li>• Traffic shaping</li> <li>• Anti-virus/anti-phishing</li> <li>• IPS</li> <li>• Web caching (not available on MX64/MX64W)</li> </ul>	<p>Traffic flowing through the MX security appliance for testing purposes was composed of the following protocols/applications.</p> <div style="display: flex; align-items: center; justify-content: center;">  <ul style="list-style-type: none"> <li>● 10% HTTP browsing</li> <li>● 20% HTTPS browsing</li> <li>● 20% HTTP download</li> <li>● 20% FTP</li> <li>● 20% CIFS non-VPN</li> <li>● 5% HTTP over VPN</li> <li>● 5% CIFS over VPN</li> </ul> </div>					
THROUGHPUT CONFIGURATION						
	MX64(W)	MX65(W)	MX84	MX100	MX400	MX600
Max throughput	200 Mbps	200 Mbps	320 Mbps	650 Mbps	1 Gbps	1 Gbps
Client count	50	50	200	500	2,000	10,000


## USE CASE: K-12 school with limited bandwidth

Schools need strong URL filtering, application control and security features. In addition, schools with low bandwidth also need traffic shaping and web caching.

FIREWALL CONFIGURATION		TEST TRAFFIC PATTERN				
Security features enabled: <ul style="list-style-type: none"> <li>NAT mode</li> <li>Content filtering</li> <li>Layer 7 Firewall</li> <li>Traffic shaping</li> <li>Anti-virus/anti-phishing</li> <li>Google safe-search</li> <li>YouTube for Schools</li> <li>Web caching (not available on MX64/MX64W)</li> </ul>		Traffic flowing through the MX security appliance for testing purposes was composed of the following protocols/applications. The traffic is heavily skewed towards HTTP/S (70%).  <ul style="list-style-type: none"> <li>20% HTTP browsing</li> <li>15% HTTPS browsing</li> <li>35% HTTP download</li> <li>30% FTP to simulate other TCP traffic</li> </ul>				
THROUGHPUT CONFIGURATION						
	MX64(W)	MX65(W)	MX84	MX100	MX400	MX600
<b>Max throughput</b>	200 Mbps	200 Mbps	450 Mbps	750 Mbps	1 Gbps	1 Gbps
<b>Client count</b>	50	50	200	500	2,000	10,000

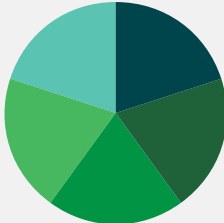
## USE CASE: K-12 school with high bandwidth

Schools with high-bandwidth may not need Web caching or traffic shaping.

FIREWALL CONFIGURATION		TEST TRAFFIC PATTERN				
Security features enabled: <ul style="list-style-type: none"> <li>NAT mode</li> <li>Content filtering</li> <li>Layer 7 Firewall</li> <li>Anti-virus/anti-phishing</li> <li>Google safe-search</li> <li>YouTube for Schools</li> </ul>		Traffic flowing through the MX security appliance for testing purposes was composed of the following protocols/applications. The traffic is heavily skewed towards HTTP/S (70%).  <ul style="list-style-type: none"> <li>20% HTTP browsing</li> <li>15% HTTPS browsing</li> <li>35% HTTP download</li> <li>30% FTP to simulate other TCP traffic</li> </ul>				
THROUGHPUT CONFIGURATION						
	MX64(W)	MX65(W)	MX84	MX100	MX400	MX600
<b>Max throughput</b>	200 Mbps	200 Mbps	450 Mbps	750 Mbps	1 Gbps	1 Gbps
<b>Client count</b>	50	50	200	500	2,000	10,000

## USE CASE: Higher-Ed firewall

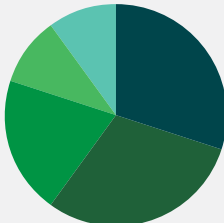
Higher-Ed institutions traditionally don't filter Web content due to freedom of speech concerns. Also, most Higher-Ed institutions have very high-throughput Internet access, so there is no need to do traffic shaping or Web caching.

FIREWALL CONFIGURATION	TEST TRAFFIC PATTERN
Security features enabled: <ul style="list-style-type: none"> <li>• NAT mode</li> <li>• Anti-virus/anti-phishing</li> <li>• Layer 7 Firewall (block BitTorrent)</li> </ul>	Traffic (for testing purposes) was composed of the following protocols/applications. Compared to the previous scenario, there is more multimedia streaming (simulating a typical dorm use case). <div style="display: flex; align-items: center; margin-top: 10px;">  <ul style="list-style-type: none"> <li>● 20% HTTP browsing</li> <li>● 20% HTTPS browsing</li> <li>● 20% HTTP download</li> <li>● 20% FTP</li> <li>● 20% streaming media (10% Amazon media, 10% Netflix)</li> </ul> </div>

THROUGHPUT CONFIGURATION						
	MX64(W)	MX65(W)	MX84	MX100	MX400	MX600
<b>Max throughput</b>	200 Mbps	200 Mbps	450 Mbps	750 Mbps	1 Gbps	1 Gbps
<b>Client count</b>	50	50	200	500	2,000	10,000

## USE CASE: Retail branch with guest access

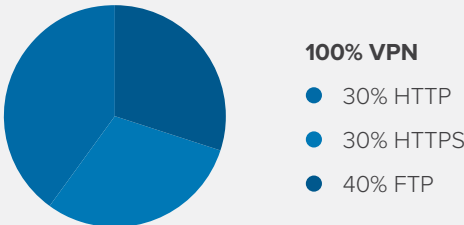
Retailers are looking for a cost-effective yet secure solution to provide reliable VPN access for corporate applications like POS transactions, while offering a guest wireless access that is safe and filtered from inappropriate content.

FIREWALL CONFIGURATION	TEST TRAFFIC PATTERN
Security features enabled: <ul style="list-style-type: none"> <li>• NAT mode</li> <li>• Split-tunnel VPN</li> <li>• Content filtering</li> <li>• Traffic shaping (max throughput on guest VLAN)</li> <li>• Anti-virus/anti-phishing</li> <li>• IPS</li> </ul>	In this use case, retail traffic is a mixture of guest traffic (HTTP/S) as well as VPN traffic for file transfers, nightly backups and other corporate data. <div style="display: flex; align-items: center; margin-top: 10px;">  <ul style="list-style-type: none"> <li>● 30% HTTP browsing</li> <li>● 30% HTTPS browsing</li> <li>● 20% HTTP download</li> <li>● 10% CIFS</li> <li>● 10% VPN</li> </ul> </div>

THROUGHPUT CONFIGURATION						
	MX64(W)	MX65(W)	MX84	MX100	MX400	MX600
<b>Max throughput</b>	200 Mbps	200 Mbps	320 Mbps	650 Mbps	1 Gbps	1 Gbps
<b>Client count</b>	50	50	200	500	2,000	10,000

## USE CASE: Head-end concentrator for retail branches

MX is deployed in the datacenter as a one-armed VPN aggregator, possibly as an Active / Passive HA pair.

FIREWALL CONFIGURATION	TEST TRAFFIC PATTERN
<p>Security features enabled:</p> <ul style="list-style-type: none"><li>• VPN concentrator mode (one-armed VPN concentrator)</li><li>• Full-tunnel VPN</li></ul>	<p>All traffic is via VPN, including HTTP/S for Web browsing and download, and considerable amount of file transfers to simulate backup and other corporate data exchange.</p>  <p><b>100% VPN</b></p> <ul style="list-style-type: none"><li>• 30% HTTP</li><li>• 30% HTTPS</li><li>• 40% FTP</li></ul>

THROUGHPUT CONFIGURATION	MX64(W)	MX65(W)	MX84	MX100	MX400	MX600
<b>Total VPN throughput (Mbps)</b>	100 Mbps	100 Mbps	250 Mbps	500 Mbps	1 Gbps	1 Gbps
<b>Max VPN Tunnels</b>	50	50	100	250	1,000	1,500

## 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(W)	MX65(W)	MX84	MX100	MX400	MX600
<b>Recommended client devices</b>	50	50	200	500	2,000	10,000

## 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 29% year over year, it is important to choose a firewall that will serve you well over many years.