MX Sizing Guide

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
Dual Wan Links	✓	✓	✓	✓	✓	✓	✓	✓
3G / 4G Failover	✓	✓	✓	✓	✓	✓	✓	✓
Built-In Wireless		✓		✓				
Built-In PoE+			✓	✓				
Hard drive (TB)					1	1	1	4
Fiber Connectivity					SFP	SFP	SFP, SFP+	SFP, SFP+
Dual Power Supply							✓	✓
Form Factor	Desktop	Desktop	Desktop	Desktop	1U	1U	1U	2U

Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com

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
Max throughput with all security features enabled	200 Mbps	200 Mbps	300 Mbps	650 Mbps	1 Gbps	1 Gbps
Recommended max clients	50	50	200	500	2,000	10,000
Max Stateful (L3) firewall throughput in passthrough mode	250 Mbps	250 Mbps	500 Mbps	750 Mbps	1 Gbps	1 Gbps
Max Stateful (L3) firewall throughput in NAT mode	200 Mbps	200 Mbps	500 Mbps	750 Mbps	1 Gbps	1 Gbps
Max connections	100,000	100,000	250,000	500,000	1,000,000	2,000,000
Max connections per second	5,000	5,000	8,000	12,000	30,000	30,000
Max VPN throughput	100 Mbps	100 Mbps	250 Mbps	500 Mbps	1 Gbps	1 Gbps
Max VPN connections (site-to-site or client VPN)	25	25	50	250	1,000	5,000
Max AV throughput	250 Mbps	250 Mbps	500 Mbps	750 Mbps	1 Gbps	1 Gbps
Max IDS throughput	200 Mbps	200 Mbps	300 Mbps	650 Mbps	1 Gbps	1 Gbps

Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com

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.

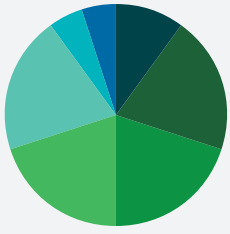|	BENEFITS	PERFORMANCE IMPACT	RECOMMENDATIONS
Anti-virus / anti-phishing	Provides flow based protection for Web traffic (port 80).	High	Consider disabling for guest VLANs and using firewall rules to isolate those VLANs. Also consider disabling AV/anti-phishing if you run a full AV client on host devices.
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.

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
Security features enabled: • NAT mode • Split-tunnel VPN • Content filtering • Traffic shaping • Anti-virus/anti-phishing • IPS • Web caching (not available on MX64/MX64W)	Traffic flowing through the MX security appliance for testing purposes was composed of the following protocols/applications. ● 10% HTTP browsing ● 20% HTTPS browsing ● 20% HTTP download ● 20% FTP ● 20% CIFS non-VPN ● 5% HTTP over VPN ● 5% CIFS over VPN

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

Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com

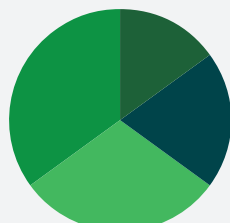**USE CASE:** **K-12 school with limited bandwidth**

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

Security features enabled:

- NAT mode
- Content filtering
- Layer 7 Firewall
- Traffic shaping
- Anti-virus/anti-phishing
- Google safe-search
- YouTube for Schools
- Web caching (not available on MX64/MX64W)

TEST TRAFFIC PATTERN

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%).

- 20% HTTP browsing
- 15% HTTPS browsing
- 35% HTTP download
- 30% FTP to simulate other TCP traffic

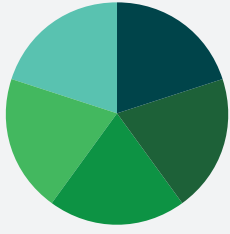| THROUGHPUT CONFIGURATION						
	MX64(W)	**MX65(W)**	**MX84**	**MX100**	**MX400**	**MX600**
Max throughput	200 Mbps	200 Mbps	450 Mbps	750 Mbps	1 Gbps	1 Gbps
Client count	50	50	200	500	2,000	10,000

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

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

FIREWALL CONFIGURATION

Security features enabled:

- NAT mode
- Content filtering
- Layer 7 Firewall
- Anti-virus/anti-phishing
- Google safe-search
- YouTube for Schools

TEST TRAFFIC PATTERN

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%).

- 20% HTTP browsing
- 15% HTTPS browsing
- 35% HTTP download
- 30% FTP to simulate other TCP traffic

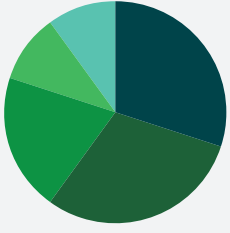| THROUGHPUT CONFIGURATION						
	MX64(W)	**MX65(W)**	**MX84**	**MX100**	**MX400**	**MX600**
Max throughput	200 Mbps	200 Mbps	450 Mbps	750 Mbps	1 Gbps	1 Gbps
Client count	50	50	200	500	2,000	10,000

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

Security features enabled:

- NAT mode
- Anti-virus/anti-phishing
- Layer 7 Firewall (block BitTorrent)

TEST TRAFFIC PATTERN

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).

- 20% HTTP browsing
- 20% HTTPS browsing
- 20% HTTP download
- 20% FTP
- 20% streaming media (10% Amazon media, 10% Netflix)

THROUGHPUT CONFIGURATION

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

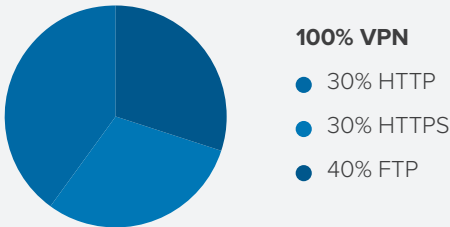## USE CASE: Retail branch with guest access

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

Security features enabled:

- NAT mode
- Split-tunnel VPN
- Content filtering
- Traffic shaping (max throughput on guest VLAN)
- Anti-virus/anti-phishing
- IPS

TEST TRAFFIC PATTERN

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.

- 30% HTTP browsing
- 30% HTTPS browsing
- 20% HTTP download
- 10% CIFS
- 10% VPN

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

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

Security features enabled:

- VPN concentrator mode
- Full-tunnel VPN

TEST TRAFFIC PATTERN

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.

100% VPN
- 30% HTTP
- 30% HTTPS
- 40% FTP

THROUGHPUT CONFIGURATION

	MX64(W)	MX65(W)	MX84	MX100	MX400	MX600
Max VPN throughput	100 Mbps	100 Mbps	250 Mbps	500 Mbps	1 Gbps	1 Gbps
Max per-tunnel VPN throughput	85 Mbps	85 Mbps	200 Mbps	375 Mbps	900 Mbps	900 Mbps
Max VPN Sessions	25	25	100	250	1,000	5,000

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.