

MX Security Appliance mit Cloud-Management



Überblick

Cisco Meraki MX Security Appliances eignen sich ideal für Unternehmen mit einer großen Zahl verteilter Standorte. Das Management der MX-Serie erfolgt vollständig über die Cloud. Dies vereinfacht die Installation und Remote-Verwaltung. Die MX-Serie ist zudem mit umfangreichen Netzwerkservices ausgestattet. Die Installation zahlreicher Appliances für verschiedene Funktionen ist daher nicht erforderlich. Neben einer Layer 7 Firewall stehen Services wie Content-Filtering, Filterfunktionen für die Websuche, SNORT®-basierte Intrusion Prevention, Web-Caching, Intelligente WANs mit mehrere WAN-Uplinks und 4G-Failover zur Verfügung.

Umfassende Unified Threat Management (UTM)-Funktionen

- Applikationsbasierte Datenverkehrssteuerung: Festlegen von Bandbreitenrichtlinien anhand des Layer-7-Applikationstyps (z. B. YouTube, Skype, P2P)
- Content-Filtering: CIPA-konforme Inhaltsfilter, Durchsetzung der SafeSearch-Filterung (Google/Bing) und YouTube for Schools
- Intrusion Prevention: PCI-konformer IPS-Sensor basierend auf der branchenführenden SNORT® Signatur-Datenbank von Sourcefire
- Antivirus und Anti-Phishing: Flow-basierte Schutz-Engine auf Basis von Kaspersky
- Identitätsbasierte Sicherheitsrichtlinien und Anwendungsmanagement

Branchenführendes Cloud-Management

- Einheitliches WAN-, LAN- und WLAN-Management über ein webbasiertes Dashboard
- Vorlagenbasierte Einstellungen ermöglichen einfache Skalierung von kleineren Umgebungen auf ausgedehnte Systemlandschaften mit vielen Standorten und Zehntausenden Geräten
- Rollenbasierte Administration, E-Mail-Benachrichtigungen bei Konfigurationsänderungen, Verbindungsproblemen und Stromausfällen, überprüfbare Änderungsprotokolle
- Archivierung von zusammenfassenden Berichten mit Details zu Benutzern, Geräten und zur Gerätenutzung in der Cloud

Ausfallsicheres Site-to-Site-VPN mit 4G-Failover

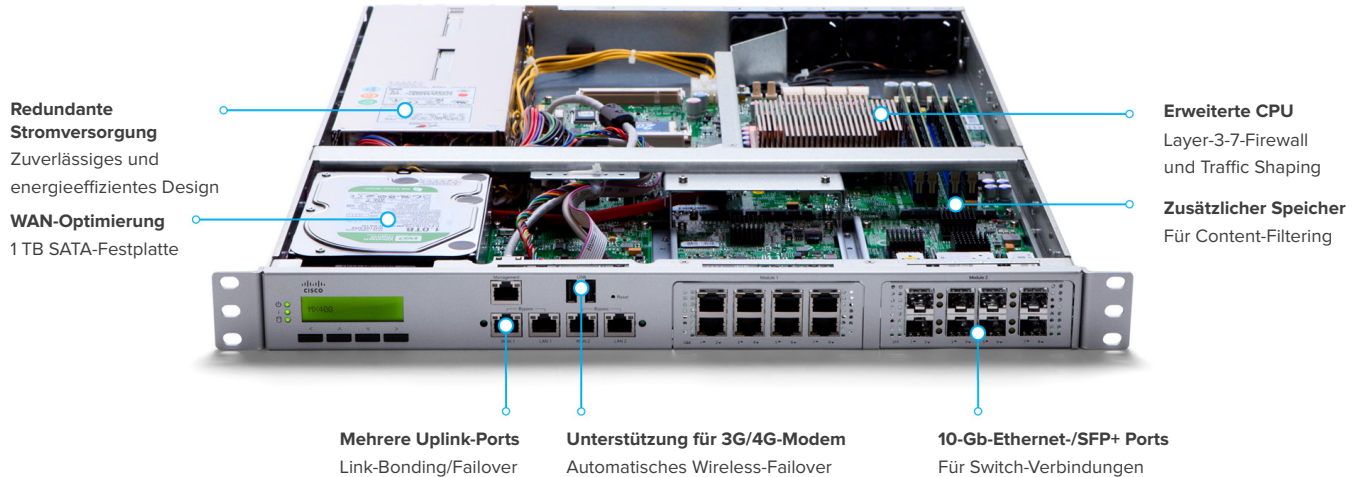
- Auto-VPN-Technologie: automatische Erstellung von Routingtabellen, IKE/IPsec-Einrichtung und Schlüsselaustausch über die sichere Cisco Meraki-Cloud
- Automatischer Failover auf sekundären WAN-Link oder eine 4G-Verbindung
- Interoperabilität mit standardbasierten IPsec-VPNs
- Automatisierter Failover von MPLS auf VPN
- Client-VPN: L2TP IPsec-Unterstützung für native Windows-, Mac OS X-, iPad- und Android-Clients ohne Lizenzgebühren pro Benutzer

Branch Gateway Services

- Integrierte DHCP-, NAT-, QoS- und VLAN-Management-Services
- Web-Caching: schneller Zugriff auf häufig genutzte Inhalte
- Link-Bonding: Bündelung mehrerer WAN-Links in einer Hochgeschwindigkeits-Schnittstelle mit Richtlinien für QoS, Traffic-Shaping und Failover
- Layer-3-Failover: automatische Erkennung von Layer-2- und Layer-3-Ausfällen und schneller Failover (einschließlich 3G/4G-USB-Modems)

Komponenten der Meraki MX-Serie

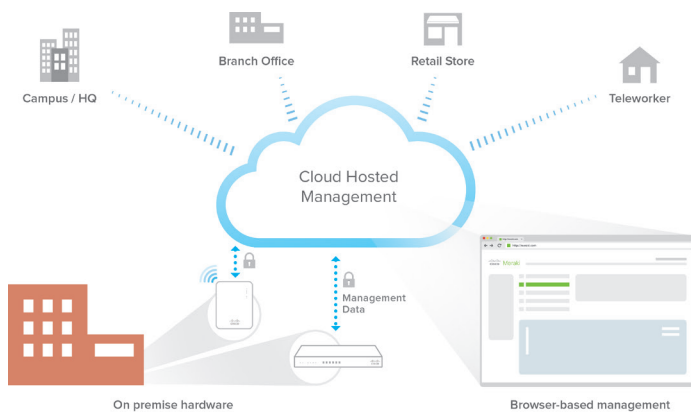
Abbildung zeigt die MX400, die Merkmale können je nach Modell variieren



Architektur mit Cloud-Management

Die MX-Serie basiert auf der preisgekrönten Cisco Meraki-Architektur mit Cloud-Management und sind die einzigen Appliances mit Unified Threat Management, die vollständig in der Cloud verwaltet werden. Die MX-Serie ruft Richtlinien und Konfigurationsdaten automatisch aus der Cloud ab und konfiguriert sich dadurch selbständig. Dank netzwerkweiter Transparenz und Kontrolle mithilfe leistungsstarker Remote-Tools kann die Administration ohne Netzwerkspezialisten vor Ort erfolgen.

Die Cloud-Services sorgen für die nahtlose Bereitstellung von Aktualisierungen für Sicherheitssignaturen und Firmware, richten automatisch Site-to-Site-VPN-Tunnel ein und überwachen das Netzwerk rund um die Uhr. Zudem lässt sich das browserbasierte Management-Dashboard der MX-Produktfamilie auch ohne spezielle Schulung bedienen.



Cisco Meraki Cloud-Management-Architektur

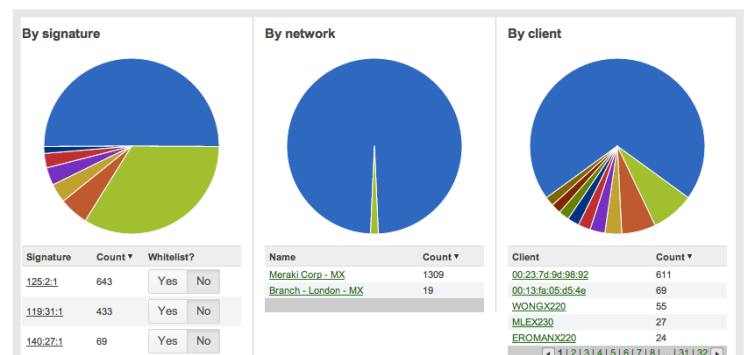
Starke Sicherheit für Edge-Netzwerke

Die Hardwareplattform der MX-Serie ist auf Deep Packet Inspection auf Layer 7 ausgelegt, ist mit erweiterten Sicherheitsfunktionen wie IPS, Content-Filtering, Filter für die Websuche, Antivirus/Anti-Phishing und IPsec-VPN ausgestattet und bietet den Datendurchsatz und die Leistung, die für moderne, bandbreitenintensive Netzwerke erforderlich sind.

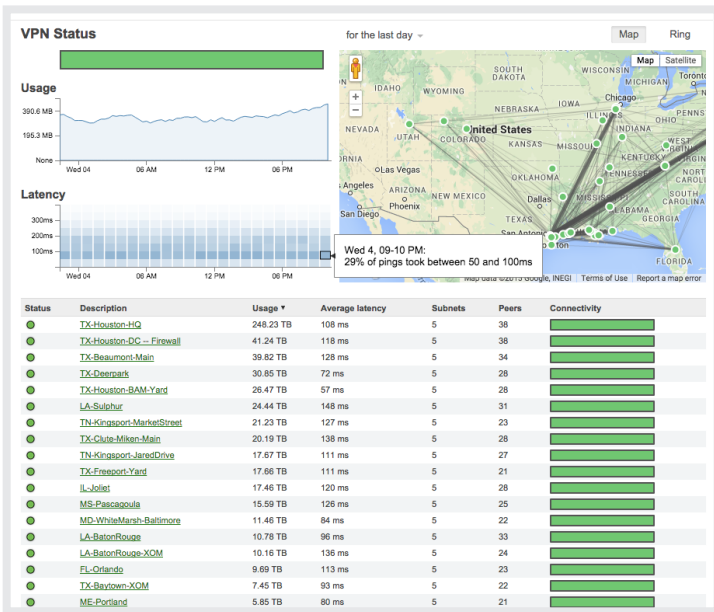
Mithilfe von Fingerprinting-Technologie auf Layer 7 können Administratoren unerwünschte Inhalte und Anwendungen identifizieren und verhindern, dass wertvolle Bandbreite durch privat genutzte Anwendungen wie BitTorrent verschwendet wird.

Die integrierte Sourcefire® SNORT®-Engine bietet leistungsstarke Intrusion Prevention-Funktionen – eine zentrale Anforderung für PCI 3.0-konforme Netzwerke. Die MX verwendet zudem die Webroot®-URL-Kategorisierungsdatenbank für CIPA/IWF-konforme Inhaltsfilterung, die Kaspersky®-Engine für Anti-Virus/Anti-Phishing-Filterung und MaxMind für Geo-IP-basierte Sicherheitsregeln.

Alle diese branchenführenden Layer-7-Security-Engines und -Signaturen sind dank Updates aus der Cloud darüber jederzeit auf dem neuesten Stand. Dies erleichtert IT-Administratoren das Management der Netzwerksicherheit.



Bedrohungseinstufung auf Organisationsebene



Automatische Konfiguration von Site-to-Site-VPNs

Group policies > **Students**

Name: Students

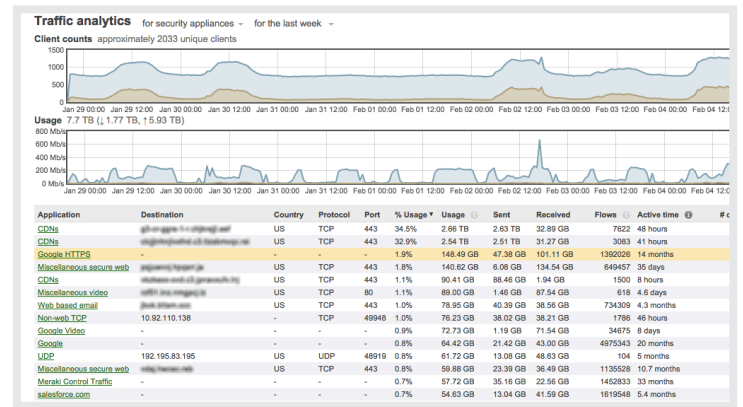
Bandwidth: Use custom bandwidth limit - unlimited

Firewall and traffic shaping: Custom network firewall & shaping rules

#	Policy	Protocol	Source	Src port	Destination	Dst port	Comment	Actions
	Allow	Any	Any	Any	Any	Any	Default rule	

#	Policy	Application	Actions
1	Deny	Peer-to-peer (P2P)	BitTorrent
2	Deny	Online backup	All Online backup

Identitätsbasiertes Richtlinienmanagement



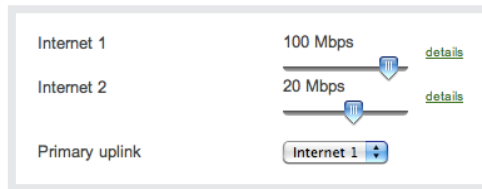
Firewall der nächsten Generation und Datenverkehrstransparenz

Search: [Advanced search >](#) [Help](#)

8 matches in 299 [Columns...](#) | [Download as XML](#)

<input type="checkbox"/>	Description	IP address	MAC address	Usage	Access	Manufacturer
<input type="checkbox"/>	1 Bobby-Longe-iPad	172.16.30.51	a4:d1:d2:10:10:9d	11.3 MB	normal	Apple
<input type="checkbox"/>	2 Brian-Tobins-iPad	172.16.30.142	7c:6d:62:d7:91:58	853 KB	normal	Apple
<input type="checkbox"/>	3 iPad	172.16.30.49	70:de:e2:40:f3:02	145.8 MB	normal	Apple
<input type="checkbox"/>	4 Meraki-Marketing-iPad	172.16.30.67	b8:ff:61:b8:78:8d	331.3 MB	normal	Apple
<input type="checkbox"/>	5 PCC-iPad-1	172.16.30.183	7c:6d:62:db:32:f5	8.5 MB	normal	Apple
<input type="checkbox"/>	6 Wilson-John-Chang-iPad-2	172.16.30.135	a4:67:06:99:da:a8	33.5 MB	normal	Apple

Benutzer- und Geräte-Fingerprinting



Link-Bonding und -Failover

Intelligente WANs leicht gemacht

Übertragungsunabhängigkeit:

Zwei WAN-Ports mit Load Balancing- und Failover-Funktionen ermöglichen die Nutzung von MPLS und redundanten herkömmlichen Internet-Verbindungen und sorgen somit für zusätzliche Bandbreite und höhere Zuverlässigkeit.

3G / 4G-Failover:

Für WAN-Verbindungs-Failover unterstützt die Cisco Meraki MX 3G/4G Service Provider weltweit. Beim Web-Caching werden Video- und Medieninhalte sowie Webdokumente vorübergehend gespeichert. So wird die Bandbreitennutzung verringert und das Herunterladen von Internetinhalten beschleunigt.

Anwendungsoptimierung:

Durch Layer 7-Traffic-Shaping und Anwendungspriorisierung wird der Datenverkehr für geschäftskritische Anwendungen und eine ideale Benutzererfahrung optimiert.

Intelligente Pfadkontrolle*:

Mithilfe von leistungs-basiertem Routing wählen Sie den besten Uplink basierend auf der Latenz oder Paketverlusten aus. Definieren Sie außerdem Richtlinien zum Senden des richtigen Datenverkehrs über den entsprechenden Pfad (senden Sie Sprachdaten beispielsweise über MPLS, Http-Daten über VPN oder Breitband).

Sichere Anbindung:

Das einzigartige Site-to-Site-VPN für die automatische Bereitstellung (Auto VPN) von Cisco Meraki sorgt für eine sichere und einfache Verbindung von Standorten. Mithilfe von AES 128-Bit-Verschlüsselung konfigurieren die MX Security Appliances automatisch die für Herstellung und Aufrechterhaltung von VPN-Sitzungen erforderlichen VPN-Parameter. Ein einzigartiger Cloud-fähiger Erkennungsmechanismus sorgt für die automatische Verbindung von VPN-Peers und das Routing durch das WAN. Außerdem ermöglicht er umfassende Aktualität in dynamischen IP-Umgebungen.

* Verfügbar Q2 2015

MX64W mit 802.11ac-Wireless

Das Modell MX64W integriert die preisgekrönte Wireless-Technologie von Cisco Meraki und die leistungsstarken Netzwerksicherheitsfunktionen der MX-Serie in einem kompakten Formfaktor für den Einsatz in Zweigstellen oder kleinen Unternehmen:

- Dualband, 802.11n/ac, 2x2 MIMO mit zwei Signalströmen
- Einheitliche Verwaltung von Netzwerksicherheit und WLAN
- Integrierte Enterprise Security und Gastzugang



MX64W Security Appliance

Z1 Telecommuter Gateway



Z1 Telecommuter Gateway

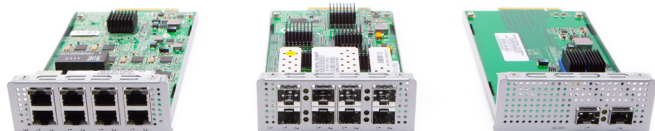
Mit dem Z1 Telecommuter Gateway kann das Cisco Meraki-Dashboard und seine Cloud-basierten Management-Funktionen auch von Mitarbeitern im Home Office genutzt werden.

Cisco Meraki Auto-VPN, eine zum Patent angemeldete Technologie, ermöglicht es IT-Administratoren, entfernten Mitarbeitern Netzwerkservices wie VoIP oder Remote Desktop (RDP) mit nur einem Klick bereitzustellen. Sie können zudem sowohl drahtlosen als auch kabelgebundenen Zugriff bereitstellen und durch Layer-7-Traffic-Shaping und -Priorisierung eine produktivere Arbeit ermöglichen.

- 1 x 802.11a/b/g/n-Funkmodul, 1 x 802.11a/n-Funkmodul, 2x2 MIMO mit 2 Signalströmen
- Site-to-Site-VPN (IPsec) basierend auf der Cisco Meraki-Auto-VPN-Technologie
- Layer-7-Applikationstransparenz und Traffic-Shaping

Zubehör

Die Meraki-Modelle MX100, MX400 und MX600 unterstützen Plug-fähige optische Module für Backbone-Hochgeschwindigkeits- oder Link-Aggregation-Verbindungen zwischen Verteilerschränken oder mit Aggregation-Switches. Ebenfalls verfügbar sind eine Reihe von standardmäßigen Gigabit- und 10-Gigabit-Modulen. Jedes Gerät wurde außerdem auf Kompatibilität mit verschiedenen Modulen von Drittanbietern getestet.



Schnittstellenmodule für MX400 und MX600



Plug-fähige optische Module für MX100, MX400,

Zubehör/optische Module

Unterstützte Cisco Meraki-Zubehörmodule für die Modelle MX100, MX400 und MX600.







MODELL	BESCHREIBUNG
IM-8-CU-1GB	Cisco Meraki-Kupferschnittstellenmodul für MX400 und MX600, 8 x 1 GbE
IM-8-SFP-1GB	Cisco Meraki-SFP-Schnittstellenmodul für MX400 und MX600, 8 x 1 GbE
IM-2-SFP-10GB	Cisco Meraki-SFP+ Schnittstellenmodul für MX400 und MX600, 2 x 10 GbE
MA-SFP-1GB-SX	Cisco Meraki-Glasfasermodul, 1 GbE, SFP, SX (1000BASE-SX, Reichweite: 550 m)
MA-SFP-10GB-SR	Cisco Meraki-SFP+ Modul mit kurzer Reichweite, 10 GbE, (10GBASE-SR, Reichweite: 400 m)
MA-CBL-TA-1M	Cisco Meraki-Twinax-Kabel mit Steckern (SFP+), 10 GbE (10GSFP+Cu, Reichweite: 1 m)

Hinweis: Weitere Single-Mode und Multi-Mode Glasfaser-Transceiver-Module finden Sie auf meraki.com.

Lebenszeitgarantie mit Hardware-Ersatz am folgenden Geschäftstag

Cisco Meraki MX-Appliances werden mit eingeschränkter Lebenszeitgarantie mit Hardware-Ersatz am folgenden Geschäftstag ausgeliefert. Das vereinfachte Software- und Support-Lizenzmodell von Cisco Meraki fasst alle Software-Upgrades, die zentrale Systemverwaltung und den telefonischen Support in einem umfassenden, transparenten Modell zusammen. Vollständige Einzelheiten finden Sie unter meraki.cisco.com/support.

Produktoptionen

	MX64 	MX64W 	MX80 	MX100 	MX400 	MX600 
Empfohlene Einsatzgebiete	Kleine Einzelhandelsfilialen, kleine Kliniken	Kleine Einzelhandelsfilialen, kleine Kliniken	Mittelgroße Zweigstellen	Große Zweigstellen	K-12-Firewall/VPN-Concentrator	Große K-12-Firewall, VPN-Concentrator
Empfohlene max. Anzahl von Benutzern	50	50	100	500	2,000	10,000
Stateful Firewall – Durchsatz	200 Mbit/s	200 Mbit/s	250 Mbit/s	750 Mbit/s	1 Gbit/s	1 Gbit/s
Erweiterte Sicherheit – Durchsatz	80 Mbit/s	80 Mbit/s	80 Mbit/s	600 Mbit/s	1 Gbit/s	1 Gbit/s
Max. Anzahl von VPN-Sitzungen	25	25	50	250	1,000	5,000
Schnittstellen	5 x GbE	5 x GbE	5 x GbE	9 x GbE 2 x GbE (SFP)	4 x GbE	4 x GbE
Zusätzliche Schnittstellenmodule	-	-	-	-	8 x GbE (RJ45) 8 x GbE (SFP) 4 x 10GbE (SFP+) (max. 2 Modules)	8 x GbE (RJ45) 8 x GbE (SFP) 4 x 10GbE (SFP+) (max. 2 Modules)
Web-Caching	-	-	Ja	Ja	Ja	Ja
Festplatte*	-	-	1 TB	1 TB	1 TB	4 x 1 TB (RAID)
USB für 3G/4G-Failover	Ja	Ja	Ja	Ja	Ja	Ja
Montage	Schreibtisch/Wand	Schreibtisch/Wand	Rack (1 HE)	Rack (1 HE)	Rack (1 HE)	Rack (2 HE)
Abmessungen	239mm x 132mm x 25mm	239mm x 132mm x 25mm	483 mm x 254 mm x 44 mm	483 mm x 254 mm x 44 mm	483 mm x 559 mm x 44 mm	483 mm x 559 mm x 89 mm
Gewicht	1.4 kg	1.4 kg	3.6kg	4.1kg	15.0 kg	24.0 kg
Stromversorgung	18 W Gleichstrom (im Lieferumfang enthalten)	18 W Gleichstrom (im Lieferumfang enthalten)	100 bis 220V 50/60Hz Wechselstrom	100 bis 220V 50/60Hz Wechselstrom	100 bis 220V 50/60Hz Wechselstrom (dual)	100 bis 220V 50/60Hz Wechselstrom (dual)
Leistungsaufnahme (Inaktivität/Max.)	4W / 10W	6W / 13W	26W / 32W	30W / 55W	123W / 215W	132W / 226W
Betriebstemperatur	0°C bis 40°C	0°C bis 40°C	0°C bis 40°C	0°C bis 40°C	0°C bis 40°C	0°C bis 40°C
Luftfeuchtigkeit	5% bis 95%	5% bis 95%	5% bis 95%	5% bis 95%	5% bis 95%	5% bis 95%

*Hinweis: Die Festplatte wird für Web-Caching und die erweiterte WAN-Optimierung verwendet. Hierbei wird ein Objekt-Caching auf Byte-Ebene durchgeführt.

Spezifikationen

Management

Verwaltung über das Internet mit dem Cisco Meraki-Dashboard

Transparente und zentrale Verwaltung kabelgebundener und Wireless-Netzwerke

Automatische Remote-Bereitstellung (kein Staging erforderlich)

Automatische Firmware-Updates und Sicherheitspatches

Vorlagenbasierte Verwaltung mehrerer Netzwerke

Zwei-Faktor-Authentifizierung und Single Sign-on auf Organisationsebene

Rollenbasierte Verwaltung mit Änderungsprotokollierung und -benachrichtigung

Überwachung und Berichterstellung

Überwachung von Durchsatz und Verbindung sowie E-Mail-Benachrichtigungen

Detaillierte Nutzungsstatistik pro Port und Client

Statistische Daten zur Anwendungsnutzung

Änderungsprotokolle auf Organisationsebene für Compliance und Change-Management

VPN-Tunnel- und Latenzüberwachung

Erkennung von Netzwerkgeräten und Benutzeridentifikation

Regelmäßige E-Mails mit den wichtigsten Nutzungsdaten

Syslog-Integration

Remote-Diagnose

Remote Packet Capture in Echtzeit

Tools zur Diagnose und Fehlerbehebung in Echtzeit

Aggregierte Ereignisprotokolle mit Sofortsuche

Netzwerk- und Sicherheitsdienste

Stateful Firewall, 1:1 NAT, DMZ

Identitätsbasierte Richtlinien

Auto-VPN-Technologie: Automatisiertes Site-to-Site-VPN (IPsec) für Hub-and-Spoke- oder Mesh-Topologien

Client-VPN (IPsec L2TP)

Mehrere WAN-IP-Adressen, PPPoE, NAT

VLAN-Unterstützung und DHCP-Services

Statisches Routing

Benutzer- und Gerätequarantäne

WAN-Leistungsmanagement

Web-Caching

WAN-Link-Aggregation

Automatischer Layer-3-Failover (einschließlich VPN-Verbindungen)

3G/4G-USB-Modem-Failover

Datenverkehrsanalyse und Traffic-Shaping auf Applikationsebene (Layer 7)

Möglichkeit zur Auswahl des WAN-Uplinks anhand des Datenverkehrstyps

Hinweis: Web-Caching steht auf den Modellen MX64 oder MX64W nicht zur Verfügung.

Erweiterte Security-Services

Content-Filtering (basierend auf der URL-Datenbank von Webroot BrightCloud, CIPA-konform)

Filterfunktionen für die Websuche (einschließlich SafeSearch für Google/Bing)

YouTube for Schools

Intrusion Prevention-Sensor (basierend auf Sourcefire SNORT® Technologie)

Antivirus-Engine und Anti-Phishing-Filterung (Kaspersky SafeStream II-Engine)

Hinweis: Für erweiterte Security-Services ist eine Advanced Security-Lizenz erforderlich.

Integrierte Wireless-Funktionen

1 x 802.11a/b/g/n (2,4 GHz oder 5 GHz)

Max. Datenrate 450 Mbit/s

3x3 MIMO mit 3 Signalströmen, Beamforming

3 externe Dual-Band-Dipol-Antennen (Steckertyp: RP-SMA)

Signalabdeckung: 3,0s dBi @ 2,4 GHz, 3,5 dBi @ 5 GHz

WEP, WPA, WPA2-PSK, WPA2-Enterprise mit 802.1X-Authentifizierung

Kennzeichnungen und Zulassungen: FCC (USA), IC (Kanada), CE (Europa), C-Tick (Australien/Neuseeland), RoHS

Hinweis: Integriertes WLAN steht nur auf dem Modell MX64W zur Verfügung.

Kennzeichnungen und Zulassungen

FCC (USA)

CB (IEC)

CISPR (Australien/Neuseeland)

Garantie

Lebenszeitgarantie mit erweitertem Hardware-Ersatz am folgenden Geschäftstag

Bestellanleitung

Um eine Bestellung für eine MX-Appliance aufzugeben, kombinieren Sie das gewünschte Hardware-Modell mit einer bestimmten Lizenz, die Cloud-Services, Software-Upgrades und Support einschließt. Möchten Sie z. B. das Modell MX64 mit 3 Jahren Advanced Security-Lizenz erwerben, bestellen Sie MX64-HW mit der Lizenz LIC-MX64-SEC-3YR. Die gesamte Hardware wird ohne zusätzliche Kosten durch eine Lebenszeitgarantie mit erweitertem Hardware-Ersatz am folgenden Geschäftstag abgedeckt.

MODEL	LICENSE	DESCRIPTION
MX64-HW	LIC-MX64-ENT-1YR	Cisco Meraki MX64, 1 Jahr Enterprise-Lizenz und -Support
	LIC-MX64-ENT-3YR	Cisco Meraki MX64, 3 Jahr Enterprise-Lizenz und -Support
	LIC-MX64-ENT-5YR	Cisco Meraki MX64, 5 Jahr Enterprise-Lizenz und -Support
	LIC-MX64-SEC-1YR	Cisco Meraki MX64, 1 Jahr Advanced Security-Lizenz und -Support
	LIC-MX64-SEC-3YR	Cisco Meraki MX64, 3 Jahr Advanced Security-Lizenz und -Support
	LIC-MX64-SEC-5YR	Cisco Meraki MX64, 5 Jahr Advanced Security-Lizenz und -Support
MX64W-HW	LIC-MX64W-ENT-1YR	Cisco Meraki MX64W, 1 Jahr Enterprise-Lizenz und -Support
	LIC-MX64W-ENT-3YR	Cisco Meraki MX64W, 3 Jahr Enterprise-Lizenz und -Support
	LIC-MX64W-ENT-5YR	Cisco Meraki MX64W, 5 Jahr Enterprise-Lizenz und -Support
	LIC-MX64W-SEC-1YR	Cisco Meraki MX64W, 1 Jahr Advanced Security-Lizenz und -Support
	LIC-MX64W-SEC-3YR	Cisco Meraki MX64W, 3 Jahr Advanced Security-Lizenz und -Support
	LIC-MX64W-SEC-5YR	Cisco Meraki MX64W, 5 Jahr Advanced Security-Lizenz und -Support
MX80-HW	LIC-MX80-ENT-1YR	Cisco Meraki MX80, 1 Jahr Enterprise-Lizenz und -Support
	LIC-MX80-ENT-3YR	Cisco Meraki MX80, 3 Jahr Enterprise-Lizenz und -Support
	LIC-MX80-ENT-5YR	Cisco Meraki MX80, 5 Jahr Enterprise-Lizenz und -Support
	LIC-MX80-SEC-1YR	Cisco Meraki MX80, 1 Jahr Advanced Security-Lizenz und -Support
	LIC-MX80-SEC-3YR	Cisco Meraki MX80, 3 Jahr Advanced Security-Lizenz und -Support
	LIC-MX80-SEC-5YR	Cisco Meraki MX80, 5 Jahr Advanced Security-Lizenz und -Support
MX100-HW	LIC-MX100W-ENT-1YR	Cisco Meraki MX100, 1 Jahr Enterprise-Lizenz und -Support
	LIC-MX100W-ENT-3YR	Cisco Meraki MX100, 3 Jahr Enterprise-Lizenz und -Support
	LIC-MX100W-ENT-5YR	Cisco Meraki MX100, 5 Jahr Enterprise-Lizenz und -Support
	LIC-MX100W-SEC-1YR	Cisco Meraki MX100, 1 Jahr Advanced Security-Lizenz und -Support
	LIC-MX100W-SEC-3YR	Cisco Meraki MX100, 3 Jahr Advanced Security-Lizenz und -Support
	LIC-MX100W-SEC-5YR	Cisco Meraki MX100, 5 Jahr Advanced Security-Lizenz und -Support
MX400-HW	LIC-MX400-ENT-1YR	Cisco Meraki MX400, 1 Jahr Enterprise-Lizenz und -Support
	LIC-MX400-ENT-3YR	Cisco Meraki MX400, 3 Jahr Enterprise-Lizenz und -Support
	LIC-MX400-ENT-5YR	Cisco Meraki MX400, 5 Jahr Enterprise-Lizenz und -Support
	LIC-MX400-SEC-1YR	Cisco Meraki MX400, 1 Jahr Advanced Security-Lizenz und -Support
	LIC-MX400-SEC-3YR	Cisco Meraki MX400, 3 Jahr Advanced Security-Lizenz und -Support
	LIC-MX400-SEC-5YR	Cisco Meraki MX400, 5 Jahr Advanced Security-Lizenz und -Support
MX600-HW	LIC-MX600W-ENT-1YR	Cisco Meraki MX600, 1 Jahr Enterprise-Lizenz und -Support
	LIC-MX600W-ENT-3YR	Cisco Meraki MX600, 3 Jahr Enterprise-Lizenz und -Support
	LIC-MX600W-ENT-5YR	Cisco Meraki MX600, 5 Jahr Enterprise-Lizenz und -Support
	LIC-MX600W-SEC-1YR	Cisco Meraki MX600, 1 Jahr Advanced Security-Lizenz und -Support
	LIC-MX600W-SEC-3YR	Cisco Meraki MX600, 3 Jahr Advanced Security-Lizenz und -Support
	LIC-MX600W-SEC-5YR	Cisco Meraki MX600, 5 Jahr Advanced Security-Lizenz und -Support

* Hinweis: Für jedes MX-Produkt stehen zusätzliche Enterprise- oder Advanced Security-Lizenzen für 7 oder 10 Jahre zur Verfügung (z. B. LIC-MX100-