

Meraki MX Series User Guide

November 2011



1- Introduction

Welcome to cloud-based management

The Meraki MX series products are enterprise-class routers designed for distributed deployments. They are ideal for network administrators who demand easy-to-deploy and highly manageable devices that offer a rich set of network services, including application bandwidth management, site-to-site VPN, robust security features, and basic routing capability. The following lists and describes the currently available MX series products: *the MX50, MX60, and MX70.*

The MX series are managed through the Meraki Dashboard (<https://dashboard.meraki.com>), with an intuitive browser-based interface that lets you get up and running quickly without the need for training or certifications. Because the MX series are self-configuring and managed over the web, you can deploy them at remote locations without the need for an on-site IT staff.

The MX series are monitored 24x7 from the Meraki Dashboard, which delivers real-time network alerts. Remote diagnostic tools enable real-time troubleshooting over the web, so that multi-site, distributed networks can be managed remotely.

The MX firmware is always kept up to date from the cloud, with new features and enhancements delivered seamlessly. You never have to download software updates manually, or worry about missing security patches.

How to use this document

This document applies to all Meraki MX series products. For specifics about your hardware, refer to the setup guide specific to your product, at www.meraki.com/products. The sections in this manual begin with more basic topics and progress to more advanced topics.

The sections and their topics are grouped roughly as follows:

Section	Description
1–4	Overview: Introduction to the Meraki Cloud-Managed Device solution
5–8	Basic topics: Instructions to get a simple network up and running
9	Advanced topics
10–16	Appendixes addressing special applications: Branch office configuration examples, IPSec, NAT firewall
17	References: Additional documents and troubleshooting information

Predeployment setup

Predeployment setup is not addressed in this document. For the details of getting your MX series up and running for the first time, refer to the individual setup guides, available at <http://www.meraki.com/support/#documentation>

2 - Key Features

The following lists the advantages of the MX series and the special features that they provide.

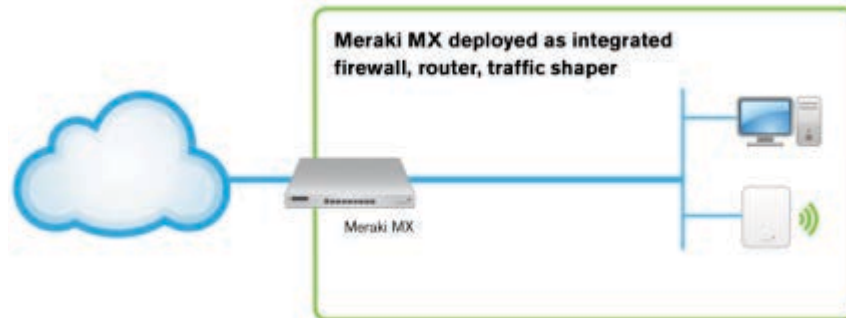
Advantage	Feature	Description
Basic deployment/ease of use	DHCP Service	MX series act as a DHCP server, assigning IP addresses to network clients out of a configurable IP address pool. Alternatively, administrators can rely on third-party DHCP services, such as Windows Server 2008 DHCP service.
	Network Address Translation	MX series operate as a gateway of a private subnet with its own local IP address pool. NAT can be enabled in conjunction with DHCP service.
	Port Forwarding	With NAT enabled, MX series allow incoming traffic on a given port to be forwarded to a local device in the subnet behind the MX series.
	Passthrough	MX series support traffic shaping at Layer 2, without modifying the source or destination of client traffic.
	Layer 2 Switch	MX series have four LAN ports that can be used for Layer 2 networking if DHCP or NAT functionality is enabled. Switch functionality provides direct connection to end devices such as computers, printers, IP phones, and access points.
Security	Firewall	With NAT enabled, the firewall service blocks incoming traffic to the private subnet, unless a port has been designated specifically to forward traffic to a given local client.
	1:1 NAT	Often referred to as DMZ. With NAT enabled, you can host additional servers with different WAN public IP addresses and still protect them by means of inbound firewall connection rules.
	Content Filtering	Blocks or permits access to individual web-content categories or websites.
	Security Filtering	Eliminates malware such as worms and Trojans. Blocks malicious content such as from phishing websites.
	Site-to-Site VPN	Creates secure links between sites. Hole-punching technology reduces need for complicated firewall configurations or upstream-traffic port forwarding. VPN tunnel has fully featured firewall rules for inbound/outbound traffic.
Management and Troubleshooting	Centralized Management	Administrators can access the cloud-based Dashboard, Meraki's management interface, through a web browser from anywhere in the world. This allows networks to be administered and monitored securely in real time.
	Application Visibility/Traffic Shaping	The Traffic Shaper feature monitors application, port, and HTTP content utilization, allowing administrators to see precisely how their networks are being used, and to reserve bandwidth for business-critical applications while restricting network use. For example, administrators can see how much enterprise traffic is being used for video or peer-to-peer applications, and apply traffic shaping filters to block them.

	Network Insight and Monitoring	Packet inspection engines running custom parsers on each MX series provide insight into applications, content, devices, and users on your network. In addition to monitoring network connectivity, throughput, and bandwidth utilization, advanced heuristics enable fingerprinting and identification of users, devices, and traffic flowing in and out of your network, including evasive or encrypted traffic. Because the signature database is provisioned through the Meraki cloud-based Dashboard, it is always current.
	Event Logs and Alerts	The Dashboard provides extensive reporting, including recurring automatic reports, logs for network events such as connectivity, and configuration change alerts.

3 - Basic Deployment Options

The Meraki MX series can be deployed in two basic modes: NAT or Passthrough.

NAT mode: Multi-service Gateway to the Internet



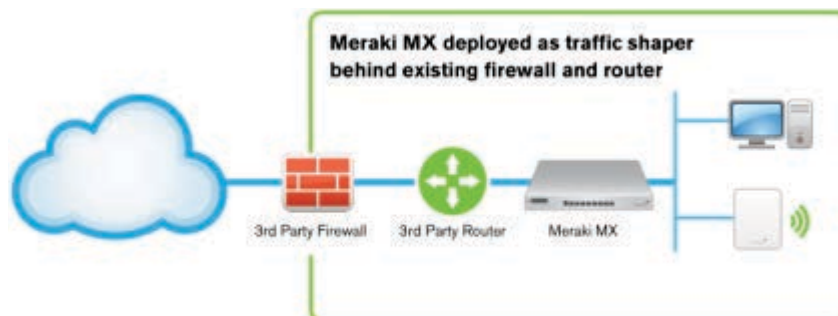
In Network Address Translation (NAT) mode, an MX series serves as the gateway to the ISP, providing all necessary networking services to manage a branch office network remotely through the Meraki Dashboard:

- Application-aware (L7) firewall/NAT service
- Port forwarding
- DHCP service

Note that firewall/NAT service and DHCP service can be enabled or disabled independently of each other. For example, organizations that rely on Microsoft Windows Domain Controllers for DHCP service can disable the DHCP service running on the Cloud-Managed Router but can still enable the firewall/ NAT service.

The MX series also provide the management and visibility services explained below.

Passthrough mode: Behind an existing router or firewall



The MX series can also be used behind an existing router to provide additional monitoring and management control over the resources in a remote branch office network. In Passthrough mode, the MX series provide management and visibility services such as the following:

- Application-aware (L7) traffic shaping and analysis
- Network asset discovery and reporting
- Network event logging

These features allow you to manage, gain insight into, and optimize your remote office networks. For example, by using the Traffic Shaping feature, you can choose to prioritize and accelerate your organization's VoIP traffic, while throttling tertiary Internet traffic such as for social networking or recreational video.

4 - The Meraki Dashboard

Because the Meraki Dashboard is a cloud-based management system, all control, configuration, and reporting functions for the MX series are managed centrally. There is no need for specialized management appliances or third-party software applications.

The MX series tunnel back to the Meraki Dashboard through a secure Internet connection. The Dashboard is hosted in Meraki's secure network operations centers (NOCs), which are distributed geographically around the world. These NOCs provide physical security to the Meraki Dashboard, as well as high availability through power backups and redundant servers in hot standby mode. The geographical distribution of the NOCs also improves the performance of Meraki networks, by minimizing the physical distance between the administrator and the Dashboard.

You can use the Dashboard to make configuration changes and obtain reporting information on your networks. For example, you may wish to change the traffic shaping policy or to enable or disable NAT services. Once a change is made through the Dashboard, the MX series automatically receive the new configuration.

Meraki Dashboard overview

Centralized management and monitoring

The Dashboard can be accessed by means of any JavaScript-capable Internet web browser, including Firefox, Internet Explorer, Safari, and Chrome. Through the Dashboard, you have access to standard troubleshooting tools, such as ping and throughput tests. In addition, you can monitor bandwidth and usage data, either through the Dashboard or with your existing monitoring infrastructure, by using Meraki's XML-based APIs. You can build custom monitoring and reporting applications based on historical statistics without having to install additional software or hardware on site.

Out-of-band architecture

The Dashboard is accessed out of band, which means that client traffic never flows through the Dashboard. In other words, only device management-related control packets are exchanged between the Dashboard and the MX series. This architecture is important for security and performance reasons. It is not possible for an unauthorized person who has access to the Dashboard to see user data, and the Dashboard is not a bottleneck for data traffic flows. Thus, the system operates securely and efficiently.

Security

Control traffic flows between the MX series and the Dashboard through a persistent secure tunnel. All sensitive data, such as configuration details, user names, and passwords, is encrypted.

High availability

Multiple geographically distributed Meraki data centers are used to ensure that networks continue to function even in the event of a catastrophic failure. In case the Dashboard is ever unreachable (for example, because the Internet route to the Dashboard has gone down temporarily), Meraki networks continue to operate without any loss of functionality. Configuration changes and firmware upgrades resume when the Dashboard is reachable again.

Automatic upgrades

New features require no client- or server-side upgrades, but instead are added to the Dashboard several times per year with minimal downtime. Meraki also manages firmware upgrades centrally, freeing the administrator from having to worry about keeping the MX series up-to-date. Firmware upgrades take place over the air in a secure, fault-tolerant fashion. As a network administrator, you will receive an email alert several weeks in advance of a firmware upgrade, and a notice will be posted in the Dashboard notifying you of the exact time that the upgrade will occur. If necessary, to ensure that your traffic is affected minimally, you can delay or reschedule an upgrade by contacting Meraki Support.

Dashboard entities

There are three major logical entities for organizing and managing the Meraki routers.

- *Organizations*: An organization is the top-level entity. Organizations often have multiple administrators and contain multiple networks.
- *Administrators*: Administrators belong to organizations. An organization may have multiple administrators. Administrators have access to and modify privileges for all networks within the organization to which they belong. An administrator may have read/write or read-only access.
- *Networks*: Each network has its own configuration and settings. Currently, each network can have only one router. This limitation may change in the future.
- *Routers*: Routers are the networking devices that are managed through the Dashboard. Routers belong to networks.

Additional information on these topics and other advanced administration topics is provided later in this document.

5 - Monitor Tab

This chapter describes the monitoring features under the **Monitor** tab in the Dashboard.

Overview

You can access the all-network overview page by choosing **Overview > Overview** at the top of the page. The **Overview** page displays periodical reports on the following:

- Total network usage, including bandwidth consumption
- Top 10 network applications by usage
- Top operating systems
- Top 10 clients by usage
- Total amount of client devices detected per day
- Top device manufacturers detected in the network

You can specify time frames that you would like to view, dating back up to one year. You can adjust the time frame by clicking on the calendar symbol to the right of the network name on the overview page. These time frames can be broken down by day, week, or month. The default is one week.

Router status

The **Router status** page is accessible through **Overview > Router status** and contains the following information and functionality:

- Serial number and physical location. Click **Enter an address** to add a location and enter other identifying information.
- Editing configuration. Click **Edit configuration** to edit the name, network, address, notes, and tag information for the MX series.
- Configured IP address information (IP address, default gateway, and DNS servers assigned to Internet ports)
- Identifying information (such as MAC address, serial number, model, tags, and location)
- Status information displaying what ports are currently physically connected to the MX series; usage data, accessible through the client's link; history data, accessible through the event log link
- Performance data (such as connectivity, throughput, latency, and active client devices). Click on the zoom or pan links to view the connectivity, network usage, and latency data for particular time ranges.
- Live tools for troubleshooting and debugging networking issues remotely. For example:
 - Click **Internet traffic** to see real-time WAN throughput.
 - Click the **Active client devices** button to see a list of current clients, and click **Ping** to ping each one. Other live tool buttons allow you to ping the MX series itself or particular MAC addresses.
 - Use the **Traceroute** function to troubleshoot routing issues
 - Click the **DNS** button to test whether the DNS settings of the MX series accurately resolve host names on the Internet.
 - Click **Throughput** to run a throughput test from <https://dashboard.meraki.com>.
 - Determine which router in the Dashboard corresponds to a particular physical router, by issuing a **Blink LEDs** command on the Dashboard and seeing which physical router device blinks. This tool is useful if you have multiple routers.
 - Click **Reboot router** to reboot the router.

Clients

The **Clients** page shows how the network is being used and by which client devices. The information on the page can be filtered by two-hour, day, week, or month time intervals. The **Clients** page also offers access to traffic analysis.

Clients overview

The **Clients** page includes the following features:

- A Summary graph displaying network bandwidth usage and how it has fluctuated over a given time span.
- Traffic analysis pie graphs displaying applications, ports, and HTTP content. You can view configured customized pie graphs.
- The list of connected clients.
- A **Search** function for clients by MAC address, operating system, device type or NetBIOS/Bonjour name. (For details, see [Search tool](#) section below)

- Zoom control, which enables the administrator to see only those clients that have been connected within the specified time span. You can adjust the time span by clicking on 2 hours, day, week, or month.
- A customizable client device list with a variety of available information columns. Sort columns by clicking on a column header. Add or remove columns by clicking **Columns** and shifting options in or out of the **Displayed columns** window.
- Mouse over a row in the device list to see a new line appear in the usage graph. This line depicts the fraction of total bandwidth that the highlighted device used.
- Export list data in XML format for further processing and analysis outside of the Dashboard. Click **Download as XML** to retrieve the data. Most spreadsheet programs, such as Microsoft Excel, can open an XML file.

Client details

You can click on a particular device in the client device list to obtain additional information about the device. This page provides detailed information about the client device and user as well as the device's network usage.

Configuration

The top of the page contains device status information, including client configuration details, MAC address, IP address, hostname, manufacturer, operating system, port forwarding, one-to-one IP addresses, event log, and the device to which it is connected.

Edit configuration

You can edit the device configuration by clicking **Edit configuration** on the **Clients details** page. You can do the following:

- Change the name of the device
- Choose whether the device should get an IP assignment through DHCP or a fixed (static) IP assignment. If the device should have a fixed IP assignment, enter the fixed IP address.
- Create port forwarding rules
- Create a 1:1 NAT mapping
- Allow or block access to the network

Traffic analysis

Pie charts similar to those on the **Client** page show details about this particular client's usage of the network.

Live Tools

Similar to the live tools on the **Router details** page, you can locate a client, ping a client, or even see a real-time packet counter showing the user's activity.

Traffic analysis

Meraki Enterprise networks offer powerful application visibility and control tools. Packet inspection engines running custom parsers in each router provide this information by fingerprinting and identifying applications and application groups. The [traffic shaping](#) then provides the ability to create custom per-user shaping policies based on this application-level visibility. Because Meraki's parsers run at line rate, there is no performance decrease when Traffic Analysis or Traffic Shaping is enabled.

On the main **Clients** page, the pie chart at the top right of the screen displays the traffic within the specified time period, broken down by application, HTTP content type, port number, or customized criteria. The gray arrows flip from one chart option to the next. Custom pie charts can be configured on the traffic shaping page under the **Configure** tab.

Clicking on either the pie chart itself or the **More** link underneath the pie chart opens up the **Traffic analysis details** page, showing a detailed list of the specific applications and content types that make up the data shown in the pie chart. The applications have been assigned to groups to make classifying applications and creating shaping policies simpler. An up-to-date list of which applications are included in each group can be found here:

<http://bit.ly/cUFXnv>

Clicking on a particular application or content type within the **Traffic analysis details** page takes you to the **Rule details** page. Rules are traffic patterns (also known as signatures) that allow the MX series to understand and classify the network traffic. This page provides detailed information about the particular application or network traffic that the device was able to detect based on current activity. This page also shows which users are contributing to usage of a given type, and it displays details such as the application group to which the item belongs and a description of the application or rule.

Live updates

The **Clients** page supports live updates, which provide real-time information about network status and client usage. You can click on the starred **Live updates** link near the top of any page that offers the feature. When live updates are enabled, the Dashboard delivers up-to-date information for that page from the network approximately every 30 seconds, for as long as you stay on the page. The live updates are disabled as soon as you browse to a different page.

Live updates are an effective way to troubleshoot and monitor router status (for example, when network connectivity is lost) and client usage (for example, to see which clients are currently connected and how much bandwidth they are using).

Search tool

The **Clients** and **Event log** pages under the **Monitor** tab have search capabilities, enabling you to find or filter a list of client devices. Any search string can be entered, and the Dashboard attempts to match that search string across all available fields. For example, you can search or filter by device description, Ethernet address, IP address, user, MAC address, and so on. In addition, searches can be bookmarked for future use.

The search tool also supports a number of keywords that can be used to search or filter by specific characteristics. All of the available keyword options are enumerated under the **Help** link next to the search tool.

The search tool operates over the data in the database pertaining to all the devices in a given network. This is an effective way to manage and monitor a large number of client devices.

VPN

This page shows the status of configured site-to-site VPNs. Choose **Configure > VPN** to enable site-to-site VPNs. On the **VPN configuration** page, you can enable or disable VPN mode, as well as set site-to-site firewall Access Control Lists (ACLs) by clicking **Add a rule** and setting values for Policy, Protocol, Source, Src Port, Destination, and Dst Port.


Event log

The **Event log** page provides a detailed record of various client and router activities, including the following:

- DHCP: Events related to DHCP leases provided by the MX series
- Auth: Events related to Active Directory authentication
- ARP
- DNS: Events related to D
- IP
- NTP: Events related to Network Time Protocol and clock synchronization for the MX series
- Dropped: In rare instances, there may be a burst of events in a short period of time, and some events may not get recorded because of memory and bandwidth constraints.
- Status: Events related to LAN/WAN connectivity
- Filtering: Events related to security and content filtering
- Site-to-site VPN: Events related to VPN tunnel information and issues

You can use these logs to troubleshoot connectivity or VPN issues or to get additional data on a client that may be experiencing issues on the network. Click **Reset filters** to change search parameters.

6 - Configure Tab

This chapter describes the configuration options under the **Configure** tab in the Dashboard. Hovering over the  icon beside many configuration features in the Dashboard provides additional information.



At the end of each configuration page, always click **Save Changes** to confirm and write your changes, or **cancel** to revert to your starting point.

Changes can take up to several minutes to take effect in the network.

Router settings

Router settings include passthrough or NAT mode, subnet and VLAN configuration, and site-to-site VPN settings.

Name

This field allows you to set the name of the network for the router.

Mode

The MX series can be deployed in two possible modes:

- Passthrough or VPN concentrator mode
- NAT mode

Passthrough or VPN concentrator mode

As a Layer 2 passthrough device

Choose this option if you simply want to deploy the MX series for traffic shaping and additional network visibility. In this mode, the device does not provide any address translation and operates as a passthrough device between the Internet and the LAN ports (Acting as a Layer 2 bridge). DHCP requests from the LAN are forwarded upstream.

As a VPN concentrator

Choose this option if you want to use MX series as a VPN concentrator device in the data center. In this mode, the device simply provides VPN tunneling functionality.

Network Address Translation (NAT)

Choose this option if you want to use the MX series as a Layer 7 firewall to isolate and protect the LAN traffic from the Internet (WAN). Client traffic to the Internet is modified so that it appears to have the device as its source. In this mode, the device is also the default gateway. This section also provides a link to DHCP settings (see below).

Network partitioning

Single LAN

All downstream hosts are on the same subnet and in a single broadcast domain. The MX series is the default gateway on the LAN.

- **Local subnet:** Use this option to enter the local subnet (LAN) IP range for NAT. Note that you need to provide the information in CIDR notation (for example, 192.168.1.0/24).
- **MX* LAN IP:** This is the address for the router in the local subnet (LAN). This is also known as the local subnet gateway address. You can ping the router by using this IP address, from a client on the subnet that is connected to any one of the LAN ports.

*String changes according to model number (for example, MX60, MX70, ...)

Multiple subnets, partitioned by VLAN

This section allows you to configure VLANs on your router. VLANs allow you to partition your network into different subnets separated at Layer 2. Downstream hosts are on multiple subnets, in different broadcast domains. The VLAN-based network separation can be an effective tool for isolating different networks and therefore providing an additional layer of security and reliability. The MX series is the default gateway on each VLAN.

Do the following to add a new VLAN:

1. Click **Add a VLAN**, and set the following parameters as appropriate:

- **Name:** Name of the VLAN
- **VLAN ID:** Number that is assigned to the VLAN
- **Subnet:** Use this option to enter the subnet/VLAN IP range for a NATed subnet. Note that you need to provide the information in CIDR notation.
- **Router LAN IP:** IP address of the router in this particular VLAN/subnet. This is the default gateway IP address on that VLAN.
- **Actions:** The **X** button under **Actions** allows you to remove the VLAN from the router configuration.

2. Save your changes by clicking **Save Changes** at the bottom of the page.

VLAN for untagged traffic

This option allows you to select how you want the router to handle any untagged traffic. You can either assign it to a particular VLAN or choose **None-drop untagged traffic**.

DHCP

DHCP settings include running or disabling the built-in DHCP service, specifying DNS servers, and creating fixed IP assignments on your MX series.

Client addressing

Choose **Run a DHCP server** if you do not have any third-party DHCP service in your network and you would like to use your MX series for DHCP. (DHCP addressing is specified on the **Router settings** page where you configure subnets).

If you would like to use a third-party DHCP server, choose **No DHCP server**.

DNS nameservers

This is the DNS information that the MX series supply in DHCP lease responses to clients. Nameservers should be IP addresses or fully qualified domain names. You have the option to use Google Public DNS or Open DNS, or to specify a name server.

Fixed IP assignments

This option allows you to reserve an IP assignment for a specific client device, based on the device's MAC address. For example, if you have a local server that should always get assigned the same IP address from the DHCP service, you can create a rule by simply clicking **Add a fixed IP assignment** and providing a name, MAC address, and the desired LAN IP address.

Firewall

The MX series can be configured for inbound and outbound firewall rules, port forwarding rules, and 1:1 NAT mappings.



Inbound traffic is restricted to the router services and forwarding rules configured on this page. If you want to allow additional inbound traffic, you need to create a new 1:1 NAT rule and explicitly allow connections based on protocols, ports, or remote IP addresses (see below).

Outbound rules

Configure deny and permit Access Control List (ACL) statements based on policy, protocol, source IP address and port, and destination IP address and port.

Click **Add a rule** to set values for Policy, Protocol, Source, Src Port, Destination, and Dst Port. You can enter additional information in the Comments field.

Under **Actions**, you can move your configured rules up or down in the list, or click the **X** to remove it.

Router services

- **ICMP Ping:** Use this setting to allow the MX series to reply to ICMP ping messages coming from specific addresses. Values are **None**, **Any**, or a specific IP range (of the format X.X.X.X/24).
- **Web (local status & configuration):** Use this setting to allow or disable access to the local management console (setup.meraki.com) from the WAN/Internet interface. Values are **None**, **Any**, or a specific IP range (of the format X.X.X.X/24).

Forwarding rules

Use this area to configure port forwarding rules and 1:1 NAT mappings as required.

Port forwarding

Use this option to redirect traffic on a specific port to any IP address within the local subnet. Click **Add a port forwarding rule** to obtain access to a particular device behind a branch router. You need to provide the following:

- **Description:** A description of the rule
- **Protocol:** TCP or UDP
- **Public port:** Port on which traffic arrives
- **LAN IP:** Local IP address to which traffic is to be directed
- **Local port:** Port number for the server or client behind the router to which traffic is to be forwarded
- **Allowed remote IPs:** IP addresses of allowed traffic sources

1:1 NAT

Use this option to map a public IP address to a local IP address on your network. Click **Add a 1:1 NAT mapping** to allow a local web server to be accessible through the public Internet. You need to provide the following:

- **Name:** A descriptive name for the rule
- **Public IP:** The public (routable) IP address that can be accessed from the worldwide Internet
- **LAN IP:** The local IP address to which the traffic is routed
- **Allowed inbound connections:** To enable an inbound connection, click **Allow more connections** and enter the following information:
 - **Protocol:** Choose among **TCP**, **UDP**, **ICMP**, or **any**.
 - **Ports:** Enter the range of ports that are allowed for inbound traffic.
 - **Remote IPs:** Enter the range of WAN public IP addresses that are allowed for the inbound traffic.

Under **Actions**, you can move your configured rules up or down in the list, or click the **X** to remove it.



Creating a 1:1 NAT rule does not automatically enable inbound traffic.

By default all inbound connections are denied.

VPN



The site-to-site VPN feature is available only in the Advanced Security Edition.

Meraki's site-to-site VPN solution is unique in many ways. Through the Dashboard, each participating MX series device does the following:

- Advertises its local subnets participating in the VPN.
- Advertises its WAN IP addresses on Internet1 and Internet2 ports.
- Downloads the global VPN route table from the Dashboard (automatically generated by the Dashboard, based on each MX's advertised WAN IP/local subnet in the VPN network).
- Downloads the preshared key for establishing the VPN tunnel and traffic encryption.

The net result is an automatic mesh site-to-site VPN solution that is configured with a single click.

VPN Mode

You have two options to configure site-to-site VPN:

- **Split tunnel:** Send only site-to-site traffic, meaning that if a subnet is at a remote site, the traffic destined for that subnet is sent over the VPN. However, if traffic is destined for a network that is not in the VPN mesh (for example, traffic going to a public web service such as www.google.com), the traffic is not sent over the VPN but instead is routed directly to the Internet from the local MX device.
- **Full tunnel:** Send all traffic through a **Full tunnel concentrator**, meaning that regardless of the mesh VPN route map, redirect all traffic to a VPN concentrator. No traffic goes directly to the Internet. You need to specify which device is to act as the full tunnel concentrator (see below).

Subnet settings

If you have multiple VLANs, you have the option to specify which VLANs participate in the mesh VPN network.

Full tunnel concentrator

This option is available only if you choose **Full tunnel** for the VPN mode. This option lets you designate the remote MX device that is to receive all network traffic from the local MX device.

NAT Traversal

There are two options for NAT traversal:

- **Automatic:** In the vast majority of cases, the MX series can automatically establish site-to-site VPN connectivity by means of this option, even if there are other firewalls or NATing devices between the MX devices. While the **Automatic** option is the recommended (and default) option, it applies a technique known as "firewall hole-punching" that can be detected by some advanced firewalls.
- **Manual Port Forwarding:** If the **Automatic** option does not work, you can use this option. In this case, VPN peers contact the MX router by using the specified public IP address and port number.

Remote VPN participants

You can see a full list of other MX devices participating in the mesh VPN network in this page.



Two or more MX routers cannot be in the same site-to-site VPN network and have the same (overlapping) subnets.

Ensure that the same subnet is not configured on another remote MX network.

Organization-wide VPN settings

These options apply to all MX devices that are in the mesh VPN network.

Non-Meraki VPN peers

This option allows you to establish a VPN connection between Meraki MX devices and those from other manufacturers, such as a Cisco ASA, Juniper SRX, or SonicWall NSA device, by using the standard IPsec VPN settings, with parameters as follows:

- **Name:** Name of the third-party device
- **Public IP:** The public (WAN) IP address of the device
- **Private subnets:** The private (LAN) subnet that the device is servicing

- **Preshared secret:** The secret key for establishing the VPN tunnel
- **Actions:** You can move your third-party VPN device configuration up or down in the list, or click the **X** to remove it.

Site-to-site firewall

You can configure site-to-site firewall rules that apply to all VPN peers in your organization. These rules allow and deny traffic across the the whole VPN network.

Click **Add a rule** to set values for Policy, Protocol, Source, Src Port, Destination, and Dst Port. You can enter additional information in the Comments field. Under **Action**, you can move your configured rules up or down in the list, or click the **X** to remove it.

Alerts and administration

This page allows you to monitor and change administrative access, determine the conditions and responses for alerts, set a time zone, and manage firmware upgrades.

Network administration

View and assign both organization and network administrators here.

Organization admins

In this section you can view who is configured as an organization administrator. Organization admins have full control over all the networks that have been configured for your account.

To make changes to the organization admins, click **organization configuration** in this section.

Network admins

This option allows you to add additional administrators or read-only administrators for the current network. You can add an existing user or create a new user.

Network alerts

Enabled Alerts

You can enable email alerts in case the router goes offline for a specified duration of time or in case configuration options are changed. The time sensitivity of these alerts is configurable from five minutes to one hour, which can help to reduce false positives.

Send alerts via email to

This is where you can specify email addresses to which alerts should be sent.

Network time zone

Local time zone

This option allows you to set the network time zone. This is important so that time-sensitive operations such as device maintenance (see below) can be scheduled accurately.

Firmware upgrades

From time to time, Meraki may perform maintenance (such as firmware upgrades) on your MX series.

Upgrade window

This option defines a two-hour window when device maintenance may occur. Choose a time with low network usage, because maintenance may reduce network performance. You will receive a notification through email and on the Dashboard prior to maintenance.

Firmware upgrade

This section specifies whether a firmware upgrade is available for your network.

Try beta firmware

This option allows the MX series to access the latest beta firmware when it becomes available. Beta firmware may be unstable and is not suitable for a production network, but it provides early access to new features for in-house testing.

Active Directory



Active Directory-based content filtering is available only in the Advanced Security Edition.

Active Directory (AD) authentication allows content/URL filtering based on Active Directory group policies. You can setup the MX device to connect to a Microsoft Domain Controller to authenticate users with AD.

Currently, Active Directory-based authentication works only if the MX is in NAT mode and one of the following is true:

- the Microsoft Domain Controller is on the LAN side of the MX device, or
- the Microsoft Domain Controller is accessible through the VPN.

Active Directory

This option toggles AD integration on or off.

Per VLAN settings

This option allows you to describe which VLANs should require AD authentication. If a VLAN does not require AD authentication, it falls back to default content filtering settings (see below). This option is available only if you have multiple VLANs in your network.

Active Directory servers

- **Short Domain:** Short name of the domain, as opposed to the fully qualified domain name (FQDN). For example if the FQDN is "mx.meraki.com", the short domain is "mx".
- **Server IP:** The LAN or WAN IP address of the domain controller
- **Domain admin:** Name of the domain administrator (for example, administrator)
- **Password:** The password of the administrator so that the MX device can connect to the domain controller
- **Actions:** Click **X** to delete the AD server settings.

Note that you can add multiple domain controllers by clicking **Add an Active Directory domain server**.



You have to run the following commands on your Windows Domain Controller to allow communication with the MX device:

- Windows Server 2008:

```
netsh advfirewall firewall set rule group="Remote Event Log Management" new enable=yes
```

- Windows Server 2003:

```
netsh firewall set service RemoteAdmin enable
```

Group Policies

You can import user groups by using either the full LDAP syntax or the **List LDAP Groups** functionality, by listing and clicking on individual AD groups. Once a new group is imported to the LDAP membership window, you can add web content categories for blocking.



If clicking on [List LDAP Groups](#) do not return any list, the MX device may be unable to connect to the AD server.

Please check the Event log (Auth events) for additional information.

Traffic shaping

The MX series includes an integrated Layer 7 packet inspection, classification, and control engine, enabling you to set QoS policies, load balancing, and prioritization based on traffic type and applications.

Uplink configuration (MX70 only)



Multiple uplink configuration is available only with the MX70.

When you have two WAN uplink connections, you can configure the throughput, primary uplink, and aggregation settings to allow the device to manage and prioritize the incoming and outgoing traffic accurately.

Internet1

This option lets you enter the bandwidth for the Internet1 WAN uplink. This information is needed for traffic load balancing between the active Internet ports.

Internet2

This option lets you enter the bandwidth for the Internet2 WAN uplink, as above.

Primary uplink

This option determines which WAN uplink should be the primary connection (when the MX series is operating in **Link aggregation disabled** mode). VPN traffic and management traffic to the Meraki Dashboard use the primary uplink.

Link aggregation

When enabled, **Link aggregation** spreads Internet traffic across both uplinks, proportional to the Internet1 and Internet2 bandwidths, respectively (specified above in the Internet1 and Internet2 bandwidth sliders).

Example: If Internet1 bandwidth is 9 Mbps and Internet2 bandwidth is 1 Mbps, the load-balancing algorithm sends 90% of the traffic through the Internet1 uplink.

Uplink preferences

Use this option to redirect traffic from a specific subnet, or from a specific port, or any traffic going to a particular destination WAN IP range or port through a preferred uplink. A common use case involves separating LAN traffic to one of two VLANs (for example, a voice VLAN or a data VLAN), and then sending each VLAN's traffic through a different Internet uplink, such as sending voice traffic through MPLS by means of the Internet1 uplink, and data through cable or DSL by means of the Internet2 uplink.

Traffic analysis

Custom pie chart

Custom pie charts give you a quick way to visualize web traffic and application access patterns that are not available by default. For example, you can create a pie chart that displays the percentage of network traffic going to various multimedia sites, such as netflix.com, youtube.com, or vimeo.com.

You can also use custom charts to better understand and optimize your network traffic type. For example, you can create a pie chart based on various port numbers to measure how much of your traffic is related to Microsoft file sharing (SMB/CIFS), remote desktop protocol (RDP), printer traffic, or simple web traffic. You can then decide whether you need additional network optimization techniques targeted to particular traffic types.

To create a new pie chart, click **Add a slice**, and choose whether you want to track an HTTP host name, port number, IP address range, or a combination of port number and IP address range.

Global bandwidth limits

These settings allow you to put limits on total aggregate network traffic, as well as on each client's incoming and outgoing network traffic. The minimum limit on the throughput is 20 kb/s for both the total network limit and the per-client limit. Click **details** or **simple** to switch between two possible modes.

- **simple**: Single setting that applies to both upload and download traffic throughput. Move the slider control right or left to set the limits.
- **details**: Allows you to set different limits on upload and download throughput. Enter the limits manually in kb/s. You can also use this mode to create more-precise per-client limits than in simple mode.
- **Enable SpeedBurst**: To provide a better user experience in bandwidth shaping, an administrator can enable SpeedBurst by selecting the **Enable Speedburst** checkbox. SpeedBurst allows users to exceed their assigned limit in a "burst" for a short period of time, providing a more satisfying Internet browsing experience while still preventing any one user from using more than his or her fair share of bandwidth over the longer term. Users are allowed up to four times their allotted bandwidth limit for a period of up to five seconds.

Traffic shaping rules

To optimize your network, you can create shaping policies to apply per-user controls on a per-application basis. This allows you to reduce bandwidth for recreational applications such as peer-to-peer file sharing programs, and to prioritize bandwidth for your business-critical enterprise applications.

Creating Shaping Rules

Click **Create a new rule** to add a traffic shaping rule. Traffic shaping policies consist of a series of rules that are performed in the order in which they appear in the policy, similar to custom firewall rules. There are two main components to each rule: the type of traffic to be limited or shaped (rule definition), and how that traffic should be limited or shaped (rule actions).

Rule Definition

Rules can be defined in two ways:

- You can select from various predefined application categories such as Video & Music, Peer-to-Peer, or Email.
- You can create rules by specifying HTTP hostnames (for example, salesforce.com), port numbers (such as 80), IP ranges (such as 192.168.0.0/16), or IP address range and port combinations (such as 192.168.0.0/16:80).

The rule action is enforced on all traffic that matches the specifications you select. By clicking **Add an expression**, you can create additional specifications for traffic that is shaped according to the same rule action.

Rule Actions

Traffic-matching-specified rule sets can be shaped or prioritized.

- Bandwidth limits can be specified to ignore any limits specified for the whole network, to obey the specified limits, or to apply more-restrictive limits than the network limits. Use the bandwidth slider control to choose the appropriate limit for each type of traffic. To specify asymmetric limits on uploads and downloads, click **details** next to the bandwidth slider control.
- Priority can be set to **High**, **Normal**, or **Low**, allowing the MX series to prioritize a given network flow relative to the rest of the network traffic.
- Quality of Service (QoS) prioritization can be applied to Layer 3 traffic. To prioritize traffic at Layer 3, select a value for the DSCP tag in the IP header on all incoming and outgoing IP packets. This also affects the Wi-Fi Multimedia (WMM) priority of the traffic.



For the Priority feature to work as desired, ensure that uplink throughput settings are accurate. For QoS prioritization to work as desired, ensure that upstream networking equipment supports QoS prioritization as well.

Creating a Sample Traffic-Shaping Rule

Here is an example of how to set up a traffic shaping policy with multiple traffic-shaping rules. (For detailed examples, refer to the Deployment Guides chapter.)

To prioritize VoIP and minimize peer-to-peer traffic and gaming, create a new traffic-shaping policy by following the steps below:

1. In the Rule #1 **Definition** pull-down menu, choose **VoIP & video conferencing**.
2. Under **Bandwidth limit**, choose **Ignore network limit**.
3. In the **Priority** pull-down menu, choose **High**.
4. Under **DSCP tagging**, ensure that **Do not set DSCP tag** is set.
5. Click **Add a new shaping rule**.
6. In the Rule #2 **Definition** pull-down menu, choose **Peer-to-peer (P2P)**.
7. Click **Add an expression**.
8. In the new pull-down menu, choose **Gaming**.
9. In the **Bandwidth limit** section, click **Choose a limit** and use the slider to choose a low throughput (the minimum is 20 kb/s).
10. Save your changes by clicking **Save Changes** at the bottom of the page.

Content filtering



The content filtering feature is available only in the Advanced Security Edition.

Content filtering allows you to block certain categories of websites based on your organizational policies. You can also block or whitelist (allow) individual websites for additional customization. For example, you can block the "Chat" category; this also blocks gmail.com and facebook.com, because both websites also offer chat functionality. You can whitelist gmail.com and facebook.com, to make sure that both websites are fully operational while all other websites providing chat functionality are blocked.

- **Blocked websites:** The URLs of locations you want to block
- **Additional blocked domains:** One domain per line
- **Whitelisted domains:** One domain per line

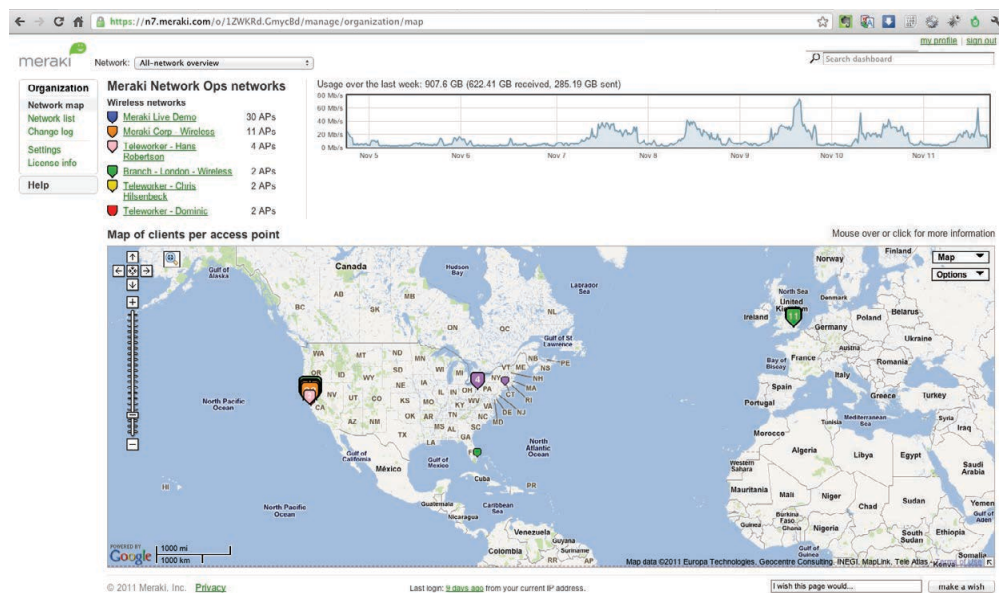
7 - Organization Tab

This chapter describes the organization-level management features under the **Organization** tab of the Meraki Dashboard.

Network map

By choosing **Network > All-network overview** at the top of the page, you can see a summary of all of the networks in a particular organization. The usage graph at the top summarizes cumulative usage across all networks, and the map shows network locations with color-coded markers corresponding to the network list to the left of the usage graph. Mouse over a network in the list and the network marker on the map is highlighted.

In addition, the usage for that particular network is displayed in the usage graph. Click on a particular network marker on the map or click on a network name in the list to "drill down" to the **Overview** page for that particular network. Below is an example of an all-network Overview page.



Network list

Click **Network list** to see all networks in a sortable table, including name, network type, usage, access point/router count, offline devices, active devices, the original administrator who created the network, and the date of creation.

Change log

Click **Change log** to see critical change-management and tracking functionality for large organizations, where administrators need to track changes to firewall rules and other critical network settings. The change log lists changes and administrators who have made those changes.

Settings

Click **Settings** to update the name of the organization, add or modify organization admins, and modify their privileges. Additionally, you can configure security settings such as the following:

- Password expiration
- Policy for used or old passwords
- Strong password policy
- Account lockout settings

- Idle timeout settings
- Two-factor authentication

SNMP settings



Currently, this feature works only with MR wireless access points.

This feature allows the Dashboard to send SNMP data to an external SNMP server.

License info

Click **License info** for licensing details. There are two licensing options for the Meraki MX series:

- Enterprise Edition
- Advanced Security Edition

Check the Meraki website (www.meraki.com/mx) for feature differences between the two licensing options.

An organization must have a valid Enterprise Edition license or Advanced Security Edition license for the MX series in order to work properly. Each organization is licensed for a maximum number of routers for a certain amount of time (typically from one year to five years). For example, the organization may be licensed for 25 routers with the Enterprise Edition through January 30, 2012.

In addition, each organization is required to use either the Enterprise Edition or the Advanced Security Edition uniformly. For example, you can have all 25 routers using Enterprise Edition or Advanced Security Edition, but you cannot have 20 routers using one edition and 5 using the other edition. If you wish to use Enterprise Edition for some routers and Advanced Security Edition for other routers, you need to create two organizations, one for your routers with the Enterprise Edition, and another for the routers with the Advanced Security Edition.

You can manage a given organization's licenses on the **License info** page under the **Configure** page. The page displays the following information:

- Status: OK or problem
- Wireless Cloud Controller version (currently Enterprise only)
- MX Cloud Controller version (Enterprise or Advanced Security)
- Expiration date
- Licensed device limit
- Current device count
- License history (list of licenses that have been applied to the network)

When a new organization is created, the organization is granted a 30-day grace period. Before the grace period expires, you must enter a valid license key, whose format is a 12-character string (for example, Z2A7-32TE-A8Y4). (The string is not case-sensitive.)

Adding licenses

You can add a license by clicking **Increase device limit**. The period of the new license must fulfill the following criteria:

- Be at least as long as the existing license.
- Be the same edition as the existing license (Enterprise or Advanced Security).

The Dashboard automatically extends the renewal date of the organization's license in order to enforce cotermination.

Example: An organization has one Enterprise network with ten MX60 routers, each of which was purchased at the same time with a one-year license. Four months into the license term, six more MX60 routers are added, each with one-year licenses.

The new network license structure looks like this:

- 10 original MX60 * 8 months remaining on license = 80 MX60-months
- 6 new MX60 * 12 months purchased on license = 72 MX60-months
- 152 total MX60-months divided by 16 MX60s = 9.5 months of license

The licenses for all 16 MX60 routers will now expire in 9.5 months, adding an additional 1.5 months onto the one-year term of the original ten-router network. The license prorating calculation below illustrates how this prorated calculation works.



If a different type of router is added to an existing organization, (for example, you add an MX70 with one year of Enterprise Edition license to the organization example above), the prorating calculation takes into account the price difference between the two MX series types.

Renewing licenses

You can renew the license within 30 days of the renewal date. To renew, simply click **Renew license** on the **License info** page and enter a license key. To obtain a new license key, contact your Meraki sales representative.

Expired licenses or exceeding the licensed device limit

If an organization's license is expired or the number of devices in the organization exceeds the licensed limit, the administrator has 30 days to return the organization to a valid licensed state. During this grace period, the system reminds the administrator to add additional licenses. After 30 days, administrators are not able to access the Dashboard (except to add additional licenses).

8 - Advanced Topics

This chapter discusses additional features that are supported by the Meraki Dashboard.

Organizations

An "organization" consists of a collection of networks and a collection of administrative accounts. Every administrator has an account in the Dashboard that is part of an organization. Administrators can edit the organization's information, including the organization's name, phone number, and address. An organization is covered by a single license. Organizations can only be created. To delete an organization, please contact Meraki Support.

Administrators and roles

An administrator can perform the following operations within a given organization:

1. Create, edit, and delete administrator accounts for the organization.
 - a. Administrative accounts are managed from the **Alerts and administration** page. Choose **Organization admins > organization configuration**.
 - b. Administrative accounts can have full access or read-only access.
 - c. When an administrator resets the password on an administrative account, a new password is emailed to the administrator. Administrators can reset their own passwords by clicking **my profile** at the top of any page in the Dashboard.
2. Create, edit, and delete networks for which the administrator has been granted administrative privileges.

By definition, an administrator has administrative privileges over any network the administrator creates. However, another administrator who did not create the network must first be granted administrative access to the network (by another administrator with administrative access to the network) before accessing that network.

Moving MX series devices between networks or organizations

You can move an MX series between networks in a given organization, as follows:

1. Choose **Monitor > Router** status.
2. Click **Edit configuration**.
3. From the **Change network** pull-down menu, choose the new network you want and click **Save**.

You can also move routers between organizations. This is accomplished through the following steps:

1. Record the serial number of the device you want to move.
2. Remove the device from its current network.
3. Choose **Monitor > Router status**.
4. Click **Edit configuration**, and then click **Remove**.
5. Log out of the current organization, then log into the target organization. Select or create a new network that does not contain an MX series. You can add your existing device either at the creation of the network or by choosing **Configure > Add access points**. The aforementioned serial number is required for this step.

NOTE: The **Add Meraki devices** page appears only if the network does not already contain an MX series.

Automatic software upgrades

New features require no client- or server-side upgrades, but instead are added to the Meraki Dashboard several times per year with minimal downtime. Meraki also manages firmware upgrades centrally, freeing the administrator from having to worry about keeping the routers up-to-date. Firmware upgrades take place in a secure, fault-tolerant fashion.

When a Meraki MX device receives notification from the Dashboard to download new firmware updates, the device buffers the update. The update is applied only when the integrity and the authenticity of the firmware is verified. You will receive an email alert several weeks in advance of a firmware upgrade, and a notice will be posted in the Dashboard to notify you of the exact time that the upgrade will occur. If necessary, you can delay or reschedule the upgrade by contacting Meraki Support.

For a Meraki MX series to upgrade to the latest firmware, the device simply needs to be connected to the Internet to

reach the Meraki Dashboard. If an upgrade is available, it is scheduled and deployed. The device's local web page shows whether an upgrade is in progress. An upgrade typically takes less than a few minutes over a fast Internet connection. When the upgrade completes, the device reboots itself.



For additional tips and troubleshooting, refer to the [Meraki Knowledge Base](#), which can be accessed from the [Help](#) tab.

9 - Deployment Guides

This chapter provides detailed instructions for common deployment topologies.

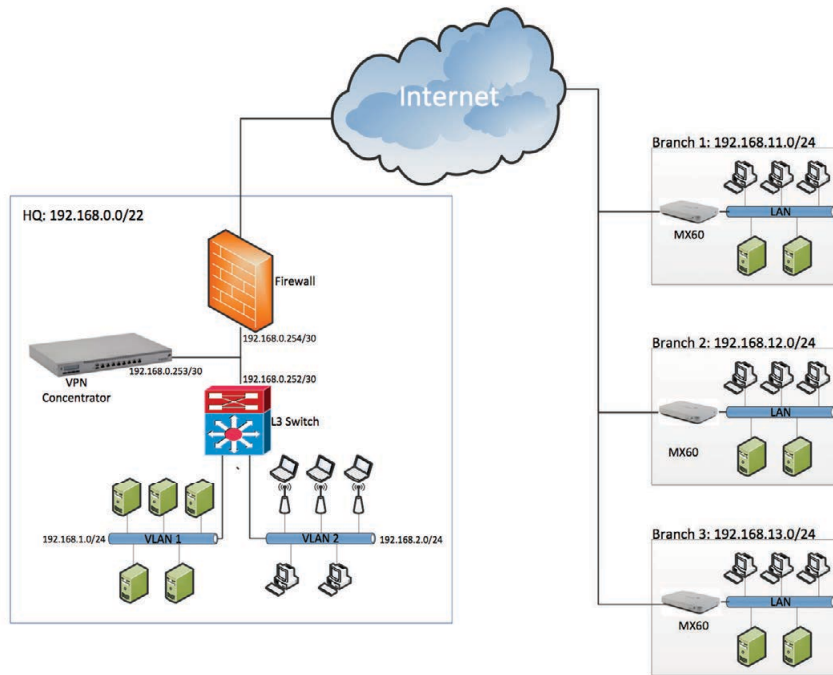
Section	Description
Branch Network Setup	A quick start guide to setup a branch network in NAT mode
VPN concentrator	Deployment options for terminating VPN connections at the data center
3rd party VPN	Step by step instructions on creating IPSec VPN connection between Cisco and MX
Content filtering with AD	Windows Server setup and integration with MX for AD based content filtering

Branch network setup

This section provides additional information on how to configure MX routers as the Internet gateways for branch locations.

Example topology

In this example, there are three remote locations that use MX60 devices. The devices are connected to HQ by means of a Meraki site-to-site VPN.



Branch WAN and LAN settings

First, you need to make sure that the router can connect to the Internet and access the Meraki Dashboard. Once this is done, you can use the Dashboard to set the subnet range and DHCP settings, as well as to assign fixed IP addresses to devices such as printers and access points within the branches.

Here are the WAN and LAN settings for the Branch #1:

1. Connect the router to the DSL or cable modem through the modem's Ethernet output.
2. Set the MX series WAN IP address and DNS settings, with the following two options
 - a. You can let the device negotiate these settings with the local ISP automatically through DHCP.
 - b. Alternatively, if your ISP has provided you with a static IP address and DNS settings, you can enter them manually. (For more on how to set the device WAN IP address, refer to the appropriate installation guide for your MX series device.)
3. Login to your Dashboard account at <https://dashboard.meraki.com>.
4. To verify that the device is accessible in the Dashboard, choose **Monitor > Router status**.
5. Assign a subnet for each branch:
 - a. Choose **Configure > Router settings**.
 - b. Choose **Mode > NAT**.
 - c. Choose whether you want a single LAN or multiple VLANS through **Network partitioning**.
 - d. Enter the local subnet scope in CIDR notation in **Local subnet** field. For example, if your subnet is from 192.168.11.1 to 192.168.11.254, you'll need to enter the following information in the **Local subnet** field: 192.168.11.0/24.
 - e. Enter the **MX LAN IP** (for example, 192.168.11.1). This sets the IP address of the MX device on this LAN.
6. Choose your DHCP option.

- a. For locations with a third-party DHCP server (such as a Microsoft Windows server that serves as the local domain controller):
 - i. Choose **Configure > DHCP**.
 - ii. Choose **No DHCP server**.
 - b. For locations, where you'd like the MX to provide DHCP services:
 - i. Choose **Configure > DHCP**.
 - ii. Choose **Run a DHCP server**.
7. Connect a laptop to one of the LAN ports of the MX, and then make sure that you have Internet access and that you are getting an IP address within the subnet field you have assigned.



If you are using the DHCP service on the MX series, you can reserve IP addresses for devices such as printers and APs by adding fixed IP assignments (see Fixed IP assignments on the [Configure > DHCP](#) page).



In NAT mode, the MX series is the default gateway on the LAN/VLANs that you've created above. If you are going to connect branches through a site-to-site VPN connection, each network must have a different (nonoverlapping) subnet.

Site-to-site VPN

Traditional site-to-site VPN

Although there are a variety of solutions for site-to-site VPN connection, all peering devices need the following information:

- Preshared key (PSK) or certificate
- Public IP addresses of other peer devices
- NATed subnets behind the peer devices
- VPN phase1 and phase2 parameters to ensure matching encoding and various other settings

Based on the information above, peer devices establish the VPN tunnel through the following:

- Connecting to each other directly
- Jointly negotiating VPN phase1 and phase2 offers
- Adding one or several routes to their route maps to reach the other peer's NATed subnets through the VPN interface

Meraki site-to-site VPN is different

Traditionally, most of the steps above are manual and therefore are prone to user errors (such as mistyped subnet information or nonmatching VPN configs). MX devices are different. They are all connected to the Dashboard and they each use Dashboard to help broker VPN connections to their peer networks in a given organization, as follows:

- Each MX device constantly advertises its public IP address and its NATed subnets to the Dashboard.
- When VPN is enabled, VPN peers automatically contact each other and initiate an IPSec VPN connection.
- The Dashboard assigns a unique preshared key for all participating VPN peers.
- Finally, the Dashboard sends a globally adjusted route map to each device, so that they all know how to reach each other's NATed subnets.

The end result of this automated process is a site-to-site VPN that is always up-to-date, dynamically adjusting to any changes in the network and that is up and running with a single click.



While the Meraki VPN solution uses the power of the Dashboard during the setup and control of the VPN, the actual VPN traffic never flows through the cloud, but instead travels directly between peered VPN devices.

Setting up site-to-site VPN with Meraki MX devices

Creating a site-to-site VPN tunnel to the HQ from branches is simple:

1. Choose **Configure > VPN**.
2. Choose **Split tunnel** from the **VPN mode** pull-down menu.
3. Choose **Automatic** from the **NAT traversal** options.

You are done!

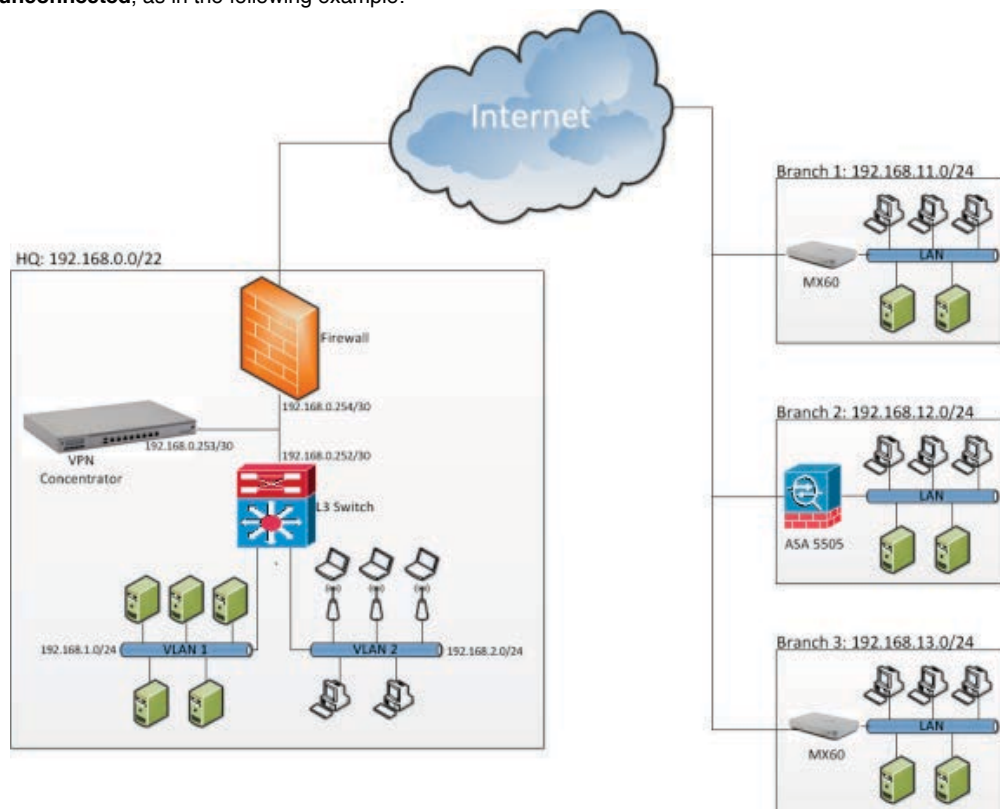
Configuring VPN Concentrator for the data center

You have two options for deploying an MX series at your data center: either in *VPN Concentrator* or *NAT* mode. Use the table below to choose the appropriate mode.

Deployment Mode	Recommended When . . .
VPN Concentrator (1-Armed)	There is already a firewall in the HQ/data center. The MX is simply a VPN concentrator for the site-to-site VPN traffic.
NAT	The MX is the Layer 7 application firewall in the HQ/data center.

Deploying VPN Concentrator (1-Armed) mode

In this mode, simply connect the Internet1 port of the MX to the desired VLAN at the HQ/data center and **leave the LAN ports unconnected**, as in the following example:



In this example, the HQ has 3 VLANs:

- VLAN 0: 192.168.0.252/30
- VLAN 1: 192.168.1.0/24
- VLAN 2: 192.168.2.0/24

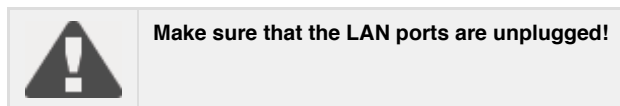
There are also three branches:

- Branch 1: 192.168.11.0/24
- Branch 2: 192.168.12.0/24
- Branch 3: 192.168.13.0/24

Configuring the MX

- **Set the IP address of the MX:** Connect MX's Internet1 port to VLAN 0, and (using the local setup.meraki.com

page) statically set the MX IP address to 192.168.0.253/30, with the default gateway set to 192.168.0.254. You can use the same DNS servers as you use for the rest of your network (with an internal/private or a public DNS address such as 8.8.8.8).



- **Enable VPN Concentrator mode:** Choose **Configure > Router configuration > Passthrough or VPN Concentrator**.

Router configuration

Name:

Mode:

- Passthrough or VPN concentrator**
The router acts as a Layer 2 bridge, and does not modify client traffic. Configure VPN to enable communication with remote peers. Only one WAN uplink can be used in this mode.
- Network Address Translation (NAT)**
Client traffic to the Internet is modified so that it appears to have the router as its source. Configure DHCP on the [DHCP settings](#) page.

- **Advertise the HQ subnets:** The HQ MX, which is the VPN concentrator, needs to advertise the HQ subnets to the branch sites. This allows MX devices at the branch networks to receive routing information about the HQ and update their route maps for the newly available subnets through the VPN tunnel. By entering the HQ subnet information (see below), you allow the Dashboard to advertise these subnets to all other MX devices that are part of the site-to-site mesh network. To advertise the subnets:
 - Choose **Configure > VPN** and ensure that VPN is enabled.
 - Click **Add a route**, and enter the new networks as appropriate.

VPN configuration

VPN mode:

NAT traversal:

- Automatic**
Connections to remote peers are arranged by the Cloud Controller.
- Manual: Port forwarding**
Remote peers contact the MX router using a public IP and port that you specify. Use this if your MX router is behind another NAT and "Automatic" traversal does not work.

Local networks:

Subnet	Name	Actions
<input type="text" value="192.168.1.0/24"/>	<input type="text" value="VLAN 1"/>	<input type="button" value="X"/>
<input type="text" value="192.168.2.0/24"/>	<input type="text" value="VLAN 2"/>	<input type="button" value="X"/>

[Add a route](#)

- **Add routes to the HQ Layer 3 switch:** You need to instruct the HQ Layer 3 switch to route any traffic destined for the branches through the MX VPN Concentrator. For the three branches in our example, here are the commands you need to enter on a Cisco Layer 3 switch:

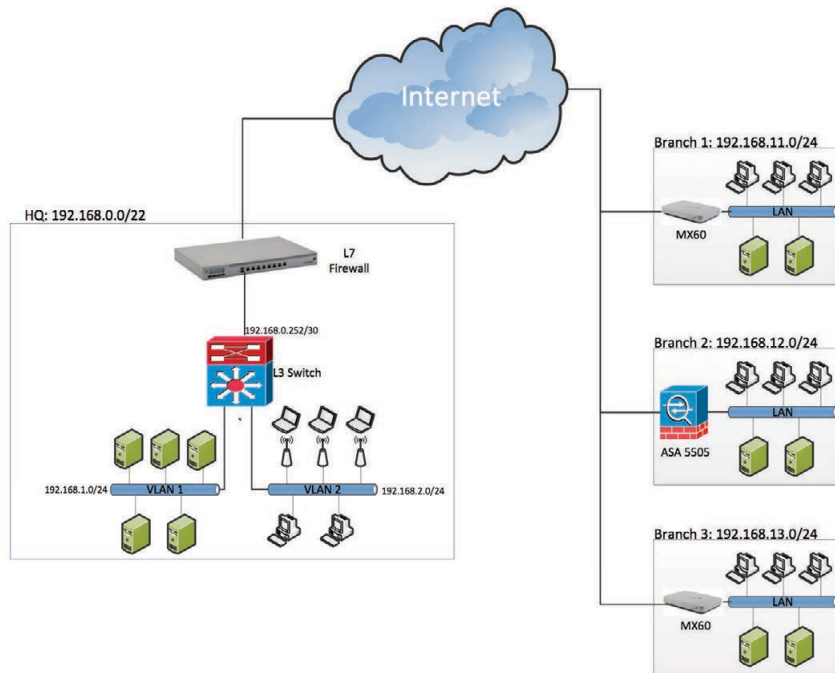
```
ip route 192.168.11.0 255.255.255.0 192.168.0.253
ip route 192.168.12.0 255.255.255.0 192.168.0.253
ip route 192.168.13.0 255.255.255.0 192.168.0.253
```

Testing

You should be able to ping any of the HQ subnets from one of the branches.

Deploying in NAT mode

In this mode, you must connect the Internet1 port to your local ISP connection, and then connect any of the LAN ports to your local network, as illustrated in the following example.



In this example, the HQ has 3 VLANs:

- VLAN 0: 192.168.0.252/30
- VLAN 1: 192.168.1.0/24
- VLAN 2: 192.168.2.0/24

There are also three branches:

- Branch 1: 192.168.11.0/24
- Branch 2: 192.168.12.0/24
- Branch 3: 192.168.13.0/24

Configuring the MX

- **Set the IP address of the MX:** Connect the MX's Internet1 port to the interface to the local ISP, and statically set the MX Internet1 IP address to 192.168.0.253/30, with the default gateway set to 192.168.0.254. You can use the same DNS servers as you use for the rest of your network (with an internal/private or a public DNS address such as 8.8.8.8).
- **Enable NAT mode:** Choose **Configure > Router settings > Network Address Translation (NAT)**.
 - In the **Local subnet** field, enter **192.168.0.254/30**.
 - In the **MX LAN IP** field, enter **192.168.0.254**.

Network partitioning	<input checked="" type="radio"/> Single LAN All downstream hosts are on the same subnet and in a single broadcast domain. <input type="radio"/> Multiple subnets, partitioned by VLAN Downstream hosts are on multiple subnets, in different broadcast domains. Downstream switches can add VLAN tags to partition hosts.
Local subnet ⓘ	<input type="text" value="192.168.0.254/30"/> <small>(e.g., "192.168.1.0/24")</small>
MX90 LAN IP ⓘ	<input type="text" value="192.168.0.254"/>

- **Add static LAN routes:** The HQ MX needs to know about the additional two subnets behind the Layer 3 switch at the HQ. This information is required to route packets destined for these two subnets. Also, the Dashboard uses this information to advertise the HQ routing information to remote branch MXs. For example, if someone at Branch 1 wants to connect to a file server at the HQ (VLAN1, 192.168.1.15), the remote MX at Branch 1 must know that the 192.168.1.0/24 subnet is located at the HQ. By entering static LAN routes at the HQ (see below), you allow the Dashboard to advertise these subnets to all other MX devices that are part of the site-to-site mesh network.
 - To add static LAN routes, still under **Router configuration**, click **Add a static route**.
 - Enter the **Name**, **Subnets**, and **Gateway IP** fields (assuming that 192.168.0.252 is the Layer 3 switch's

IP address).

Static LAN routes

Name	Subnets	Gateway IP	Actions
VLAN1	192.168.1.0/24	192.168.0.252	X
VLAN2	192.168.2.0/24	192.168.0.252	X

[Add a static route](#)

Configuring the HQ Layer 3 switch

You need to configure the HQ Layer 3 switch to route any traffic destined for the branches to the MX VPN Concentrator so that the traffic can be tunneled through the VPN. For the three branches in our example, below are the commands you need to enter on a Cisco Layer 3 switch:

```
ip route 192.168.11.0 255.255.255.0 192.168.0.254
ip route 192.168.12.0 255.255.255.0 192.168.0.254
ip route 192.168.13.0 255.255.255.0 192.168.0.254
```

Testing

You should be able to ping any of the HQ subnets from one of the branches.

Connecting to a third-party VPN device

This example outlines the process for establishing an IPsec VPN tunnel between a Meraki MX device and a Cisco ASA appliance. While some of the steps below are specific to Cisco configuration, the overall IPsec VPN connection concept is generic and applies equally well to devices such as Juniper SRX, FortiNet FG, or SonicWall firewalls.

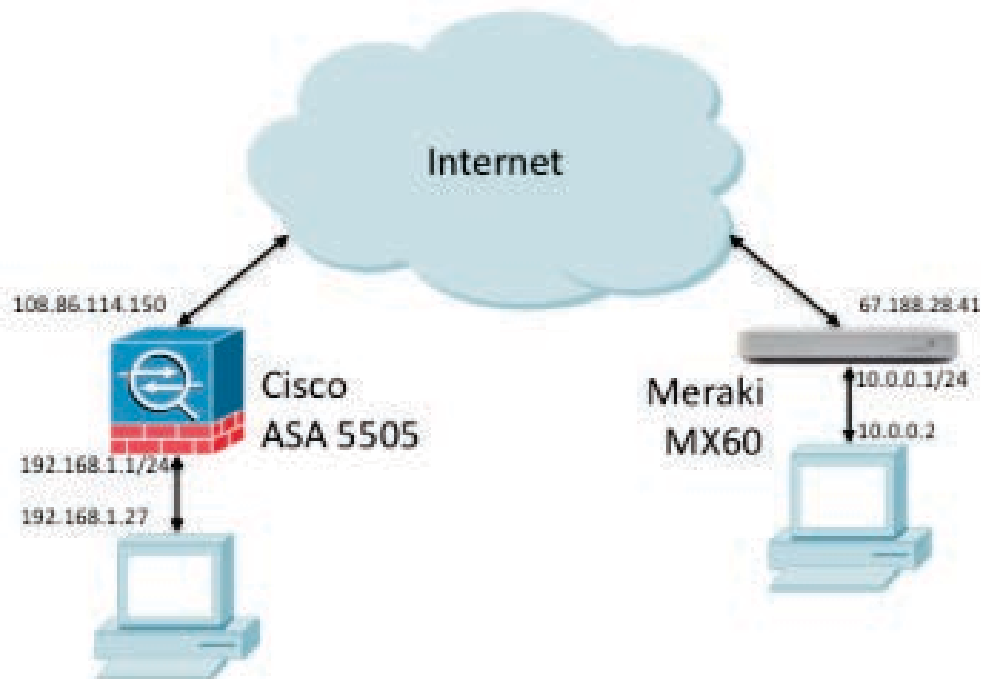


Currently, MX series support for third-party VPN interoperability requires the following:

- Preshared keys (no certificates)
- LAN static routes (no routing protocol for the VPN interface)
- Phase 1 (IKE Policy): 3DES, SHA1, DH group 2, lifetime 8 hours
- Phase 2 (IPsec Rule): Any of 3DES, DES, or AES; either MD5 or SHA1; PFS disabled; lifetime 8 hours

Cisco ASA Example

The following figure shows an example setup that uses a Meraki MX60 with a Cisco ASA 5505 firewall.



Network details

- **Cisco ASA 5505 IP settings**
 - WAN IP: 108.68.114.150
 - LAN subnet: 192.168.1.0/24
 - LAN IP: 192.168.1.1
 - Example client: 192.168.1.27
- **Meraki MX60 IP settings**
 - WAN IP: 67.188.24.41
 - LAN subnet: 10.0.0.0/24
 - LAN IP: 10.0.0.1
 - Example client: 10.0.0.2
- **Preshared Key (PSK): "ThatWasEasy"**

Configuring the Cisco ASA 5505

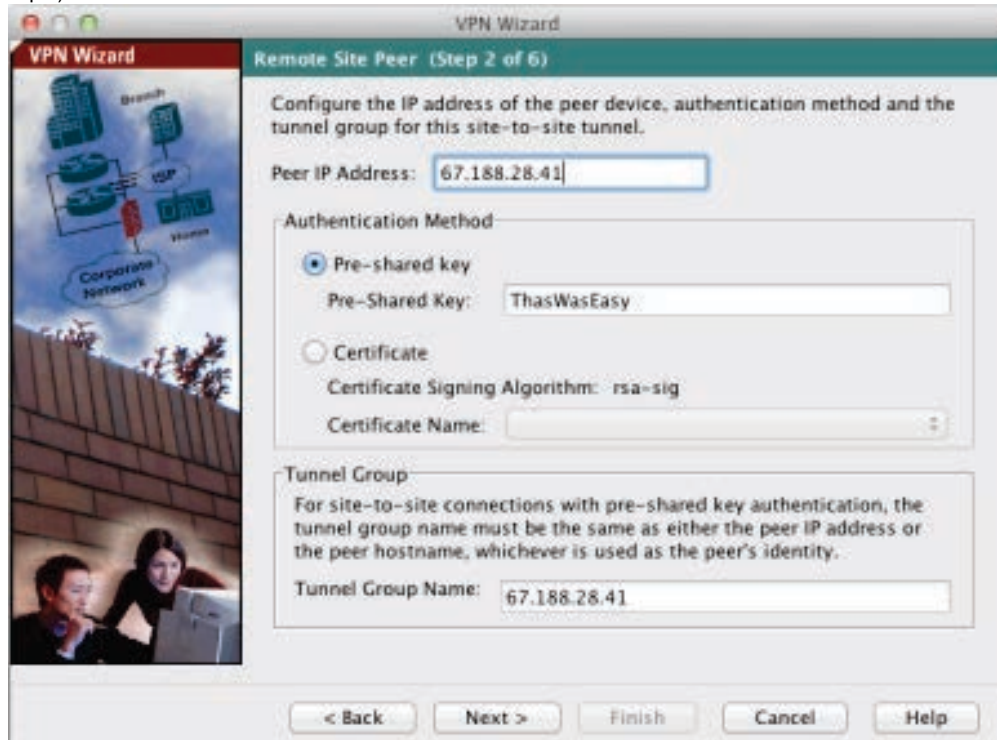
NOTE: You need the Cisco Adaptive Security Device Manager (ASDM) management tool to follow these instructions.

Using the Cisco ASDM:

1. Launch the IPsec VPN Wizard from the top menu, choosing **Wizards > IPsec VPN Wizard** and choosing **Site-to-site** from the VPN Tunnel Type options.
2. Choose **outside** for the VPN Tunnel Interface.
3. **Check** Enable inbound IPsec sessions to bypass interface access list.



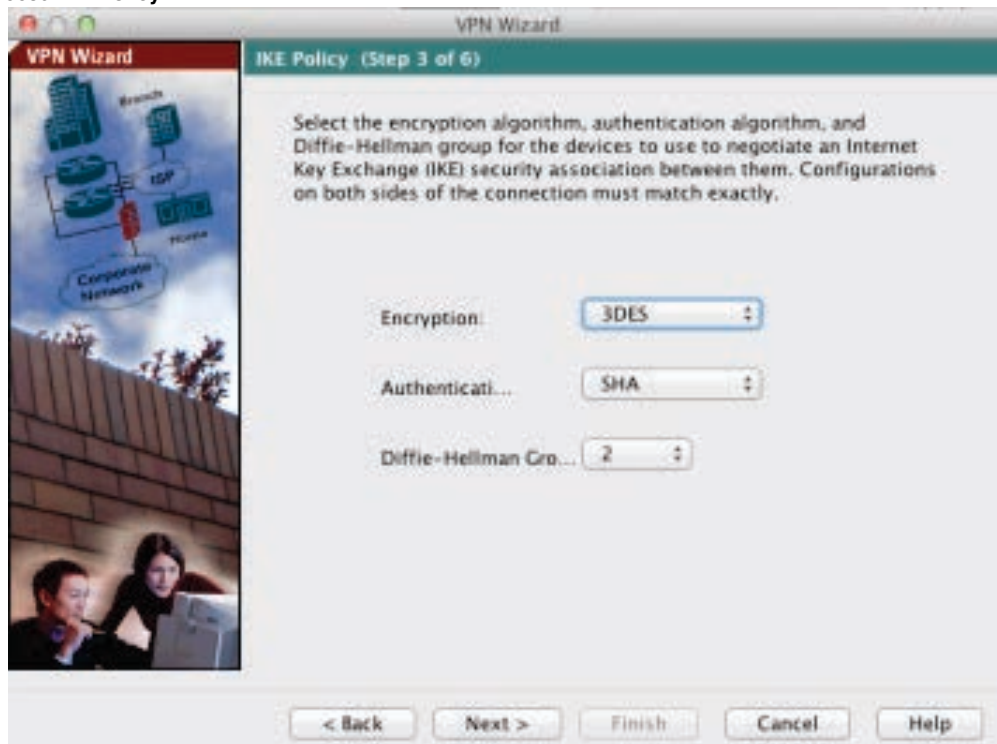
4. Enter the public IP address of the MX60 and enter a preshared key (PSK) of your choice ("*ThatWasEasy*" in this example).





Remember the PSK, as you'll need to reenter it on the MX60 VPN config page.

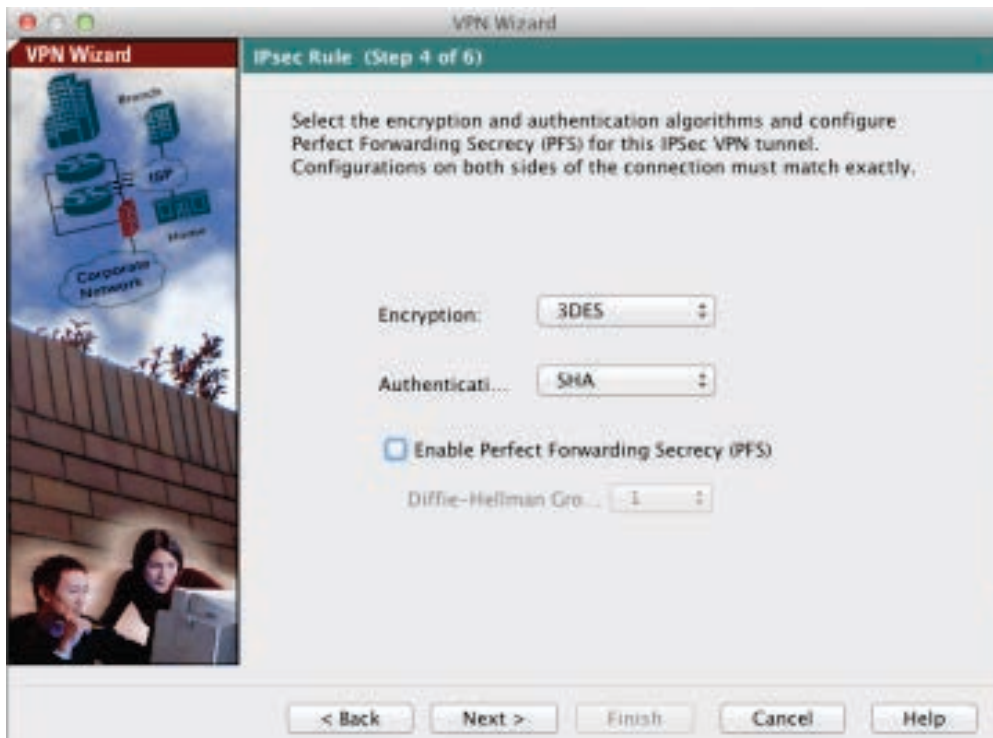
5. Choose IKE Policy.



At Phase 1 (IKE policy) negotiation, only the following options are supported:

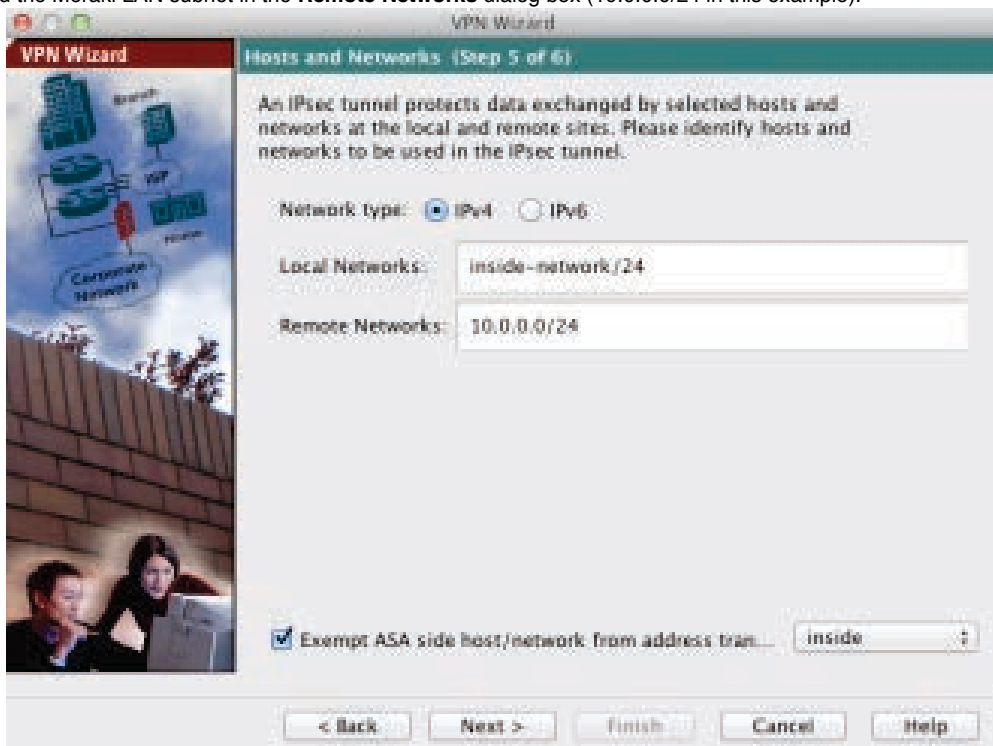
- Encryption: 3DES
- Authentication: SHA
- DH Group: 2
- Lifetime: 8 hours

6. Choose IPSec Policy.



You must ensure that Enable Perfect Forwarding Security (PFS) is **NOT** selected.

7. Enter the LAN subnet for the Cisco ASA in the **Local Networks** dialog box (192.168.1.0/24 in this example), and the Meraki LAN subnet in the **Remote Networks** dialog box (10.0.0.0/24 in this example).



8. Verify the settings.
9. Click **Finish**.
10. Click **Apply** in the main ASDM window.

Configuring the Meraki MX60

1. In the Dashboard, choose **Configure > VPN** for the MX60.
2. Click **Add a peer**.
3. Add the public IP address of the ASA 5505 along with the subnet and pre-shared secret ("ThatWasEasy" in this example).

Organization-wide settings

Options in this section apply to all VPN peers in this organization.

Non-Meraki VPN peers

Name	Public IP	Private subnets	Preshared secret	Actions
Cisco ASA 114	108.86.114.150	192.168.1.0/24	*****	✚ ✕

[Add a peer](#)

Site-to-site firewall

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

[Add a rule](#)



If the Cisco ASA have multiple private subnets, you enter them separated by commas in the "Private subnets" field

Testing the configuration

Using a computer behind the MX60, ping 192.168.1.5 (a host on the 192.168.0.0/24 LAN of the ASA) and confirm that you are receiving the response to your ping.

Syslog Messages

Below is the sequence of messages you should see if the tunnel was established successfully:

```
Group = 67.188.28.41, IP = 67.188.28.41, PHASE 2 COMPLETED (msgid=d8bb723b)
Group = 67.188.28.41, IP = 67.188.28.41, Automatic NAT Detection Status: Remote end IS
behind a NAT device This end IS behind a NAT device
AAA retrieved default group policy (DfltGrpPolicy) for user = 67.188.28.41
Group = 67.188.28.41, IP = 67.188.28.41, PHASE 1 COMPLETED
Group = 67.188.28.41, IP = 67.188.28.41, Security negotiation complete for LAN-to-LAN
Group (67.188.28.41) Responder, Inbound SPI = 0x9263dde9, Outbound SPI = 0x098ebc99
IPSEC: An outbound LAN-to-LAN SA (SPI= 0x00AFCE2A) between 108.86.150.114 and
67.188.28.41 (user= 67.188.28.41) has been created.
IPSEC: An inbound LAN-to-LAN SA (SPI= 0xF05C7DAD) between 108.86.150.114 and 67.188.28.41
(user= 67.188.28.41) has been created.
Group = 67.188.28.41, IP = 67.188.28.41, PHASE 2 COMPLETED (msgid=ff1029b3)
Built inbound ICMP connection for faddr 10.0.0.1/13000 gaddr 192.168.1.5/0 laddr
192.168.1.5/0
Built outbound ICMP connection for faddr 10.0.0.1/13000 gaddr 192.168.1.5/0 laddr
192.168.1.5/0
```

Troubleshooting

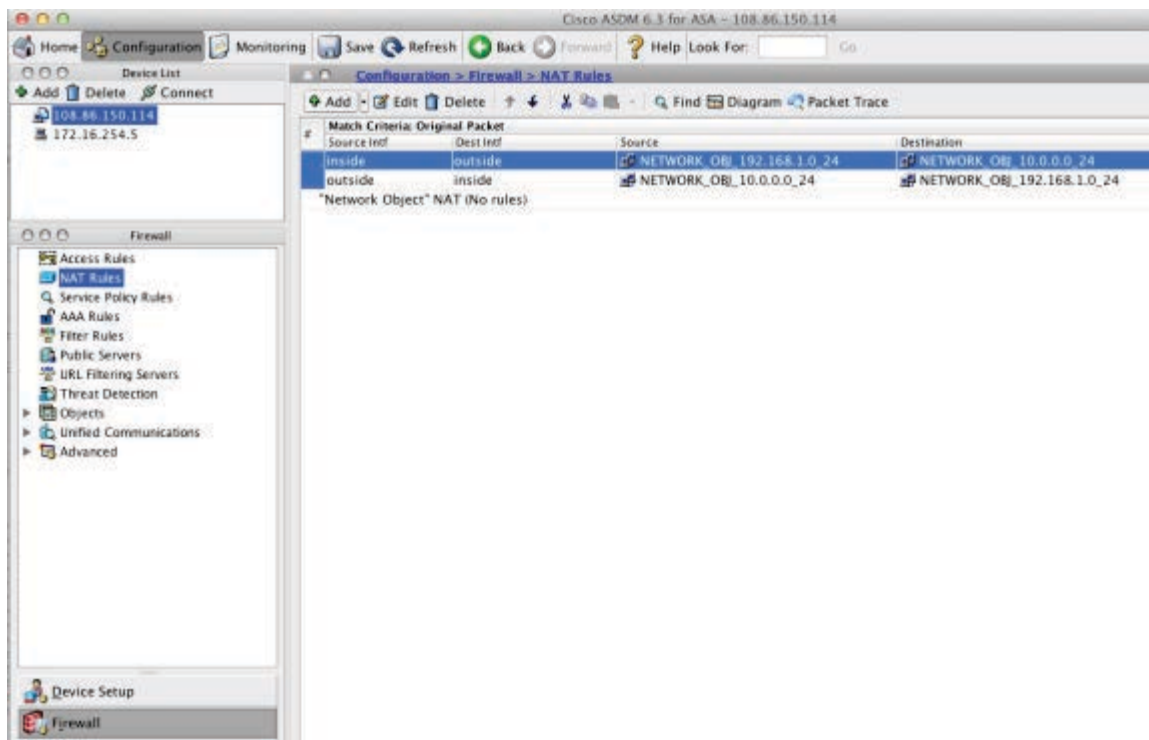
This section addresses some common problems that can occur.

Cisco Syslog Message

```
Asymmetric NAT rules matched for forward and reverse flows; Connection for icmp src
outside:10.0.0.1 dst inside:192.168.1.27 (type 8, code 0) denied due to NAT reverse path
failure
```

Cause

This happens when you are trying to ping a device behind the ASA from a device behind the MX, but the Cisco ASA doesn't have the proper NAT rules. It may be NATing the outgoing traffic through the VPN tunnel. Fixing this issue may be tedious. If you want to fix it, go to the **Configure > Firewall > NAT** page and look at all your NAT rules. Make sure that you have a rule that matches the following screen shot.

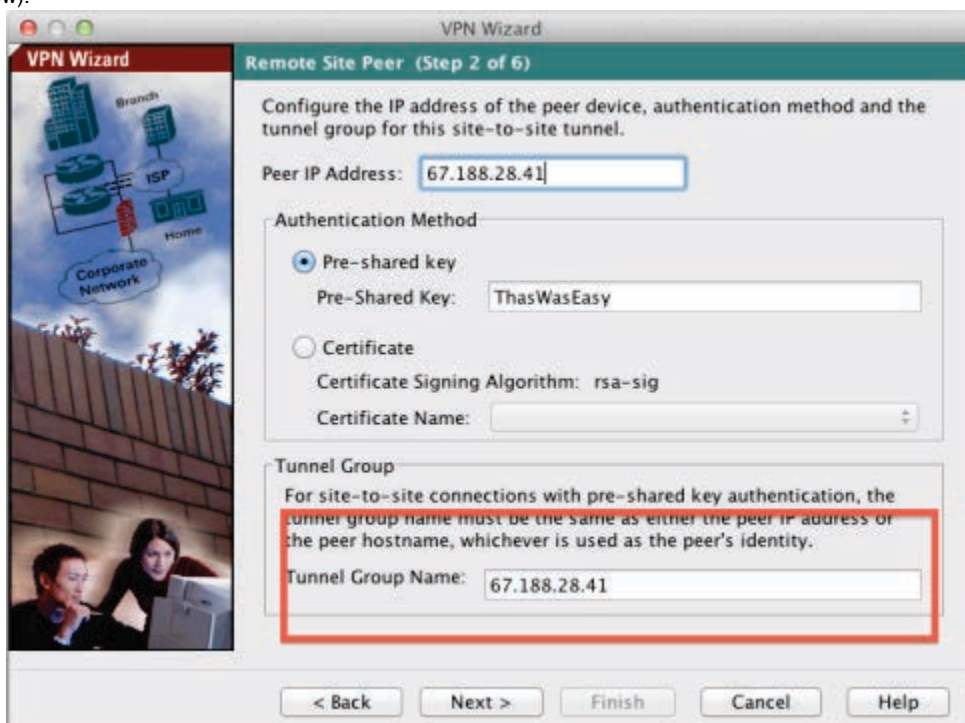


Cisco Syslog Message

Group = 67.188.28.41, IP = 67.188.28.41, Can't find a valid tunnel group, aborting...!

Cause

Make sure the tunnel group (from Step 2 on the Cisco ASA) matches the public IP address of the MX device (see the red box below).



Getting additional help

The ASDM Syslog window provides a wealth of information in case the VPN tunnel is not established. You can also

compare your ASA configuration to the sample configuration shown in the [Cisco ASA 5505 Configuration file](#) . If you are still unable to sort out the problem, contact support@meraki.com.

Example Cisco ASA 5505 Configuration File

This example configuration output is used to add further detail to the configuration of IPSec Interoperability.

```
> show running-config
: Saved
:
ASA Version 8.3(1)
!
hostname lab-asa1
domain-name meraki.local
enable password aa2VYqHCVmgGxYjF encrypted
passwd aa2VYqHCVmgGxYjF encrypted
names
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 108.86.114.150 255.255.255.248
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
boot system disk0:/asa831-k8.bin
ftp mode passive
dns domain-lookup inside
dns domain-lookup outside
dns server-group DefaultDNS
name-server 8.8.8.8
name-server 8.8.4.4
domain-name meraki.local
object network NETWORK_OBJ_10.0.0.0_24
 subnet 10.0.0.0 255.255.255.0
object network NETWORK_OBJ_192.168.1.0_24
 subnet 192.168.1.0 255.255.255.0
object-group icmp-type DM_INLINE_ICMP_1
 icmp-object echo
 icmp-object echo-reply
object-group service DM_INLINE_TCP_1 tcp
 port-object eq www
 port-object eq https
 port-object eq telnet
access-list outside_access_in extended permit icmp any any object-group DM_INLINE_ICMP_1
access-list outside_access_in remark remote access
access-list outside_access_in extended permit tcp any interface outside object-group DM_INLINE_TCP_1
access-list outside_1_cryptomap extended permit ip 192.168.1.0 255.255.255.0 10.0.0.0 255.255.255.0
access-list outside_access_in_1 extended permit tcp any any eq ssh
access-list RemoteAccessVPN_splitTunnelAcl standard permit 192.168.1.0 255.255.255.0
pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
ip local pool 192.168.10.0 192.168.10.10-192.168.10.99 mask 255.255.255.0
icmp unreachable rate-limit 1 burst-size 1
```

```

asdm image disk0:/asdm-631.bin
no asdm history enable
arp timeout 14400
nat (inside,outside) source static NETWORK_OBJ_192.168.1.0_24 NETWORK_OBJ_192.168.1.0_24 destination static
NETWORK_OBJ_10.0.0.0_24 NETWORK_OBJ_10.0.0.0_24
access-group outside_access_in_1 in interface outside control-plane
access-group outside_access_in in interface outside
route outside 0.0.0.0 0.0.0.0 108.86.114.151 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 0.0.0.0 0.0.0.0 inside
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set transform-set ESP-AES-128-SHA
ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA
ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto map outside_map 1 match address outside_1_cryptomap
crypto map outside_map 1 set peer 67.188.28.41
crypto map outside_map 1 set transform-set ESP-3DES-SHA
crypto map outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map outside_map interface outside
crypto isakmp enable outside
crypto isakmp policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
telnet 0.0.0.0 0.0.0.0 inside
telnet 0.0.0.0 0.0.0.0 outside
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd auto_config outside
!
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd dns 8.8.8.8 8.8.4.4 interface inside
dhcpd enable inside
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
group-policy RemoteAccessVPN internal
group-policy RemoteAccessVPN attributes
dns-server value 8.8.8.8 8.8.4.4
vpn-tunnel-protocol IPSec
split-tunnel-policy tunnelspecified
split-tunnel-network-list value RemoteAccessVPN_splitTunnelAcl
default-domain value meraki.local
group-policy "Site-to-site with Meraki" internal
group-policy "Site-to-site with Meraki" attributes
vpn-idle-timeout 30
vpn-filter none
ipv6-vpn-filter none

```

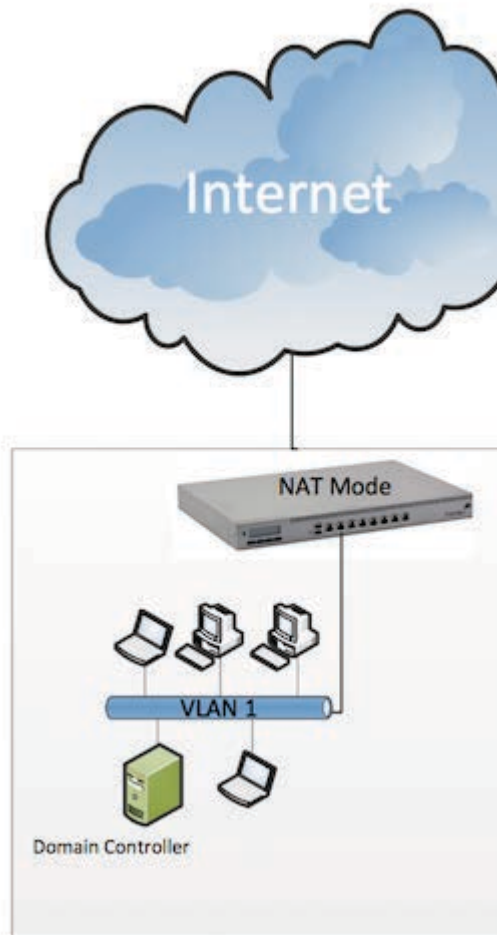
```
vpn-tunnel-protocol IPSec
username test password 274Y4GRAbNElaCoV encrypted privilege 0
username test attributes
vpn-group-policy RemoteAccessVPN
tunnel-group 67.188.28.41 type ipsec-l2l
tunnel-group 67.188.28.41 ipsec-attributes
pre-shared-key *****
tunnel-group RemoteAccessVPN type remote-access
tunnel-group RemoteAccessVPN general-attributes
address-pool 192.168.10.0
default-group-policy RemoteAccessVPN
tunnel-group RemoteAccessVPN ipsec-attributes
pre-shared-key *****
!
!
prompt hostname context
call-home
profile CiscoTAC-1
no active
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
destination address email callhome@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic monthly
subscribe-to-alert-group configuration periodic monthly
subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:82e279d988d2dd312a29cb8eef31a6ce
: end
```

Content filtering with Active Directory

With the Active Directory (AD)-based content filtering feature, the MX series use the Microsoft Light Directory Access Protocol (LDAP) to connect to a Microsoft Domain Controller (DC) and discover the user groups and users in those groups. Administrators can use this feature to set different content filtering policies for different user groups.

Example

A typical example of AD integrated content filtering involves providing a Children's Internet Protection Act (CIPA)-compliant Internet access at a K-12 education institution. Administrators can enforce stricter content filtering rules for students, while relaxing constraints for administrators, staff, and teachers.

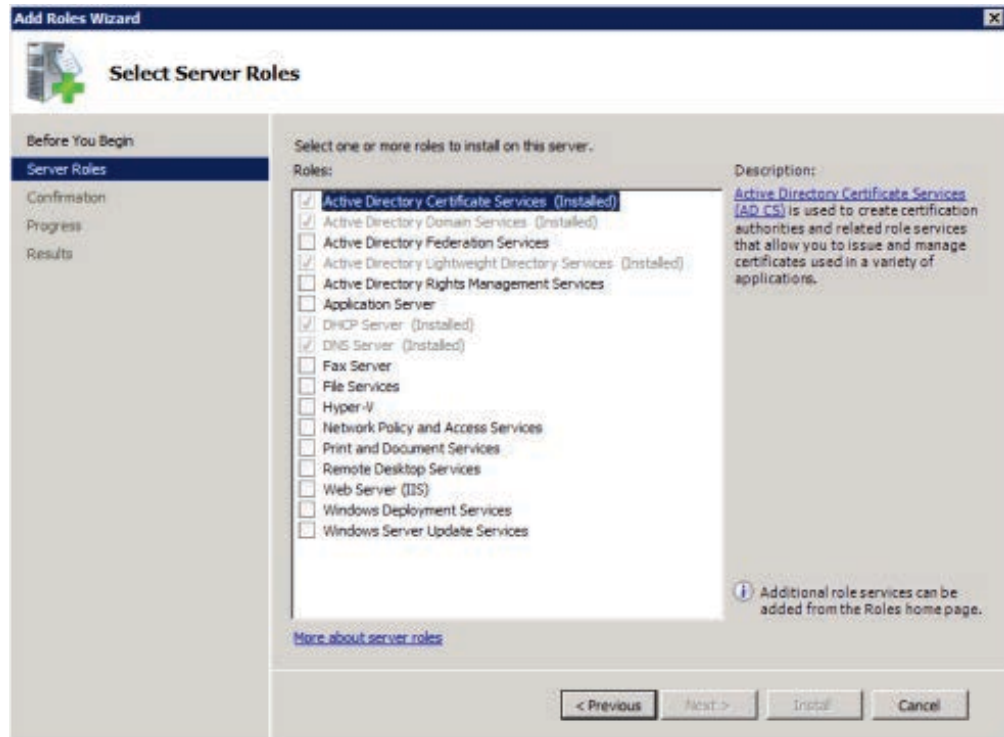


In this example:

- The DC is a Windows Server 2008 R2 machine.
- The domain is called mx.meraki.com.
- The server's name is dc.mx.meraki.com.
- The server's static IP address is 192.168.1.2 (on the MX LAN subnet).

Predeployment requirements

1. Ensure that the following roles are installed on the DC (see the following screenshot from Windows Server 2008 R2 Server Manager):
 - a. Active Directory Domain Services
 - b. Active Directory Lightweight Directory Services
 - c. Active Directory Certificate Services



2. The DC is in Enterprise mode, and not Standalone.
3. The DC is on the LAN side of the MX.
4. The DC uses a static IP address, with the following options:
 - a. You can assign a static IP address through Windows network settings.
 - b. Alternatively, you can reserve an IP address for the DC, by choosing **Configure > DHCP > Fixed IP assignments**.
5. No L3 switch or device is between the MX and client devices (the MX must be able to see client MAC IDs in the traffic).

Configuring Windows firewall rules


If you're running a firewall, run the following commands from the command line to allow the MX to connect to the appropriate services running on the DC:

- Windows 2008:

```
netsh advfirewall firewall set rule group="Remote Event Log Management" new enable=yes
```

- Windows 2003:

```
netsh firewall set service RemoteAdmin enable
```



Running these commands is absolutely critical!

Without these firewall rules, the MX will not be able to connect to the DC.

Configuring Dashboard settings

1. Enable AD Authentication.
2. Add the domain controller to the Dashboard by choosing **Configure > Active Directory**.

Active Directory authentication

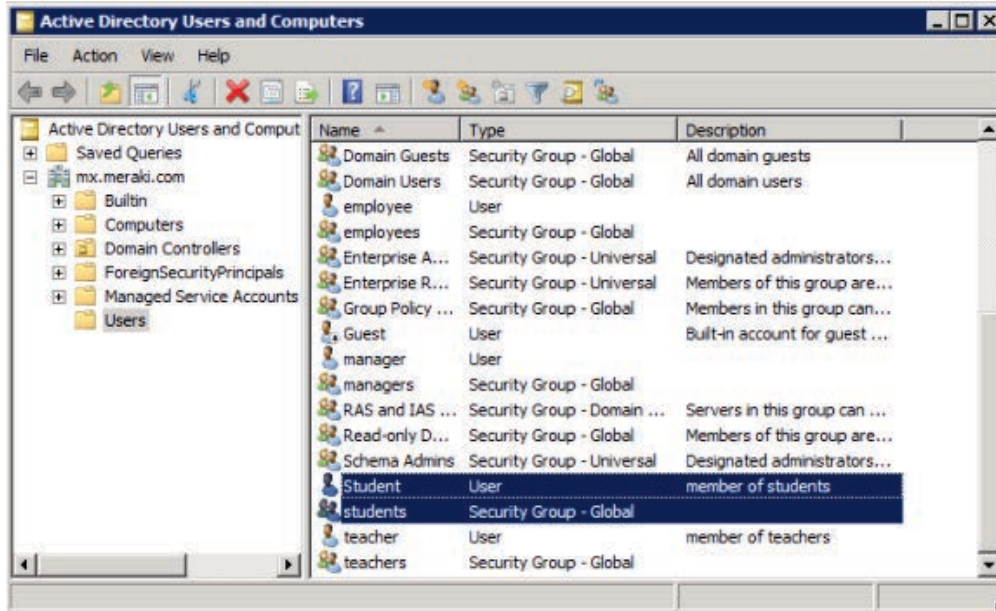
Active Directory **Authenticate users with Active Directory**
 No authentication
 Require login via splash page

Unauthenticated users

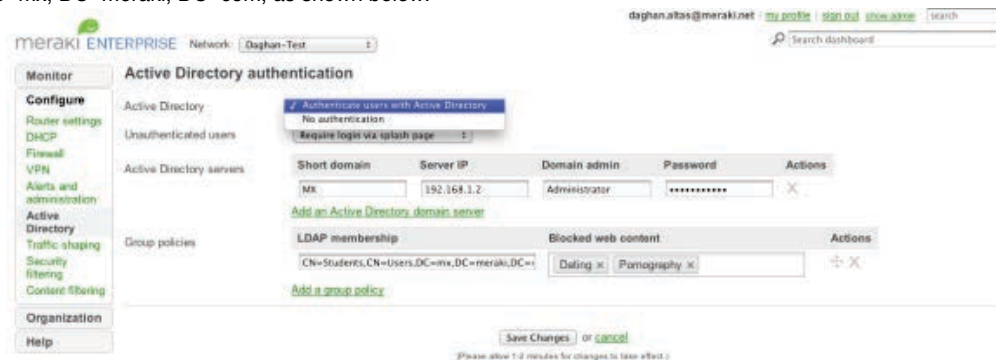
Active Directory servers	Short domain	Server IP	Domain admin	Password	Actions
	MX	192.168.1.2	Administrator	*****	X

[Add an Active Directory domain server](#)

3. Add to the Dashboard the list of user groups that you want to control through content filtering. For example, you may have a "students" group whose members include individual users such as "Student" in the following example:



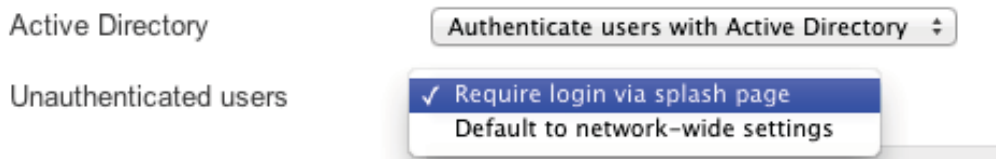
The LDAP membership field should contain an LDAP group name, for example, CN=students, CN=Users, DC=mx, DC=meraki, DC=com, as shown below.



In case a user is a member of two or more groups, the list is searched in order, from top down, until there is a match.

4. **Unauthenticated users:** Decide how you want to handle users who are using devices such as iPads or Android phones that are not signed into the Active Directory. For those users, you can either force them to inherit the default content filtering settings (through **Configure > Content filtering**), or require them to authenticate to the AD domain through a splash page. The latter option is illustrated below.

Active Directory authentication



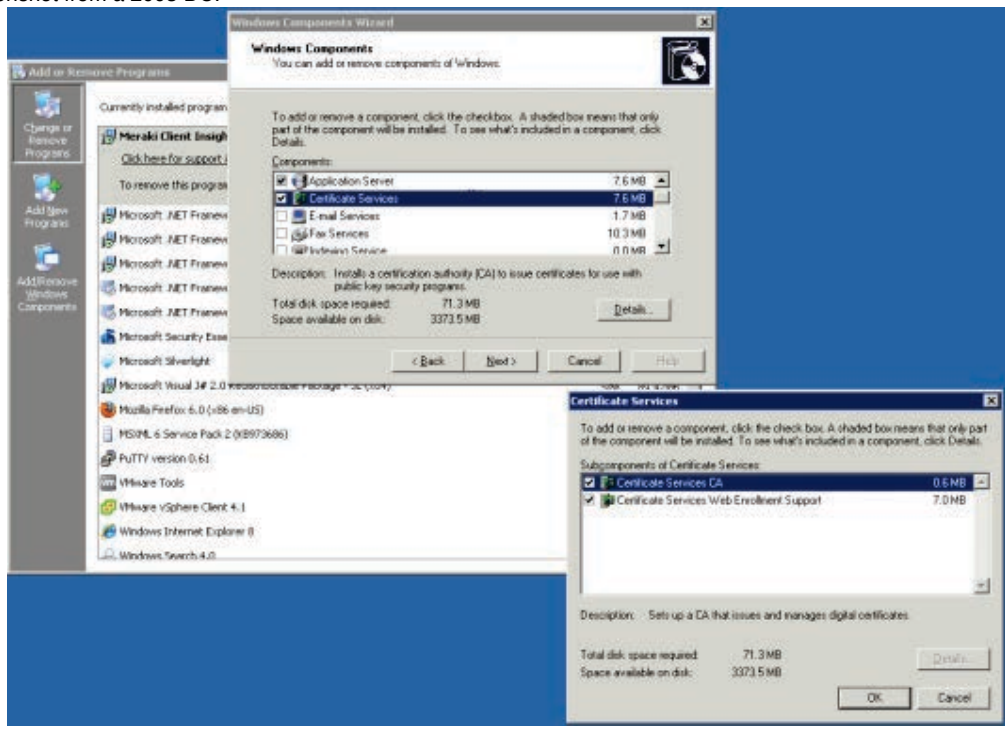
On splash pages, users can enter their credentials as DOMAIN\User or User@domain.

Additional Information

The Active Directory integration generates activity in the Event Log. User credentials are all under the auth filter. If the credentials are broken or the server is temporarily unreachable, you will see a "Failed to connect Active Directory" event in the MX event log.

In Windows Server 2003, to install the right services, you have to go to **Add/Remove Windows Components**. Below is

a screenshot from a 2003 DC.



10 - Additional Resources

Meraki provides documents that administrators can reference when implementing and managing a Meraki wireless network, including the following:

- *Meraki Network Design Guide*
- *Meraki Hosted Architecture White Paper*

These and other resources are available at <http://meraki.com/support/#documentation>.

In addition, the most up-to-date information on troubleshooting the Meraki MX series can be found at the Meraki online knowledge base, at <http://www.meraki.com/support/>.