cisco Meraki

White Paper

Cisco Meraki Auto VPN

JULY 2013

This white paper describes Auto VPN (Layer 3 site-to-site IPsec) and how to deploy it between Cisco Meraki Security Appliances.

Table of Contents

Introduction	3
Cisco Meraki's Solution	4
For More information	8

Introduction

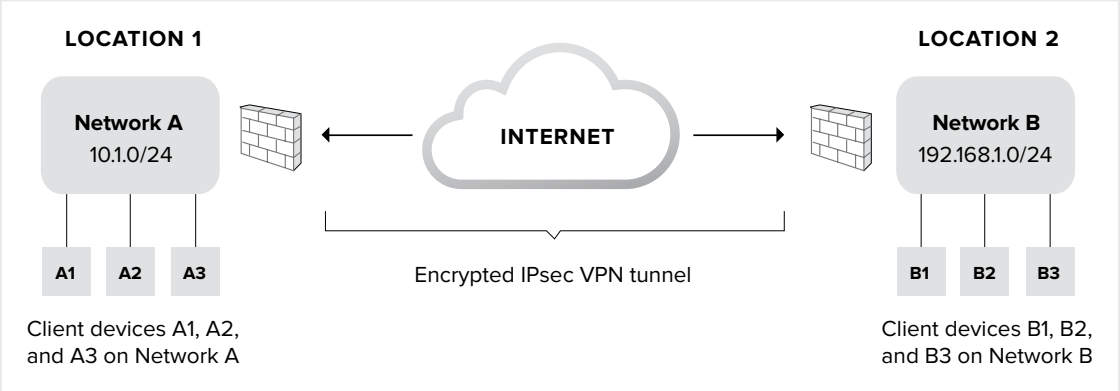
What is VPN?

Virtual Private Networks (VPNs) are used by most organizations seeking to provide teleworkers with pseudo on-site access to core network resources or to connect branch offices to a core network. VPNs are encrypted tunnels that allow for the secure, confidential transfer of data across unsecured, public infrastructure — typically, the Internet.

What is site-to-site VPN?

One of the most common implementations of VPN is site-to-site VPN, where one location hosting network resources is securely connected via VPN to another location (which may also be hosting resources); usually the two locations are part of the same organization.

The diagram below shows a site-to-site VPN:



Site-to-site VPNs are deployed between the security appliances/firewalls at each location. The client devices (such as laptops or workstations) behind these firewalls do not need software installed or local settings configured to enable them to send or receive data with the other sites.

In a **mesh** site-to-site VPN (also known as “spoke-to-spoke”), all of an organization’s individual networks are connected to one another via VPN. In a **hub-and-spoke** topology, all of the satellite branch office networks (“spokes”) tunnel back to a central office (“hub”) over VPN; the spokes do not exchange data directly with one another.

Why is VPN hard?

With traditional architectures, the configuration and management complexity of multi-site VPN can become prohibitive as the number of distributed sites increases. This is because both ends of each VPN tunnel need to be manually created and tuned, often through a complex command line interface. This is a time-consuming and error-prone process: variables such as the IP addresses of both security appliance interfaces, a pre-shared key or certificate, authentication and encryption protocols, a list of exportable subnets, and more need to be manually specified and configured twice for each tunnel. Imagine: if a primary WAN uplink fails over to a 3G/4G link and the external IP address of the VPN changes, all of these settings would need to be re-established for the new address for VPN functionality to resume.

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

Cisco Meraki's Solution

Auto VPN: rapid, painless setup

The Cisco Meraki MX is a cloud-based security appliance with fully integrated networking and security features such as an enterprise-class stateful firewall, deep layer 7 application visibility and control, WAN optimization, CIPA-compliant content filtering, and more. Additionally, all MX models support Auto VPN, the ability to configure site-to-site, Layer 3 IPsec VPN in just two clicks in the Cisco Meraki dashboard — compressing a time-consuming exercise into mere minutes.

To enable Auto VPN, the Cisco Meraki cloud uniquely acts as a broker between MXs in an organization, negotiating VPN routes, authentication and encryption protocols, and key exchange automatically. The process is as follows:

1. **MXs advertise their WAN IP addresses and any active NAT traversal UDP ports to the Cisco Meraki cloud.** Device-to-cloud communication is encrypted twice: once via Meraki-proprietary encryption and again using SSL.

2. **Cisco Meraki's cloud receives MX advertisements and public IP addresses.** The dashboard receives the WAN IPs and NAT traversal information from the MXs, as well as their public IP addresses (which differ from their WAN IPs if the MXs sit behind NAT devices).

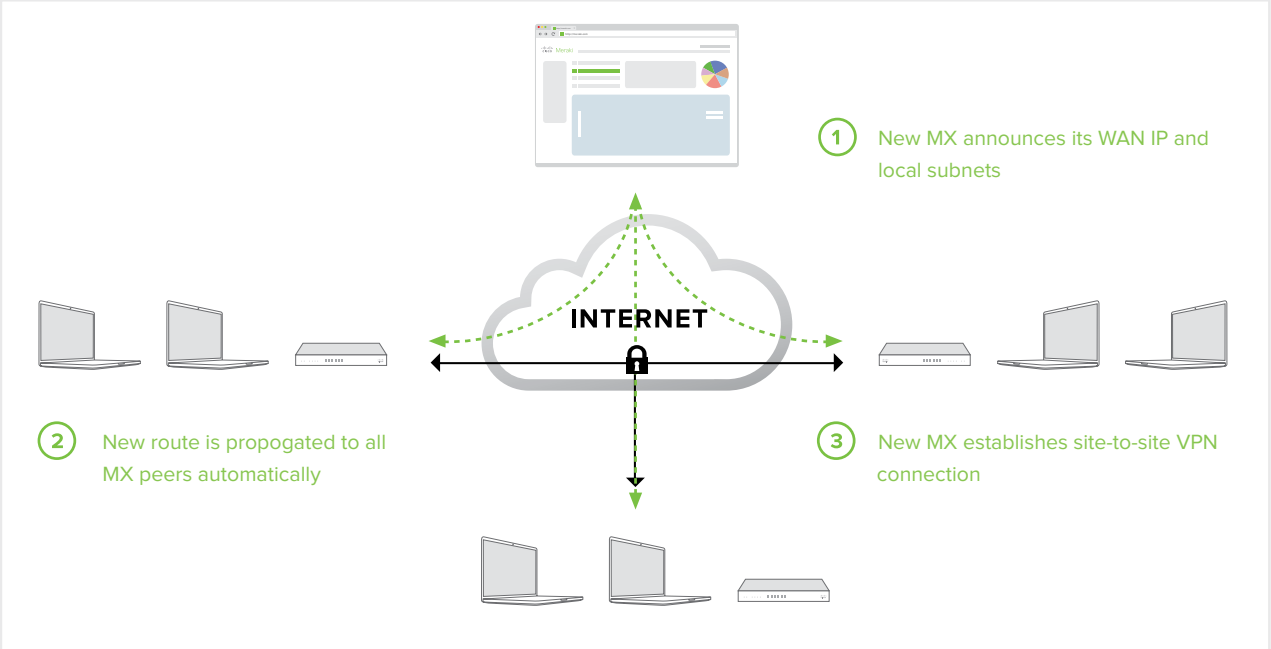
3. **The cloud maintains a dynamic table to track all MXs in an organization.** The WAN IP address, public IP address, NAT traversal port, and local subnets are tracked for every MX in an organization. When a new MX is brought online, it's information is added to this table.

4. **The appropriate IP address is chosen.** For each MX, the cloud decides whether to use its WAN or public IP address to establish a secure VPN tunnel. When possible, an MX's WAN IP address will be used; this can provide shorter VPN paths between peer MXs (e.g. when multiple VPN peers are connected through MPLS to a primary data center, and from there, out to the Internet).

5. **The VPN tunnel is negotiated.** The Cisco Meraki cloud already knows VLAN and subnet information for each MX, and now, the IP addresses to use for tunnel creation. The cloud and MXs establish a 16-character pre-shared key (one key per organization), and a 128-bit AES encrypted IPsec tunnel. Local subnets specified in the dashboard by IT admins are exported across VPN.

6. **VPN routes are pushed from the dashboard to MXs.** Finally, the dashboard will dynamically pushes VPN peer information (e.g., exported subnets, tunnel IP information) to each MX. Every MX stores this information in a separate, static routing table.

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



Cisco Meraki's MXs and cloud negotiate VPN settings via Auto VPN.

That Auto VPN leverages the cloud in this unique, intelligent way means less manual configuration and time spent by IT admins to set up VPN tunnels between sites, and fewer opportunities to introduce human error into the process.

Built-in and configurable redundancy for site-to-site VPN

Losing VPN functionality can prevent workers from checking email, accessing file shares, securely sending data, or using a VoIP phone, among other things — wrenching productivity to a standstill. To protect against this, Auto VPN leverages the cloud to provide built-in redundancy. If, for example, your MX hosts two Internet uplinks and the primary uplink serving VPN traffic fails, the second uplink will assume primary status — and all site-to-site VPN tunnels for that link will be immediately re-negotiated via the cloud. This means that when an active link fails over to a secondary (say, to a 3G/4G uplink, causing the MX's public VPN IP address to change), Auto VPN self-heals. Self-healing works for both the mesh and the hub-and-spoke VPN topologies available with Auto VPN.

Additionally, to protect against the rare failure of an entire security appliance, you can configure one Meraki MX Security Appliance as a primary VPN concentrator and have a secondary, live ("warm") MX ready to take over in the event of a failure with the first.

Configuring a warm spare is straightforward: both MXs are placed inside the perimeter of your network and configured as VPN concentrators. The MXs are each assigned individual IP addresses so that they can communicate with the Meraki cloud, yet they also share a common virtual IP (vIP). This communal, virtual address receives all VPN traffic and by default, the primary concentrator responds to that traffic. If the primary MX fails, however, the warm spare can immediately step in to handle VPN traffic (failure detection and full failover occurs in less than 30 seconds). No manual change of IP address is needed to direct traffic to the warm spare, as it shared a vIP with the primary MX.

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

How to configure Cisco Meraki Auto VPN

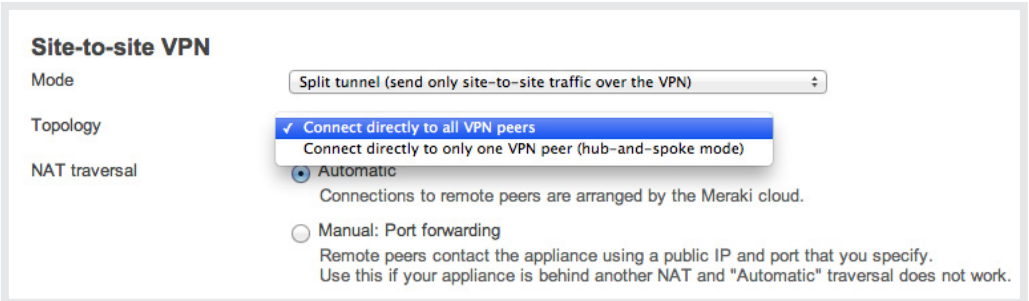
To enable site-to-site VPN between MX Security Appliances, simply login to the Cisco Meraki dashboard and navigate to the Configure > Site-to-Site VPN page.

1. **Enable Auto VPN by selecting whether you'd like a split or full tunnel VPN:**

Split tunnel mode will only send site-to-site traffic over the VPN, leaving other traffic (such as direct Internet requests) to be directed to its final destination without needing to go through the secure VPN tunnel. In other words, email or file server requests between two offices would traverse the split tunnel VPN; a user's request to view a website such as www.nytimes.com would not.

Full tunnel mode directs all traffic through the secure VPN tunnel. So even a user's request to view a web page will be encrypted and sent through VPN to a concentrator first.

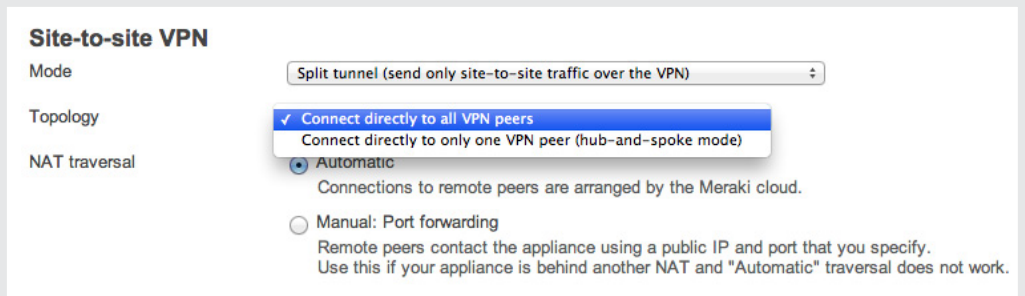
2. **Decide VPN topology—mesh or hub-and-spoke:**



Configuring a mesh VPN.

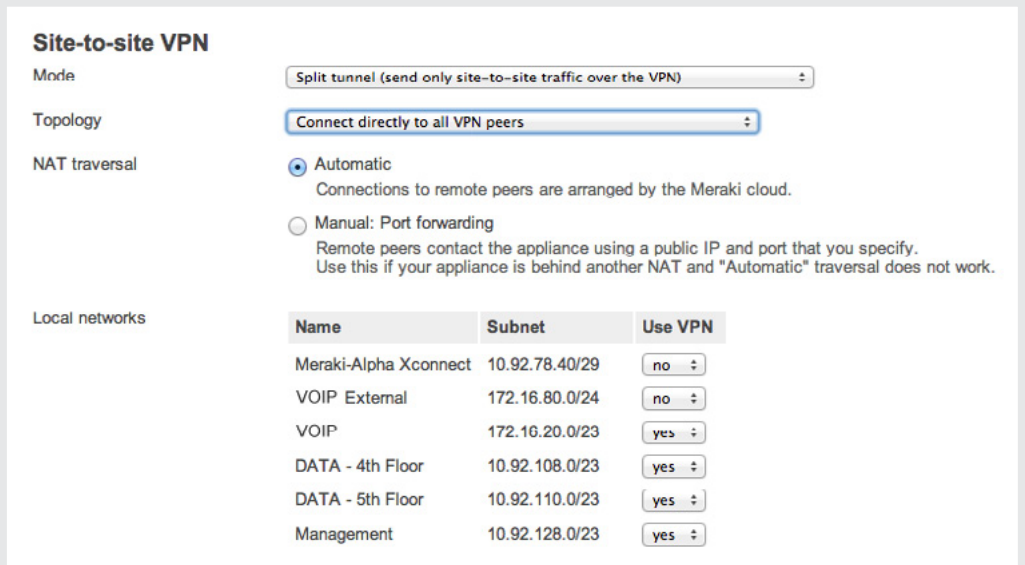
Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com

If configuring a mesh topology, ensure every participating MX has the “Connect directly to all peers” option selected. If configuring a hub-and-spoke topology, ensure that the hub MX is configured to mesh to all peers, while every branch (“spoke”) MX is configured to “Connect directly to only one VPN peer (hub-and-spoke mode)”:



A teleworker site configured in a hub-and-spoke topology, tunneling back to the “Meraki Corp - Appliance” hub MX.

3. Choose which subnets (local networks) to export over VPN:

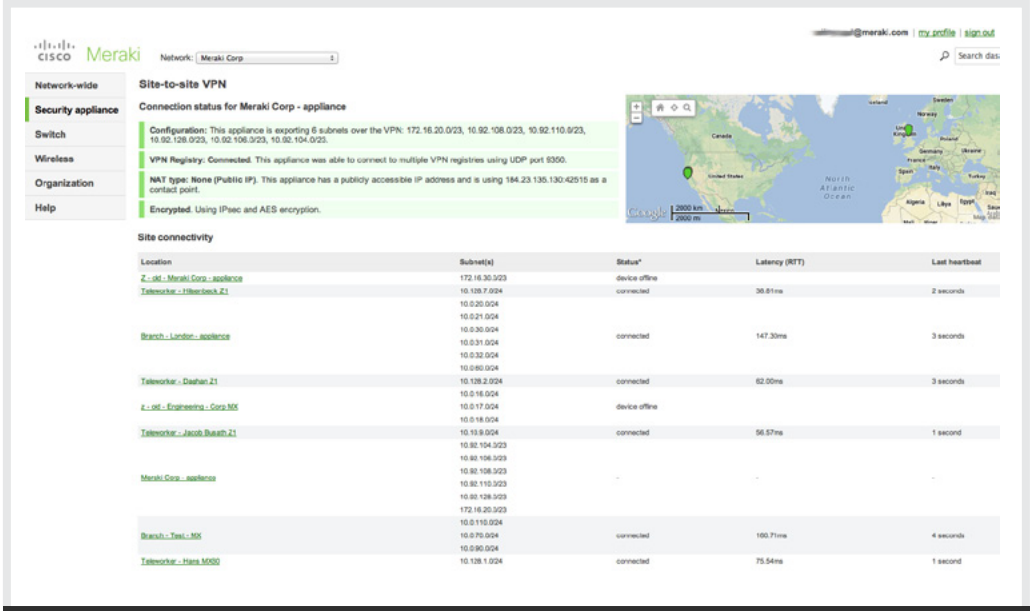


Select “yes” or “no” to export local subnets over the site-to-site VPN.

4. Click “save” in the dashboard

That’s it! You’ve now configured a split or full tunnel VPN in either a mesh or hub-and-spoke topology.

If you want to check the status of all the VPN peer MXs (or Z1 teleworker gateway appliances, which also support Auto VPN) in your network, you can easily do so from the Monitor >> VPN Status page in the Cisco Meraki dashboard. Status of each MX or Z1 is displayed, along with their exported subnets; latency and connectivity for each peer is checked every couple of seconds, providing a near real-time view.



See VPN status in real-time in the Cisco Meraki dashboard.

For more information

In short, the Cisco Meraki MX makes creating and maintaining site-to-site VPN between remote offices a simple, intuitive process. Our unique approach of leveraging the cloud for Auto VPN also provides built-in redundancy, as well as the ability to manage your VPN network from any Internet-accessible location. All MX security appliances come with Auto VPN functionality at no additional cost.

All Cisco Meraki MX models are available for free evaluation (**meraki.cisco.com/eval**), and you can find additional information here:

meraki.cisco.com/library for a VPN redundancy white paper, MX datasheets, and more

meraki.cisco.com/blog for posts on Auto VPN, MX features, and more

Also search for MX Auto VPN videos on youtube.com

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