cisco Meraki

White Paper

Cisco Meraki Auto VPN

JAN 2020

This white paper describes Auto VPN and how to deploy it between Cisco Meraki MX Security & SD-WAN Appliances

Table of Contents

Introduction

Virtual Private Networks (VPN) have been a mainstay in corporations for the past 20 years. They allow companies, government agencies, and departments to securely send communication over an untrusted network. In the last few years, they have become the transport independent overlays of most SD-WAN solutions.

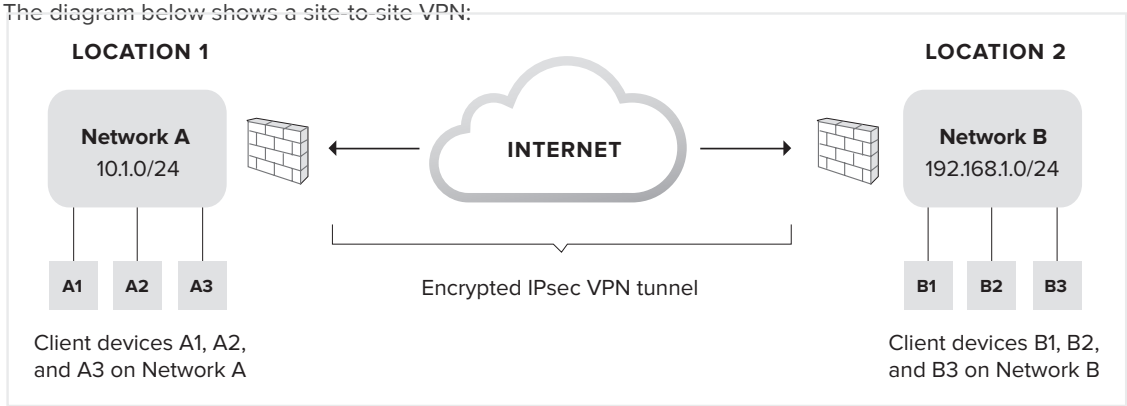
The problem is that the configuration of these technologies and the plethora of phases, modes, and encryption algorithms means that getting and staying secure can be a laborious task. This is where Auto VPN from Cisco Meraki offers a quick and easy way to become, and automatically stay, secure via the cloud.

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

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. This involves variables such as the IP addresses of both security appliance interfaces, a pre-shared keys or digital certificates, authentication mechanisms and encryption protocols, a list of exportable subnets, and more need to be manually specified and configured twice for each tunnel. In order to address the

potential issues that can be introduced in such configuration, Cisco has introduced a number of technologies over the years, Cisco Meraki’s cloud based management allows us to address this problem in an innovative way.

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

Cisco Meraki Auto VPN

Auto VPN: Rapid, painless setup

The Cisco Meraki MX is a cloud-based security & SD-WAN appliance with fully integrated networking and security features such as an enterprise-class stateful firewall, deep layer 7 application visibility and control, dynamic VPN path selection, WAN load balancing, automatic VPN and WAN failover, next generation intrusion prevention, and more. Additionally, all MX models support Auto VPN, the ability to configure site-to-site, Layer 3 VPN in just a few clicks in the Cisco Meraki dashboard — compressing a time-consuming exercise into seconds.
In order to achieve this Auto VPN builds upon the inherent trust that the dashboard creates when all Meraki device first come online. Whilst the full process is outside the scope of this document, the Meraki dashboard and the Meraki devices connecting to it are mutually authenticated with one another.

At a high level though, this is achieved by the Meraki devices utilising TLS (the technology used to create secure web applications) to ensure the authenticity of dashboard infrastructure. Then each Meraki device uses secure information that is unique to each Meraki device in order to authenticate itself to the dashboard. Thus creating a trust relationship between the dashboard and the Meraki device in what was previously a zero-trust system.

Auto VPN builds upon this trust relationship with the Meraki cloud acting as a broker between MXs in an organization, negotiating VPN routes, authentication mechanisms and encryption protocols, and key material automatically and securely. 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 TLS.

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.

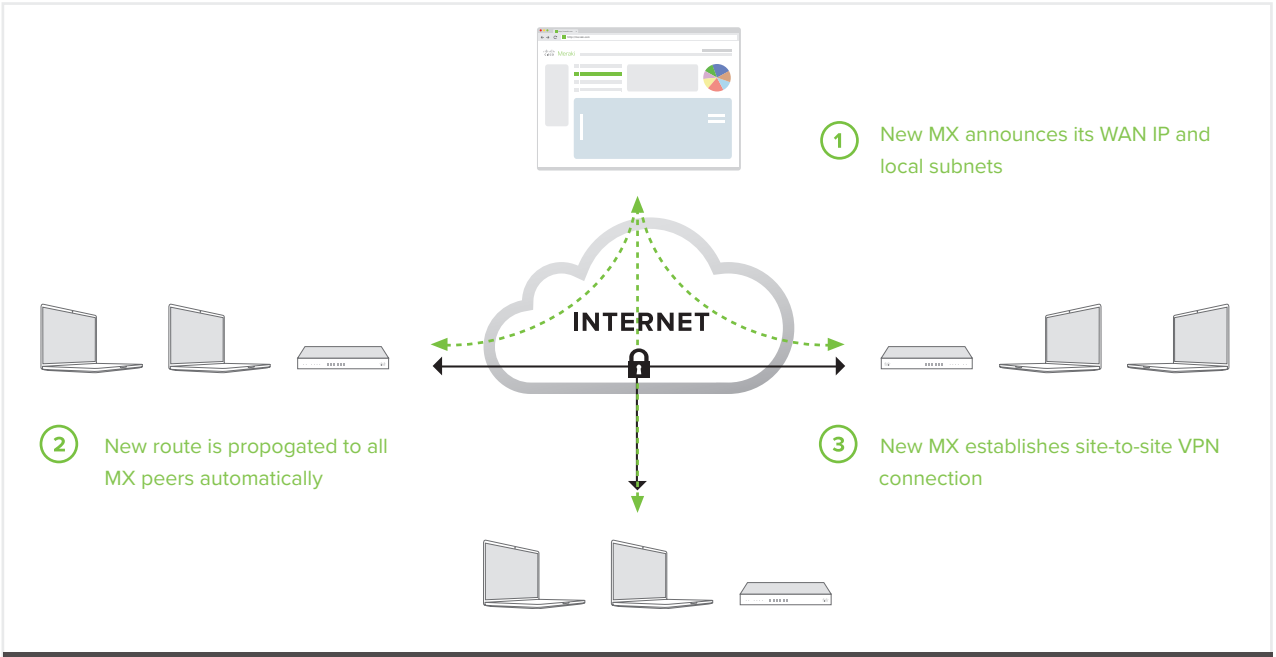
4. **The appropriate IP address is chosen.** For each MX, the cloud decides whether to use its interface (potentially private) or public IP address to establish a secure VPN tunnel. When possible, an MX's WAN IP address will be used; this can provide shorter VPN paths between peer MXs (e.g. when multiple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

5. **The VPN tunnel is established.** The Cisco Meraki cloud already knows VLAN and subnet information for each MX, and now, the IP addresses to use for tunnel creation. The dashboard and MXs establish two 16-character pre-shared keys (one per direction) and create a 128-bit AES-CBC tunnel. Meraki Auto VPN leverages elements of modern IPSec (IKEv2, Diffe-Hellman and SHA256) to ensure tunnel confidentiality and integrity. Local subnets specified in the dashboard by admins are exported across the VPN.

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

6. **VPN routes are propagated across the Auto VPN domain to all member MXs.** Finally, the dashboard will either dynamically push VPN peer information (e.g. exported subnets, tunnel

   IP information) to each MX. Every MX stores this information in a separate, static routing table. Or if BGP is configured in the organization then iBGP is used between all configured Auto VPN hubs in a full mesh and between all spoke and their configured hubs to ensure full IP route propagation.



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. This means that when an active link fails over to a secondary (say, to a 4G/LTE 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.

In SD-WAN deployments all of the available VPN paths, referred to as transport independant overlays, can be dynamically selected to route the traffic flows. This can be done either on a policy basis, a performance basis or in a load balanced manner.

At critical hub locations to protect against the rare failure of an entire MX appliance, you can configure one Meraki MX Security & SD-WAN 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.

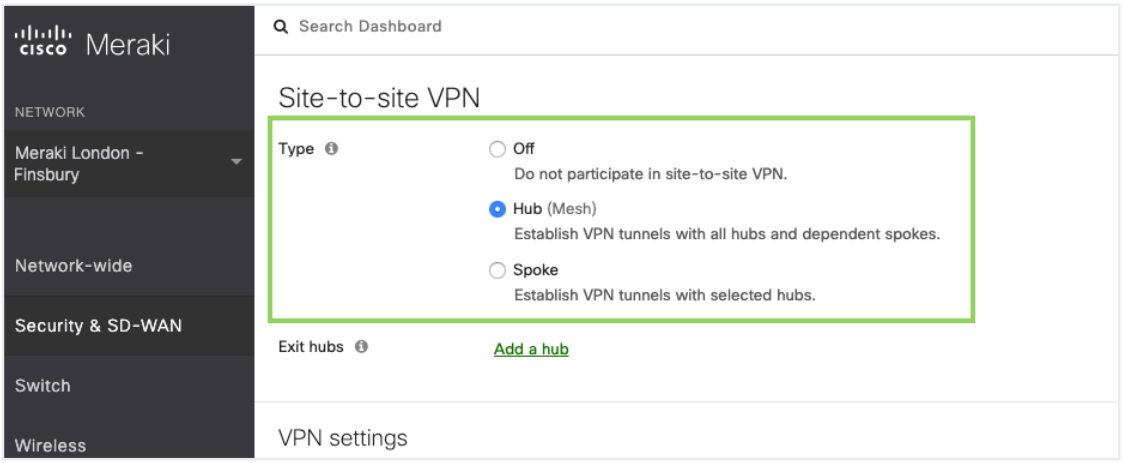
Configuring a warm spare is straightforward: both MXs are placed inside the perimeter of your network and configured as VPN concentrators. The MXs are each assigned an individual IP address so that they can communicate with the Meraki cloud, yet they also share a common virtual IP (vIP). This communal, virtual address receives all VPN traffic and by default, the primary concentrator responds to that traffic. If the primary MX fails, 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.

How to configure Cisco Meraki Auto VPN

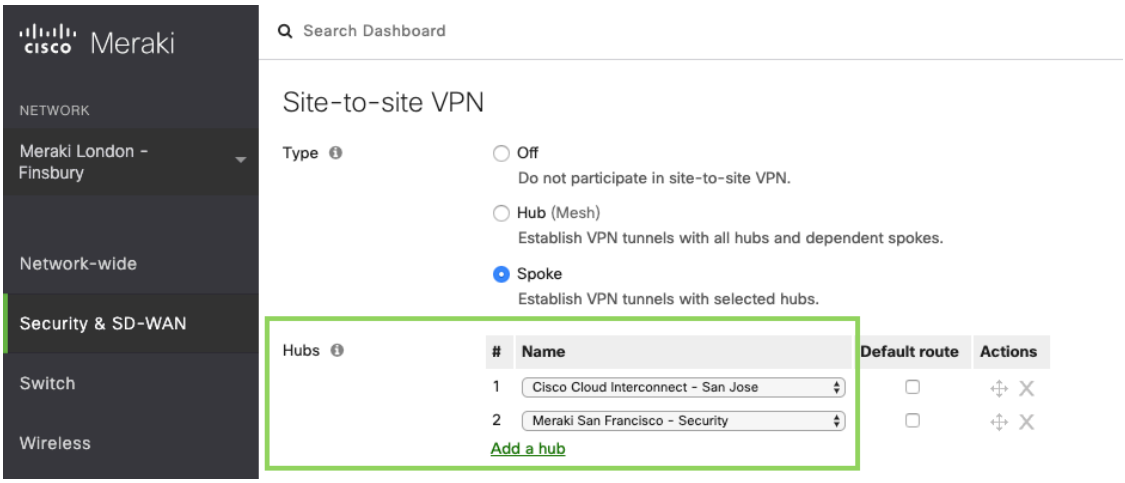
To enable site-to-site VPN between MX Security Appliances, simply login to the Cisco Meraki dashboard and navigate to the Configure > Site-to-Site VPN page.

1. Enable Auto VPN type based on desired topology

If an MX is configured as a 'Hub' it will build a full mesh of VPN tunnels to all other hub MXs in the Auto VPN domain and point-to-point tunnels to all spoke MXs that have this MX configured as a hub. If all MXs in the Auto VPN domain are configured as 'Hub' then the Auto VPN has a full mesh topology.



If an MX is configured as a 'Spoke' it will only build tunnels to other MXs that are configured as its 'Hubs'. If the majority of MXs in the Auto VPN domain are configured as 'Spoke' with a few key locations (such as data centers or headquarters) configured as 'Hubs' then the Auto VPN has a hub-and-spoke topology.

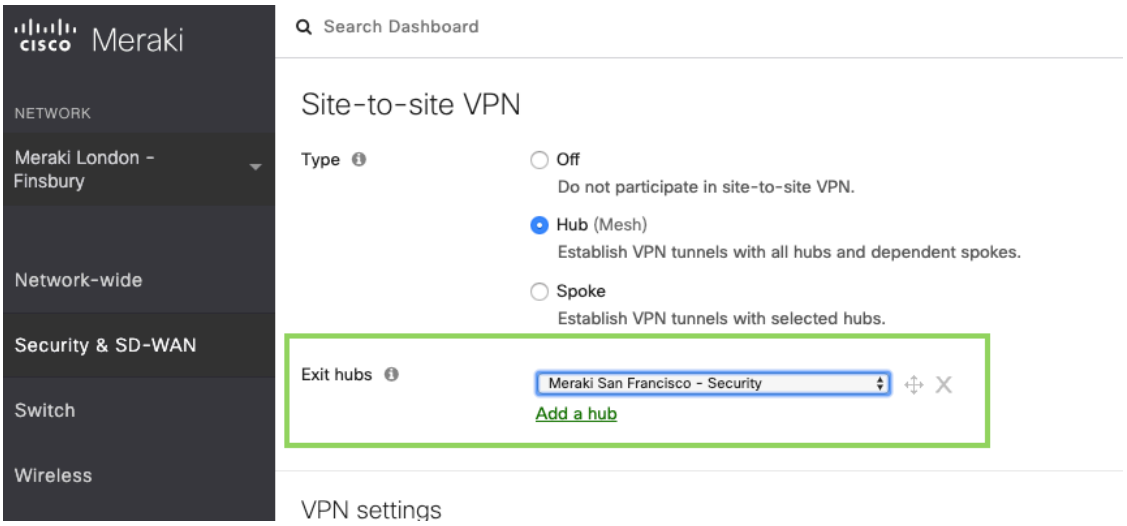


Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com

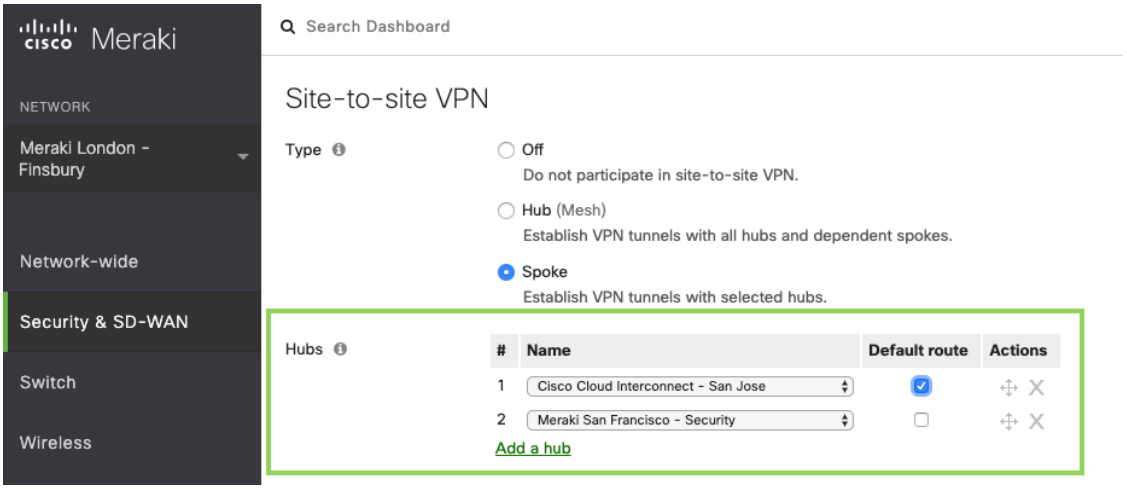
2. Full Tunnel or Split Tunnel

By default all MXs in the Auto VPN domain will only send traffic to an Auto VPN peer for a subnet contained within the Auto VPN domain, this is often referred to as 'split-tunnelling'. If an organization wants to route all traffic traffic not contained within the Auto VPN domain through a specific hub site, this is referred to as 'full-tunnelling'. Note that full-tunnelling only affects client data and all Meraki management traffic will egress directly via the primary WAN.

To configure full-tunnelling in a full mesh topology simply define an 'Exit hub' from the MXs in the Auto VPN domain as follows:



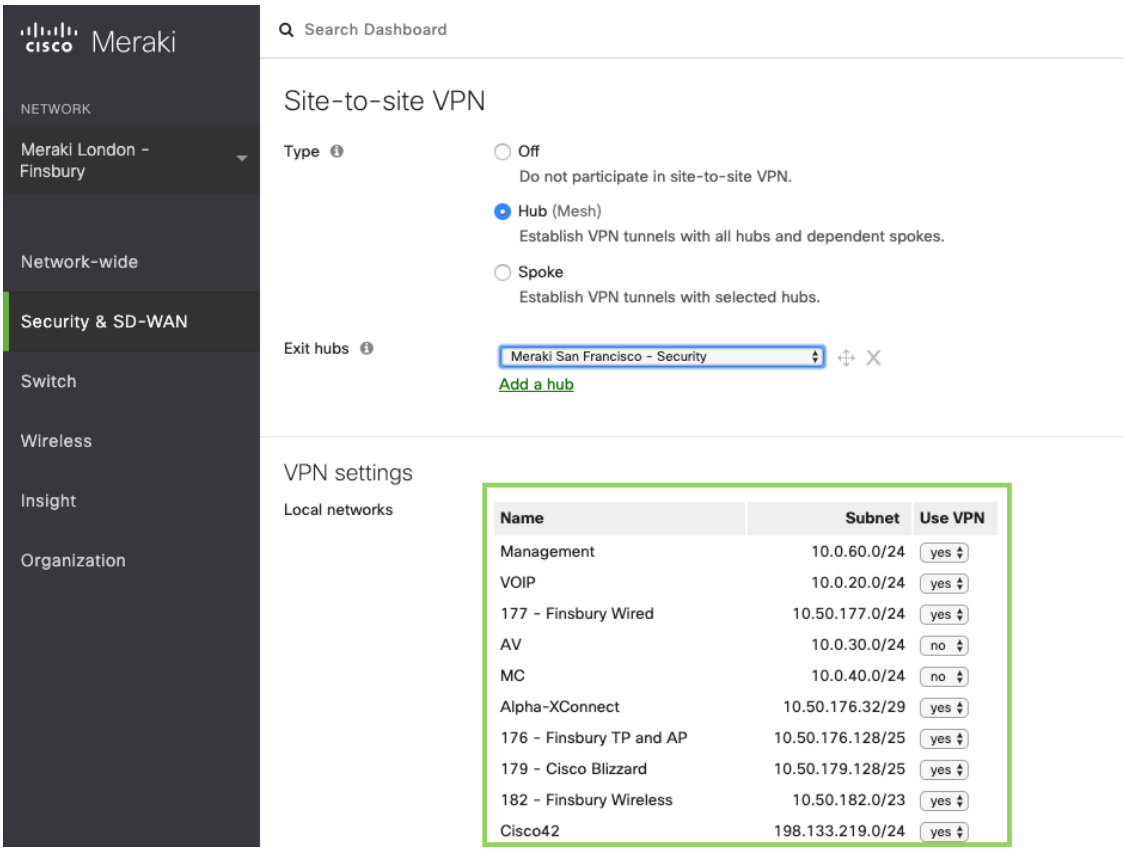
To configure full-tunnelling in a hub-and-spoke topology, simply associate a 'Default route' with one or more hub MXs:



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

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

Next we need to select which locally defined or available subnets should be exported to the Auto VPN domain. To do this we simply select ‘yes’ or ‘no’ to include or omit the subnet from the Auto VPN domain.



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 Z teleworker gateway appliances, which also support Auto VPN) in your network, you can easily do so from the VPN Status page in the Cisco Meraki dashboard (Security & SD-WAN > Monitor > VPN Status). The status of each MX or Z device is displayed, along with their exported subnets; live latency, connectivity and routing decisions that are being made over the Auto VPN domain are reported here.

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, whilst providing a platform to enable SD-WAN. All MX security appliances come with Auto VPN and SD-WAN functionality at no additional cost.

MORE RESOURCES

The following references can be reviewed for further detailed information:

Cisco Meraki Auto VPN Configuration Video
https://www.youtube.com/watch?v=xgsPFuye-Ec

Cisco Meraki Auto VPN Blog
https://meraki.cisco.com/blog/2018/06/all-about-autovpn

Cisco Meraki Auto VPN General Best Practices
https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Best_Practice_Design_-_MX_Security_and_SD-WAN/Meraki_Auto_VPN_General_Best_Practices

Cisco Meraki Auto VPN Hub Deployment Recommendations
https://documentation.meraki.com/Architectures_and_Best_Practices/Auto_VPN_Hub_Deployment_Recommendations

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

VPN Redundancy white paper, MX datasheets, and more
https://meraki.cisco.com/library

Detailed configuration, troubleshooting, best practice guides
https://documentation.meraki.com

Latest posts on Auto VPN, MX features, and more
https://meraki.cisco.com/blog

Search for MX Auto VPN videos
https://youtube.com

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