Meraki SD-Wan Configuration

Meraki devices have become quite prevalent in customer networks. Proper configuration is essential to obtain reliable voice / video communications and maintain high quality.

Global Configuration Requirements

Regardless of what type of configuration options you implement, you must configure all Meraki devices to perform two functions:

1. Apply traffic shaping prioritization rules to ensure that voice and video have priority over other traffic and that data is only transmitted to the carrier at the allowed rate (exceeding the allowable data rate results in very poor quality).

2. Apply layer-3 firewall rules to ensure that RingCentral traffic is allowed to ingress and egress.

Manual entry of the myriad required rules is a very tedious and error-prone task; therefore, RingCentral has developed a Meraki API client program to perform this task. It may be downloaded from the RingCentral Custom Engineering website (https://www.celab.ringcentral.com).

Please note that you must **manually** set the speed on the two ISP link interfaces.

Please also note that ***load-balancing of RingCentral traffic over multiple links is not allowed*** and will create **major** quality issues if attempted! Triple-check to ensure that load-balancing is completely disabled.

Topology

Meraki routers are typically configured to access RingCentral services in one of the following manners:

1. **Standalone/LocalEgress** – All RingCentral traffic to/from the branch site goes directly out to the Internet over one of two ISP links. If the primary ISP link fails, the secondary ISP link takes over. This is a simple fail-over configuration and will not be discussed any further in this document.

   Note that the global configuration requirements described in the section above are still required to provide firewall access and quality of service.

   a. Pros:
      i. Simple and quick setup
      ii. Uncomplicated
   b. Cons:
      i. Failover from primary to secondary ISP link results in lost SIP registration. Endpoints must timeout to reregister with RingCentral based upon their new SNAT addresses. This configuration does not take advantage of any enhanced

SD-WAN features.

2. **SD-Wan** – Branch sites are set up as spokes feeding to one or more hub sites using SD-Wan AutoVPN tunnels. RingCentral traffic is sent over the SD-Wan AutoVPN tunnels to the hub sites where the traffic is sent to RingCentral after undergoing SNAT.

   Hub sites may be set up in standard ***Routed mode*** or in ***One-armed VPN Concentrator*** mode as described in the Meraki documentation. ***One-armed VPN Concentrator*** mode offers significant advantages as discussed later in this document.

   Every branch site maintains at least two SD-Wan AutoVPN tunnels to each hub site over which RingCentral traffic is delivered to the hub site. Failure of the branch site's primary ISP link will transparently shift the RingCentral traffic to the alternate tunnel across the secondary ISP link.

   Individual branch sites may be configured to use different hub sites as their primary hub, thus allowing geographic clustering and traffic optimization, for instance units in the East of the US would prefer an Eastern hub and units in the West of the US would prefer a Western hub. If the branch site's primary hub site fails and there are alternate hub sites defined, traffic will shift to an alternate hub site, otherwise traffic will shift to local egress. Note that a fail-over to a different hub site will result in a change of SNAT source address, thus dropping current calls and requiring endpoint re-registration.

   a. Pros:
      i. Simple and relatively quick to set up
      ii. Protects against single branch site ISP link failure
      iii. Failover from primary to secondary ISP link at the branch site will not result in lost SIP registration. There will only be a brief period of silence in current phone calls as traffic transitions to the tunnel on the alternate link.
      iv. BGP peering with RingCentral over direct connections is possible (optional)

   b. Cons:
      i. Requires a hub site with very reliable ISP service
      ii. Hub sites will require significantly more ISP bandwidth

SD-Wan Configuration Logical Network Diagrams

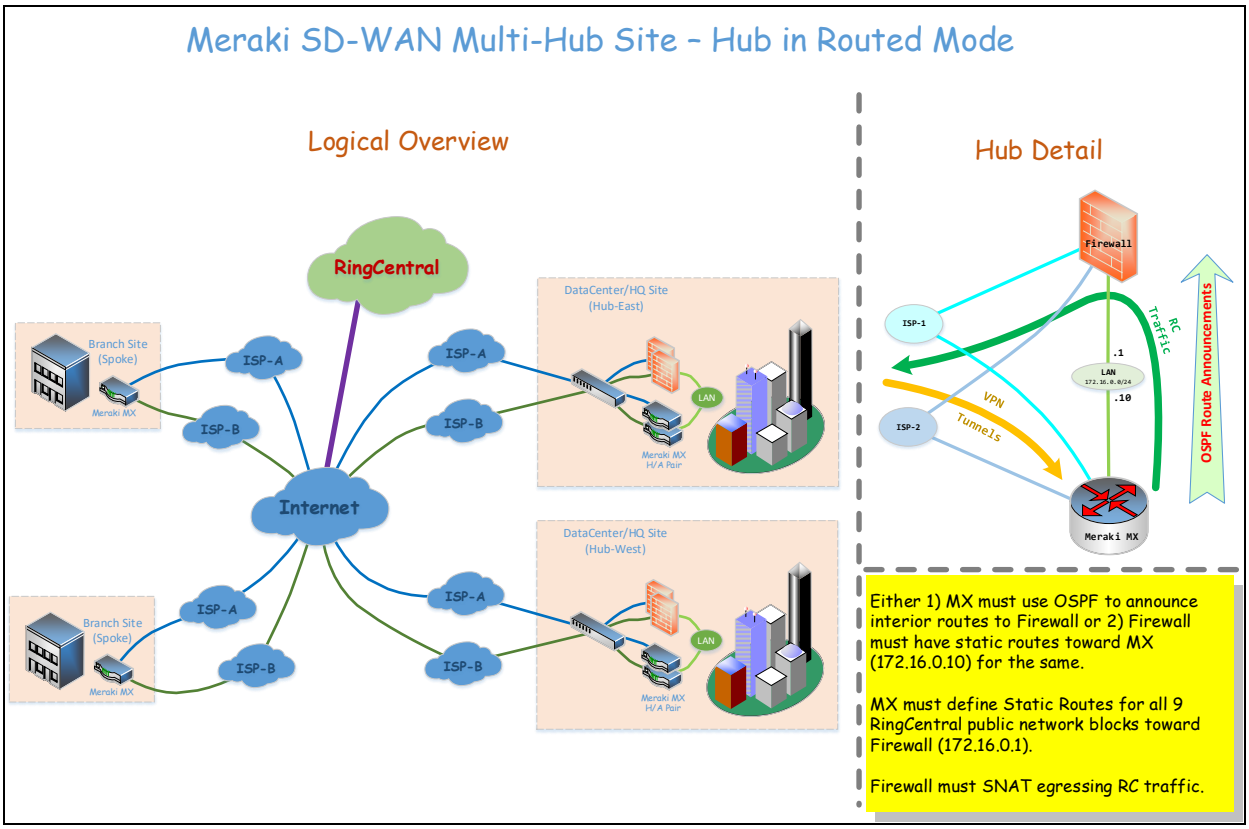
The following discussions and diagrams assume that you implement two 'hub' sites for your SD-WAN mesh. If you do not need redundancy, you may elect to use a single 'hub' site or, due to traffic engineering requirements, you may need more than two.

There are two ways in which the SD-Wan capabilities of the Meraki MX platform may be deployed in a 'hub' site, ***Routed mode*** and ***One-armed VPN Concentrator mode***.

Routed mode is somewhat limited and can only be used for RingCentral traffic transport over Internet (OTT). There are limitations in the current Meraki software that make this solution undesirable as routes to the 9 RingCentral public address blocks cannot be added/withdrawn atomically.

One-armed VPN Concentrator mode is much more flexible as the firewall device can use iBGP to communicate routing information to/from the Meraki devices. This may be used for RingCentral traffic transport over Internet (OTT) or transport over dedicated layer2/3 connections.

Routed Mode



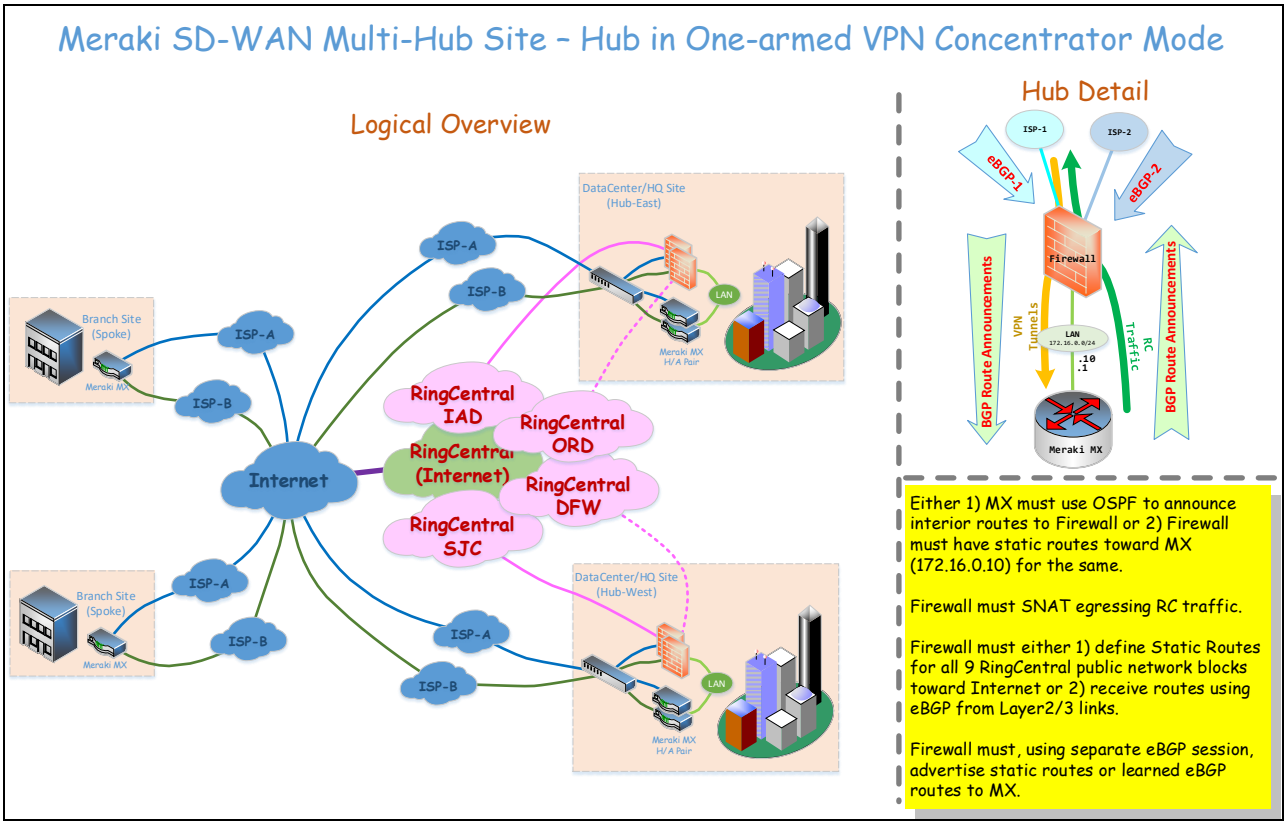
In this mode, the ISP links are directly attached to the WAN1 and WAN2 interfaces of the Meraki(s) and carry the SD-Wan AutoVPN tunnel traffic. RingCentral traffic will be directed through the LAN interface. The LAN interface is connected to a firewall device which provides SNAT services to/from the Internet for the RingCentral traffic. There is no way to use the directly connected WAN links on the Meraki to pass RingCentral traffic; the traffic MUST pass through the LAN interface to the firewall device.

The firewall device must have routing information to allow routing of return traffic to the Meraki appliance. You may utilize either static routes or implement an OSPF link so that the Meraki can advertise interior routes to the firewall. (Note that OSPF on the Meraki is one-way – announce-only.)

The hub site Meraki devices must have floating static routes for the 9 RingCentral public network blocks defined pointing to the firewall device.

Problem: Current Meraki software does not allow the aggregate group of 9 routes to be treated atomically; the closest we can come is to have the critical 199.255.120.0/22 route float based upon ping testing to 199.255.120.129 and the other 8 routes testing based upon the gateway address. This issue can be resolved by using the much more capable ***one-armed VPN Concentrator mode*** and allowing the firewall device to control routing information via iBGP.

One-armed VPN Concentrator Mode



In this mode, the Meraki has only one active port, WAN1, which is connected to and assigned an address as part of the LAN. The LAN is connected to a firewall device which manages the ISP links. The firewall device must provide SNAT services for the RingCentral traffic and 1:1 DNAT/SNAT services for AutoVPN tunnel origination/termination. An iBGP session is established between the Meraki appliance and the firewall device.

As in ***Routed mode***, the firewall device must have routing information to allow routing of return traffic to the Meraki appliance. The iBGP session should be used to advertise the interior routes to the firewall.

Customers can implement direct connections to RingCentral datacenters using one or more layer2/3 links terminating on their firewall. RingCentral will establish eBGP Peering relationship with you and advertise all the RingCentral public network space. It may be advertised in multiple subnets to perform traffic engineering/optimization.

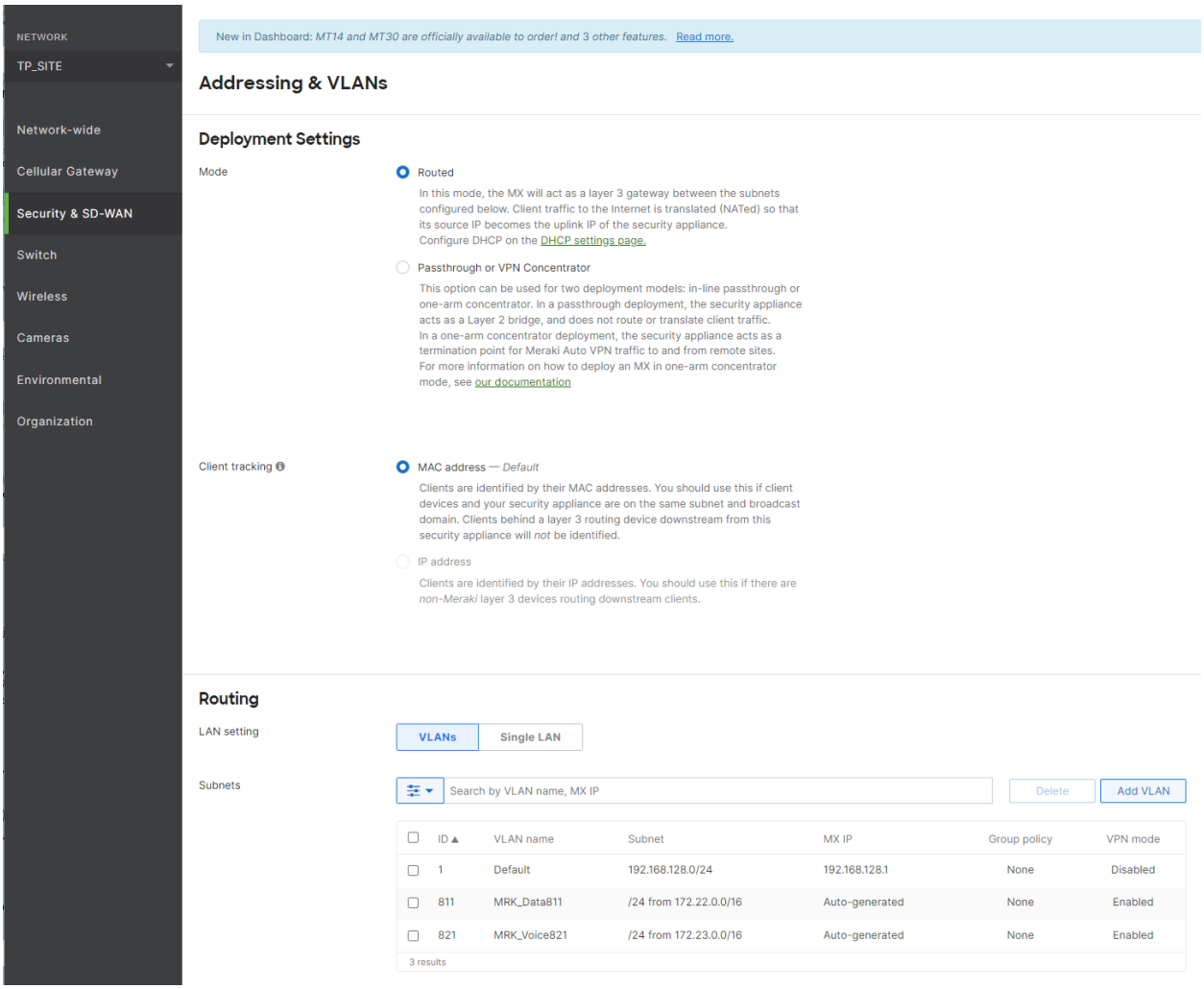
Alternately, you may use the Internet to deliver traffic to RingCentral by defining 9 floating static routes (ping test point for all is 199.255.120.129) and redistributing them via iBGP. These routes will be automatically added and withdrawn as the ping test site controls route status.

Implementation Specifics

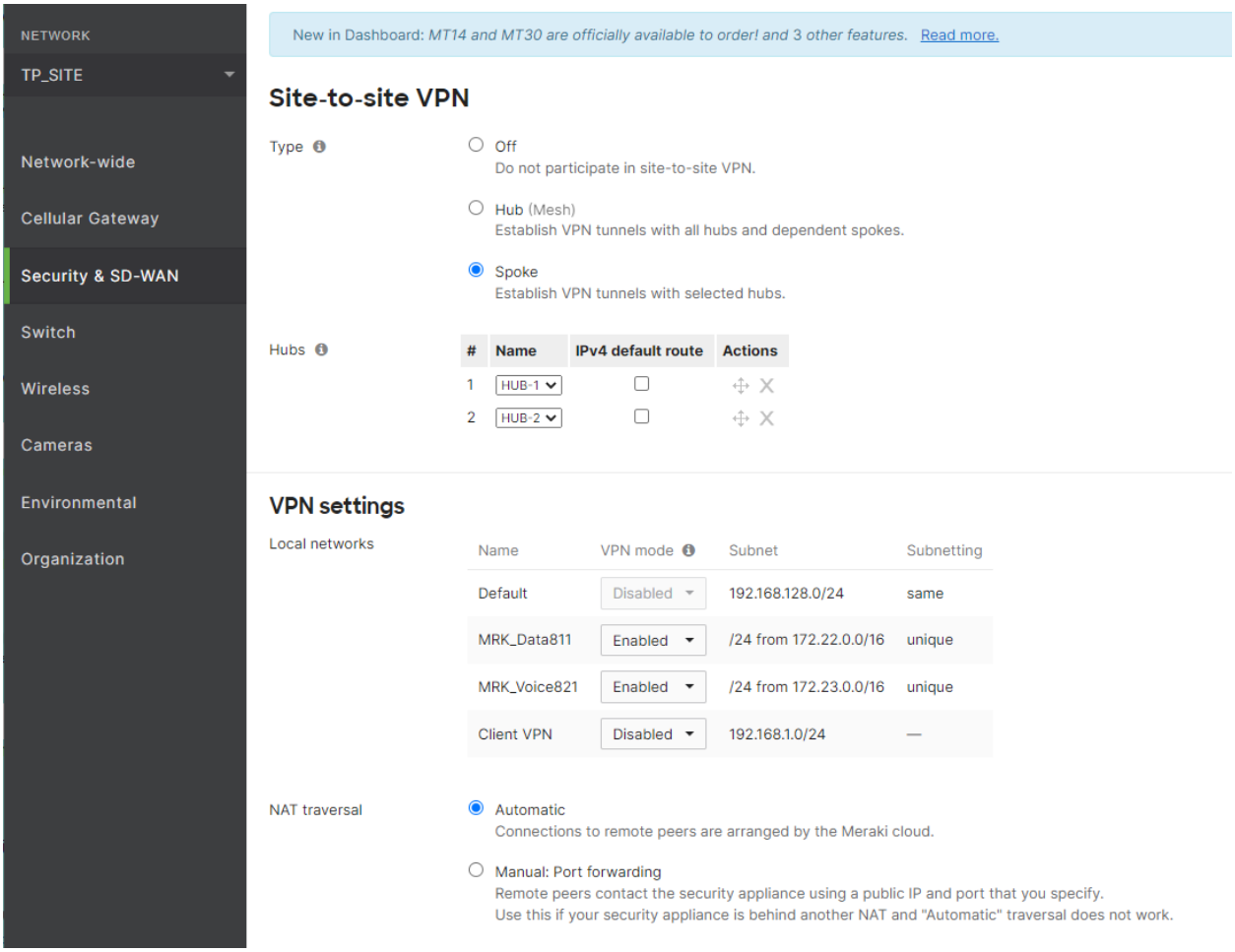
It is strongly suggested that you utilize templates to deploy your branch (spoke) sites. One or more templates should be established that treat a specific hub site as the primary hub. This provides an easy mechanism for assigning new appliances to a specific geographical primary hub site, for instance Eastern US and Western US. The only difference in the templates would be the order in which the VPN hubs are assigned.

Branch Sites (Templates)

This template (TP-Site) is set up in ***Routed mode*** with two automatically addressed Vlans, both of which are set to participate in the AutoVPN.



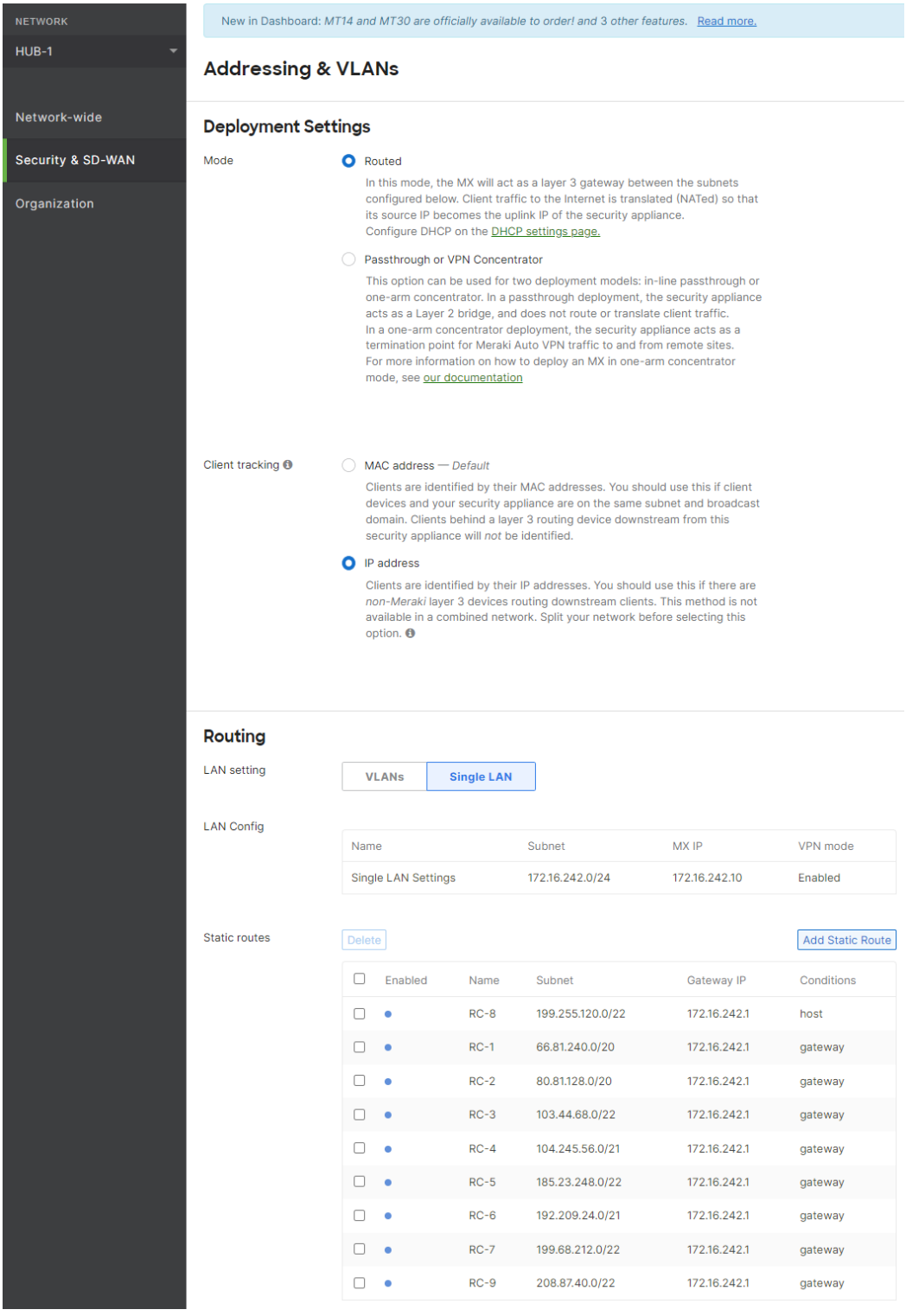
The template shown above and below will place sites bound to it in Spoke mode and link the created sites to HUB-1 as a primary hub site and HUB-2 as a secondary/failover hub site. You must enable VPN mode for the site subnets so that the Meraki system will include them in the AutoVPN Mesh.



Hub Sites (Routed Mode)

Hub sites created in ***Routed mode*** have their two WAN interfaces connected to the two different ISP Vendors and their LAN interface connected to a firewall / router. RingCentral traffic from branch sites is delivered to the preferred hub site using the AutoVPN tunnels. Static routes are present on the hub Meraki pointing to the LAN based firewall / router. The firewall / router then applies SNAT to the egressing traffic and sends it out to the Internet.

This hub site mechanism is less then desirable due to the Meraki's inability to treat the static routes in an atomic manner. It cannot add and withdraw all nine of them as a single entity. We test ping an address of 199.255.120.129 to verify connectivity, but only one of the routes, the 199.255.120.0/22 route, can be set to test using this address. The best we can do for the others is to test the gateway address. Please see the discussion of the ***One-armed VPN Concentrator mode*** for the preferred alternative.


NETWORK
HUB-1
Network-wide
Security & SD-WAN
Organization
New in Dashboard: MT14 and MT30 are officially available to order! and 3 other features. Read more.
Addressing & VLANs
Deployment Settings
Mode
Routed
In this mode, the MX will act as a layer 3 gateway between the subnets configured below. Client traffic to the Internet is translated (NATed) so that its source IP becomes the uplink IP of the security appliance.
Configure DHCP on the DHCP settings page.
Passthrough or VPN Concentrator
This option can be used for two deployment models: in-line passthrough or one-arm concentrator. In a passthrough deployment, the security appliance acts as a Layer 2 bridge, and does not route or translate client traffic.
In a one-arm concentrator deployment, the security appliance acts as a termination point for Meraki Auto VPN traffic to and from remote sites.
For more information on how to deploy an MX in one-arm concentrator mode, see our documentation
Client tracking
MAC address — Default
Clients are identified by their MAC addresses. You should use this if client devices and your security appliance are on the same subnet and broadcast domain. Clients behind a layer 3 routing device downstream from this security appliance will not be identified.
IP address
Clients are identified by their IP addresses. You should use this if there are non-Meraki layer 3 devices routing downstream clients. This method is not available in a combined network. Split your network before selecting this option.
Routing
LAN setting
VLANs
Single LAN
LAN Config
Name
Subnet
MX IP
VPN mode
Single LAN Settings
172.16.242.0/24
172.16.242.10
Enabled
Static routes
Delete
Add Static Route
Enabled
Name
Subnet
Gateway IP
Conditions
RC-8 199.255.120.0/22 172.16.242.1 host
RC-1 66.81.240.0/20 172.16.242.1 gateway
RC-2 80.81.128.0/20 172.16.242.1 gateway
RC-3 103.44.68.0/22 172.16.242.1 gateway
RC-4 104.245.56.0/21 172.16.242.1 gateway
RC-5 185.23.248.0/22 172.16.242.1 gateway
RC-6 192.209.24.0/21 172.16.242.1 gateway
RC-7 199.68.212.0/22 172.16.242.1 gateway
RC-9 208.87.40.0/22 172.16.242.1 gateway

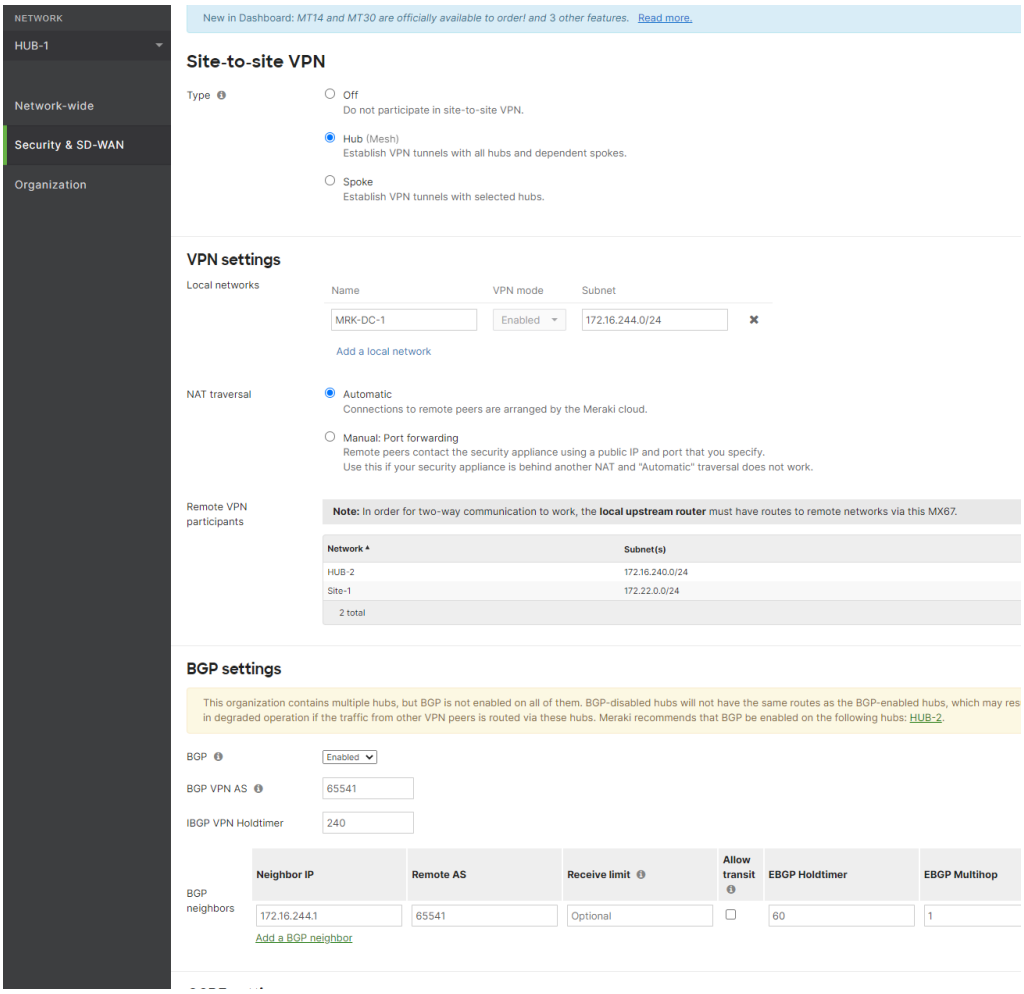
Hub Sites (One-armed VPN Concentrator Mode)

Hub sites created in ***One-armed VPN Concentrator mode*** use a single interface (WAN1) to connect with a firewall / router. This interface is responsible for both delivery of the AutoVPN tunnel traffic to the Meraki as well as delivery of the branch site RingCentral traffic to the firewall / router.

An iBGP peering relationship is established between the Meraki hub device and the firewall / router. This iBGP session is used to do the following:

1. Provide firewall / router with all branch site routes so that return traffic can make it back to the source.
2. Provide Meraki hub device with exterior routing information so that all traffic to those exterior sites will flow through this hub site and out to the Internet. This information is obtained in two different ways:
    a. If the firewall / router is sending the RingCentral traffic out over the Internet, you set up static routes for the RingCentral public address blocks gatewayed through the firewall / router. These static routes should be configured as floating static routes with an administrative distance of 240. There should be a health check pinging 199.255.120.129 that will automatically withdraw all the RingCentral routes upon failure; thus, forcing the traffic to egress locally rather then through the hub site.
    b. If the firewall / router is terminating one or more Layer2/3 links to RingCentral, then you set up eBGP peering relationships between RingCentral and the firewall / router with each of them. The routes learned from these peers will be passed on to the Meraki devices. If you want to fail over to the Internet at the hub site rather than fail back to local egress, then do #2a in addition to these eBGP sessions.

This hub site mechanism is the most flexible and is preferred over ***Routed mode***.


NETWORK
HUB-1
Network-wide
Security & SD-WAN
Organization
New in Dashboard: MT14 and MT30 are officially available to order! and 3 other features. Read more.
Site-to-site VPN
Type
Off
Do not participate in site-to-site VPN.
Hub (Mesh)
Establish VPN tunnels with all hubs and dependent spokes.
Spoke
Establish VPN tunnels with selected hubs.
VPN settings
Local networks
Name
VPN mode
Subnet
MRK-DC-1
Enabled
172.16.244.0/24
Add a local network
NAT traversal
Automatic
Connections to remote peers are arranged by the Meraki cloud.
Manual: Port forwarding
Remote peers contact the security appliance using a public IP and port that you specify.
Use this if your security appliance is behind another NAT and "Automatic" traversal does not work.
Remote VPN participants
Note: In order for two-way communication to work, the local upstream router must have routes to remote networks via this MX67.
Network
Subnet(s)
HUB-2
172.16.240.0/24
Site-1
172.22.0.0/24
2 total
BGP settings
This organization contains multiple hubs, but BGP is not enabled on all of them. BGP-disabled hubs will not have the same routes as the BGP-enabled hubs, which may res
in degraded operation if the traffic from other VPN peers is routed via these hubs. Meraki recommends that BGP be enabled on the following hubs: HUB-2.
BGP
Enabled
BGP VPN AS
65541
IBGP VPN Holdtimer
240
BGP neighbors
Neighbor IP
Remote AS
Receive limit
Allow transit
EBGP Holdtimer
EBGP Multihop
172.16.244.1
65541
Optional
60
1
Add a BGP neighbor