MIST TELEWORKER GUIDE

Experience the corporate network @ home

DOCUMENT OWNERS:

Robert Young – ryoung@juniper.net

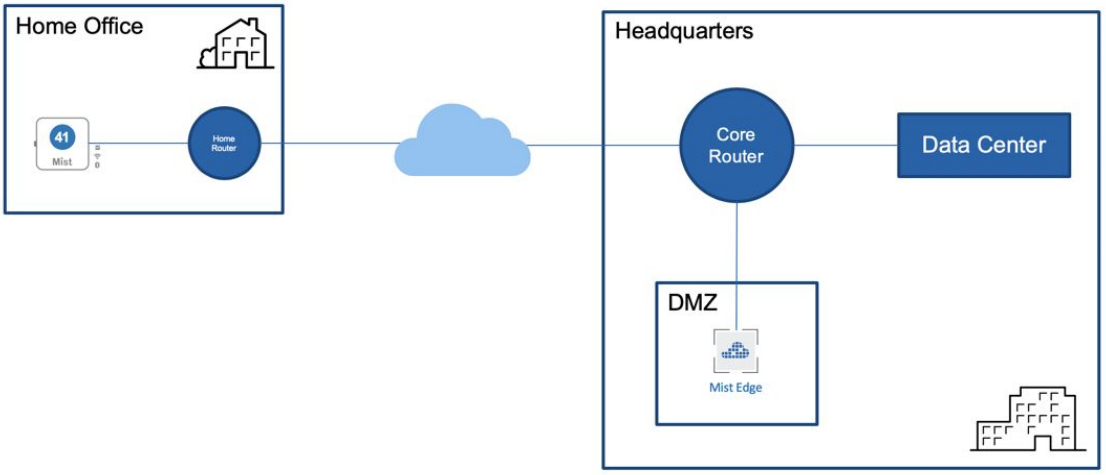
Slava Dementyev – vdementyev@juniper.net

Jan Van de Laer – djanvan@juniper.net

Table of Contents

Solution Overview

Mist Teleworker solution leverages Mist Edge for extending a corporate network to remote office workers using an IPSEC secured L2TPv3 tunnel from a remote Mist AP. In addition, MistEdge provides an additional RadSec service to securely proxy authentication requests from remote APs to provide the same user experience as inside the office.



WIth Mist Teleworker solution customers can extend their corporate WLAN to employee homes whenever they need to work remotely, providing the same level of security and access to corporate resources, while extending visibility into user network experience and streamlining IT operations even when employees are not in the office.

What are the benefits of the Mist Teleworker solution with Mist Edge compared to all the other alternatives?

Agility:

- Zero Touch Provisioning - no AP pre-staging required, support for flexible all home coverage with secure Mesh
- Exceptional support with minimal support - leverage Mist SLEs and Marvis Actions

Security:

- Traffic Isolation - same level of traffic control as in the office.
- Automated Security - machine-driven site deployment, no IPSec credential exposure.
- Endpoint Protection - easily secure wireless and wired endpoints via POE-out

Flexibility:

- Full re-usability of hardware
- Support for flexible all-home coverage with secure Mesh capabilities
- Allow employees to self-manage their home SSID

The components of the Teleworker solution include the following:

- Mist AP
- Mist Edge Appliance:

Key Metrics	Mist Edge –X1	Mist Edge –X5	Mist Edge – X5-M	Mist Edge – X10	Mist Edge - VM
# AP	500	5000	5000	10000	500
# Clients	5000	50000	50000	100,000	5000
Throughput	2 Gbps	20 Gbps	40 Gbps	40 Gbps	2 Gbps

- Mist WiFi Assurance subscription (1x per AP) where X is 1,3 or 5 Years of service:

  SUB-1S-<**X**>Y

- Mist Edge subscription (1x per AP), where X is 1, 3 or 5 years service:

  SUB-ME-1S-<**X**>Y

Recommended additional components:

- Mist Marvis subscription (1x per AP) where X is 1, 3 or 5 years of service:

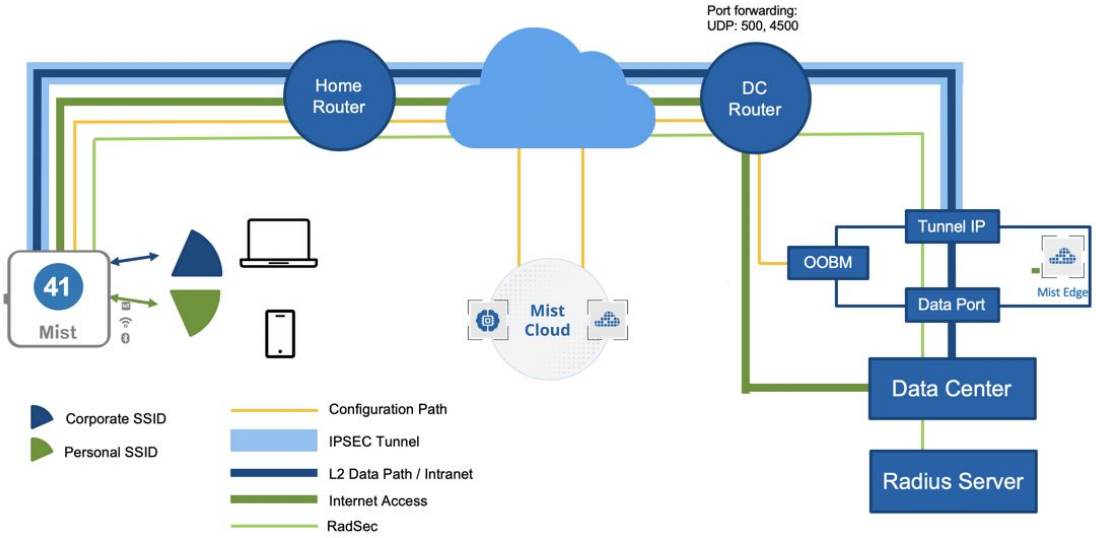
  SUB-1S-<**X**>Y

Note : Mist Edge VM has part number ME-VM that needs to be used for quotes. 1 ME-VM license allows any number of Mist Edge VM per org for a 1000 AP limit.

How it works

Mist Teleworker solution leverages Mist Edge for extending a corporate network to remote office workers using an IPSEC secured L2TPv3 tunnel from a remote Mist AP. In addition, MistEdge provides an additional RadSec service to securely proxy authentication requests from remote APs to provide the same user experience as inside the office.

Mist cloud-driven AI provides unprecedented user experience visibility via Service Level Expectations (SLE) framework, AI-driven Marvis engine with natural language processing for troubleshooting and root cause analysis and Marvis actions, which IT can leverage for remote troubleshooting of user issues without spending any additional resources.



Configuration Steps

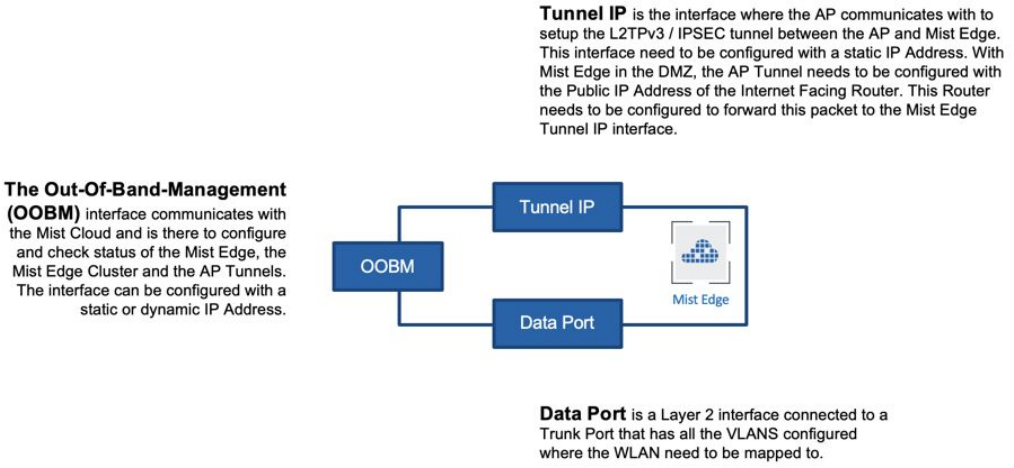
The configuration process is very straightforward and consists of the following steps. Once the initial configuration is done, no pre-staging of the Access Points is required, they can be shipped directly to the employee's house and be ready to serve clients within 20 seconds.

Setup Mist Edge

Mist Edge typically resides in the DMZ with one arm connected to the Internet and another arm going into a trusted corporate network. First, it is necessary to understand physical port connections before proceeding to the actual configuration.

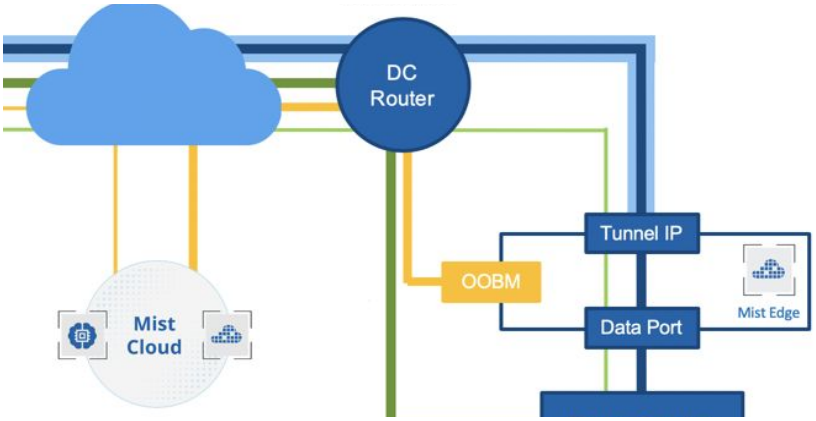
Connect Cables - Physical Port Connections:

The following snippet outlines Mist Edge port configuration requirements:



Note : OOBM IP and Tunnel IP are different IP addresses and need to be from different subnets.

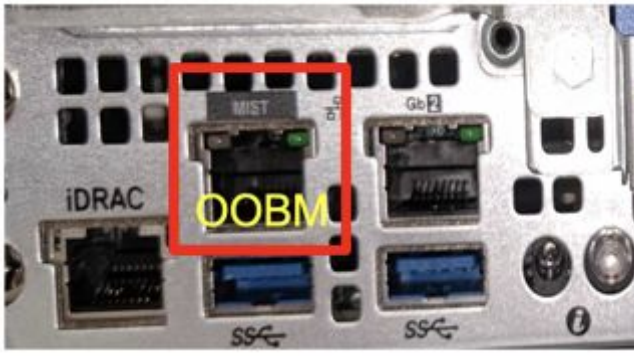
1. **Out of Band Management Port:**



Connect Out-Of-Band-Management Port (OOBM) of the Mist Edge to an untagged interface of your switch. OOBM port is used by the Mist Edge to communicate to the Mist Cloud:

Note: OOBM port on the Mist Edge appliance is marked as "MIST". By default OOBM port is configured to obtain an IP address via DHCP, it can be later changed to use static IP configuration.

The following figures shows OOBM port on X1 Mist Edge appliance:



Mist Edge comes pre-loaded with a custom debian linux installed. To configure static IP on the OOBM port, add the following lines to the interfaces config. Use iDrac interface or connect keyboard and monitor to the appliance for the OOBM initial staging if DHCP is not available. The default username and password for Mist Edge appliance is *mist / Mist@1234*, default root (su -) password is *mist*. Note the right interface id based on your MistEdge Appliance Model:

```
nano /etc/network/interfaces

iface eno1 inet static
      address 192.168.50.50/24
      gateway 192.168.50.1
      dns-nameservers 8.8.8.8 8.8.4.4
```

After saving the file, reboot the Mist Edge to apply the settings.

OOBM Interface ID per Mist Edge (ME) model:

Mist Edge Appliance Model	Interface Id
X1	eno1
X5	eno3
X5-M / X10	enp59s0f0 (for Deb9 based ME) , ens1f0 (for Deb-10 based ME)

Note: The 'OOBM IP' received through DHCP or assigned static while bringing up the Mist Edge VM is different from 'Tunnel IP' that is entered in the Mist Edge details on Mist Dashboard (Mist UI

So 2 IP addresses need to be set aside for Mist Edge , one for OOBM and other for Tunnel IP, they should be from different subnets.

In order for the Mist Edge to communicate to the Mist Cloud the following FQDNs and ports must be allowed for the OOBM interface.

For US cloud environment:

```
ep-terminator.mistsys.net : TCP port 443
```

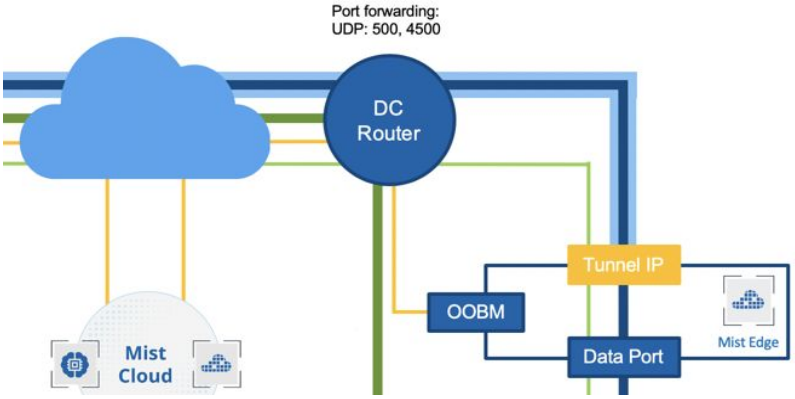
For EU cloud environment:

```
ep-terminator.eu.mistsys.net : TCP port 443
```

2. **Tunnel IP or Downstream Port**:

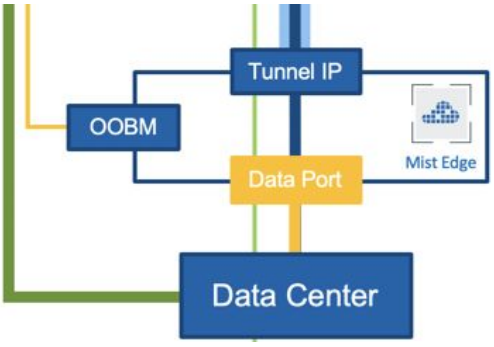
   Connect your Downstream port to the untrusted side of your network that typically goes to your DMZ firewall. Downstream Port must be connected to the *untagged* interface.

   Make sure that your router/FW either does Port Forwarding to the Tunnel Interface IP address (UDP ports 500 and 4500 for **IPSec** and TCP port 2083 for **RadSec**) or Mist Edge has a public IP address on the Tunnel Interface. This is the interface to which remote APs will be talking to in order to establish a secure IPSEC tunnel:



3. **Upstream Data Port**:

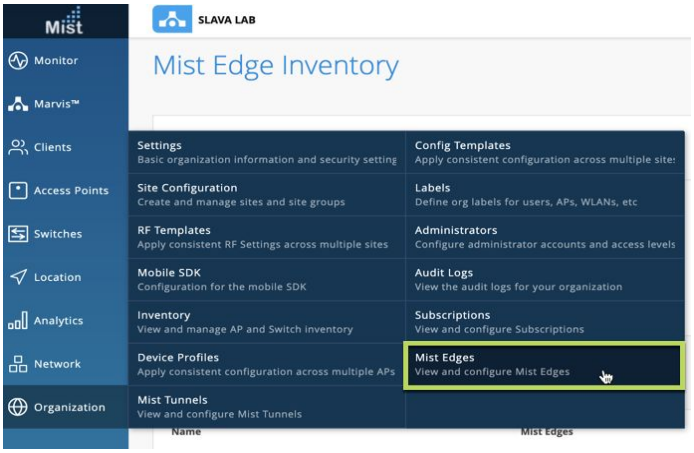
   Connect your Upstream port to the trusted side of the network. This interface would typically connect to your core switch with all the necessary user VLANs *tagged*.



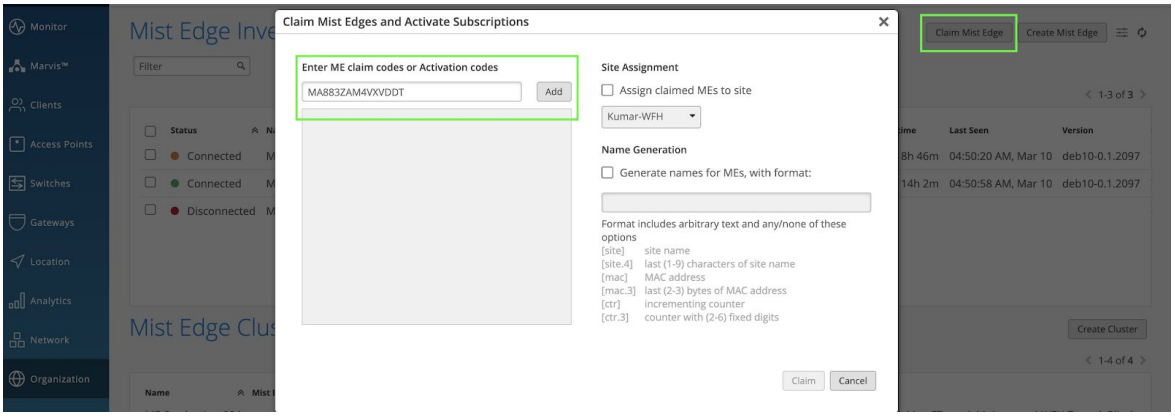
Now after all interfaces have been connected to the correct ports, it is time to register and configure Mist Edge in the Mist Cloud Dashboard.

Mist Edge Claim on the Mist Dashboard:

On the Mist Dashboard navigate to Organization → Mist Edges and Click 'Claim Mist Edge':



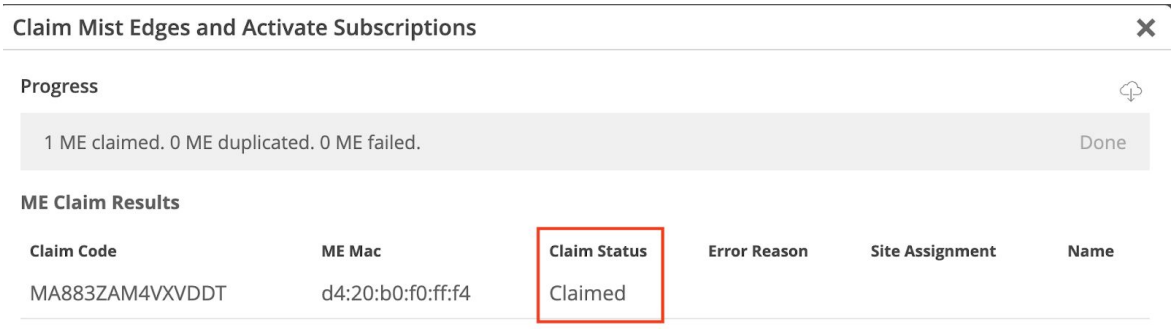
Enter the claim code received in PO or present on the service Tag:



Claim Code can be found on the service Tag of Mist Edge located below the power button as shown below. Service Tag can be pulled out:

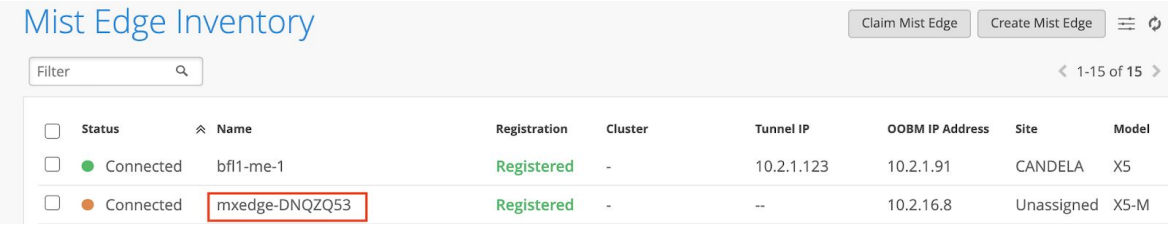
Ensure Mist Edge is powered on and the Power button shows Green.

After the Mist Edge is claimed it will show up as Disconnected and Registered, select it to edit settings:



Mist Edge will download Tunnel terminator service and Reboot in 3 minutes to show connected.

This reboot is only the first time when Mist Edge is brought online, future upgrades does not require Reboot.

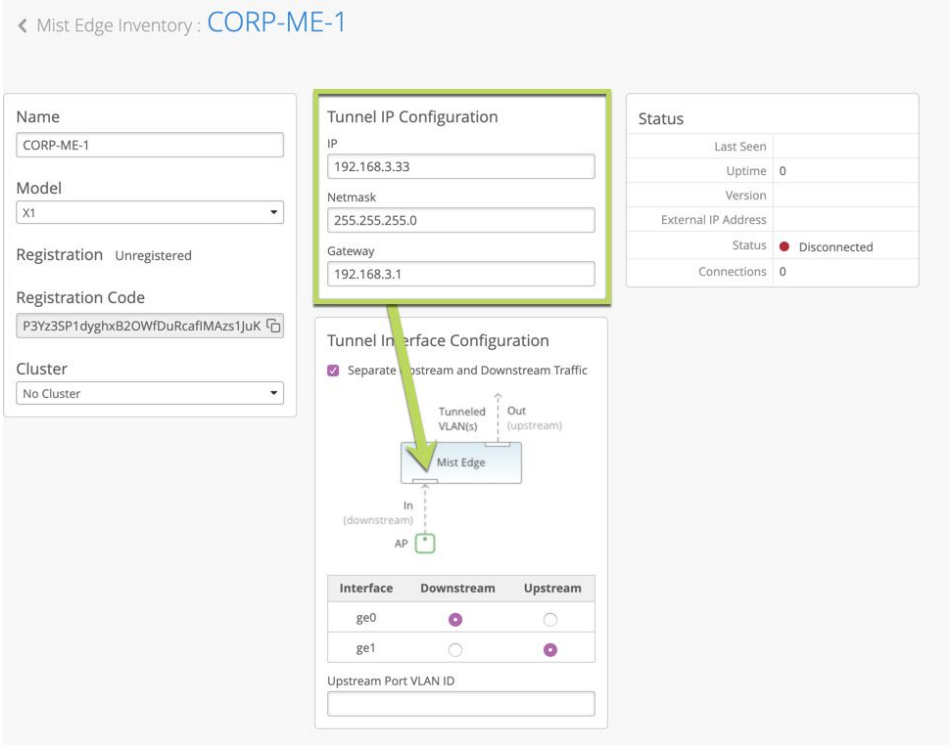


In case of Mist Edge not showing connected even after 5 minutes , one can SSH to the Mist Edge appliance using the Out-Of-Band management IP address that we have configured in the previous step. The default username and password for Mist Edge appliance is *mist* /<Claim-code>, default root password is <Claim-code>. Make sure you drop into root (`su –`) for the bootstrap procedure. Issue the following commands to check connectivity to Mist Cloud:

ping ep-teerminator.mistsys.net

If Ping is successful , request to ensure 443 outbound to ep-terminator.mistsys.net is allowed , which should ensure Mist Edge shows up connected.

In the setting page first enable “Separate Upstream and Downstream Traffic” as this is the recommended setup for the Remote Teleworker use-case. Assign correct interface IDs to the correct interfaces. In the below example we are using X1 Mist Edge, where ge0 interface is connected to the public untrusted side and ge1 interface is connected to the corporate network with all the user VLANs tagged:



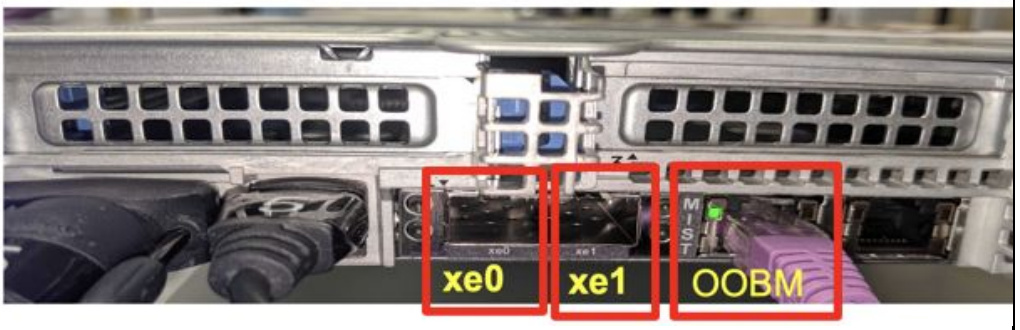
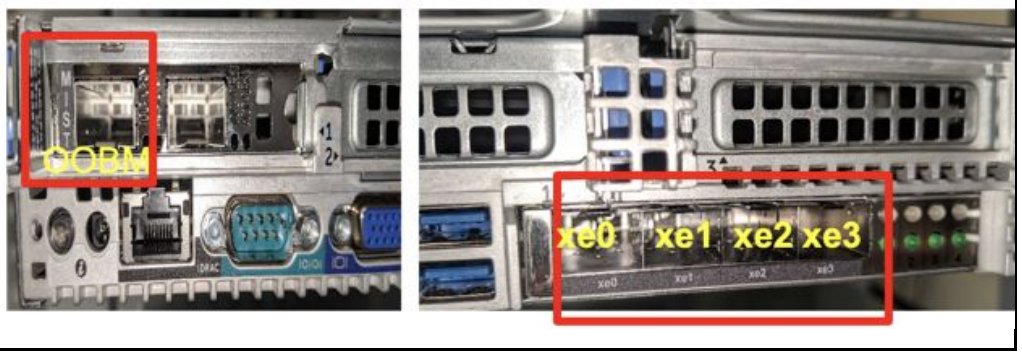
Note: a. Upstream Port VLAN ID is optional and should only be used whenever the upstream switchport is configured as an access port with a single VLAN untagged.

b. The 'OOBM IP' received through DHCP or assigned stac while bringing up the Mist Edge VM is different from 'Tunnel IP' that is entered in the Mist Edge details on Mist Dashboard (Mist UI).

So 2 IP addresses need to be set aside for Mist Edge , one for OOBM and other for Tunnel IP, they need to be from different subnets.

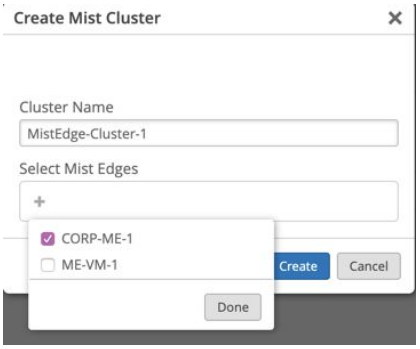
Based on your Mist Edge model the interface IDs might be different. Please use the image below that show individual model port mappings:

Note: Request to keep the data ports on switch side , that is corresponding ports to ge0,ge1 or xe0,xe1 or xe0,xe1,xe2,xe3 shutdown until Mist Edge is configured with Tunnel IP and Mist Tunnel vlan.

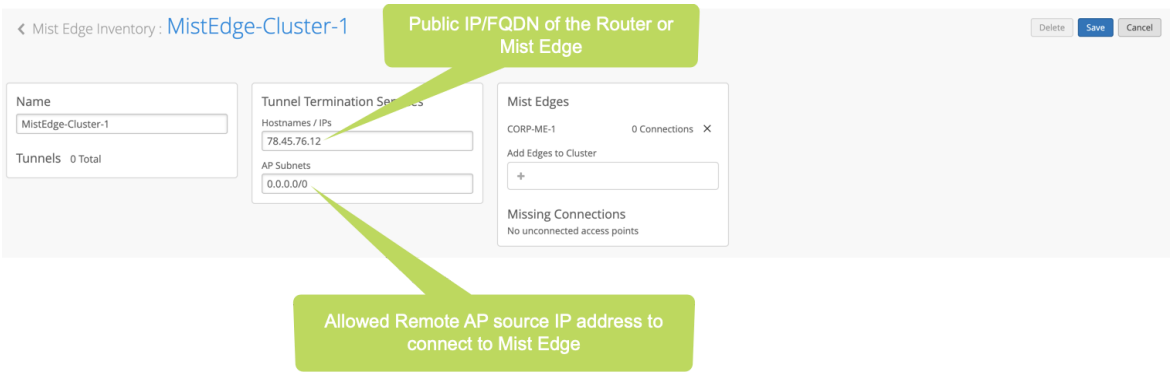
X1	
X5	
X5-M and X10	

Create a Mist Edge Cluster:

Now that all the necessary services have been provisioned let's create a Mist Edge Cluster and add our Mist Edge in there:



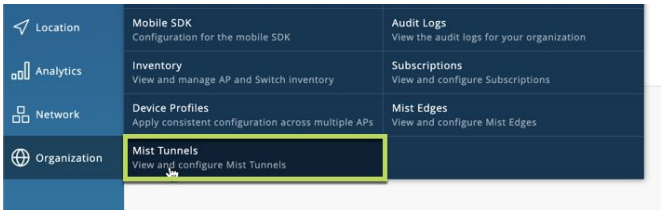
Under Mist Edge Cluster configuration, we will need to set our Cluster IP address(es) or FQDNs for the remote APs to communicate to. In case your Firewall/Router is doing a port forward to the Tunnel IP interface, you will need to specify the public IP address of your Firewall/Router. In case your Tunnel IP of the Mist Edge is a public IP address, specify that IP address in the Cluster configuration. In case multiple Mist Edges are part of the cluster, their respective IP addresses should be listed there, comma separated:



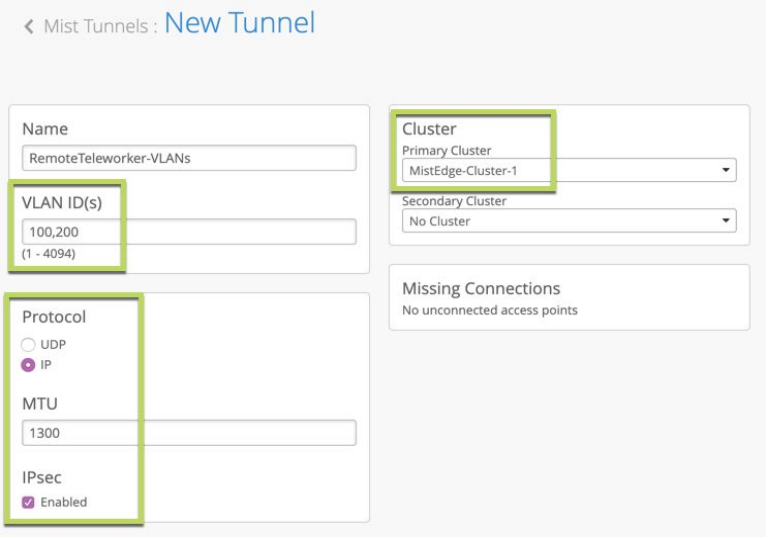
Time to move to the next step and create a Mist Tunnel.

Setup the Mist Tunnel

Navigate to Organization → Mist Tunnels and Create a new Tunnel. Typically this is where you would list all your user VLANs that you would like to extend from a remote home office back to your corporate network. The VLAN list should be comma separated. Also, this a place where we specify that all the user traffic should be encrypted via IPSec:



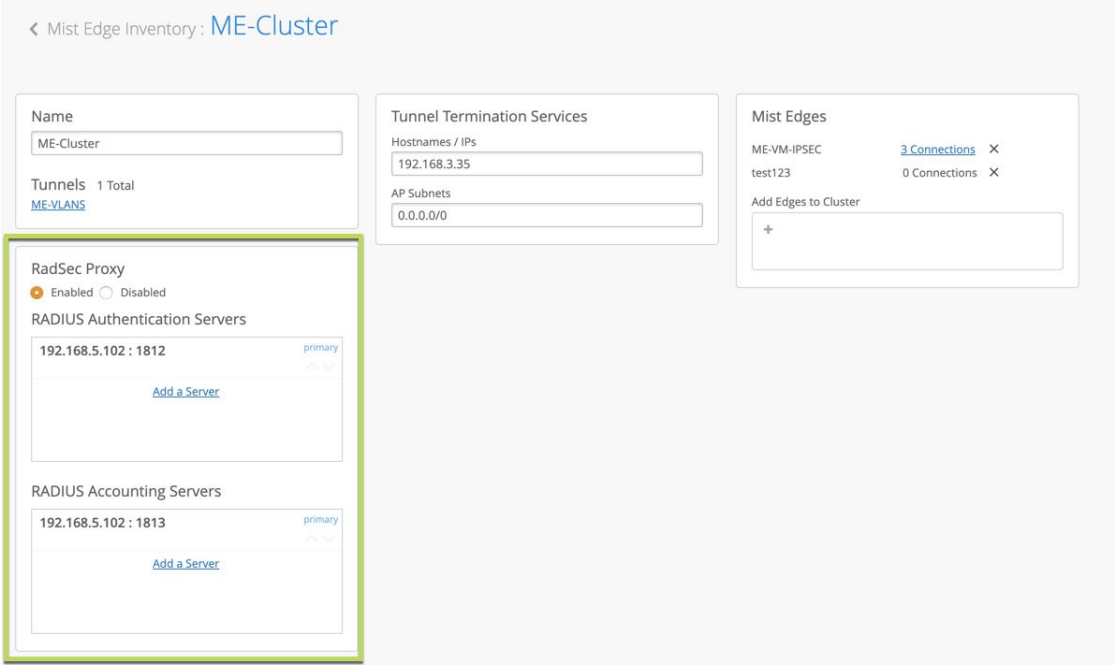
Once you create a Mist Tunnel, specify all user VLANs required to be tunneled back, assign the tunnel to the Mist Edge Cluster (s) we have created earlier, also lower the max MTU size to 1300, to allow for IPSec overhead and enable tunnel IPSec encryption:



Enable RadSec Proxy service

With Mist Edge it is possible to deploy a RadSec service to secure proxy authentication requests from remote APs to provide the same experience as inside the office.

To enable a RadSec service navigate to the Mist Cluster setup page:



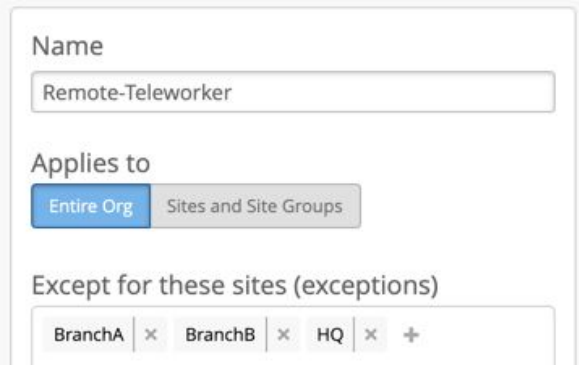
Important Note: RadSec Proxy service is listening on any MistEdge interface on TCP port 2083 (Tunnel IP or OOBM interface), however it sources RADIUS requests via the OOBM port.

Configure and prepare the SSID

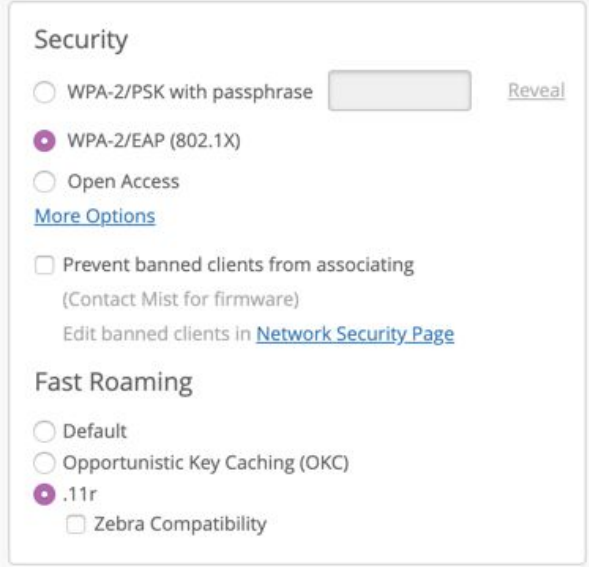
The best way to provision your corporate SSID to the remote APs is to leverage Config Templates.

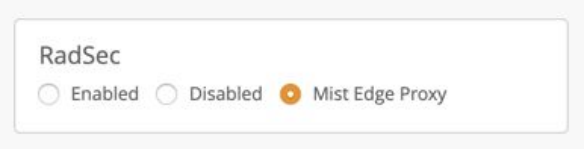
Navigate to Organization → Config Templates.

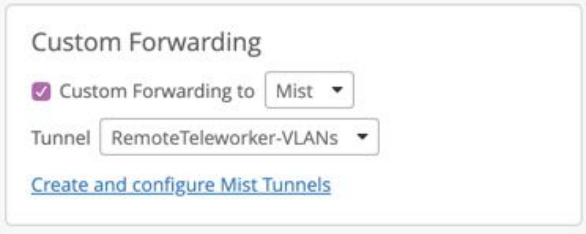
Create config template and use template assignment for either a) specific Site Group, where each remote home office site will be placed into a Site Group "Remote Teleworker" or b) Entire Org with actual office Sites added as exceptions. For example the following template will be assigned to all Sites, *except* Sites "HQ", "BranchA", and "BranchB".



SSID settings would depend upon particular customer requirements, but below are the most important parts with regards to user data tunneling back to the corporate network. Below example is walking through the configuration of the 802.1X secure WLAN with RadSec proxy configured via the Mist Edge:





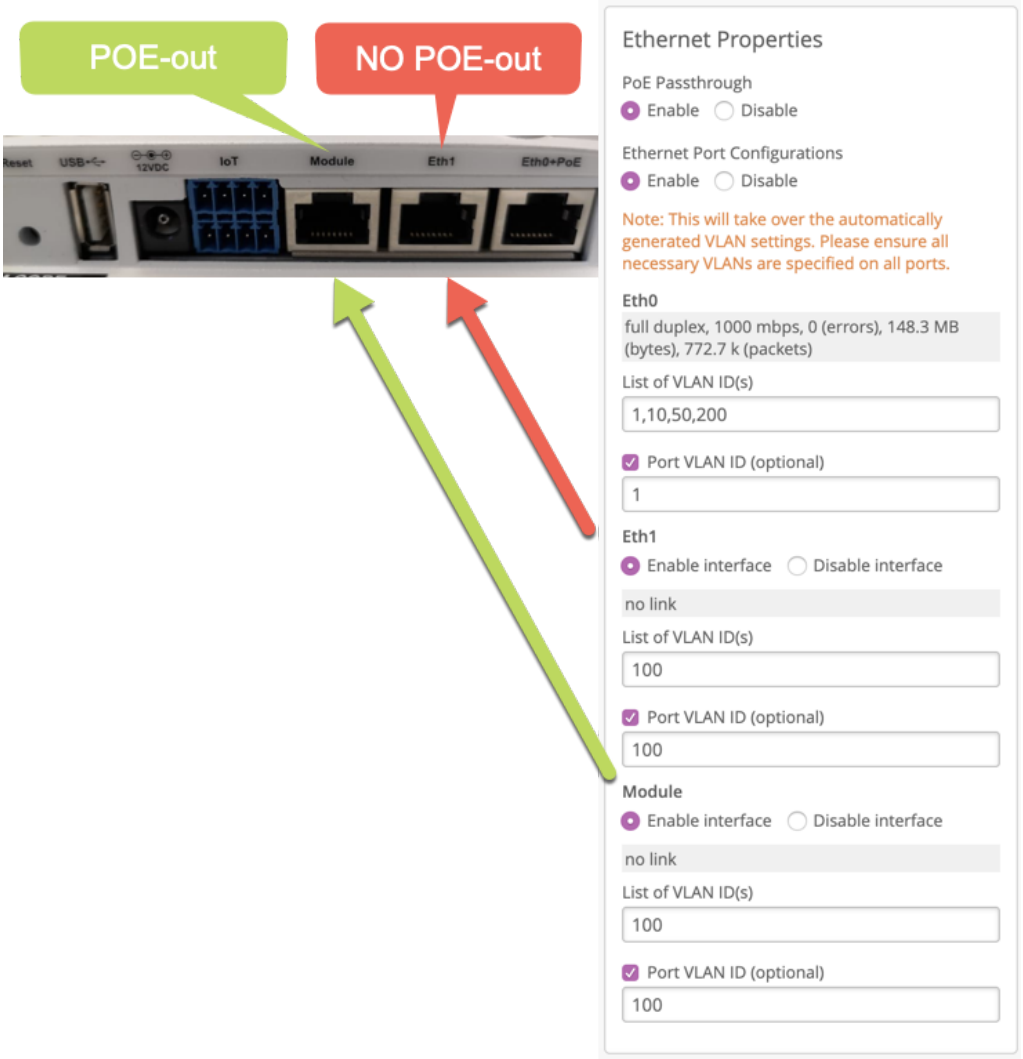


Enable Wired client connection via ETH1 / Module port of the AP

In some cases it is required to connect wired devices and extend connectivity to the corp network for those devices as well. An example could be a security camera, an IP phone, etc. It is typical that those devices will require tight security policing on the firewall, once they are onboarded, hence they will usually be placed into a unique VLAN.

The configuration can be achieved on a per-AP basic via AP overrides, or by leveraging Device Profiles. In either case the configuration would be exactly the same.

Below is an example of the second port configuration for the **AP41**. “Port VLAN ID” is the same as “Native VLAN ID” or “Untagged VLAN”. Note that only the Module port is capable of providing POE-out to power a low-powered device, for example an IP phone. POE Passthrough is only supported if an AP is powered by a POE injector, not DC power supply:



Example of AP12 wired port Config for tunneling:

If the same port config is required by multiple remote user APs , we can do it on a device profile and map the device profile to AP.

We can also do the config on individual AP as well.

Port 0 : APs management traffic is sent untagged , all local wlan vlan are auto tagged on Eth0.

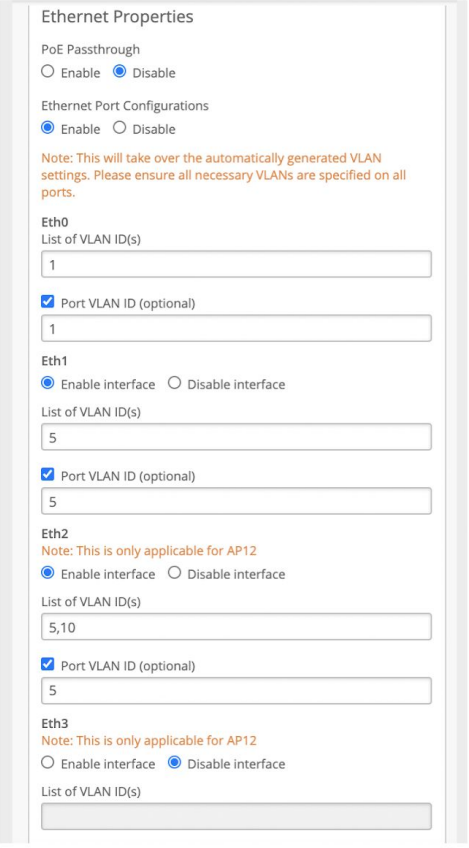
Hence we can leave Eth0 as below, where 'List of VLAN ID(s)' and 'Port VLAN ID both are configured as 1.

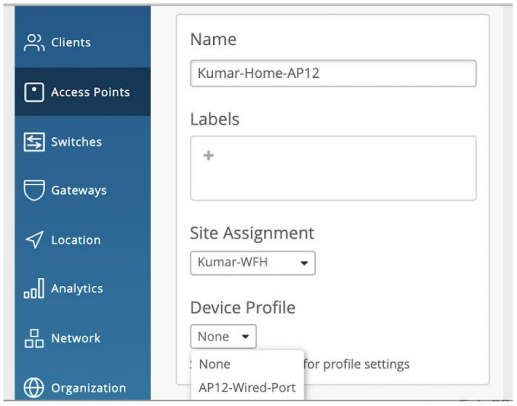
Other ports: Other ports can be mapped to single vlan or multiple vlan as shown below, if single vlan , wired host connected will receive IP address from that vlan.

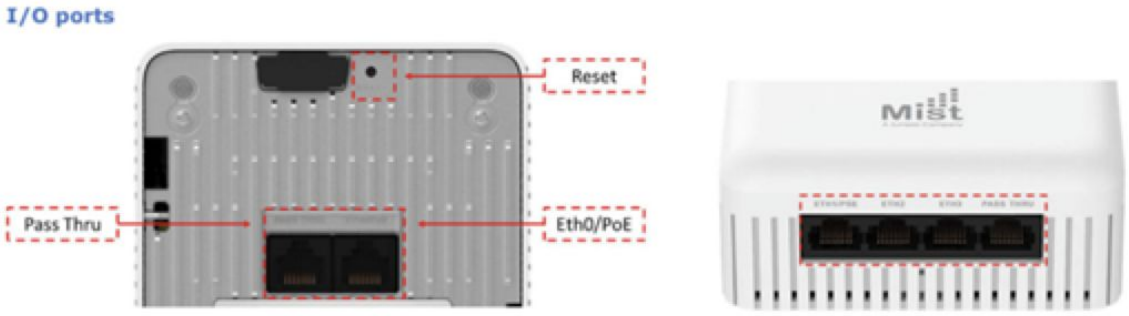
If configured as a trunk with multiple allowed vlan and one of them as native vlan, it will behave as a trunk.

Usually additional wired ports will be used to extend Tunneled vlan to on wired port.

Note: Split tunnel for wired port is yet to be supported, so vlan 1726 cannot be mentioned on the config, vlan 110 when specified on wired port will still do a full tunnel for wired device.







Eth0+PoE is the port that which is plugged into the POE switch or POE brick to power up the AP12 and serve a DHCP IP address for management.
Pass Thru – Ports marked Pass Thru just act as a patch from back to the side port and no config is required for this . This is useful in cases where a port behind wall mount needs to be allowed to connect , example TVs in Hotels etc.

Eth1 to Eth3 , config is available on AP details or Device profile UI page and can be mapped to management vlan or tunneled vlan.

Enable Split Tunneling for the Corp SSID

To allow corporate clients to connect to local home devices (printers, media systems etc), while connected to the corporate network, Mist Edge provides split tunnel capability that can be enabled under Mist Tunnel settings. Note that this feature only works with one single remote AP

Once Split Tunnel feature is enabled, everything under “Destination Subnet” will be tunneled back to the Mist Edge, rest will be locally bridged. In addition, DNS Servers field provides a way to use corporate DNS servers to resolve URLs/FQDNs for both tunneled and locally bridged traffic

Tunnel Gateway setting needs to be configured with Client subnet Gateway . This is the gateway for the vlan mapped to the wireless LAN.

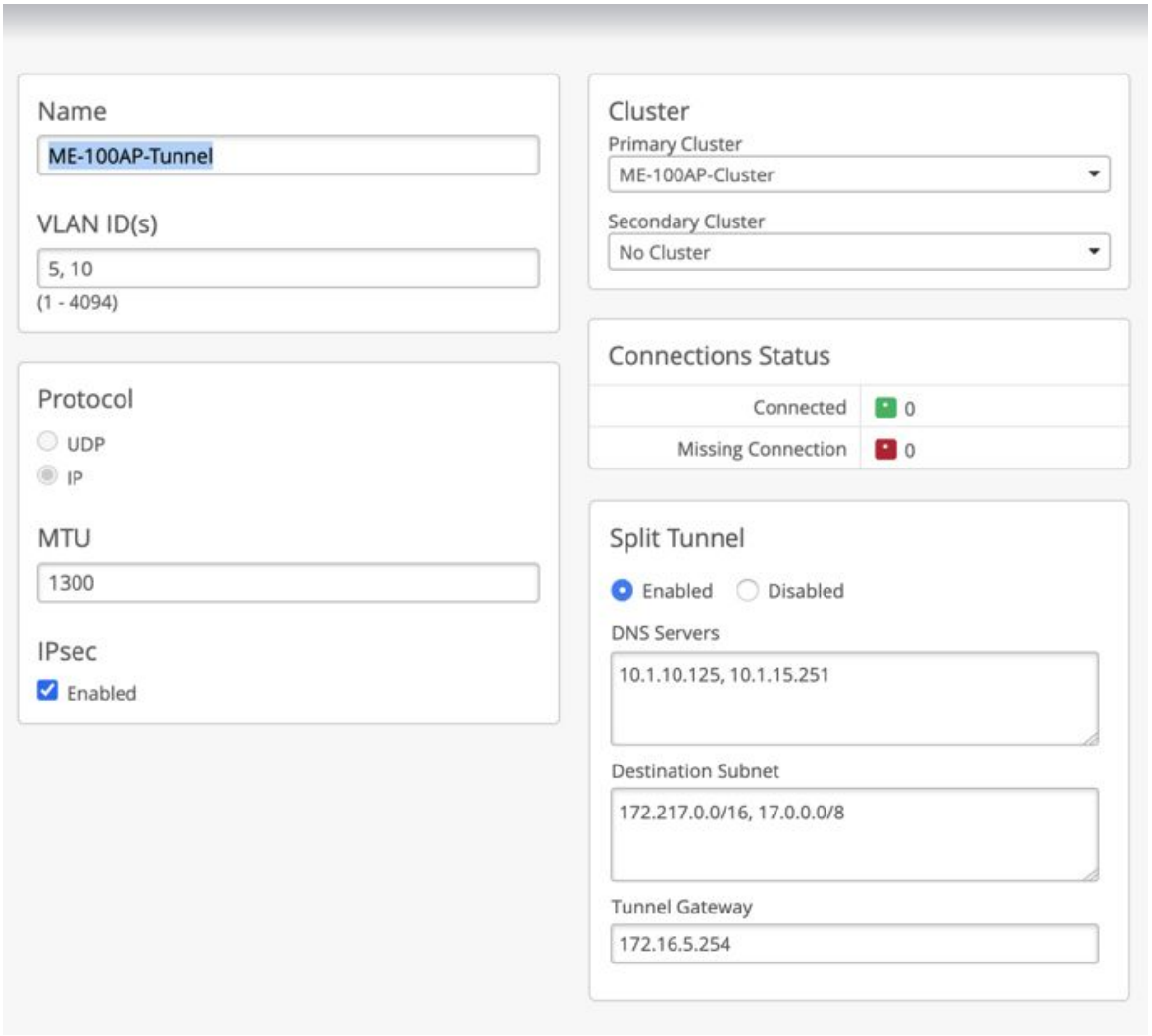
Please note multiple destination subnets can be configured with comma separation.

Corporate DNS servers need to be part of the Destination subnet or they can be added as a /32 Entry.

Traffic Flow: When Split Tunnel is enabled , AP serves 192.168.157.X/27 IP address from private subnet it runs for clients.

Traffic destined to corporate, defined in ‘Destination Subnet’ is NAT to corporate IP that AP receives from the corporate wireless LAN’s vlan.

Rest of the wireless client traffic is NAT to AP’s management vlan IP Address.



Create a Site for Remote Office Workers

Sites can be created using UI under Organization → Site Configuration

Please note the following guidelines:

- For AP41, AP43, minimum AP firmware version required to support IPSec & Split Tunneling is: **0.7.20289**
- For AP32/33, AP12, minimum AP firmware version required to support IPSec with Split Tunneling: **0.8.21022**

Claim an AP and ship it to Employee's location

Use MistAI app to claim an AP before shipping it to the remote home office location.

https://www.mist.com/documentation/mist-ai-mobile-app/

In the Mist AI app, select the Site, Claim an AP to that site using the QR code on the back of the AP and ship it to the employee's location. No need to plug it to the network before shipping!

Now plug in the AP into any of the Ethernet ports of the local home router (use PoE injector or DC power). AP is ready to serve your new remote office in <20 seconds

Troubleshooting

To list all IPSEC connections from the Mist Edge shell:

```
root@ME-VM-IPSEC:~# curl http://localhost:9110/debug/ipsec

1 servers running.


IPsec server listening at 192.168.3.35

  7 configured peers

  3 connected peers

  3 connections

  3 IKE SAs

  1 ESP SAs


  IKEv2 SA 0xc000084a80 (SPIi 2b4dd664ff867577, SPIr bbcc57612c4fada7)

   {192.168.51.142 500 } <-> {192.168.3.35 500 }

   IDi/user: "@#5c5b35513083", IDr: "192.168.3.35"

   IKE SA created 2020-05-04T09:40:19Z (3s), parent IKE SAs connected
since 2020-05-04T09:40:19Z (3s), SA index 7211

   state: INITed, KEYed, AUTHed

   IKE encr ENCR_AES_CTR (keylen 256), integ AUTH_HMAC_SHA2_512_256, DH
DH_Curve22519, PRF PRF_HMAC_SHA2_512

   IKE tx_queue len 0; tx req MsgID 0, rx req MsgID 3

   0 ESP SA pairs

  IKEv2 SA 0xc000085c00 (SPIi 6bbe607f2f2921a0, SPIr 58a03a1091648bd0)

   {192.168.51.62 500 } <-> {192.168.3.35 500 }

   IDi/user: "@#5c5b3551323b", IDr: "192.168.3.35"

   IKE SA created 2020-05-04T09:40:19Z (3s), parent IKE SAs connected
since 2020-05-04T09:40:19Z (3s), SA index 7212

   state: INITed, KEYed, AUTHed
```

```
   IKE encr ENCR_AES_CTR (keylen 256), integ AUTH_HMAC_SHA2_512_256, DH
DH_Curve22519, PRF PRF_HMAC_SHA2_512

   IKE tx_queue len 0; tx req MsgID 0, rx req MsgID 3

   0 ESP SA pairs

  IKEv2 SA 0xc000041880 (SPIi 8f327739dcd23e06, SPIr f485ebdf6b8d511e)

   {192.168.51.122 500 } <-> {192.168.3.35 500 }

   IDi/user: "@#d420b002635e", IDr: "192.168.3.35"

   IKE SA created 2020-05-04T09:40:20Z (2s), parent IKE SAs connected
since 2020-05-04T09:40:20Z (2s), SA index 7213

   state: INITed, KEYed, AUTHed

   IKE encr ENCR_AES_CTR (keylen 256), integ AUTH_HMAC_SHA2_512_256, DH
DH_Curve22519, PRF PRF_HMAC_SHA2_512

   IKE tx_queue len 0; tx req MsgID 0, rx req MsgID 2

   1 ESP SA pairs

    ESP pair 0xc0000ebb00: peer SPI cbb7b1df, local SPI 8bd36bae

     ESP SA created 2020-05-04T09:40:20Z (2s), parent ESP SAs since
2020-05-04T09:40:20Z (2s)

     ESP encr ENCR_AES_CTR (keylen 256), integ AUTH_HMAC_SHA2_512_256, ESN
true

     flags: USE_TRANSPORT_MODE, local ESP_TFC_PADDING_NOT_SUPPORTED,
Active Tx SA

     1 TSi:

      TS{192.168.51.122,L2TP}

     1 TSr:

      TS{192.168.3.35,L2TP}
```

To see established **L2TPv3 tunnels** from the MistEdge perspective:

```
root@ME-VM-IPSEC:~# curl http://localhost:9110/debug/l2tp

1 tunnels, 1 listeners.



Tunnels by state:
```

```
  State established-with-sessions: 1




tunnel between IPsec(7213)⊕192.168.51.122 - BRQ-Lab-2 - router-id
176.2.99.94 and IPsec⊕192.168.3.35

 state established-with-sessions

 spawned by listener 00000000-0000-0000-1000-0a6fc06adf84 at
IPsec⊕192.168.3.35

 last established 2020-05-04 09:40:23 +0000 UTC, uptime 1m13s

 config uuid f8d56541-f104-4068-8b49-3cda8a465b57

 hostname "ME-VM-IPSEC", router-id 00000000, peer-router-id b002635e

 local connection id 1424620686, remote connection id 3622409912

 peer pseudowire capabilities [VLAN Ethernet]

 tx pkts 5, rx pkts 4, last rx 2020-05-04 09:40:23 +0000 UTC

 tx queue len 0, ns 3, na 3, nr 4

 tx first hop 9c-cc-83-b1-e6-30, vlan 1

 peer mist id "d4-20-b0-02-63-5e", site
"4ee6e679-caee-49d3-ae4c-de4f97c76850", org
"2e69ddfd-8af0-4277-b143-762175f7e679"

 Path-MTU discovery WANT; outer Path-MTU 1300; inner MTU 1212 (not
including any vlan tag)

 session "mxtunnel"/"mxtunnel", s# 4098356666, state established

  local session id 2519973924, remote session id 3656949312

  vlans [100], pseudowire type VLAN, port 11

  remote_circuit_active true




listener at IPsec⊕192.168.3.35

 config uuid 00000000-0000-0000-1000-0a6fc06adf84
```

```
1 tunnels spawned
```

Lastly, to troubleshoot **RadSecProxy service**, use the following command:

```
root@ME-VM-IPSEC:~# tail -F /var/log/radsecproxy/radsecproxy.log

Apr 28 14:42:28 2020: createlistener: listening for tls on *:2083

Apr 29 08:26:41 2020: createlistener: listening for tls on *:2083

Apr 29 08:29:17 2020: createlistener: listening for tls on *:2083

Apr 30 00:36:26 2020: createlistener: listening for tls on *:2083

May  1 06:23:34 2020: tlsservernew: incoming TLS connection from
192.168.51.122

May  1 06:38:34 2020: tlsserverrd: connection from 192.168.51.122 lost

May  4 00:48:45 2020: tlsservernew: incoming TLS connection from
192.168.51.62

May  4 01:03:45 2020: tlsserverrd: connection from 192.168.51.62 lost

May  4 09:40:18 2020: createlistener: listening for tls on *:2083

May  4 09:40:20 2020: createlistener: listening for tls on *:2083
```

Packet Captures on the Mist Edge

Currently the packet capture facility on the Mist Edge is local to the appliance only, but it can be very useful to troubleshoot datapath at different entry points (inbound physical port, l2tpv3 tunnel, drop etc). In order to enable packet captures into the cli shell, it is necessary to instal tshark:

```
apt-get install tshark
```

After the tshark is installed you could use port debug command to list all the interfaces you can capture on:

```
root@ME-VM-IPSEC:~# curl http://localhost:9110/debug/ports

Port 0 "port0":

    PCI address: "0000:13:00.0"

    MAC: 00-0c-29-22-a4-d1

    PMD: "net_vmxnet3"
```

```
    link: true, duplex: true, Speed: 10000 Mbps
    state: Forwarding
    Rx: 314267822 bytes, 2253968 packets, 0+0 errors
    Tx: 282976995 bytes, 1947497 packets, 0 errors
    rx_good_packets: 2253968
    tx_good_packets: 1947497
    rx_good_bytes: 314267822
    tx_good_bytes: 282976995
    rx_q0packets: 2253968
    rx_q0bytes: 314267822
    tx_q0packets: 1947497
    tx_q0bytes: 282976995
Port 1 "port1":
    PCI address: "0000:1b:00.0"
    MAC: 00-0c-29-22-a4-db
    PMD: "net_vmxnet3"
    link: true, duplex: true, Speed: 10000 Mbps
    state: Forwarding
    Rx: 640727016 bytes, 1387326 packets, 0+79 errors
    Tx: 279571047 bytes, 1783598 packets, 0 errors
    rx_good_packets: 1387326
    tx_good_packets: 1783598
    rx_good_bytes: 640727016
    tx_good_bytes: 279571047
    rx_missed_errors: 79
    rx_q0packets: 1387326
    rx_q0bytes: 640727016
    tx_q0packets: 1783598
```

```
    tx_q0bytes: 279571047



Bridge port vlans:

[0] port0, PVID 1, Inactive Vlans [1]

[1] port1, Inactive Vlans [100]

[4] kni0, Inactive Vlans [1]

[11] L2TP session "mxtunnel" with 192.168.51.122:0 (d4-20-b0-02-63-5e),
Active Vlans [100]
```

Based on the example above, below are some sample packet capture syntax commands (more info available at `tt-pcap --help`)

```
root@ME-VM-IPSEC:~# tt-pcap -port=1 udp port 67 | tshark -nr -

Running as user "root" and group "root". This could be dangerous.

    1 0.000000000      0.0.0.0 ? 255.255.255.255 DHCP 346 DHCP Discover -
Transaction ID 0x12e3913a

    2 0.103353790 192.168.100.1 ? 192.168.100.135 DHCP 337 DHCP Offer    -
Transaction ID 0x12e3913a

    3 1.521102670      0.0.0.0 ? 255.255.255.255 DHCP 346 DHCP Request  -
Transaction ID 0x12e3913a

    4 2.133698590 192.168.100.1 ? 192.168.100.135 DHCP 337 DHCP ACK      -
Transaction ID 0x12e3913a
```