TLS Support on Mobility Express

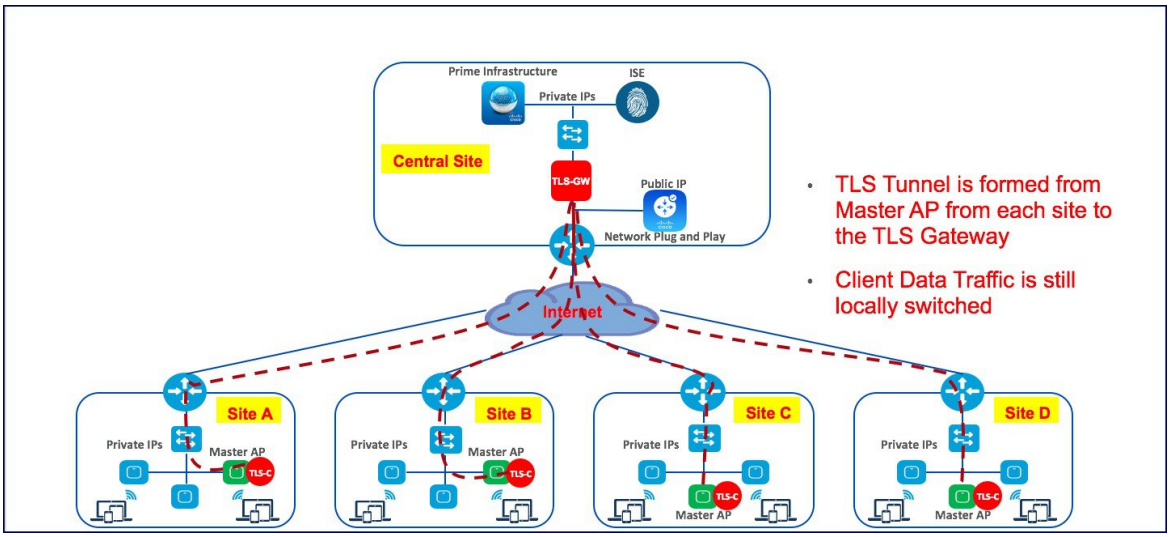
Cisco Mobility Express is a virtual wireless controller function embedded on 802.11ac Wave 2 Access points. With the flexibility of running a wireless LAN controller function on an access point, customers can deploy an Enterprise wireless solution on a single site or multiple sites with up to 100 Access Points at each site. In a multi-site deployment, customers can manage each of the sites using Cisco Prime Infrastructure which would typically be deployed in a central site. However, if the individual sites are connected to the internet via an ISP and are not connected via a dedicated WAN, managing these multi-site deployments can pose a challenge.

To overcome this challenge, starting AireOS Release 8.6, Cisco Mobility Express, customers can now manage the multi-site deployment using Cisco Prime Infrastructure over a TLS Tunnel. In addition to managing these sites, they can also aggregate their DOT1x authentication request to a RADIUS(ISE) which can be deployed along site CPI at the central site.

Please note that only SNMP, RADIUS and SSH traffic flows on the TLS tunnel to the central site and data traffic is still switched locally at individual sites.

TLS Tunnel has two components

1. TLS Client–Starting AireOS Release 8.6, TLS Client has been embedded in the Cisco Mobility Express code and will run on the Master AP
2. TLS Gateway –This is a Virtual Machine which is deployed at the central site to establish the TLS Tunnel. TLS Gateway has two network interfaces
    1. Public Network–This is the public IP which is reachable from every Master AP. The TLS client establishes a TLS tunnel between Master AP and TLS Gateway using this address.
    2. Private Network–This the IP address of the private network behind the TLS Gateway where the Cisco Prime Infrastructure, RADIUS and other network devices are deployed.



TLS Gateway

TLS Gateway is virtual machine and is deployed at the central site.

System Requirement for TLS Gateway

1. Hypervisor: VMware–ESXi 5.5.0/ESXI 6.0
2. VM Resources
    1. 4 vCPU
    2. 8GB RAM
    3. 100 GB Storage
    4. 2 NICs (One for Public network and one Private network)
3. IP routing requirements
    1. Routing enabled from TLS-GW Private network towards Prime-infra(SNMP), ISE(Radius), DHCP servers, SSH, Monitoring system and vice-versa
4. TLS-GW public IP should be Reachable from Management IP of ME-AP

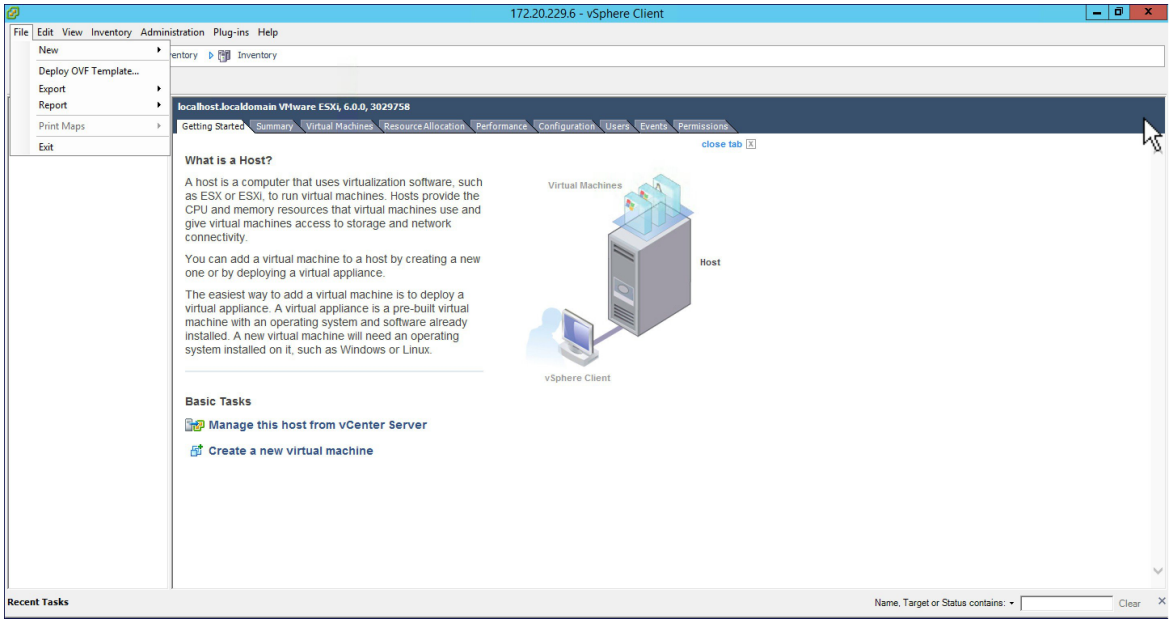
Deploying TLS Gateway

Please follow the steps below to deploy a TLS Gateway at the central site.

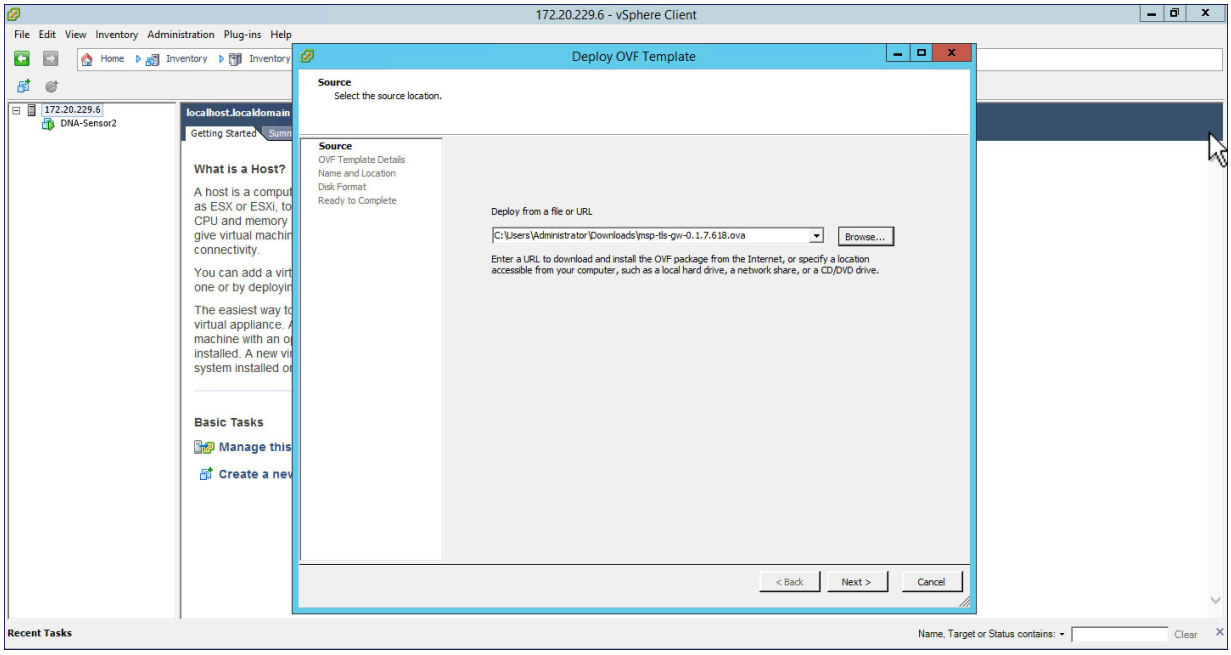
Procedure

Step 1 Secure the TLS Gateway OVA File

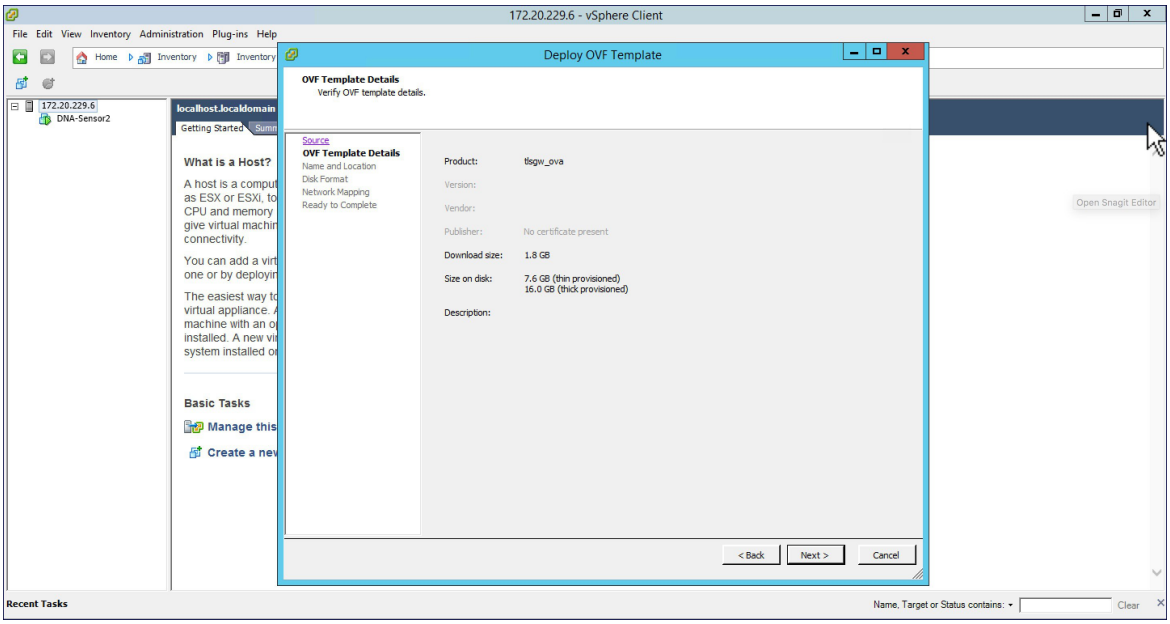
Step 2 Navigate to File > Deploy OVF Template on the vSphere Client UI.



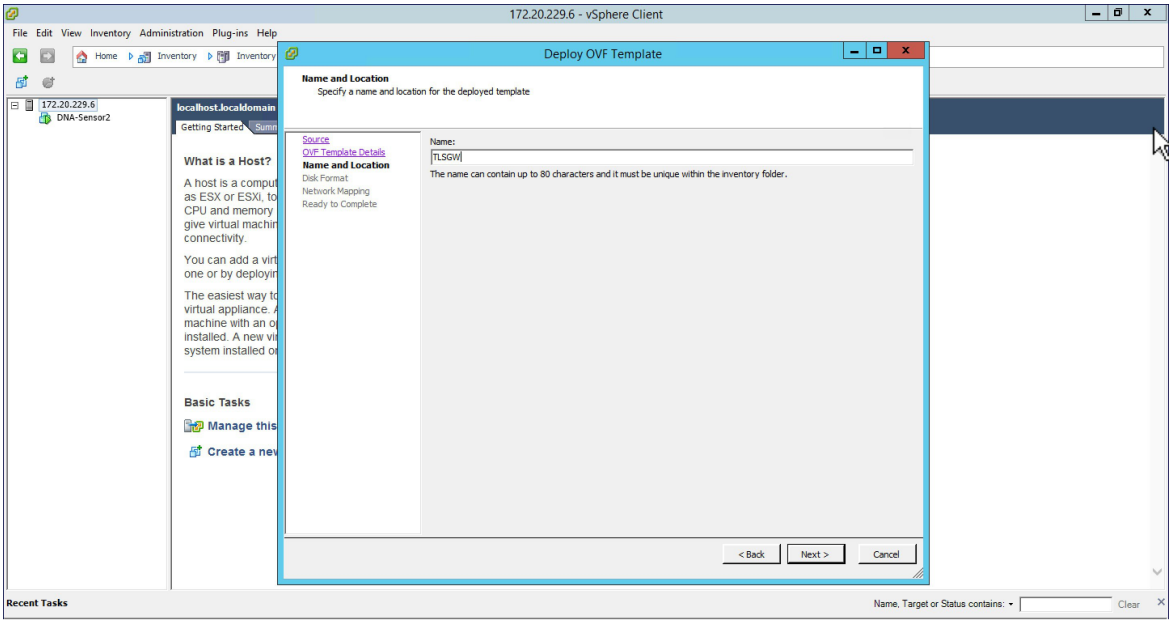
Step 3 Browse to the TLS Gateway OVA file on your local machine. Click Next.



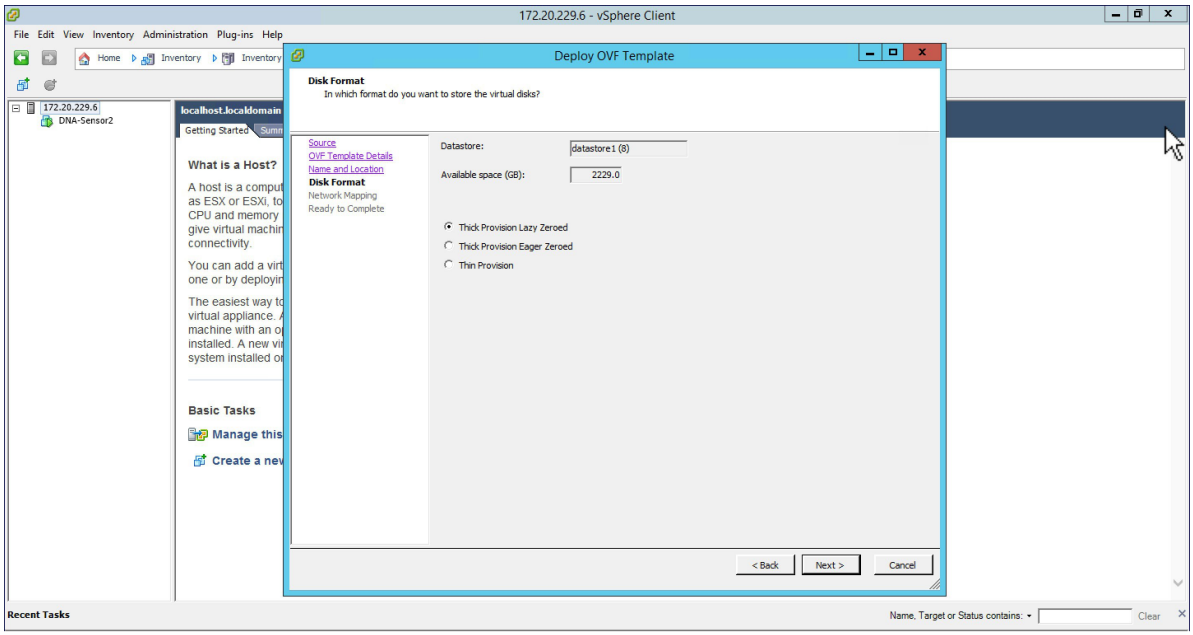
Step 4 Check the OVF Template details and click Next.



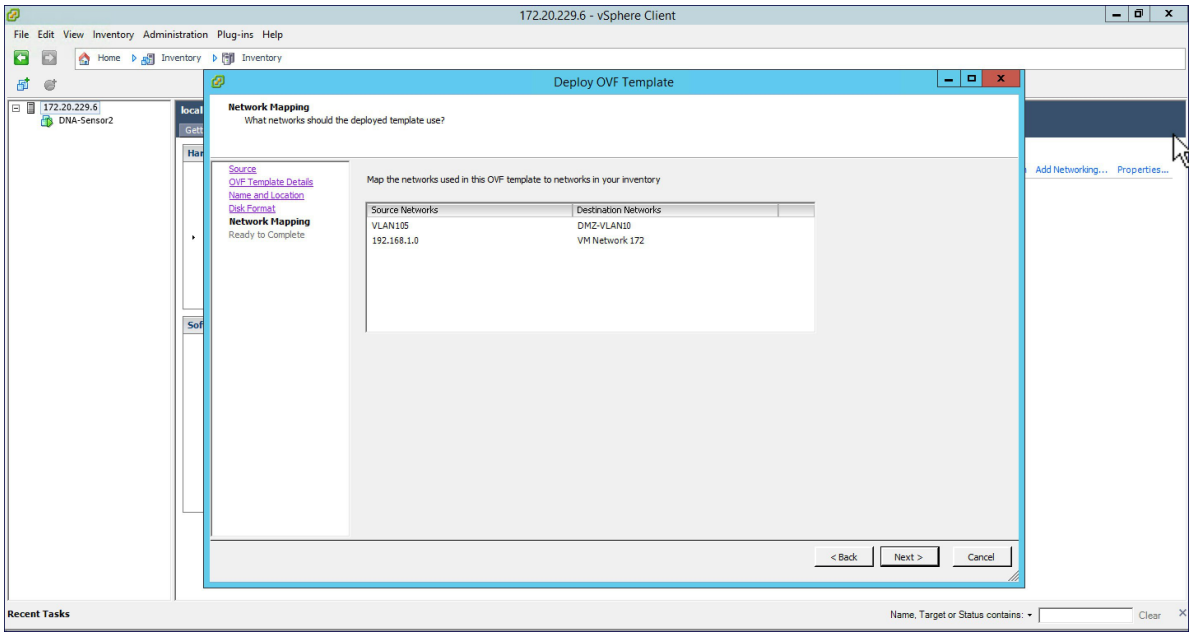
Step 5 Specify the name for the TLS Gateway Virtual Machine.



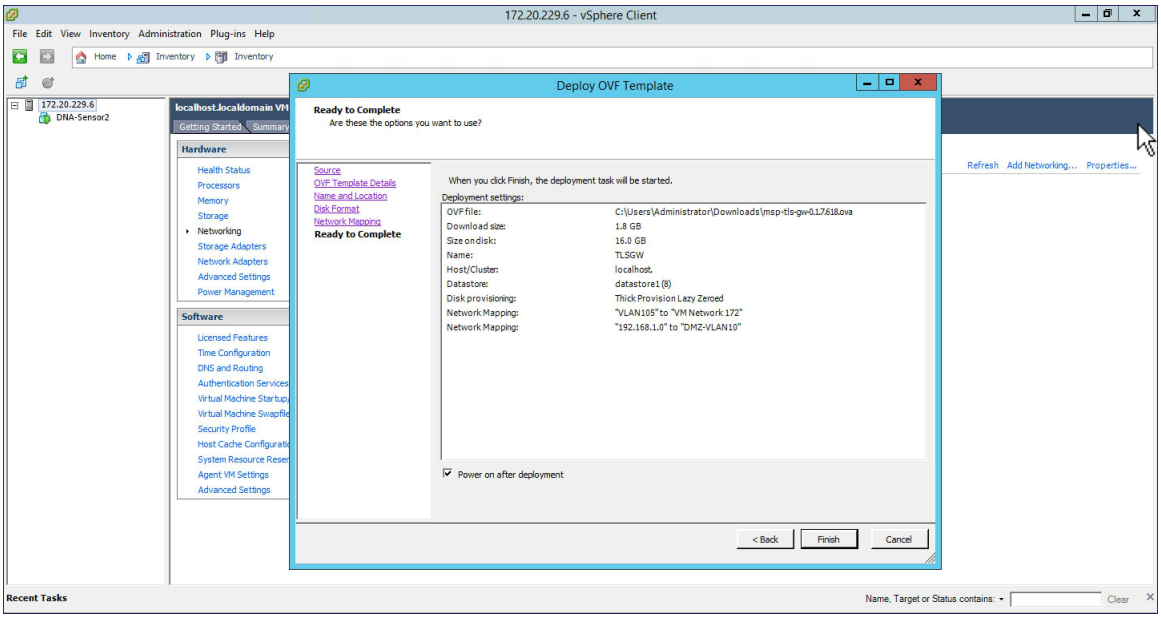
Step 6 For Disk Format, stay with the default and click Next.



Step 7 For Network Mapping, select the Destination Network for the Public Network interface. Click on Next.



Step 8 Verify the Deployment Settings. Enable the 'Power On after deployment' check box and click Finish.



Configuring TLS Gateway

Configuring the TLS Gateway comprises of 3 things:

1. Configure the IP address for Public and Private network interfaces
2. Configure the TLS Gateway configuration file and start the service
3. Configuring the PSK ID-KEY Pair

After the OVA for TLS Gateway is deployed and powered up, follow the steps below to configure the TLS Gateway.

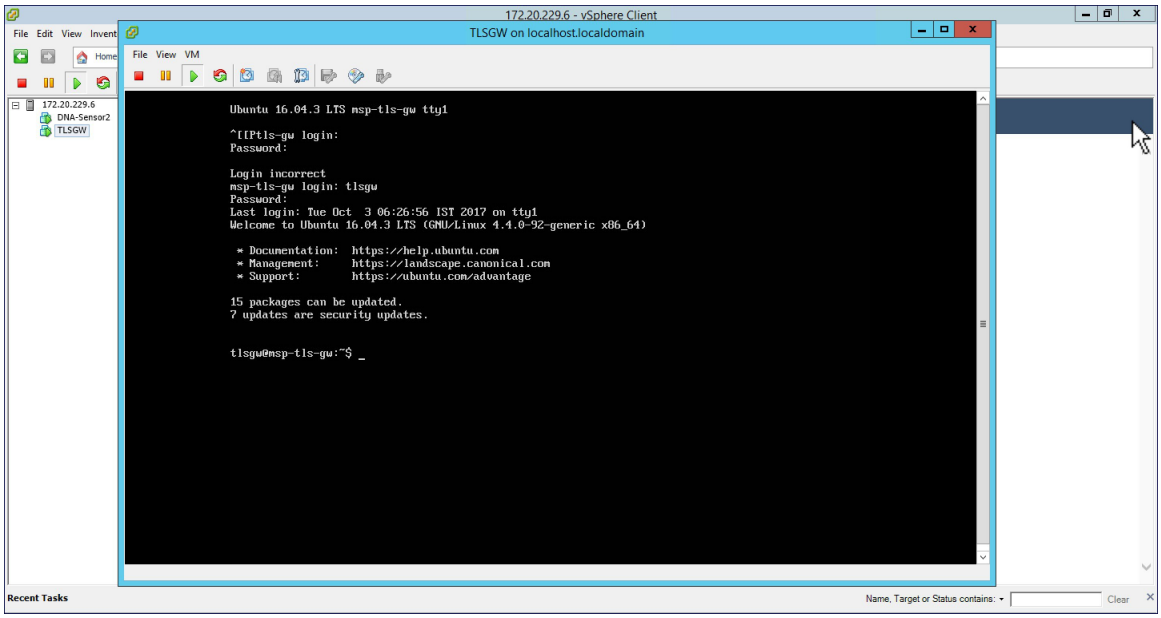
Configuring IP Address for Public and Private network interfaces

Procedure

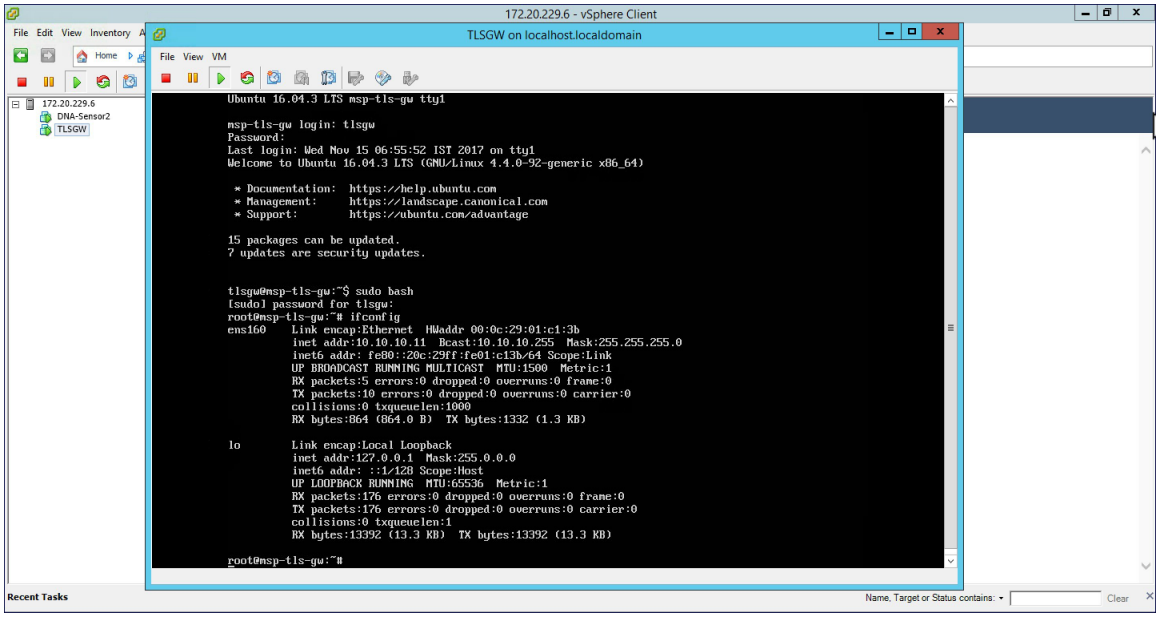
Step 1 Open a console session to the TLS Gateway VM and login using the following credentials:

username: tlsgw

password: tlsgw



Step 2 Type ***ifconfig*** to verify the IP address of the Public and Private interfaces as shown below.

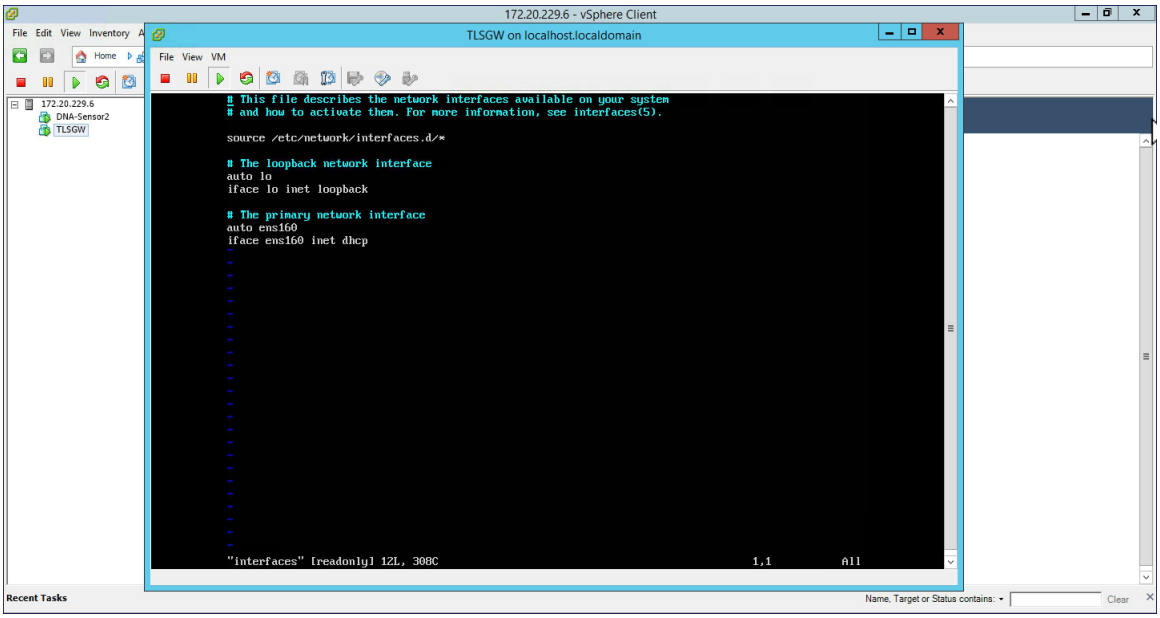


Note ***ens160*** corresponds to the Public network interface and in the above example it has got the IP of ***10.10.10.11*** from the DHCP server. One can also statically assign the IP address which will be shown the steps ahead. Also, there is no interface for the Private network in the ***ifconfig*** output above. We can also manually configure this and is shown in the steps ahead.

Step 3 At the **tlsgw@msp-tls-gw:** prompt type ***sudo bash*** and enter ***tlsgw*** as the [sudo] password for tlsgw.

Step 4 To configure IP address for Public and Private network interface go to ***/etc/network*** directory by typing ***cd /etc/interfaces*** at the shell.

Step 5 Open the ***interfaces*** file using vi editor by typing ***vi interfaces*** at the shell.

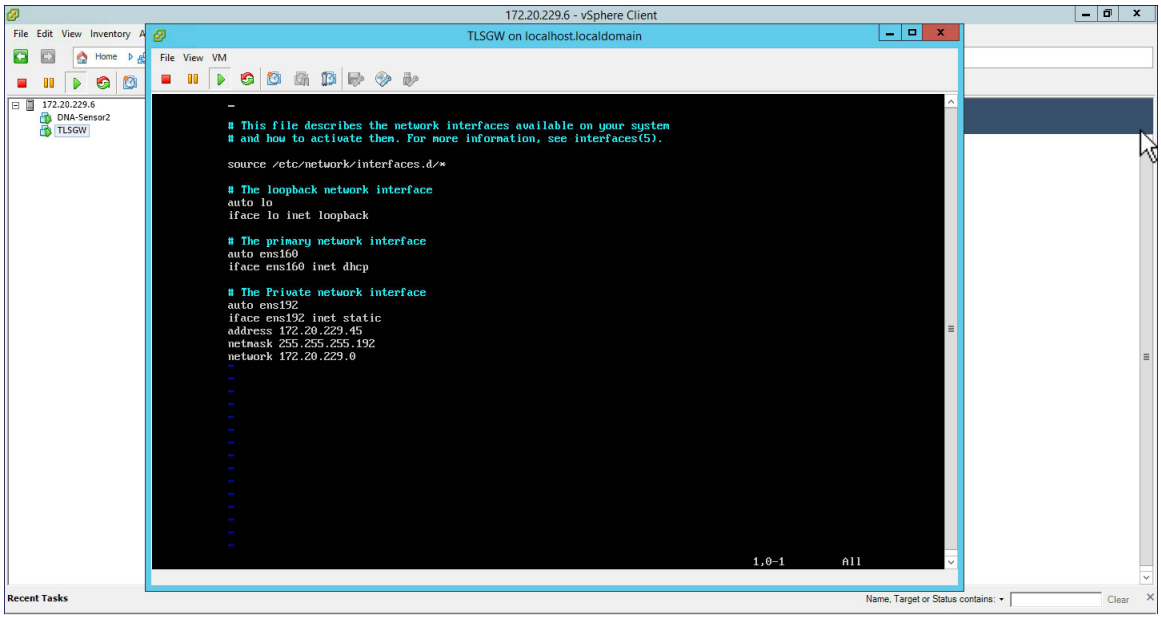


Note : ***ens160*** is Public network interface and is configured for DHCP by default. If you want to statically configure the IP address of Public network interface, replace the ***ens160*** setting with the following as shown below in the example.

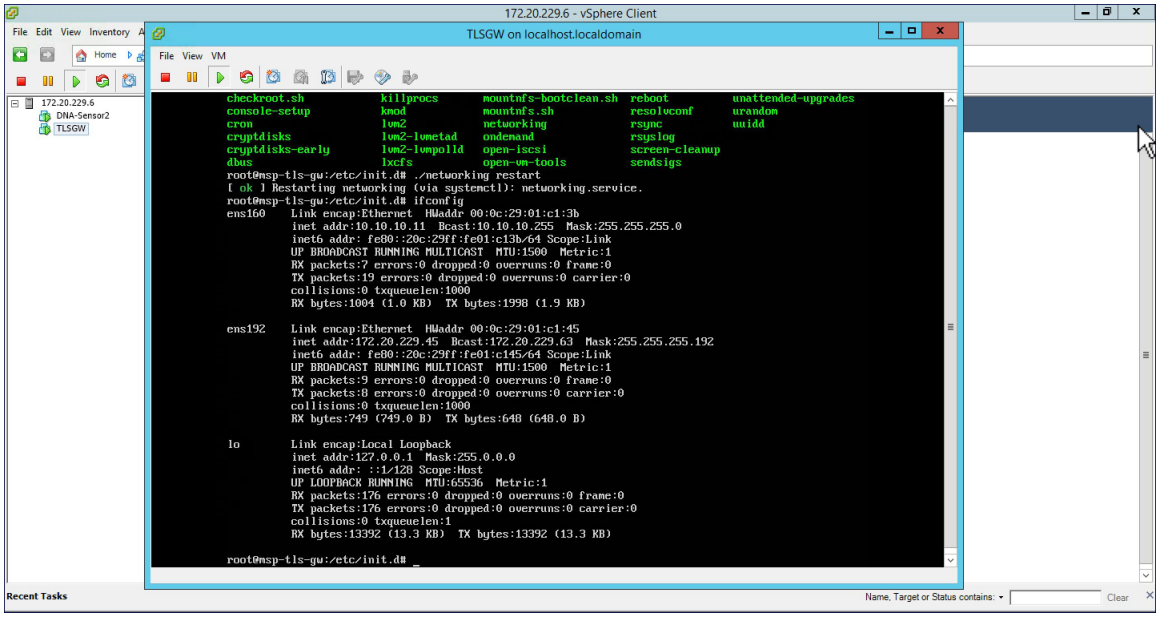
```
auto ens160
iface ens160 inet static
address 10.10.10.11
netmask 255.255.255.0
network 10.10.10.0
```

Step 6 To configure the Private network interface IP address, add the following in the ***interfaces*** file as shown below and save the file.

```
auto ens192
iface ens192 inet static
address 172.20.229.60
netmask 255.255.255.192
network 172.20.229.0
```



Step 7 To restart the network service, go to */etc/init.d* and type *./networking restart* . Now, do a ifconfig and you should see both the Public interface IP address and Private interface IP address. Ping both Public and Private IP address to verify connectivity.



Configure the TLS Gateway configuration file and start the service

Procedure

Step 1 : Go to */opt/cisco/msp-tls-gw/bin/* and edit the *tlsgw_config.txt* with the following:

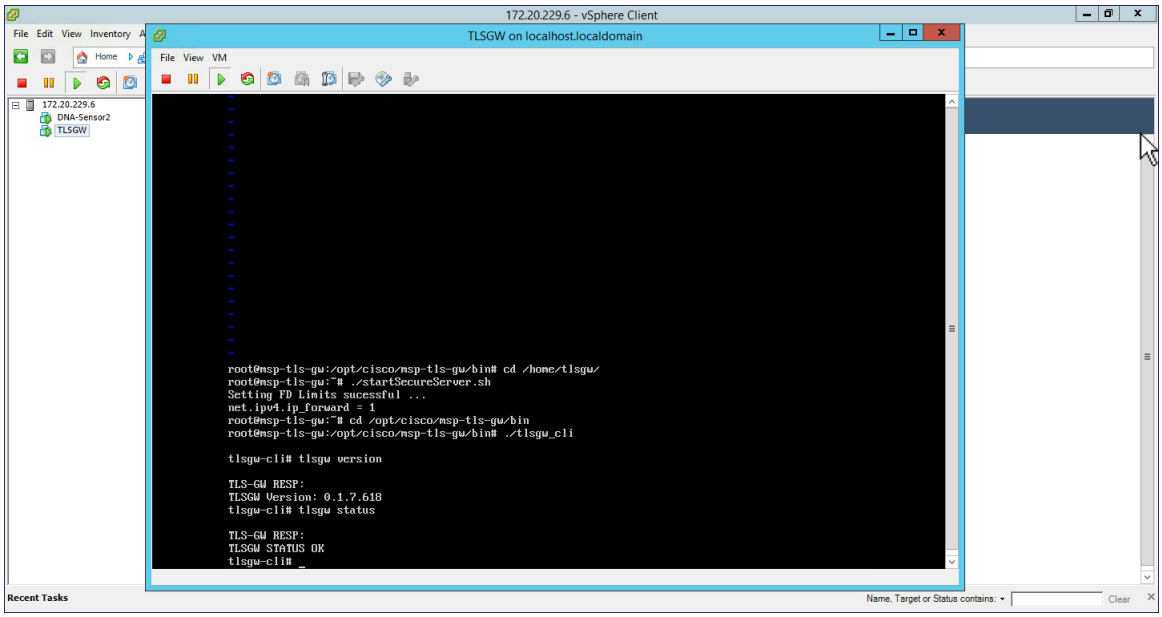
```
server_listening_ipv4_address=10.10.10.11 // Public IP of TLS Gateway
server_listening_port=443 // Port
server_private_ipv4_address=172.20.229.45 // Private IP of TLS Gateway
prefix_subnet=172.20.229.0 // Private IP network of TLS Gateway
prefix_length=26
debug_level=4 // Loglevel for TLS Gateway
dhcp_static_pool_ipv4=20.1.0.0:255.255.0.0 // Local IP pool configured for TLS Client IP
allocation
dpd_interval=60 // Dead Pear Detection timer value for client
rekey_interval=3600 // Rekey timer value  for client
retry_interval=20 // Retry timer value for client
```

Note If you are using a DHCP server behind the TLS Gateway, do not configure dhcp_static_pool_ipv4 in tlsgw_config.txt file. This is because broadcast is sent via Private IP of tls-gw and if DHCP server exists behind the TLS Gateway, it should assign TLS Client an IP address.

Step 2 Save the file.

Step 3 Go to */home/tlsgw* and start the TLS Gateway service with script *./startSecureServer.sh*

Step 4 To verify that the TLS Gateway service is running successfully, go to */opt/cisco/msp-tls-gw/bin/* and run *./tlsgw_cli* as shown below.



Configuring the PSK ID-KEY pair

Configure the Pre Shared Key(PSK) on the TLS Gateway. This will be used by the TLS client on the Master AP to authenticate with the TLS Gateway.

Note A maximum of 3 PSK ID-KEY pairs can be set for TLSGW. PSK-ID can be any character string of length (3-50), PSK password(or key) can be any character string of length (5-256) , Character ':' or 'space' or 'tab' are not allowed for both psk-id and psk-key.

To configure, follow the steps below:

Procedure

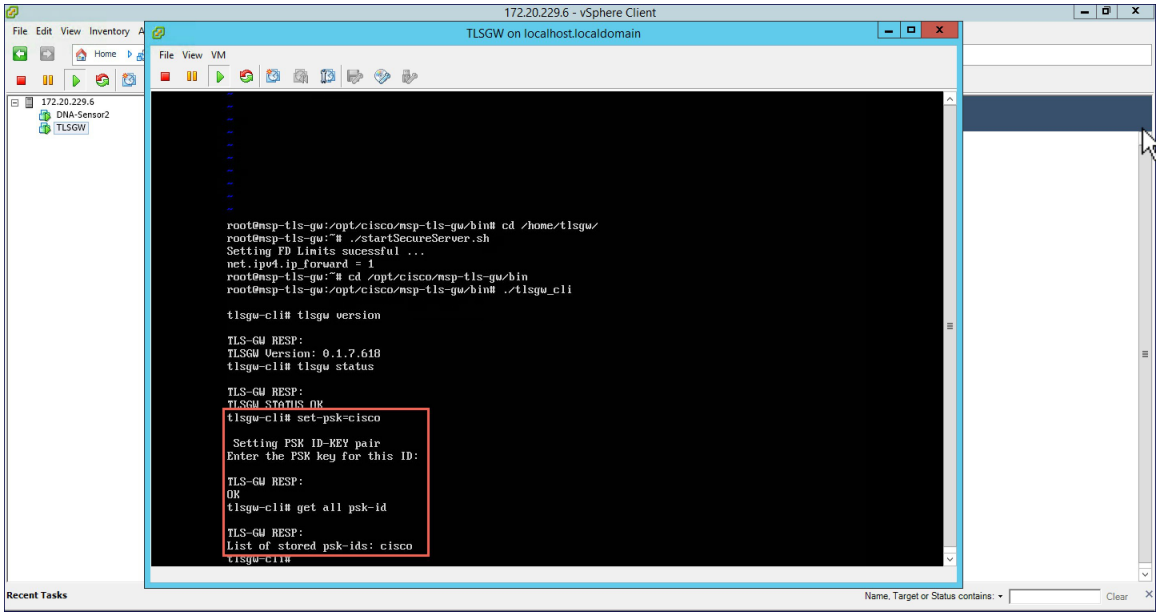
Step 1 : Go to */opt/cisco/msp-tls-gw/bin/* and run *./tlsgw_cli*

Step 2 Configure the PSK using the following CLI:

```
tlsgw-cli# set-psk=cisco
 Setting PSK ID-KEY pair
Enter the PSK key for this ID:
TLS-GW RESP:
OK
```

Step 3 Verify that the PSK ID is configured using the following CLI:

```
tlsgw-cli# get all psk-id
TLS-GW RESP:
List of stored psk-ids: cisco
```



TLS Client

TLS Client is integrated in the AireOS Release 8.6 and is natively present in the code. For TLS client to establish a TLS tunnel with TLS Gateway, Master AP should be able to communicate with the Public IP of the TLS Gateway.

Pre-Requisites for TLS Client

1. Cisco Mobility Express AireOS release 8.6 or higher
2. TLS Gateway Public IP address should be reachable from the Master AP. If TLS Gateway FQDN is used then, TLS_GW FQDN should be configured in the local DNS server, and same DNS server IP should be configuring on ME controller to Resolve the FQDN of TLS Gateway

Configuring TLS Tunnel

There are two ways to configure the TLS Tunnel between TLS Client and TLS Gateway. They are as follows:

Option 1: Zero touch provisioning using Network PnP

During Day 0, one can download the controller configuration from Network PnP. The TLS Tunnel configuration can also be included in the controller configuration file such that after the Master AP downloads the configuration file, reboots, and comes back up, it will automatically establish a TLS Tunnel with the TLS Gateway.

Option 2: Manually configure the TLS Tunnel from WebUI

To configure the TLS Tunnel from the ME WebUI, follow the steps below:

Procedure

Step 1 Switch to Expert View on the Controller WebUI

Step 2 Navigate to Services > TLS from the menu on the left

Step 3 On the TLS Tunnel page, configure the following parameters:

1. Enter the TLS Gateway Public IP address or FQDN
2. Enter the port number. Default is 443
3. Enter the PSK ID
4. Enter the PSK Key
5. Enable RADIUS and SNMP

Note RADIUS would be used for ISE and SNMP would be used for Prime Infrastructure.

Step 4 Click Apply.

Step 5 Finally, enable the TLS Tunnel at the top of the page. If all pre-requisites are met, a tunnel would be created from the Master AP to the Public interface if TLS Gateway.