Secure Overlay and Single IP Configuration

Restrictions

- Secure overlay is supported on:
  - IPSec IKEv2
  - IPv4
  - Pre-shared-key authentication
  - IKE cipher: aes128-sha1-mopd1536
  - ESP cipher: aes128-sha1
  - Local-system-ip unique to each NFVIS device
  - Local-bridge: Wan-br and Wan2-br
- When the guest VM is deployed and single-ip-mode is configured:
  - The configuration requests can be sent in one NETCONF commit.
  - If the configuration requests are sent separately, then commit single-ip-mode creation request first. NFVIS releases the WAN IP address only after the guest device is deployed.
  - If you commit the guest device deployement configuration first, commit the single-ip-mode configuration request before the guest device is active. The guest VM will have conflicting IP address if the commit is delayed.
- When the guest device and single-ip-mode configurations need to be deleted:
  - The two deletion requests can be sent in one NETCONF commit.
  - If the two deletion requests are sent separately,commit the guest device deletion first.

Supported Event Notifications

The following event types are supported

- SECURE_OVERLAY_CREATING
- SECURE_OVERLAY_UP
- SECURE_OVERLAY_DOWN
- SECURE_OVERLAY_DELETE
- SECURE_OVERLAY_ERROR
- SINGLE_IP_START
- SINGLE_IP_ACTIVE
- SINGLE_IP_FAILOVER_START
- SINGLE_IP_FAILOVER_COMPLETE
- SINGLE_IP_DELETE
- SINGLE_IP_ERROR

Secure Overlay over WAN

An overlay is a virtualized network layer on top of the physical network with the support of its infrastructure to provide additional security to the newtork. IPSec is a framework with protocols and algorithms to provide secured data transimission over unprotected or untrusted networks. IPSec secure tunnel is created between two networks to ensure virtual private network communication.

Secure overlay in NFVIS allows IPSec tunnel establishment between NFVIS supporting the vBranch platform and a VPN device in the headend orchestrator. This feature manages traffic only between the headend orchestrator and the vBranch platform. The orchestrator connects to NFVIS through the system IP address and manages NFVIS over the secure tunnel.

NFVIS can be configured with WAN IP, static IP or DHCP IP. NFVIS calls home PnP server, which pushes NFVIS Day-0 configurations including secure overlay configurations. NFVIS establishes IPSec connection between NFVIS and the headend management hub which has IPSec VPN configured. On NFVIS side, the tunnel end point has NFVIS local system IP address. When IPSec tunnel is up Network Services Orchestrator (NSO) solution, can connect to the NFVIS system throught the system IP address and manage NFVIS throught the IPSec tunnnel.

To create secure overlay with the management IP address as local system IP address:

```
configure terminal
secure-overlay myconn local-system-ip-addr 10.0.0.1 local-system-ip-bridge int-mgmt-net
remote-interface-ip-addr 172.16.10.1 remote-system-ip-addr 10.0.0.2 local-psk Admin remote-psk
 Admin
commit
```

Secure Overlay APIs and Commands

Secure Overlay APIs	Secure Overlay Commands
/api/config/secure-overlays	secure-overlay
/api/operational/secure-overlays	

Single IP Address with Secure Overlay

After secure overlay over WAN is established the orchestrator sends requests to configure single-ip-mode and deploy the guest vm that takes the public IP addres.

NFVIS deploys a VM with specific bootstrap and Day-0 configurations. NFVIS notes the IPSec tunnel and releases the public IP address. The VM takes the public IP address when it is active. NFVIS sets up IPSec tunnel again with the remote management hub. After the IPSec tunnel is established, the orchestrator solution can connect with NFVIS through its system IP address and manage NFVIS over the IPSec tunnel.

NFVIS reclaims the WAN IP address if the guest device has:

- Failed to deploy.
- Error state.
- Stopped.

NFVIS releases the WAN IP address if the guest device has:

- Deployed.
- Started.

Single IP and Secure Overlay APIs

Secure Overlay APIs	Secure Overlay Commands
/api/config/single-ip-mode	single-ip-mode
/api/operational/single-ip-mode	

Single IP Address Without Secure Overlay

Note This feature is only supported for wan-br in this NFVIS 3.10.1 release.

To reach NFVIS when secure overlay is not configured, you must first configure the guest device and manage IP addressing. The rest of the functionality, switching IP address between NFVIS and the guest device is the same.