Qualys Network Passive Sensor

Deployment Guide

April 27, 2023

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

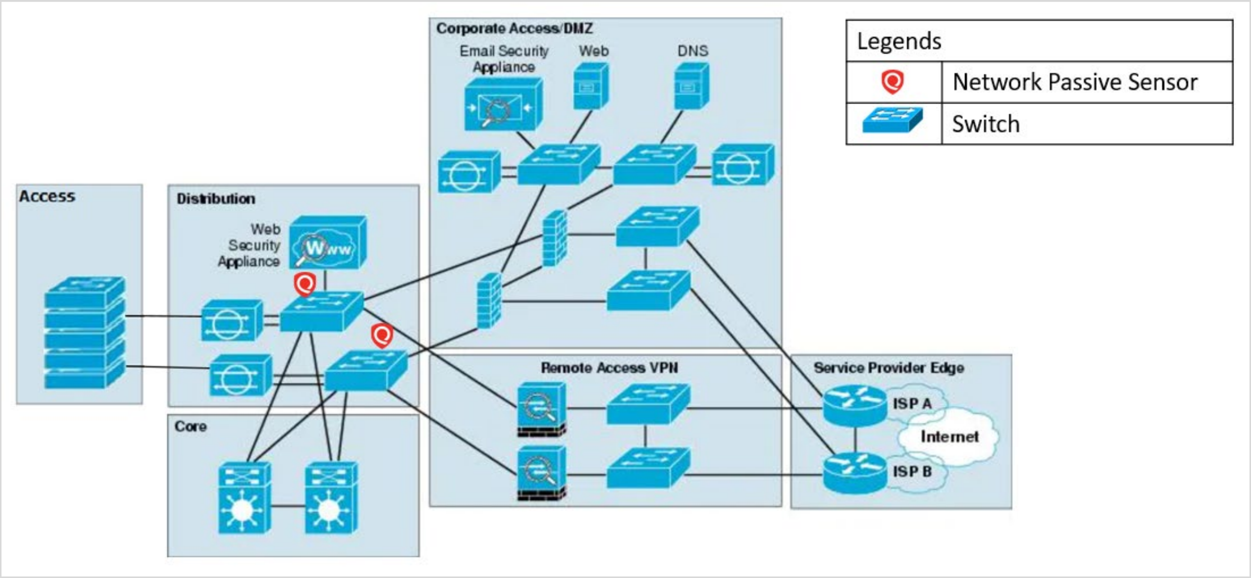
Typical Enterprise Network Topology

For Small Sized Enterprise

To ensure the best asset visibility, deploy Network Passive Sensor closer to the client access, at the distribution switch instead of deploying the passive sensor at the core. Deployments closer to access enable the Network Passive Sensor to see traffic within the client access networks, more specifically enable passive sensor to see MACs within the broadcast domain of a single distribution switch. Deployments of Network Passive Sensor at the core will only see router's MAC and have limited visibility to the traffic within client access networks, resulting in less complete discovery.

Diagram 1 shows typical deployment of network passive sensors in a small sized enterprise. Network Passive Sensors are deployed at distribution layer in the same network.

Diagram 1: Small Enterprise Deployment



For Medium and Large Sized Enterprise

The recommended deployment is to have one Network Passive Sensor in each of the physical locations, closer to the access network with all Network Passive Sensors registered to a single Qualys account.

Alternatively, if deploying Network Passive Sensor in every physical location is not possible then a single Network Passive Sensor can be deployed at one location and traffic from each of the physical locations can be mirrored to the remote location where the sensor is deployed. Refer to Passive Sensor Deployment Scenarios and Port Mirroring for more information on remote mirroring. Depending upon the volume of the network traffic aggregated across sites, use a 1G,4G or 10G appliance.

Diagram 2 shows typical topology of medium sized enterprise. It is a sample three-tier LAN network design for medium enterprises where the access, distribution, and core are all separate layers. Network Passive Sensors are deployed at distribution and core layer for different buildings at same premises.

Diagram 2: Medium Enterprise Deployment

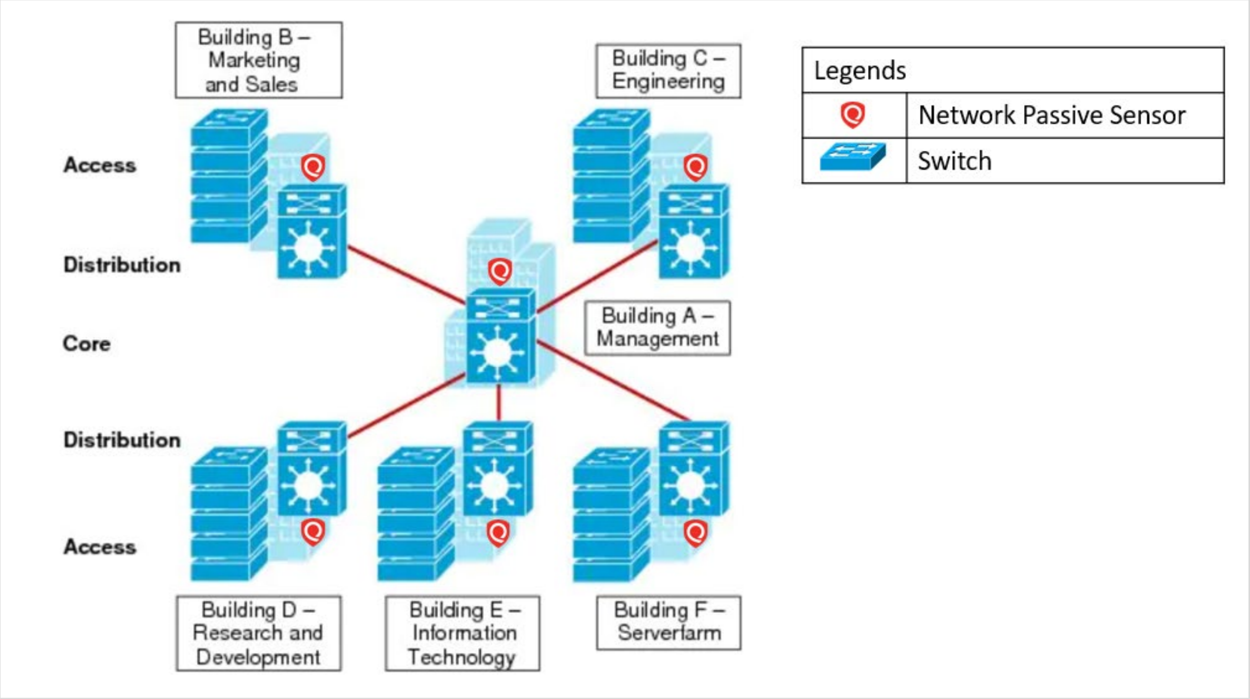
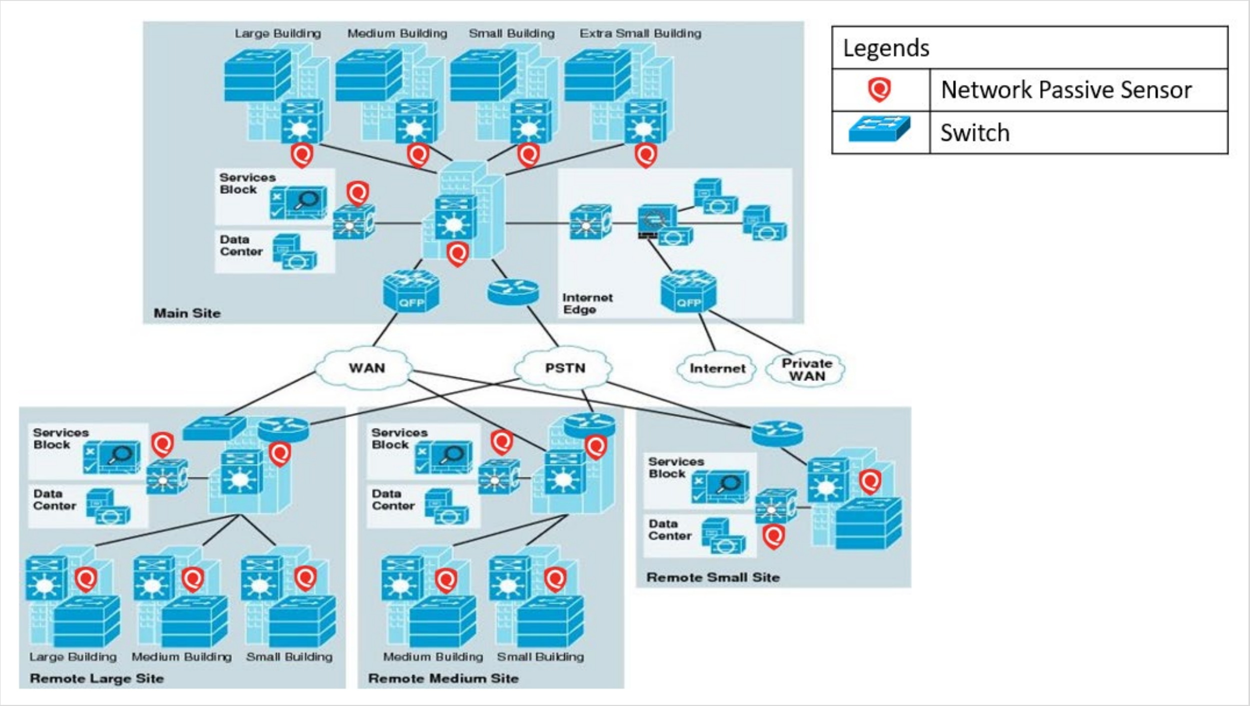


Diagram 3 shows typical topology for large size enterprises with multiple physical locations. Network Passive Sensors are deployed at distribution and core layer of different sites. There are different sites (Main Site, Remote Large Site and Remote Medium Site) connected using WAN.

Diagram 3: Large Enterprise Deployment

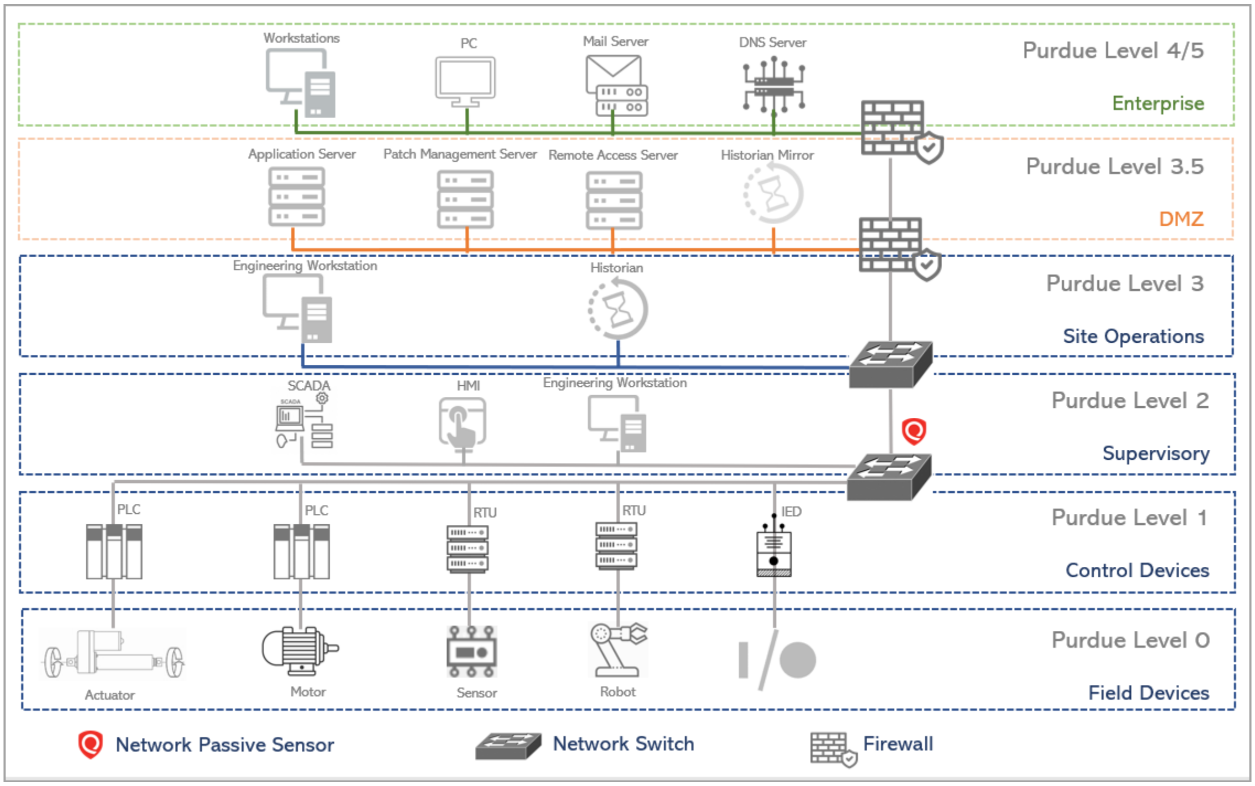


Typical Industrial Network Topology

Many industrial protocols communicate over Layer 2 and vital information related to device identification is seen in the broadcast domain. Hence, it is recommended that get the stream of packet captures from access switches.

A lot of vital device identity information is seen during the communication between the engineering workstation and controller layer. Hence placing a sensor such that we can tap into this layer is critical. Network Passive Sensor should get a copy of traffic between the Scada servers / Operator stations / Engineering workstations to PLC / RTU / IEDs / RIOs etc. Discovery and configuration of the Controllers / Drivers / IOs etc. is most important and hence ensuring that copy of traffic between from EWS like Studio 5000 / TIA portal to controller layer is covered. Typically this is the switch between Purdue level 2 and level 1 devices.

To ensure complete visibility, it is recommended that you should forward mirrored traffic to the network passive sensors for the lowest Purdue level. The Network Passive Sensors also help with high-level detection of OT endpoints and other devices, such as the DMZ, Layer 3.5, Layer 3, and Layer 2 Perdue levels. Therefore, it is recommended to acquire a copy of the mirrored traffic from the high Purdue level of the OT environment to a passive sensor for comprehensive visibility. The Network Passive Sensor can check Windows / Linux / other OS-based assets at a high level. This helps to determine the Qualys Cloud Agent and Qualys Authenticated Scan strategies for these devices.



Passive Sensor Deployment Scenarios and Port Mirroring

Enterprises that use the Qualys Network Passive Sensors to monitor their networks have to feed a copy of their network traffic to the sensor. This can be accomplished by tapping into their network at an appropriate choke point using port mirroring.

There may be different types of network environments and topologies where it may or may not be possible to deploy the passive sensor at the same location as the tap point. Based on these choices different types of port mirroring options have to be exercised.

Note: In case multiple sniffing interfaces of the Network Passive Sensor are used (as available in 4G and 10G appliances) ensure that the mirrored traffic connected to the two interfaces is not coming from networks that have overlapping IP address space.

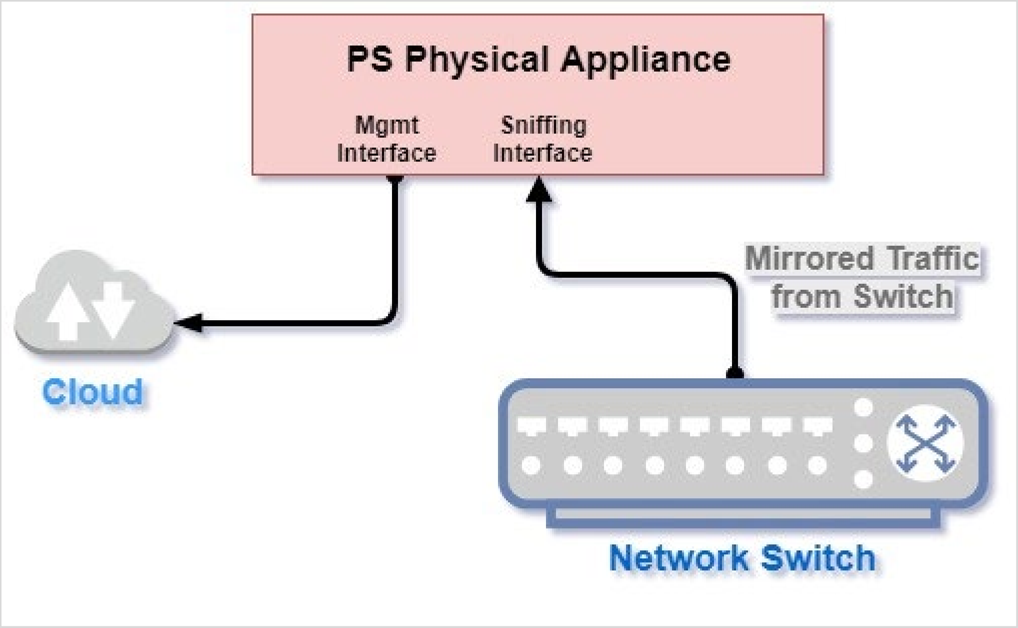
Local SPAN

Switch Port Analyzer (SPAN) is an efficient, high performance traffic monitoring system. It mirrors traffic from one or more interfaces or VLAN to one or more interfaces on the same switch. This method is also called as Local SPAN.

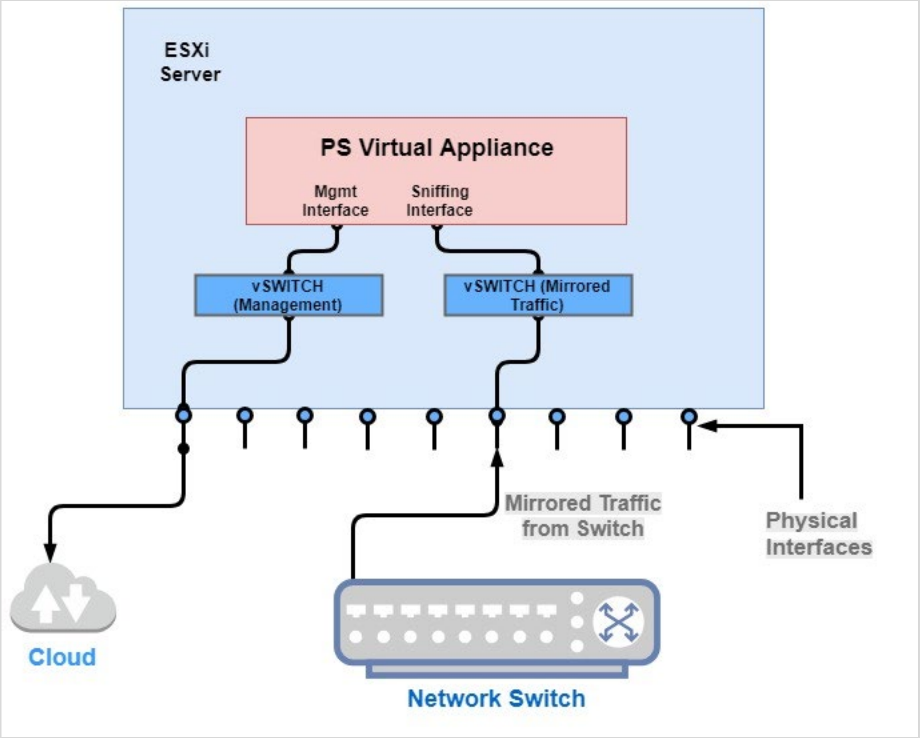
In this method appliance is connected to the switch at the same location as the switch and can be connected directly to one of the switch ports

The switch has a spare port that can be dedicated for mirroring. The passive sensor is physically co-located with the switch and is directly connected to the mirror port. For this the SPAN method should be used.

The following image shows the connectivity for a physical appliance. You'll see that the sniffing interface of the appliance is connected to the network switch and mirrored traffic is fed from the switch to the appliance. The management interface connects to the Qualys Cloud Platform.



The following picture shows connectivity for a virtual appliance. The virtual appliance is supported on the VMware ESXi Server virtualization platform and Microsoft Hyper-V. Again the sniffing interface is fed mirrored traffic from the network switch. The management interface is configured to connect to the Qualys Cloud Platform.



RSPAN

Remote Switch Port Analyzer (RSPAN) provides remote monitoring traffic from source ports distributed over multiple switches. It supports source ports, source VLANs, and destination ports on different switches.

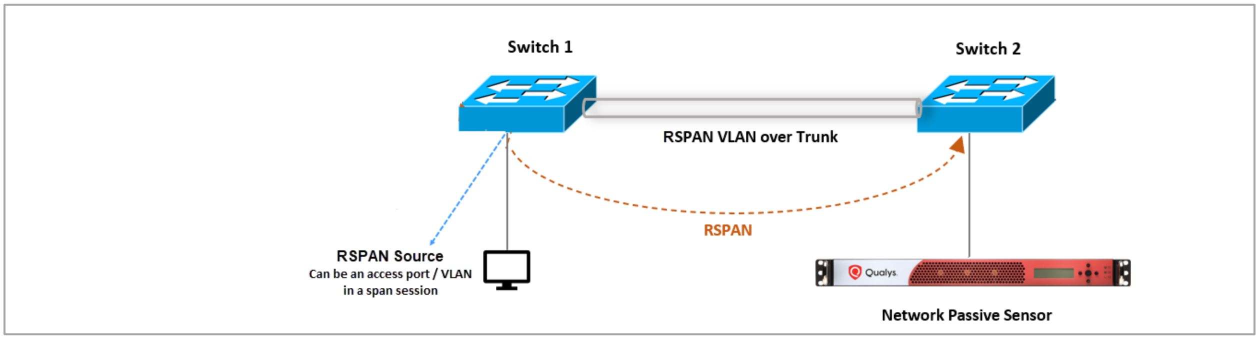
In this method, appliance is in the same Layer 2 (L2) network but cannot be connected directly to the switch.

In all the situations mentioned below, RSPAN can be used. RSPAN method centralizes the mirror traffic from one/multiple Layer 2 switches by mirroring the traffic from the source ports of an RSPAN session to a VLAN that is dedicated for the RSPAN session. This VLAN is then trunked to the other switches allowing the RSPAN session traffic to be transported across multiple switches. On the switch that contains the destination port for the session, traffic from the RSPAN session VLAN is simply mirrored out to the destination port where Network Passive Sensor sniffing interface is connected.

a) Network Passive Sensor is in the same L2 network as the switch and appliance is not physically co-located with the switch *OR*
b) Network Passive Sensor is in the same L2 network as the switch and network has many Layer 2 switches. Then it may not be possible to do local mirroring on each Layer 2 switch and deploy multiple passive sensors connecting to SPAN port of each Layer 2 switch. *OR*
c) Network Passive Sensor is in the same L2 network as the switch and Local SPAN is not possible because all ports on a switch are occupied.

For RSPAN deployment the user must know the CPU utilization of the network switch beforehand. If the switches are already utilizing high CPU then enabling RSPAN may cause the switch to drop packets.

If your network has many Layer 2 switches then it may not be possible to do local mirroring on each Layer 2 switch and deploy multiple passive sensors connecting to SPAN port of each Layer 2 switch. To handle this situation, you need to use RSPAN method to centralize the mirror traffic from various Layer 2 switches. RSPAN works by mirroring the traffic from the source ports of an RSPAN session to a VLAN that is dedicated for the RSPAN session. This VLAN is then trunked to the other switches allowing the RSPAN session traffic to be transported across multiple switches. On the switch that contains the destination port for the session, traffic from the RSPAN session VLAN is simply mirrored out to the destination port where Network Passive Sensor sniffing interface is connected.

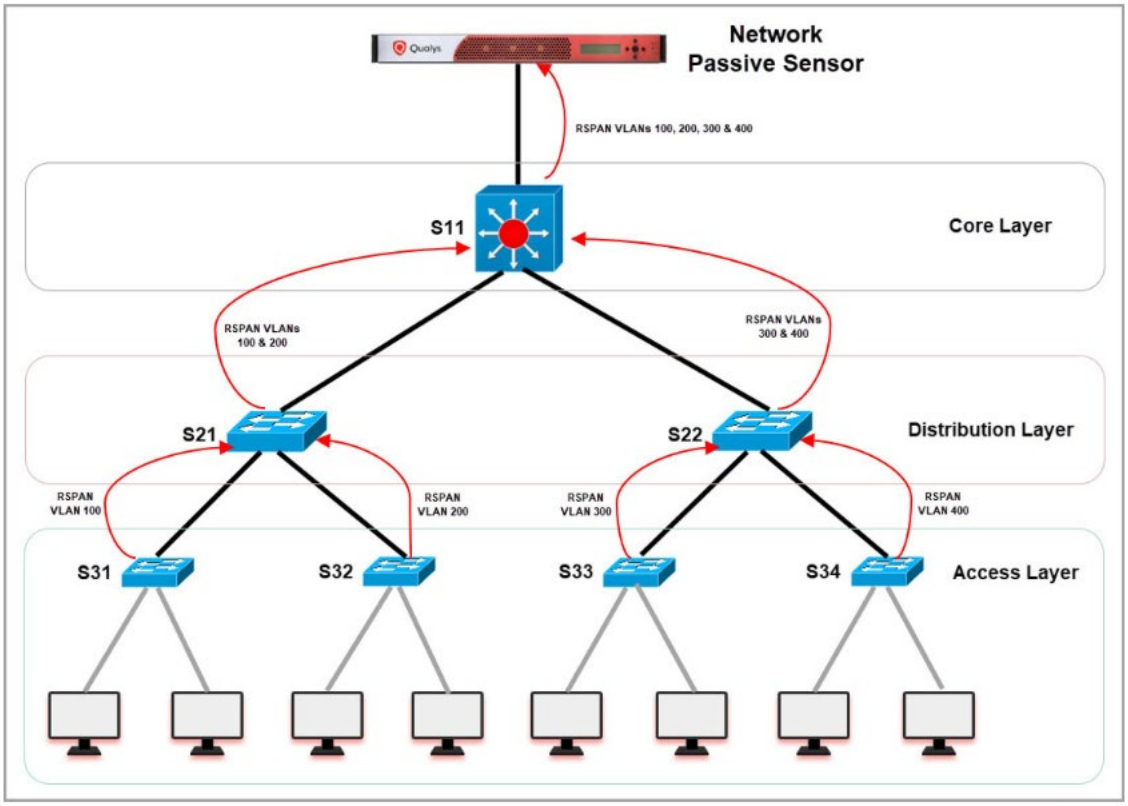


Note: The above diagram shows RSPAN connectivity for Physical Appliance, however the same connectivity works for Virtual Appliance.

Sample RSPAN Configurations

In this section, you'll understand various configurations required on core, distribution, and access layer.

Following diagram illustrates how the mirrored traffic (red arrows) flows from Access layer to distribution layer and from distribution layer to core switch.



Sample Configuration on S31

This configuration helps to mirror the traffic on access layer (user connected) switches.

1. Create RSPAN VLAN

```
vlan 100
name rspan_vlan_100
remote-span
exit
```

2. Configure S31 uplink connected to S21 to allow RSPAN VLAN

```
interface GigabitEthernet1/0/15
switchport mode trunk
switchport trunk allowed vlan add 100
no shutdown
```

3. Mirror traffic of users vlan (for example - vlan 31) connected to configured RSPAN VLAN (vlan 100) on the switch

```
monitor session 1 source vlan 31 rx
monitor session 1 destination remote vlan 100
```

Sample Configuration on S21

This configuration helps to create RSPAN VLAN and allows RSPAN traffic to pass through trunk ports for distribution layer switches.

1. Create RSPAN VLAN

```
vlan 100
name rspan_vlan_100 remote-span
```

```
exit
vlan 200
name rspan_vlan_200 remote-span
exit
```

2. Configure S21 interface connected to S31 to allow RSPAN VLAN 100

```
interface GigabitEthernet1/0/19
switchport mode trunk
switchport trunk allowed vlan add 100
no shutdown
```

3. Configure S21 uplink connected to S11 to allow RSPAN VLAN

```
interface GigabitEthernet1/0/20
switchport mode trunk
switchport trunk allowed vlan add 100, 200
no shutdown
```

Sample Configuration on S11
This configuration helps to create RSPAN VLAN and allows RSPAN traffic to pass through trunk ports for core switches.

1. Create RSPAN VLAN

```
vlan 100
name rspan_vlan_100
remote-span
exit
vlan 200
name rspan_vlan_200
remote-span
exit
vlan 300
name rspan_vlan_300
remote-span
exit
vlan 400
name rspan_vlan_400
remote-span
exit
```

2. Configure S11 interface connected to S21 switch to allow RSPAN VLANs 100,200

```
interface GigabitEthernet1/0/24
switchport mode trunk
switchport trunk allowed vlan add 100, 200
no shutdown
```

3. Configure S11 interface connected to NPS sniffing port to allow all RSPAN VLANs traffic

```
interface GigabitEthernet1/0/25
switchport mode trunk
switchport trunk allowed vlan add 100, 200,300,400
no shutdown
```

VTP Configurations

VTP configuration can be used to centralize the RSPAN VLAN configurations on Cisco switches.

For example, configure S11 as VTP server and remaining switches as VTP clients. Just adding RSPAN VLANs in S11 will advertise the new VLAN configuration to all other switches which are in VTP client mode and in the same VTP domain.

1. Sample VTP server configuration on S11

   ```
   (config)#vtp domain test
   (config)#vtp mode server
   (config)#vtp password mypassword
   (config)#exit
   ```

2. Sample VTP client configuration on other switches:

   ```
   (config)#vtp domain test
   (config)#vtp mode client
   (config)#vtp password mypassword
   (config)#exit
   ```

3. Sample config for creating RSPAN VLANs on S11

   ```
   vlan 100
   name rspan_vlan_100
   remote-span
   exit
   vlan 200
   name rspan_vlan_200
   remote-span
   exit
   vlan 300
   name rspan_vlan_300
   remote-span
   exit
   vlan 400
   name rspan_vlan_400
   remote-span
   exit
   ```

4. Now all other switches will receive RSPAN VLAN configurations from S11 (vtpserver). You can verify the configurations of VLANs using 'show vlan' command.

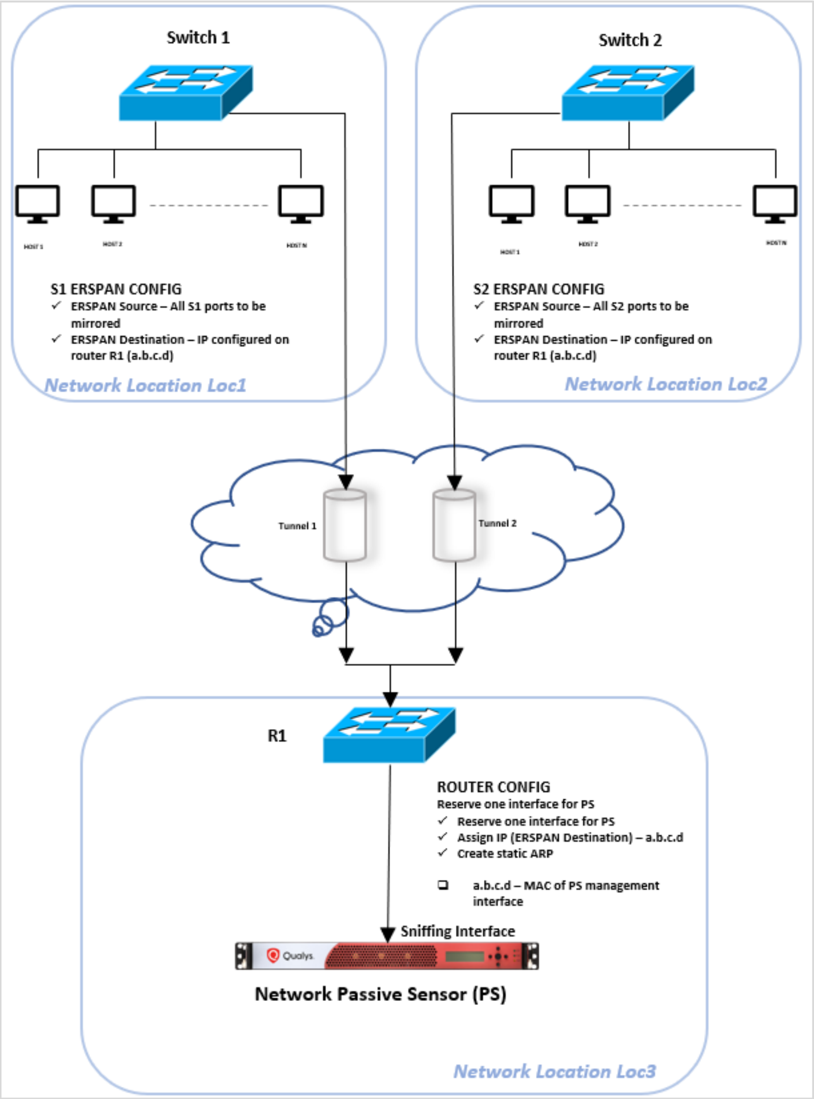
ERSPAN

In order to monitor traffic across a WAN or different networks, use Encapsulated Remote Switch Port Analyzer (ERSPAN). The ERSPAN feature supports source ports, source VLANs, and destination ports on different switches, which provides remote monitoring of multiple switches across your network.

Some enterprises may have a requirement to passively monitor their networks, including those remotely located, and it may not be possible to install a sensor in each of the remote locations. To cater to such requirements, Encapsulated Remote Switch Port Analyzer (ERSPAN) should be used. ERSPAN allows mirrored traffic to be encapsulated and transported over the L3 network to a remote destination. This requires that each location have switches having ERSPAN capability and the switches be configured to tunnel mirror traffic to a destination L3 switch/router interface.

In this method, the appliance is deployed at a remote location that is reachable over the Layer 3 (L3) network.

Following diagram shows a sample topology that explains the above deployment scenario:


Switch 1
HOST 1
HOST 2
HOST N
S1 ERSPAN CONFIG
✓ ERSPAN Source – All S1 ports to be mirrored
✓ ERSPAN Destination – IP configured on router R1 (a.b.c.d)
Network Location Loc1
Switch 2
HOST 1
HOST 2
HOST N
S2 ERSPAN CONFIG
✓ ERSPAN Source – All S2 ports to be mirrored
✓ ERSPAN Destination – IP configured on router R1 (a.b.c.d)
Network Location Loc2
Tunnel 1
Tunnel 2
R1
ROUTER CONFIG
Reserve one interface for PS
✓ Reserve one interface for PS
✓ Assign IP (ERSPAN Destination) – a.b.c.d
✓ Create static ARP
❑ a.b.c.d – MAC of PS management interface
Sniffing Interface
Qualys
Network Passive Sensor (PS)
Network Location Loc3

There are 3 networks seen in the diagram - Loc1, Loc2 and Loc3. The passive sensor appliance is deployed at location Loc3.

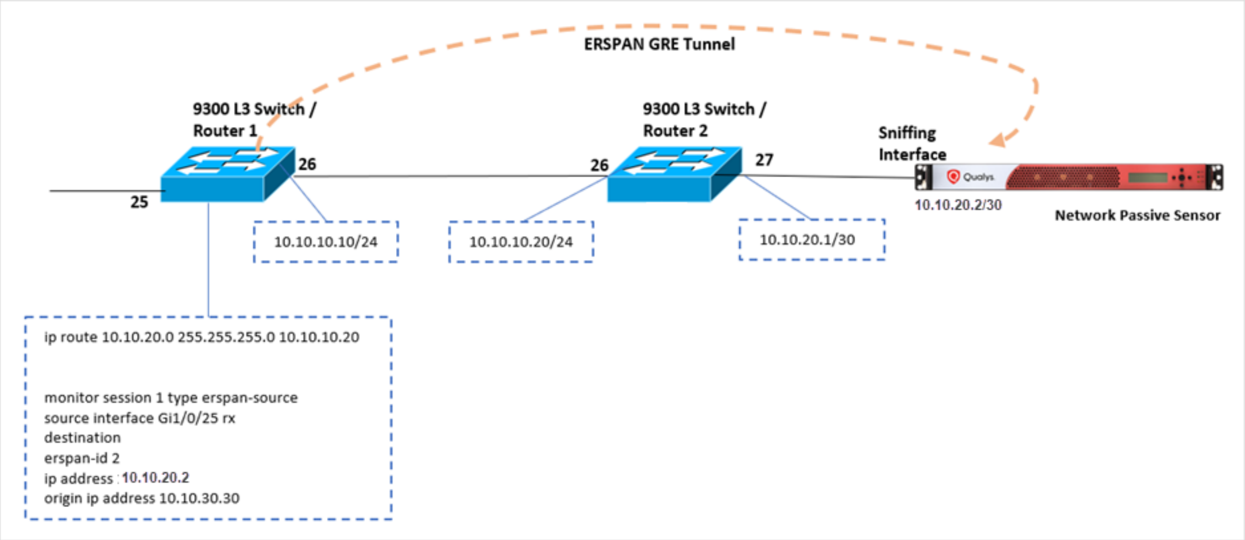
Switches S1 and S2 at Location Loc1 and Loc2 respectively, have to support ERSPAN source capability.

At location Loc3, on Router R1, reserve an interface and connect it to the sniffing interface of PS.

Configure switch S1 with ERSPAN source and destination. Similarly configure S2. On Router R1, reserve an interface and configure it with an IP address that serves as the ERSPAN destination for S1 and S2. For details see sample configurations done for Cisco catalyst 9300 in the subsequent section.

Sample ERSPAN Configurations for Physical Appliance

Sample Configurations for Cisco Catalyst 9300 Switch



```
ip route 10.10.20.0 255.255.255.0 10.10.10.20


monitor session 1 type erspan-source
source interface Gi1/0/25 rx
destination
erspan-id 2
ip address 10.10.20.2
origin ip address 10.10.30.30
```

a) 9300 L3 Switch/Router 1 config

1. Assign an IP address to interface Gi1/0/26

```
interface GigabitEthernet1/0/26
no switchport
ip address 10.10.10.10 255.255.255.0
```

2. Add routes to send ERSPAN traffic to PS sniffing interface

```
ip route 10.10.20.0 255.255.255.0 10.10.10.20
```

3. Add ERSPAN-source configuration and define source interface & src, dst IP address of GRE tunnel

```
monitor session 1 type erspan-source
source interface Gi1/0/25 rx
destination
erspan-id 2
ip address 10.10.20.2
origin ip address 10.10.30.30
```

b) 9300 L3 Switch/Router 2 config

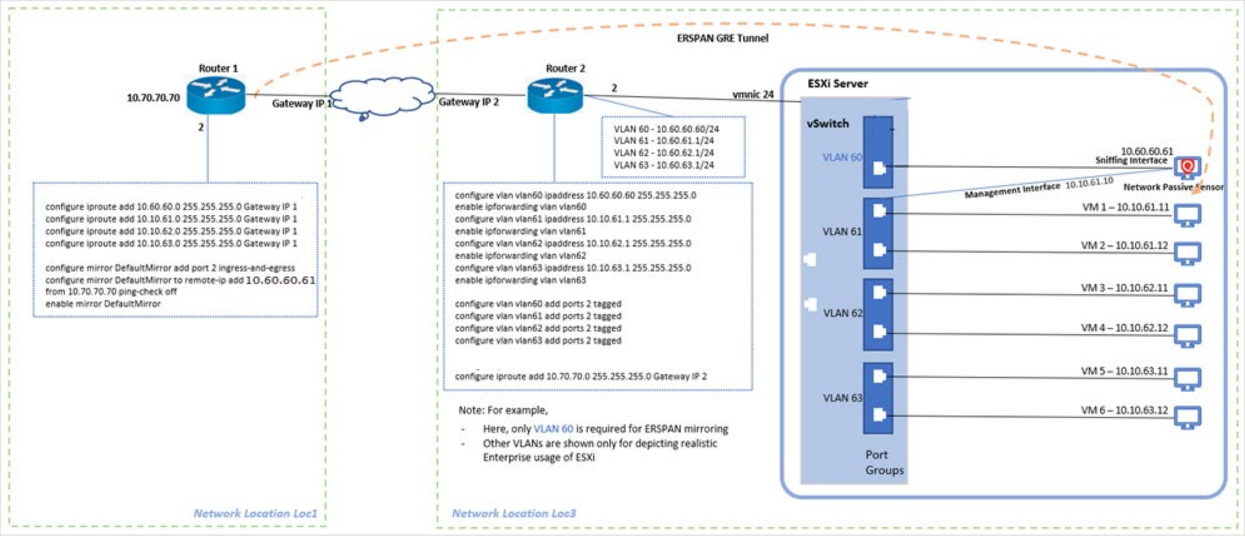
1. Assign IP address to interface Gi1/0/26

```
interface GigabitEthernet1/0/26
no switchport
ip address 10.10.10.20 255.255.255.0
```

2. Assign IP address to interface Gi1/0/27

```
interface GigabitEthernet1/0/27
no switchport
ip address 10.10.20.1 255.255.255.252
no keepalive
no cdp enable
```

Sample ERSPAN Configurations for Virtual Appliance



```
configure iproute add 10.60.60.0 255.255.255.0 Gateway IP 1
configure iproute add 10.10.61.0 255.255.255.0 Gateway IP 1
configure iproute add 10.10.62.0 255.255.255.0 Gateway IP 1
configure iproute add 10.10.63.0 255.255.255.0 Gateway IP 1

configure mirror DefaultMirror add port 2 ingress-and-egress
configure mirror DefaultMirror to remote-ip add 10.60.60.61
from 10.70.70.70 ping-check off
enable mirror DefaultMirror
```

```
configure vlan vlan60 ipaddress 10.60.60.60 255.255.255.0
enable ipforwarding vlan vlan60
configure vlan vlan61 ipaddress 10.10.61.1 255.255.255.0
enable ipforwarding vlan vlan61
configure vlan vlan62 ipaddress 10.10.62.1 255.255.255.0
enable ipforwarding vlan vlan62
configure vlan vlan63 ipaddress 10.10.63.1 255.255.255.0
enable ipforwarding vlan vlan63

configure vlan vlan60 add ports 2 tagged
configure vlan vlan61 add ports 2 tagged
configure vlan vlan62 add ports 2 tagged
configure vlan vlan63 add ports 2 tagged


configure iproute add 10.70.70.0 255.255.255.0 Gateway IP 2
```

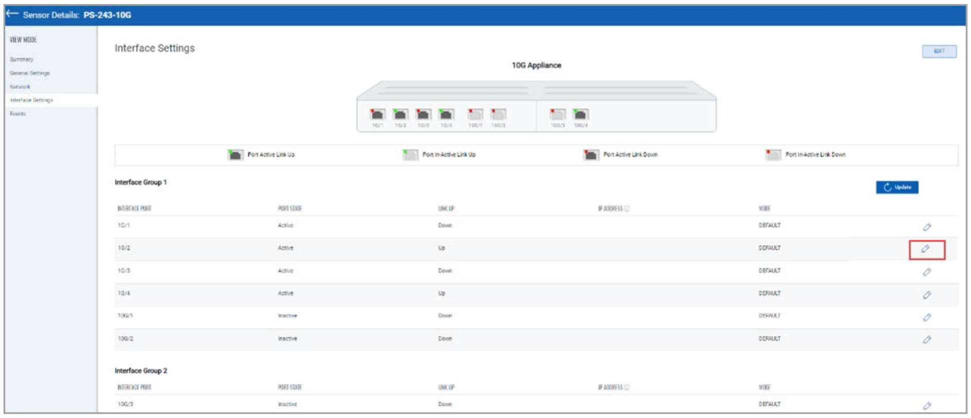
Note: For example,

- Here, only VLAN 60 is required for ERSPAN mirroring
- Other VLANs are shown only for depicting realistic Enterprise usage of ESXi

Assigning/Removing IP Addresses to the Appliance Sniffing Interfaces

To assign or remove the IP address from the appliance sniffing interface, go to the **Sensors** tab and from the Quick Actions menu of a sensor, click **View Details** > **Interface Settings**. Alternatively, you can click on the sensor to go directly to the sensor view details page.

Click the **edit** icon of the desired sniffing interface, as shown in the following screenshot.



Interface Settings

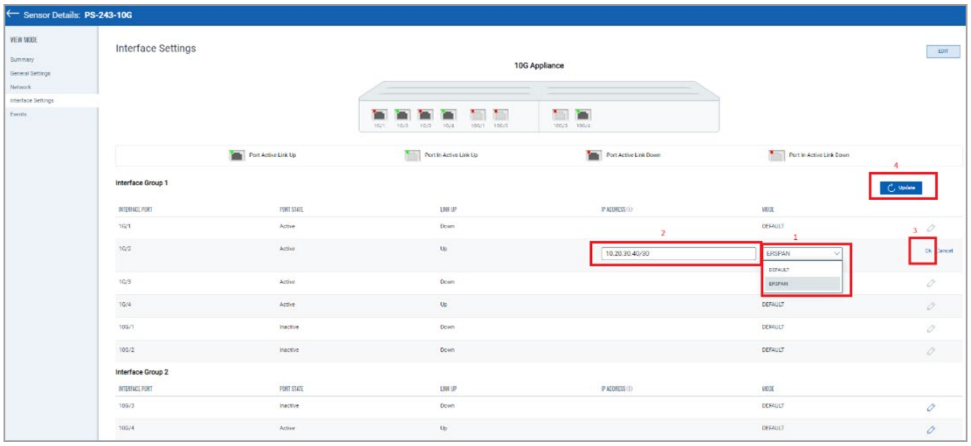
Interface Group 1

INTERFACE PORT	PORT STATE	LINK UP	IP ADDRESS	MODE
1G/1	Active	Down		DEFAULT
1G/2	Active	Up		DEFAULT
1G/3	Active	Down		DEFAULT
1G/4	Active	Up		DEFAULT
10G/1	Inactive	Down		DEFAULT
10G/2	Inactive	Down		DEFAULT

Interface Group 2

INTERFACE PORT	PORT STATE	LINK UP	IP ADDRESS	MODE
10G/3	Inactive	Down		DEFAULT

Select **ERSPAN** mode and assign IP to the interface along with subnet mask.
Click **Ok** > Click **Update** to save the configuration. Refer to the following screenshot.



Interface Settings

Interface Group 1

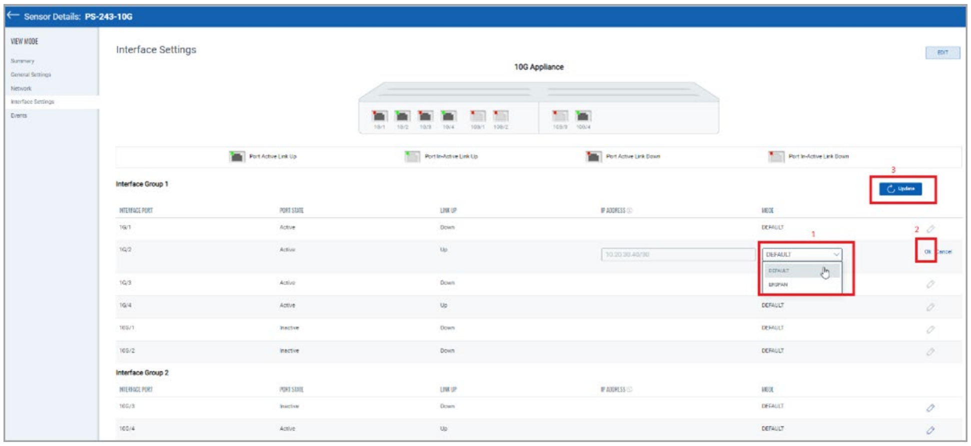
INTERFACE PORT	PORT STATE	LINK UP	IP ADDRESS	MODE
1G/1	Active	Down		DEFAULT
1G/2	Active	Up	10.20.30.40/30	ERSPAN DEFAULT ERSPAN
1G/3	Active	Down		
1G/4	Active	Up		DEFAULT
10G/1	Inactive	Down		DEFAULT
10G/2	Inactive	Down		DEFAULT

Interface Group 2

INTERFACE PORT	PORT STATE	LINK UP	IP ADDRESS	MODE
10G/3	Inactive	Down		DEFAULT
10G/4	Active	Up		DEFAULT

To remove the IP Address from the sniffing interface, click the **edit** icon of the desired sniffing interface. As shown in the above screenshot.

Select **DEFAULT** mode, click **Ok** > Click **Update** to save the configuration. Refer to the following screenshot.



Interface Settings

Interface Group 1

INTERFACE PORT	PORT STATE	LINK UP	IP ADDRESS	MODE
1G/1	Active	Down		DEFAULT
1G/2	Active	Up	10.20.30.40/30	DEFAULT DEFAULT ERSPAN
1G/3	Active	Down		
1G/4	Active	Up		DEFAULT
10G/1	Inactive	Down		DEFAULT
10G/2	Inactive	Down		DEFAULT

Interface Group 2

INTERFACE PORT	PORT STATE	LINK UP	IP ADDRESS	MODE
10G/3	Inactive	Down		DEFAULT
10G/4	Active	Up		DEFAULT

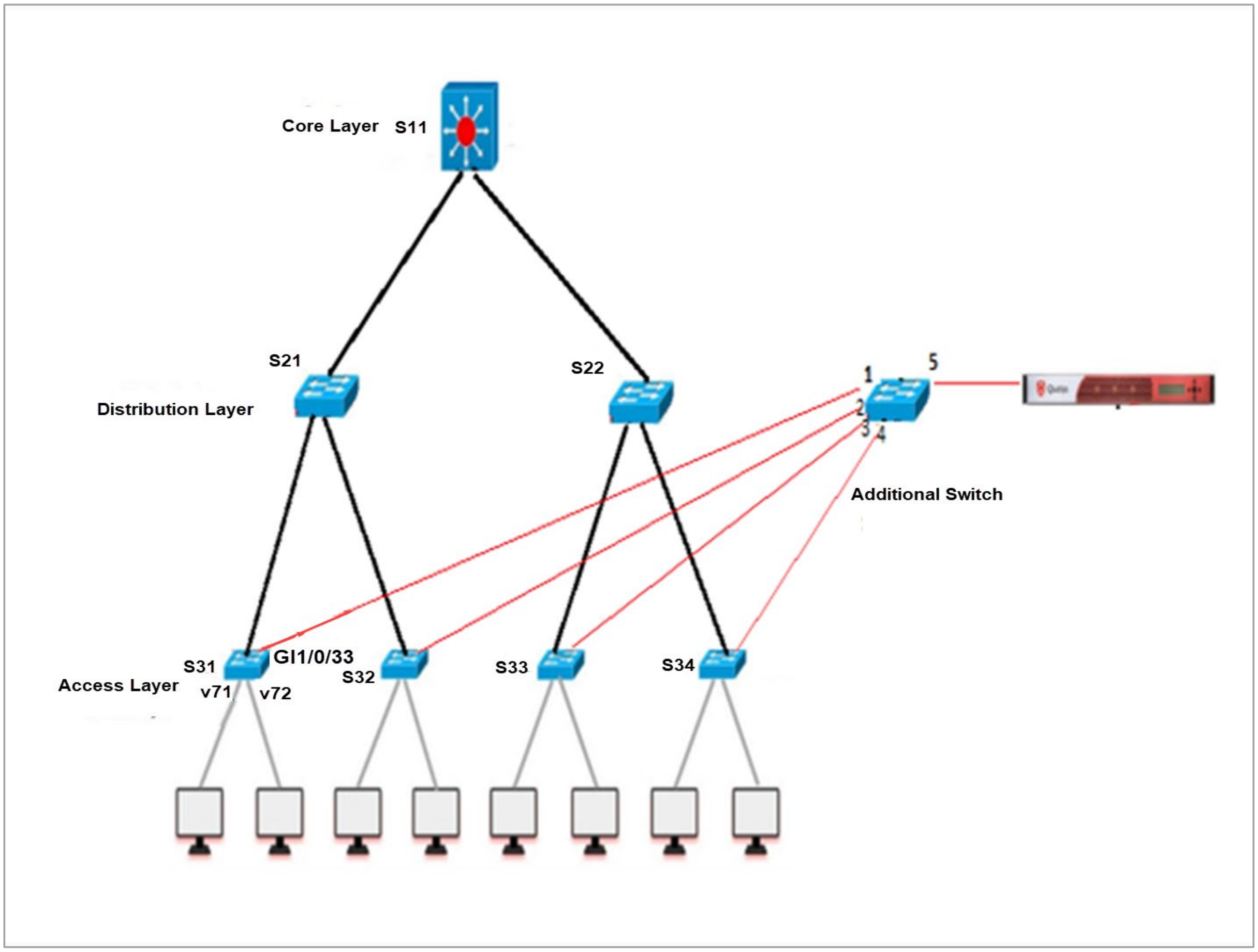
Important:

- For the 10G appliance model (QPS-10G-0404-B1), the interface needs to be active before assigning an IP address to the sniffing interface.

- The Network Passive Sensor (NPS) appliance will reboot once after adding/editing/deleting the IP address of the sniffing interface.

Note: The Network Passive Sensor (NPS) appliance version 1.3.6-12 supports assigning IP addresses on the sniffing interface. So before assigning an IP address to the sniffing interface, ensure that the NPS appliance version is 1.3.6-12 or above.

How to Extend Local Span Through Multiple Intermediate Switches to a Sniffer That is Multiple Switch Hops Away Without Using RSPAN.



1) Connect one additional switch in the network which supports the local span configuration.

2) Do a local span on the access layer switches.

- **E.g.:** config on S31 Switch:

```
monitor session 1 source vlan 71 - 72 both
monitor session 1 destination interface Gi1/0/33
```

3) Connect span ports of access layer switches to the additional switch.

4) Choose vlan’s that are not used in the network & configure on the additional switch.

- **E.g.:** config on the additional switch:

```
Interface Gi1/0/1
Switchport access vlan 81
Switchport mode access
Spanning-tree bpdufilter enable

Interface Gi1/0/2
Switchport access vlan 82
Switchport mode access
Spanning-tree bpdufilter enable
```

5) Do a local span on the additional switch.

- **E.g.:**

```
monitor session 1 source interface Gi1/0/1 – 4 both
monitor session 1 destination interface Gi1/0/5
```

Or

```
monitor session 1 source vlan 81-84 rx
monitor session 1 destination interface Gi1/0/5
```

6) Connect the span port of the additional switch to the NPS sniffing interface.

Note: This technique can be used to pass through multiple intermediate switches with each switch configured similar to the extra switch introduced in this diagram.

This mechanism of chaining multiple switches with local spans can terminate into a switch that supports RSPAN, and from there onwards, the RSPAN documentation can be used to bring the span traffic to PS.

How to Sniff the Traffic of VM's in the Standalone Esxi

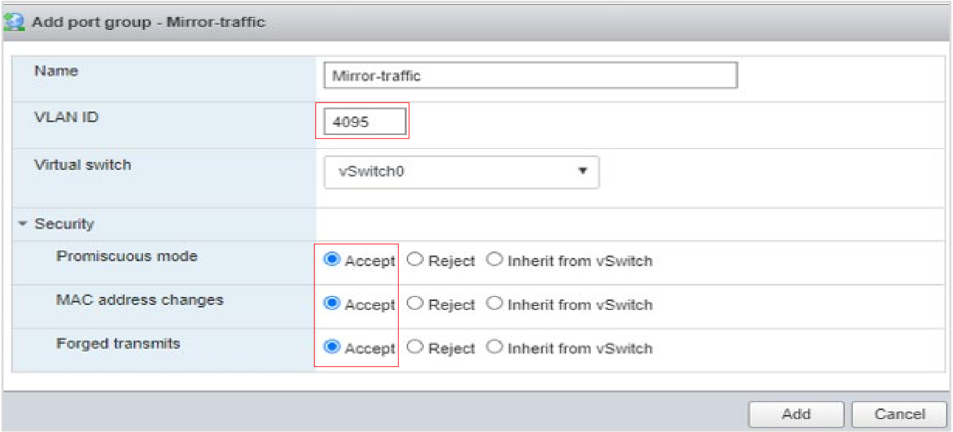
1) Create a new port-group (e.g. Mirror-traffic) and select vswitch for sniffing traffic of VM's on standalone esxi. See the IMG 01.

2) Enable promiscuous mode, mac address changes & forged transmits on newly created port-group. See the IMG 01.

3) Allow all vlans (i.e. vlan id 4095) on the newly created port-group. See the IMG 01.

4) Connect PS sniffing interface to newly created port-group. See the IMG 03.

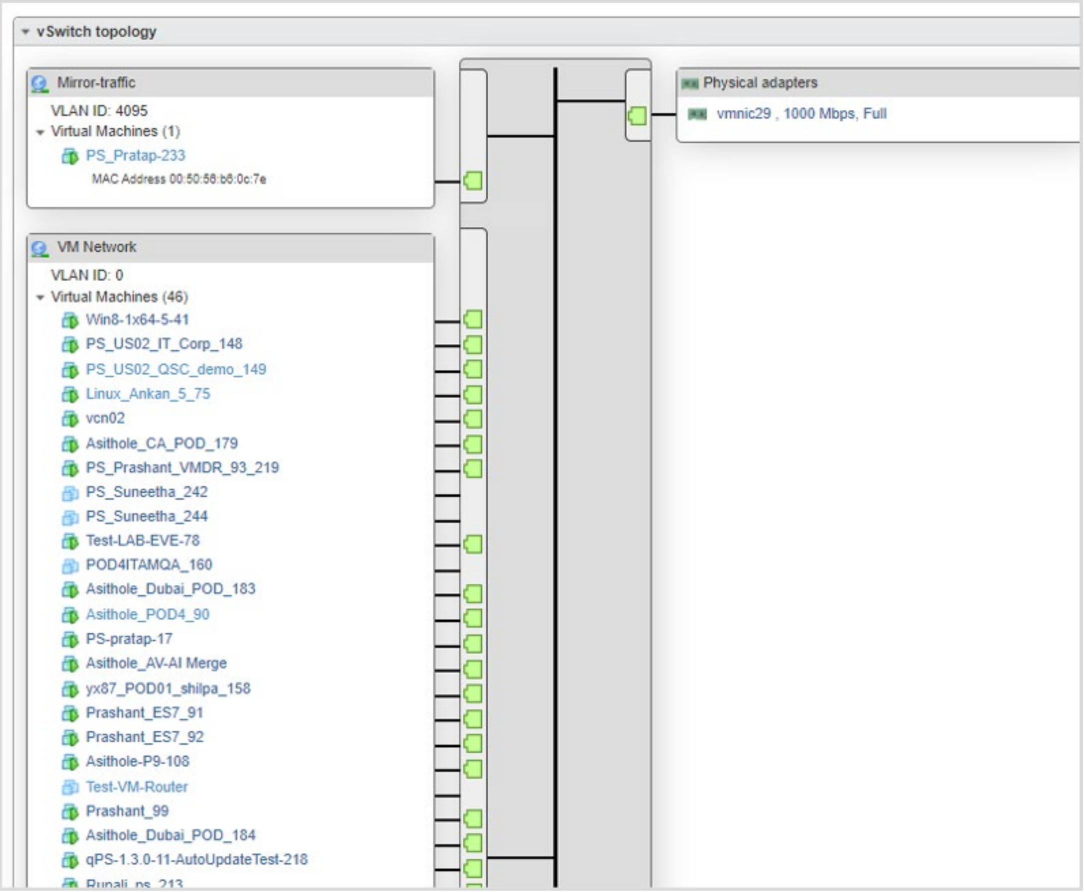
IMG: 01



Add port group - Mirror-traffic

Name	Mirror-traffic
VLAN ID	4095
Virtual switch	vSwitch0 ▾
▾ Security	
Promiscuous mode	● Accept ○ Reject ○ Inherit from vSwitch
MAC address changes	● Accept ○ Reject ○ Inherit from vSwitch
Forged transmits	● Accept ○ Reject ○ Inherit from vSwitch

IMG: 02



vSwitch topology

Mirror-traffic

VLAN ID: 4095

Virtual Machines (1)

- PS_Pratap-233
  - MAC Address 00:50:56:b6:0c:7e

VM Network

VLAN ID: 0

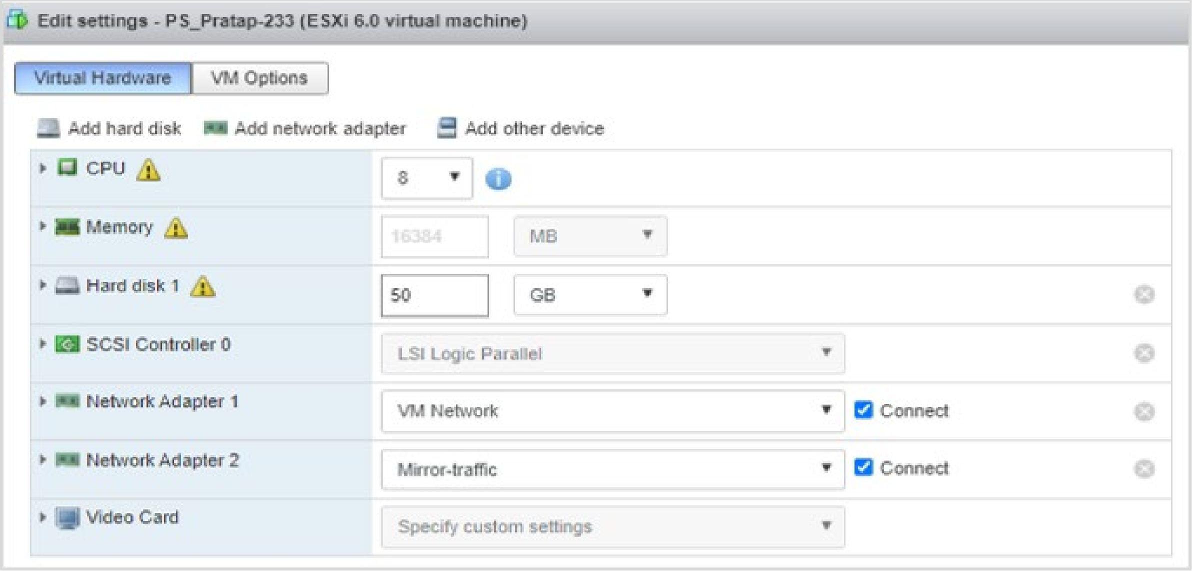
Virtual Machines (46)

- Win8-1x64-5-41
- PS_US02_IT_Corp_148
- PS_US02_QSC_demo_149
- Linux_Ankan_5_75
- vcn02
- Asithole_CA_POD_179
- PS_Prashant_VMDR_93_219
- PS_Suneetha_242
- PS_Suneetha_244
- Test-LAB-EVE-78
- POD4ITAMQA_160
- Asithole_Dubai_POD_183
- Asithole_POD4_90
- PS-pratap-17
- Asithole_AV-AI Merge
- yx87_POD01_shilpa_158
- Prashant_ES7_91
- Prashant_ES7_92
- Asithole-P9-108
- Test-VM-Router
- Prashant_99
- Asithole_Dubai_POD_184
- qPS-1.3.0-11-AutoUpdateTest-218
- Rupali_ps_213

Physical adapters

- vmnic29 , 1000 Mbps, Full

IMG: 03



Edit settings - PS_Pratap-233 (ESXi 6.0 virtual machine)

CPU ⚠	8
Memory ⚠	16384 MB
Hard disk 1 ⚠	50 GB
SCSI Controller 0	LSI Logic Parallel
Network Adapter 1	VM Network ☑ Connect
Network Adapter 2	Mirror-traffic ☑ Connect
Video Card	Specify custom settings

Backup and restore of PS VM image:

It is not recommended to backup NPS VM images to be restored later. If the VM fails to boot due to corruption, contact Qualys support instead of re-deploying the PS VM. The NPS services on Qualys cloud account retain the sensor configuration and apply it to the appliance on reboot.

Deployment of Virtual Network Passive Sensors to Support Exceeding Volume of Traffic

Qualys Virtual Network Passive Sensor is a virtual machine that can perform deep network packet inspection by listening to real-time network traffic. This can be accomplished by tapping to an appropriate choke point in the network using either VLAN mirroring or Port mirroring. Qualys recommends configuring VLAN mirroring.

A single Qualys Virtual Network Passive Sensor with 16 processor cores and 24GB memory can process 2 Gbps network traffic.

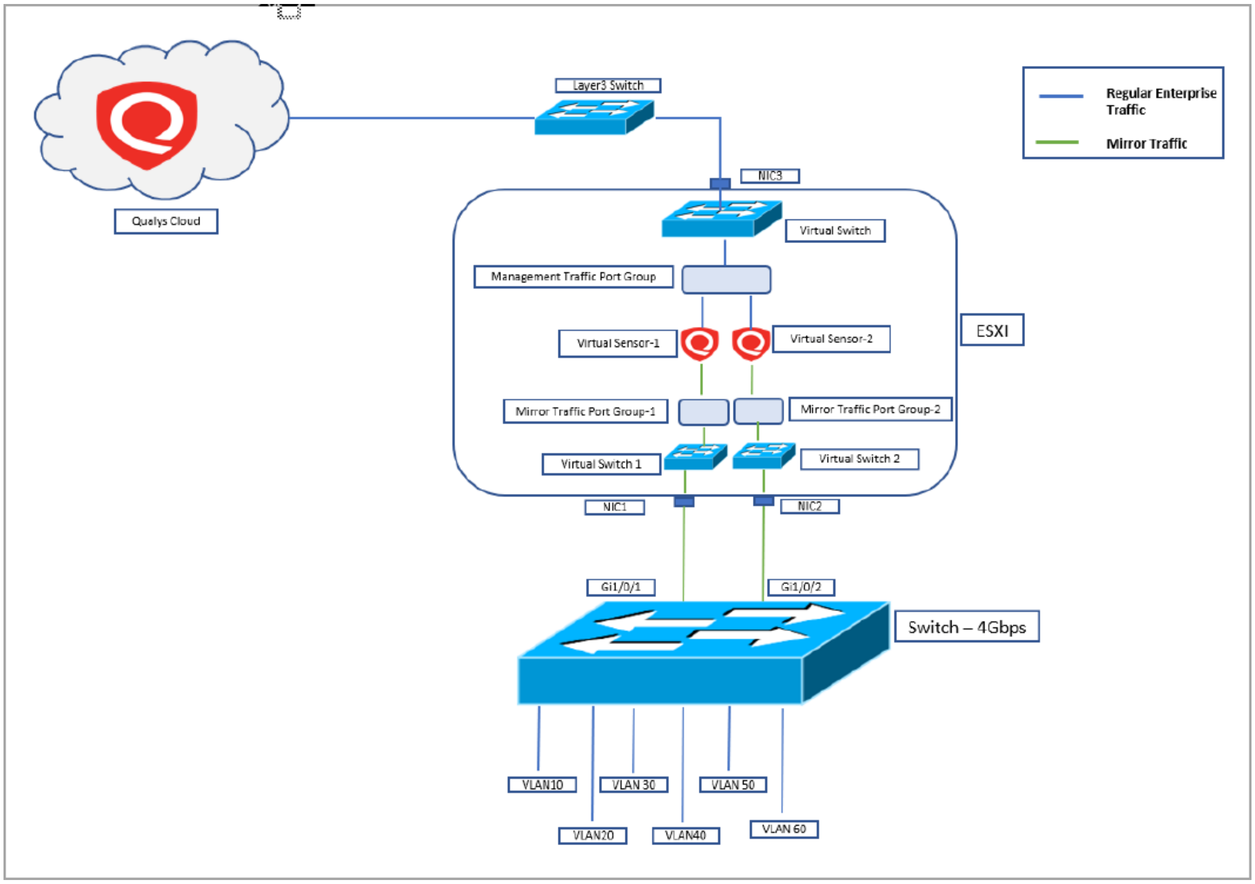
If the traffic throughput from a single source exceeds the capability of a Virtual Network Passive Sensor, the entire traffic needs to be split into a number of lower bandwidth mirrored network traffic streams. The same shall be mirrored in different sessions depending on the support and capability of the source switch.

Let’s take an example, assume a network switch is carrying 4 Gbps of network traffic across 6 different VLANs (VLAN IDs- 10,20,30,40,50,60) which need to be analyzed using the Virtual Network Passive Sensor. To do so, firstly, the 4 Gbps network traffic originating from 6 different VLANs need to be split. Assuming VLAN IDs 10,20 and 30 carry 2 Gbps of network traffic, and VLAN IDs 40, 50, and 60 carry the remaining 2 Gbps of network traffic, the traffic can be split and fed to two Virtual Network Passive Sensors in the following two ways:

Configuring Local SPAN in the physical switch and feeding the network traffic to Virtual Network Passive Sensors:

- Create monitor session 1 with VLAN IDs 10,20 and 30 as source.
- Configure destination as port Gi1/0/1.
- Create monitor session 2 with VLAN IDs 40,50 and 60 as source.
- Configure destination as port Gi1/0/2.
- Connect both the destination mirror port to two respective NICs of the virtualization host (e.g., ESXI Server).
- Configure two Vswitch inside the virtualization host and map them with the two above NICs, which relate to the mirrored ports of the physical switch (e.g., NIC1 to virtual switch 1 and NIC2 to virtual switch 2).
- Configure two port groups to collect the mirrored traffic from the above two created mirror sessions (e.g., Mirror Traffic Port Group-1 & Mirror Traffic Port Group-2).
- Configure a port group to send collected traffic to Qualys cloud (e.g., Management Traffic Port Group).
- Deploy two Qualys Virtual Network Passive Sensors and connect the sniffing interfaces of the same with respective mirror traffic port groups. i.e., connect one sensor with Mirror Traffic Port Group-1 and another sensor with Mirror Traffic Port Group-2.
- Connect both the sensors with the Management Traffic Port Group to send the data to Qualys cloud.

Diagram- Configuring Local SPAN in the physical switch and feeding the network traffic to Virtual Network Passive Sensors:



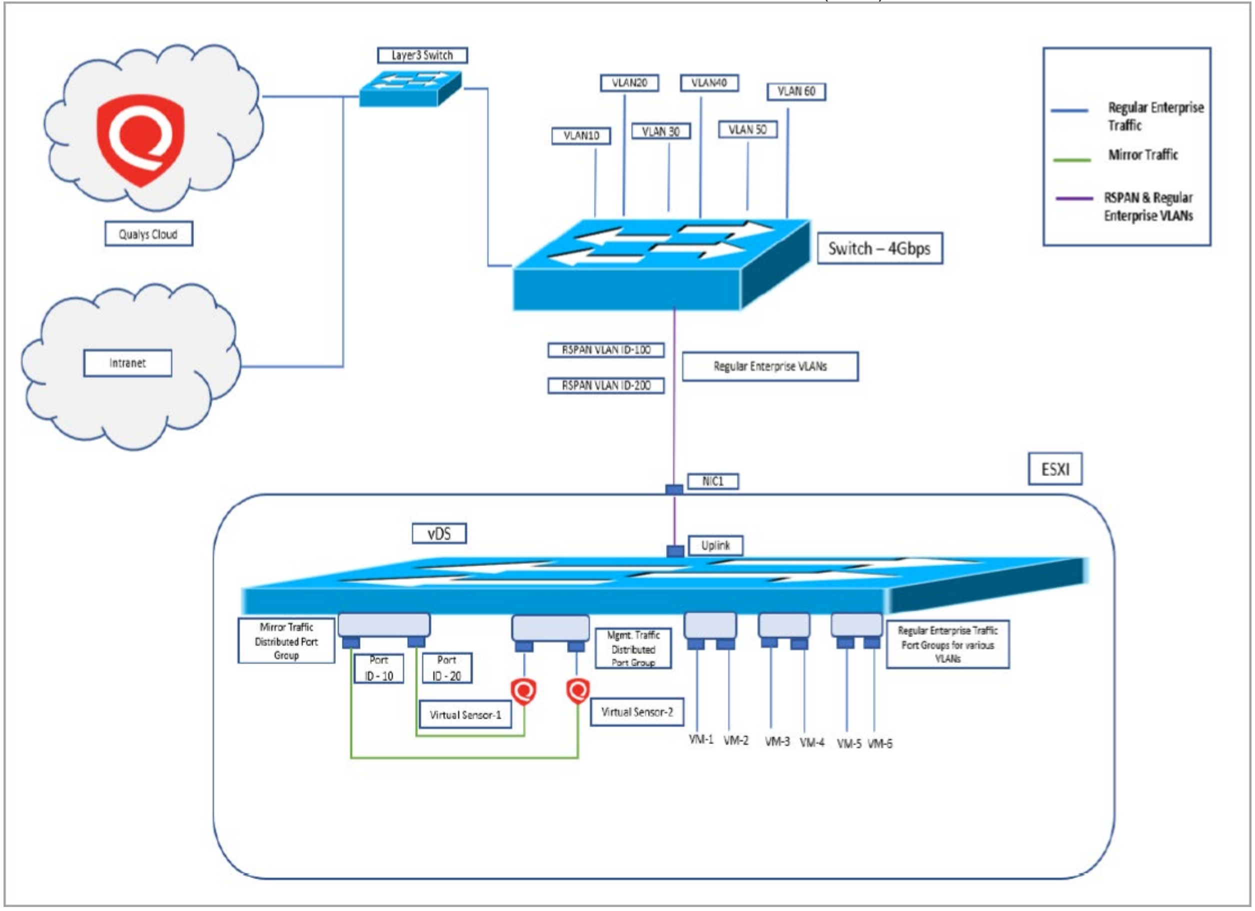
Note: In this deployment scenario, an equal number of NICs per mirrored session shall be available in the virtualization server containing the Virtual Network Passive Sensors.

Configuring RSPAN in the physical switch and feeding the network traffic to Virtual Network Passive Sensors via virtual network distributed switch (vDS)

- Create two RSPAN VLANs (e.g., VLAN ID – 100 and VLAN ID - 200) in the physical switch.
- Create monitor session 1 with VLAN IDs 10,20, and 30 as a source.
- Configure destination as the above created RSPAN VLAN, i.e., VLAN ID -100.
- Create monitor session 2 with VLAN IDs 40,50 and 60 as source.
- Configure destination as the above created RSPAN VLAN, i.e., VLAN ID – 200.
- Configure trunk port and allow the RSPAN VLANs, i.e., VLAN ID – 100 and VLAN ID – 200.
- Connect the trunk port to the physical NIC of the virtualization host (e.g., ESXI).
- Configure a vDS and map the uplink to the physical NIC of the virtualization host where the trunk port carrying RSPAN VLANs and regular enterprise traffic VLANs is physically connected.
- Create a distributed port group to collect the mirrored traffic (e.g., Mirror Traffic distributed Port Group).
- Create a distributed port group to send the collected traffic to Qualys cloud (e.g., Management Traffic Distributed Port Group).
- Navigate to the “Port Mirroring” page of the vDS, and under “Add New Port Mirroring” select “Remote Mirroring Destination.”

- Configure remote mirroring destination sessions with source as above RSPAN VLAN IDs (VLAN ID – 100 and VLAN ID - 200).
- Configure destination as destination port IDs of each session where the sniffing interfaces of virtual sensors are connected with vDS (e.g., VLAN ID – 100 to Port ID 10 and VLAN ID – 200 to port ID 20).

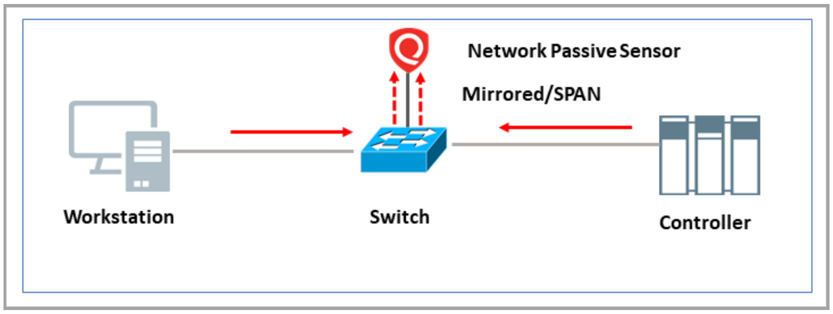
Diagram- Configuring RSPAN in the physical switch and feeding the network traffic to Virtual Network Passive Sensors via virtual network distributed switch (vDS):



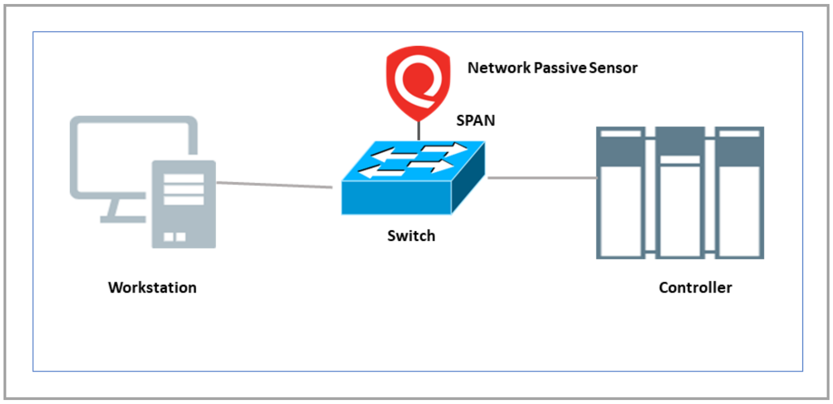
Note: If vDS is not feasible in the ESX virtual host environment, then the ERSPAN solution can be used.

Role of NPS in Industrial Network (VMDR OT)

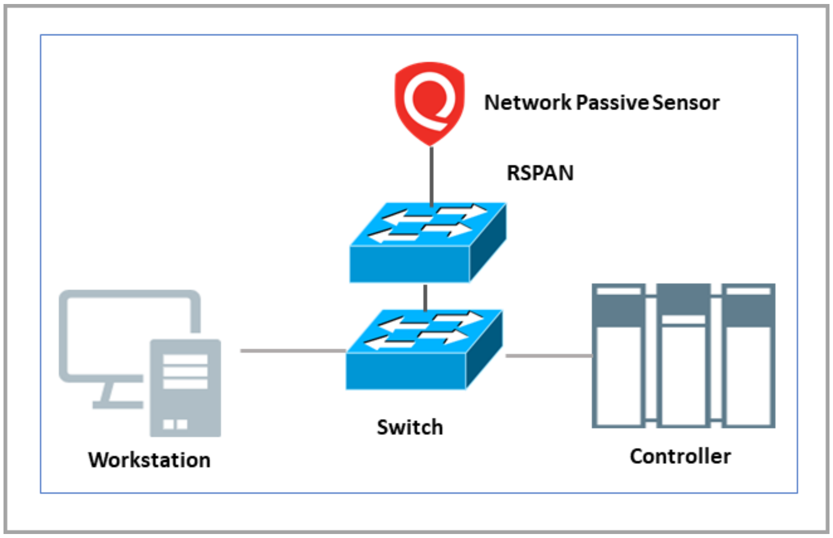
Network Passive Sensor (NPS) powers Qualys Vulnerability Management Detection and response-OT. Network Passive Sensor monitors network activity without actively probing devices and introducing network packets into the industrial network. NPS collects the required data from the industrial infrastructure. NPS listens to a mirrored port in the switch connecting critical devices like controllers and workstations to identify all the required traffic.



Spanning is a technique to replicate a specific required traffic from respective ports to a spare port, generally known as a mirror/span port. The most common span in the networking world is local span (SPAN), remote span (RSPAN) and encapsulated remote span (ERSPAN). Cisco supports all these forms of spanning methodology according to its respective models.



However, most industrial switches found across industrial infrastructure don't support RSPAN and ERSPAN.



Good to know

Port mirroring is used on a network switch or a router to send a copy of network packets seen on the source ports to destination ports. With the help of port mirroring, the packets can be monitored and analyzed.
There are two types of mirroring:

Local Port Mirroring

Local mirroring is possible when all source ports are located on the same network device as the destination ports.

Remote Port Mirroring

Remote mirroring is required when the source and destination ports are not on the same device. The source port forwards the packet copy to the destination port through the uplink connection.

Port mirroring is known as Switched Port Analyzer (SPAN) and Roving Analysis Port (RAP). Switch port Analyzer (SPAN) is a very efficient traffic monitoring system. It directs or mirrors traffic from a source port or VLAN to a destination port.
There are three types of SPANs

- SPAN or local SPAN
- Remote SPAN (RSPAN)
- Encapsulated Remote SPAN (ERSPAN)

SPAN source can be any port i.e., a routed port, physical switch port, an access port, trunk, VLAN (all active ports are monitored of the switch), an EtherChannel (either a port or entire port-channel interfaces) etc.
Note: A port configured for SPAN destination cannot be part of a SPAN source VLAN.

SPAN or Local SPAN mirrors traffic from one or more interfaces on the switch to one or more interfaces on the same switch; hence SPAN is referred to as LOCAL SPAN.

Remote SPAN (RSPAN) supports source ports, source VLANs, and destination ports on different switches, providing remote monitoring traffic from source ports distributed over multiple switches and allowing destination centralized network capture devices.
Encapsulated Remote SPAN (ERSPAN) brings generic routing encapsulation (GRE) for all captured traffic and extends it across Layer 3 domains. ERSPAN is a Cisco proprietary feature available only to Catalyst 6500, 7600, Nexus, and ASR 1000 platforms.

What is a Network tap?

A network tap is a hardware device installed on the network. It enables network traffic to pass unimpeded while duplicating all data to a monitor port where a network analyzer can access it.

Best Practices for Mirroring Configurations

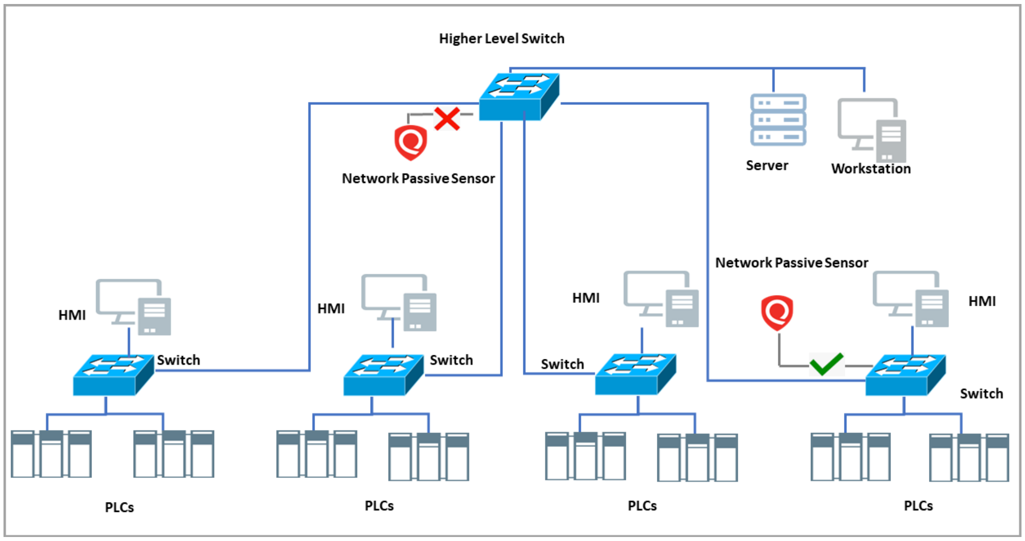
The following best practices are explicitly followed when spanning industrial traffic from switches:

- Qualys recommends configuring a VLAN-based mirroring wherever possible. Port mirroring should be considered when the option of VLAN mirroring is unavailable. Qualys recommends the industrial switch should allow multiple ports to be mirrored to a single destination port.
- In case of switch do not support port mirroring of all the ports, you can use a network tap or can deploy a new switch which support all ports.
- Selecting the SPAN source as the switch's only uplink is not recommended for OT device environments as the traffic between PLCs, HMIs, and IO devices connected to the same switch may not reach the uplink of a switch.
- Suppose engineering workstations are connected to a switch (S1), and PLCs and IO devices are connected to the switch (S2). Both S1 and S2 are connected to the aggregation switch. In that case, the uplink of S1 or S2 will see traffic between PLCs to engineering workstations. In this case, Qualys recommends mirroring traffic from the uplink of S1 or S2.
- If multiple switches are to be spanned, it is necessary to SPAN both the local Access ports and the inter-switch trunk ports. Traffic within a switch will be seen on the local access ports but not on a trunk port. Traffic on two different switches may not be seen entirely on its local access ports but only on the trunk links.
- To enhance the security and to prevent the destination port from receiving any data, it is recommended to keep the ingress keyword disabled by default while configuring SPAN in Cisco switches.
- Generally, process control switches have very low CPU utilization, so mirroring does not create problem. It is recommended to validate CPU utilization of switches before and post mirror configuration.
- You can verify if the mirroring works correctly using the switch address table dump. Ensure the switch ports learn the MAC address of all the devices you want to monitor.
- Scenarios with overlapping IP addresses generated from various facility sections need to be categorized with manually tagging locations corresponding to them.

Appendix A - Use Case Scenario for VMDR OT

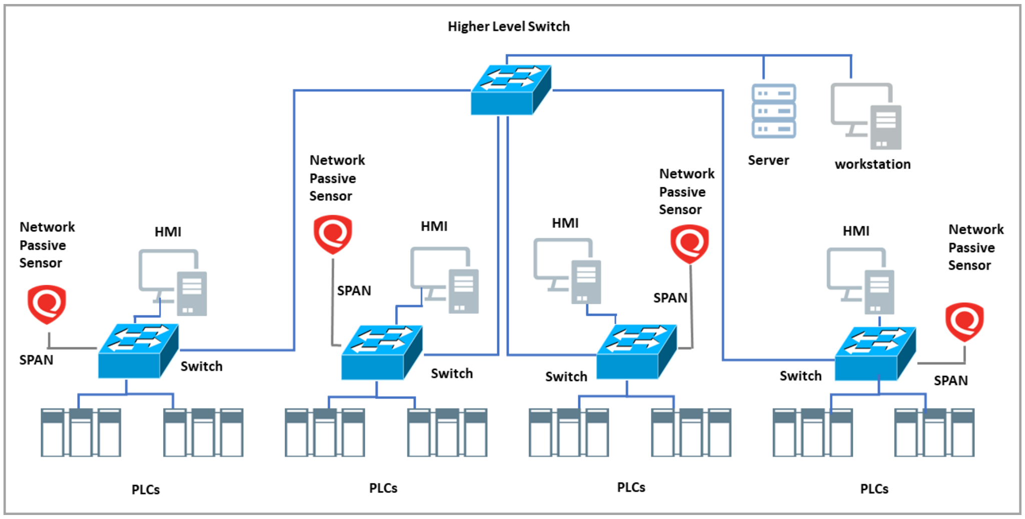
Placement of NPS Across OT Networks

The capability of a Network Passive Sensor (NPS) across an industrial network lies in identifying the critical traffic. It is essential to follow the rule of mirroring the traffic between workstations (EWS, HMI) to controllers (PLCs, RTUs, DCS). Qualys recommends identifying the best path to tap the process data between controllers and workstations and deploying the Network Passive Sensor (NPS) to get the maximum traffic to analyze.



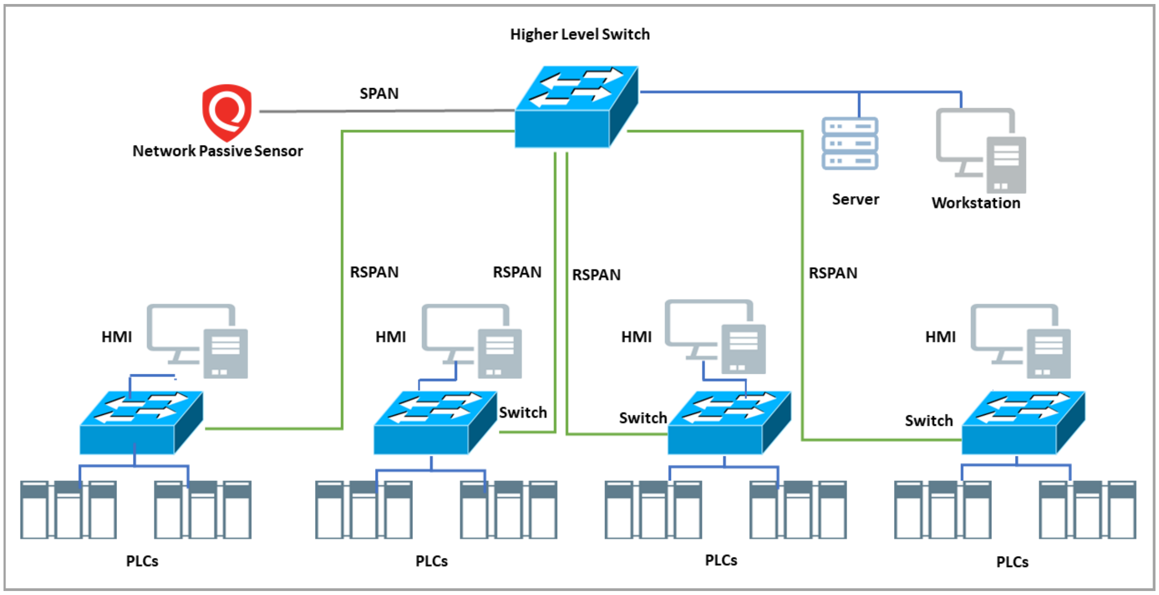
Scenario 1 - Deploying the NPS Across the Lower-Level Managed Access Switches

Most industrial switches connecting level 1 and level 2 devices across an industrial network do not support RSPAN. In this scenario, local spanning of such lower-level access switches and deploying the Network Passive Sensor (NPS) provides the best output. Tapping the higher level switch is not sufficient as the unicast traffic in the lower-level access switches may not necessarily traverse to the higher level switch.



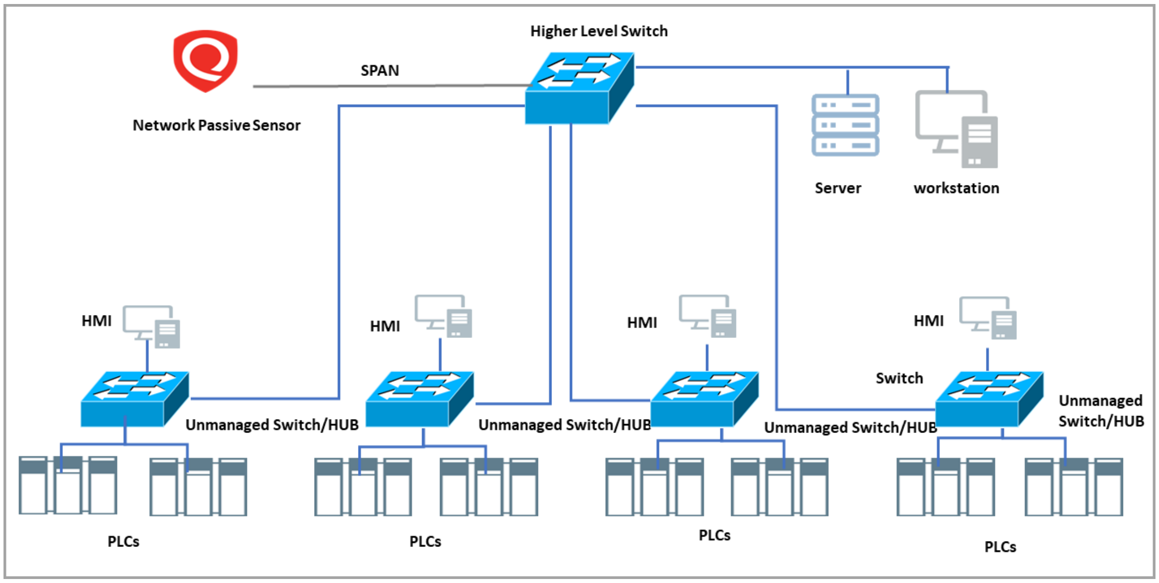
Scenario 2 – Remote Spanning the Lower Level Access Switch

If RSPAN is supported across the lower-level managed access switches in that case, it is recommended to RSPAN the traffic from the lower-level switches to the high level switch feeding into a Network Passive Sensor (NPS) to get the best output.



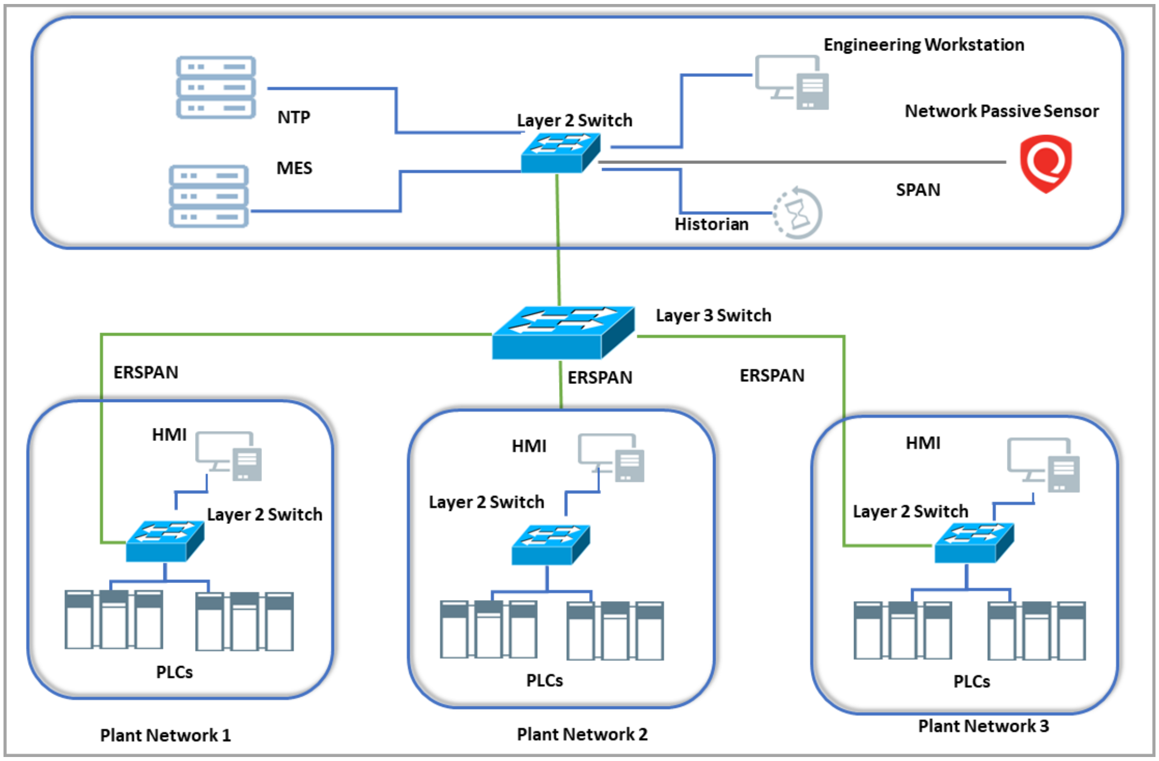
Scenario 3 - Deploying the NPS in the Higher Level Switch

If the PLCs and HMIs are connected to an unmanaged switch/hub, in such cases you can deploy Network Passive Sensor (NPS) at the switch present at a higher level. This placement of Network Passive Sensor (NPS) gives the best result with immediate visibility of industrial assets.



Scenario 4 – Deploying NPS in a Different VLAN

In case of industrial networks comprising various subnetworks corresponding to various processes, if ERSPANing capabilities are available on switches, deploying Network Passive Sensors (NPS) on a layer 2 switch gives the best result.
Note: It is recommended to verify the destination network path must have enough bandwidth to support the network traffic from all the source switches.

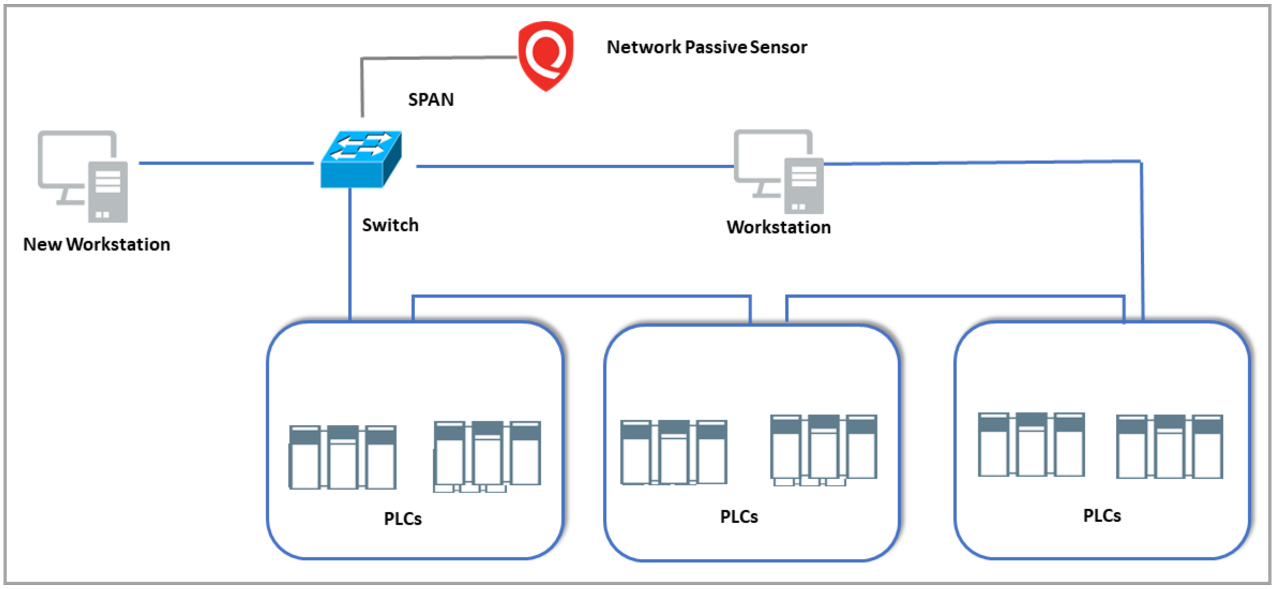


Scenario 5 – Retrieving OT Network Traffic from Ring Network

If a switch is connected with other OT devices in a ring topology, deploying Network Passive Sensor (NPS) on switch is not sufficient as traffic can traverse from other side of the ring without going through switch. In such cases, the important information can be lost.
Qualys recommends the following activities in this scenario:

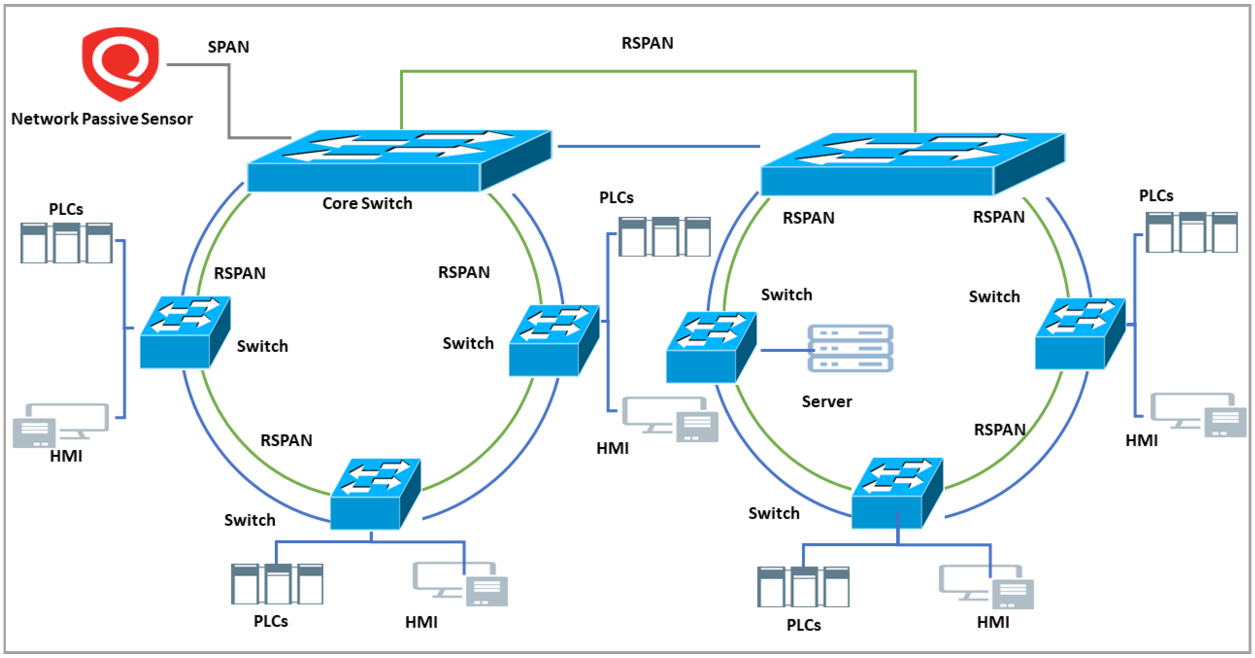
Case 1 - Simple Ring Architecture

- An engineering station needs to be connected to the existing switch
- Perform asset scanning across the OT network from the engineering station
- Configure mirroring and deploy the Network Passive Sensor (NPS) in the switch



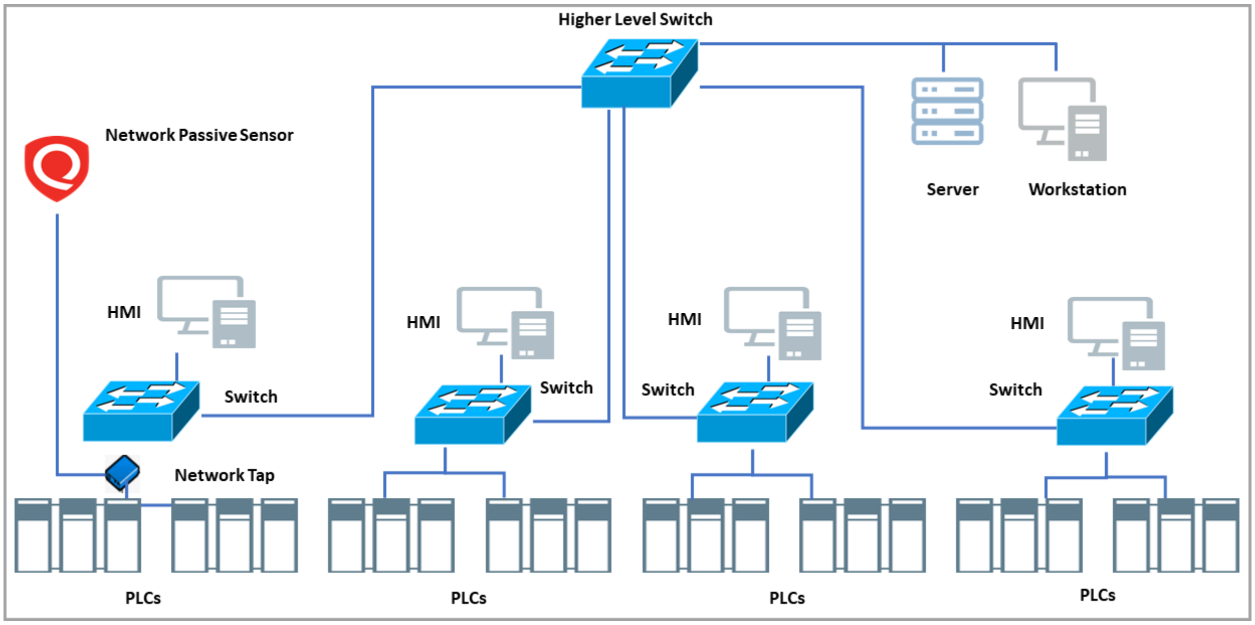
Case 2 - Simple Ring and Sub- ring Architecture

- Remote SPAN (RSPAN) traffic from all the switches connected with OT devices
- Configure mirroring and deploy the Network Passive Sensor (NPS) in the core switch
- Perform Asset discovery across the OT network from an engineering station connected to the core switch



Scenario 6 – Tapping Critical Process Data Through a Network Tap

If the industrial networks consist of network switches, which do not support mirroring configuration, Network Passive Sensor (NPS) can be deployed with an in-line network tap device such as Gigamon, Keysight, NetScout etc,.

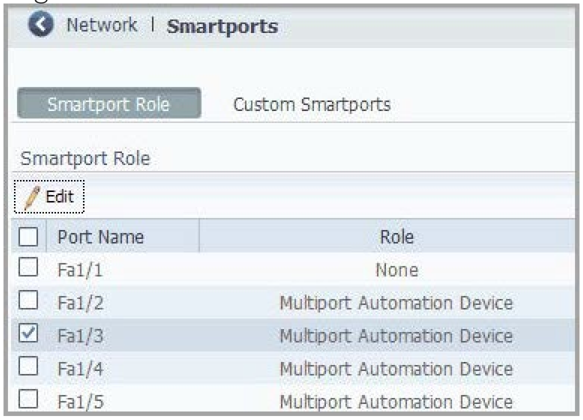


Appendix B - Mirroring Techniques and Commands for VMDR OT

Mirroring Techniques - Stratix

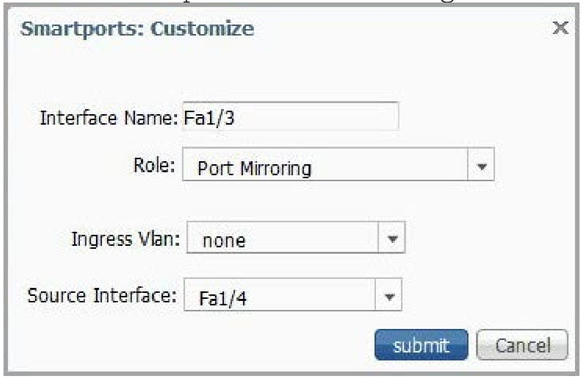
Stratix is the proprietary industrial ethernet switch by Allen-Bradley (Rockwell Automation). It is designed to support the connectivity among layer 2 supervisory devices and layer 1 devices such as PLCs and DCS controllers. The switch is widely used across various industrial infrastructures, especially Allen-Bradley manufactured controllers.
Mirroring configuration in Stratix switches could be performed from its web interface.
Following are the mirroring steps for Stratix 5400, 5410, 5700, 8000 and 3000:

1. Login to the switch.



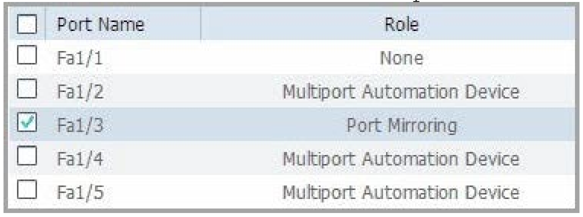
□	Port Name	Role
□	Fa1/1	None
□	Fa1/2	Multiport Automation Device
☑	Fa1/3	Multiport Automation Device
□	Fa1/4	Multiport Automation Device
□	Fa1/5	Multiport Automation Device

2. Choose Smartports from the configure menu.



Interface Name: Fa1/3
Role: Port Mirroring
Ingress Vlan: none
Source Interface: Fa1/4

3. Select the checkbox next to the port for monitoring and then click Edit.



□	Port Name	Role
□	Fa1/1	None
□	Fa1/2	Multiport Automation Device
☑	Fa1/3	Port Mirroring
□	Fa1/4	Multiport Automation Device
□	Fa1/5	Multiport Automation Device

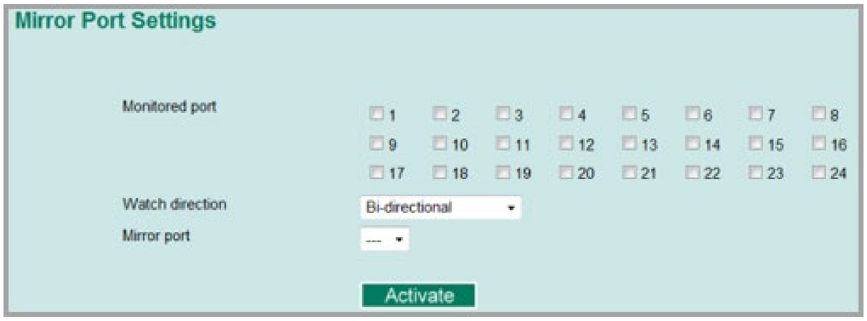
4. Complete the fields and submit
5. Verify the port mirroring configuration.

For more information on mirroring techniques on Stratix switches, refer to the Official website.

Mirroring Techniques – Moxa

Moxa is an industrial network switch specially designed for layer 2 and layer 1 network connectivity. Moxa switches are generally found in industrial infrastructure consisting of devices manufactured by Schneider Electric.
Mirroring configuration in Moxa switches is performed from web interface.
Following are the mirroring steps for EDS-728/828, IKS-6726/6726-8PoE/6728/G6524/G6824, ICS-G7000 Series:

1. Log in to the switch.
2. Select the number of the ports to monitor in the **Monitored Port**.
3. Select the type of data stream to monitor (Input, Output, Bi-directional) in the **Watch Direction**.
4. Select the number of ports to monitor the network traffic of the mirrored port in the **Mirror Port**.
5. Select **Activate** to start mirroring.



Mirror Port Settings

Monitored port
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8
□ 9 □ 10 □ 11 □ 12 □ 13 □ 14 □ 15 □ 16
□ 17 □ 18 □ 19 □ 20 □ 21 □ 22 □ 23 □ 24

Watch direction: Bi-directional

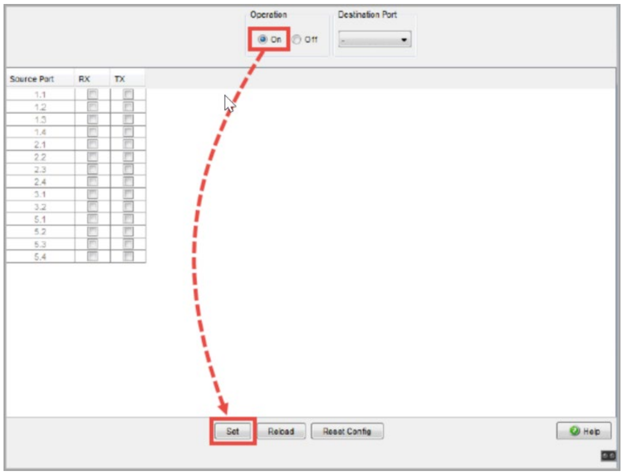
Mirror port: ---

For more information on mirroring techniques for Moxa switches, refer to the Official website

Mirroring Techniques – Hirschman

Hirschman ethernet industrial network switches are widely used across OT infrastructure consisting of devices of various manufacturers such as Yokogawa, ABB, GE etc.
Mirroring configuration in Hirschman switches could be performed from its web interface.
Following are the generic mirroring configuration steps for a Hirschman industrial switch:

1. Log in to the switch.
2. Select the **Port Mirroring** from **Diagnostics** tab.
3. Select all the applicable **Source Ports** and the data stream (RX and TX) to monitor.
4. Select the **Destination Port** to monitor all the network traffic.
5. Select **On** from **Operation** and select **Set** to start the mirroring.
6. It is required to select **Save** to save the configuration changes for permanent use.



Operation: ● On ○ Off

Destination Port: -

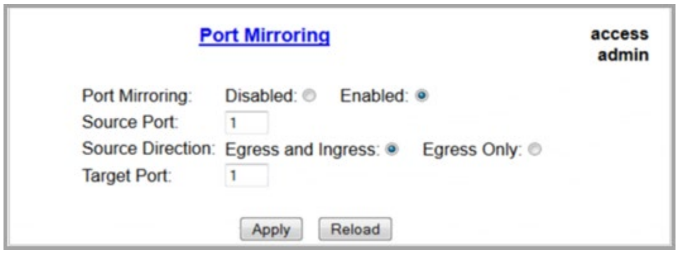
Source Port	RX	TX
1.1	□	□
1.2	□	□
1.3	□	□
1.4	□	□
2.1	□	□
2.2	□	□
2.3	□	□
2.4	□	□
3.1	□	□
3.2	□	□
5.1	□	□
5.2	□	□
5.3	□	□
5.4	□	□

For more information on mirroring techniques for Hirschman switches, refer to the [Official website]()

Mirroring Techniques – Ruggedcom

Ruggedcom is an ethernet industrial network switch manufactured by Siemens and is widely used across ICS infrastructure consisting of devices of Siemens. Ruggedcom is widely found across the utility industry, such as power transmission and distribution.
Mirroring configuration in Ruggedcom switches can be performed from its web interface.
Following are the generic mirroring configuration steps for Ruggedcom i800, i801, i802, i803 series switches:

1. Log in to the switch.
2. Navigate to Ethernet Ports and then Configure Port Mirroring.
3. Configure the following mirror configurations:
    a. From **Port Mirroring,** click **Enabled**.
    b. From **Source Port**, specify the port(s) to monitor.
    c. From **Source Direction**, specify the data stream (Egress and Ingress, Egress Only)
    d. From **Target Port,** specify the destination port to monitor the mirrored port.
    e. To start mirroring, select **Apply**.



Port Mirroring

access
admin

Port Mirroring: Disabled: ○ Enabled: ●
Source Port: 1
Source Direction: Egress and Ingress: ● Egress Only: ○
Target Port: 1

For more information on mirroring techniques for Ruggedcom Switches, refer to the Official website.

Mirroring Techniques – Cisco

Cisco network switches are used across OT infrastructure for providing connectivity among typical layer 2 and layer 1 devices.
Mirroring configurations in Cisco switches are performed from its command-line interface. Following are the generic mirroring configuration steps for cisco catalyst 2960 and 3850:
Local SPAN

1. Log in to the switch.
2. To enter global configuration mode, enter **configure terminal**.
3. To remove any existing session, enter **no monitor session all**.
4. To specify the SPAN session and the source Interface/VLAN, enter **monitor session 1 source interface interface-id/vlan vlan-id**.
5. To specify the destination interface for monitoring the mirrored ports, enter **monitor session 1 destination interface interface-id**.

Your configuration is completed.

Remote SPAN

1. Log in to all the switches through which the mirrored network traffic will traverse from the source switch to a destination switch.
2. To enter global configuration mode, enter **configure terminal.**
3. To create a VLAN, enter **VLAN xx** and configure it to a remote span VLAN and enter **remote span**.
4. Remember to allow the created VLAN in the trunk port.
5. To create a monitor session in the source switch with the source interface, enter **monitor session 1 source interface interface-id**.
6. For selecting the destination as the created RSPAN VLAN, enter **monitor session 1 destination remote vlan xx**.
7. To create a monitor session in the destination switch with source as RSPAN VLAN, enter **monitor session 1 source remote vlan xx**.
8. To select the destination as the interface where the Network Passive Sensor has been deployed, enter **monitor session 1 destination interface interface-id**.

Your configuration is completed.

For more information on mirroring techniques for Cisco Switches, refer to the Official website.