



Network Passive Sensor

Getting Started Guide

October 23, 2023

Copyright 2022-23 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

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



Table of Contents

About this Guide	4
About Qualys	4
Qualys Support	4
Welcome to Qualys Network Passive Sensor	5
What are the Benefits?	6
How it Works	7
Exclude Hostname from Asset de-duplication	9
Sensor Deployment Options	10
Appliance Connectivity and Interfaces	10
Network Placement and Sensor Sizing	12
Quick Steps	13
Before you Begin - Mirror the Traffic	13
Step 1 - Generate a Personalization Code	13
Step 2 - Deploy and Register the Appliance	14
Step 3 - Configure Assets	14
Step 4- Check the status	21
Step 5- View Asset Details in Asset Inventory	21
Classification of Assets in Passive Sensor	22
Best Practices	28

About this Guide

Welcome to Network Passive Sensor! We'll help you use the Network Passive Sensor to detect known and unknown devices on your network.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also founding member of the [Cloud Security Alliance \(CSA\)](#). For more information, please visit www.qualys.com

Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access online support information at www.qualys.com/support/.

Welcome to Qualys Network Passive Sensor

With Qualys Network Passive Sensor (PS), you can automatically detect, and profile devices connected to your network, eliminating blind spots across your IT environment. Network Passive Sensor monitors network activity without any active probing of devices in order to detect active assets in your network.

Instant, Complete Detection

Qualys NPS continuously monitors all the network traffic and flags any asset activity. It identifies and profiles devices the moment they connect to the network, including those difficult to scan, corporate owned, brought by employees, and rogue devices. The asset metadata is sent immediately to the Qualys Cloud Platform for centralized analysis.

Continuous Inventory Enhancement

Qualys PS enriches existing asset inventory with additional details, such as recent open ports, traffic summary, network services and applications in use. This helps customers gain a deeper understanding of an asset and its activity on the network in near-real time.

Network Scanner and Cloud Agent Complement

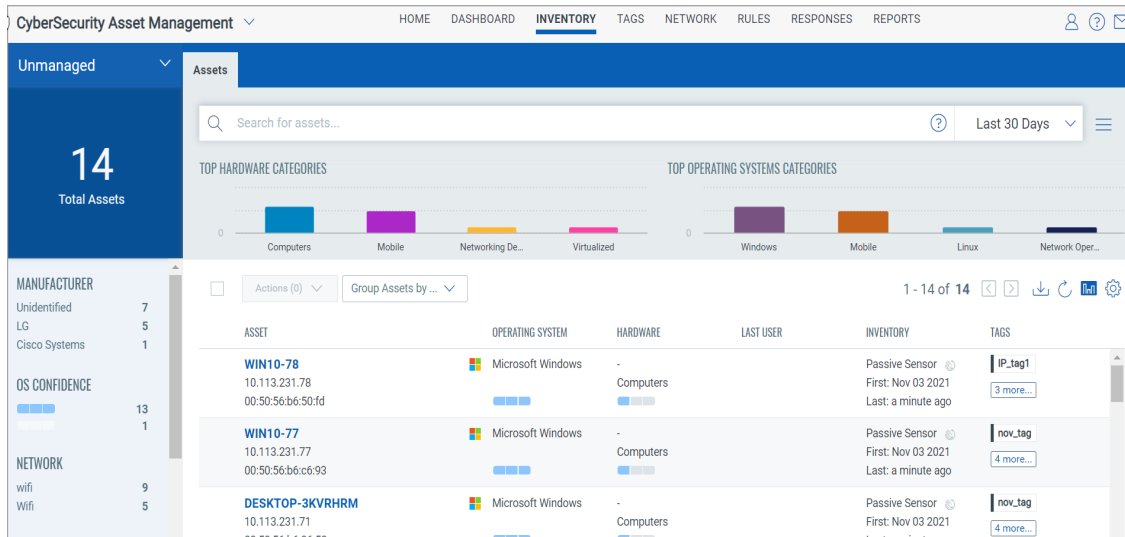
Qualys PS identifies assets that for different reasons can't be actively scanned or monitored with agents. That's often the case with assets like industrial equipment, IoT and medical devices.

Centralized Control and Visibility of Assets

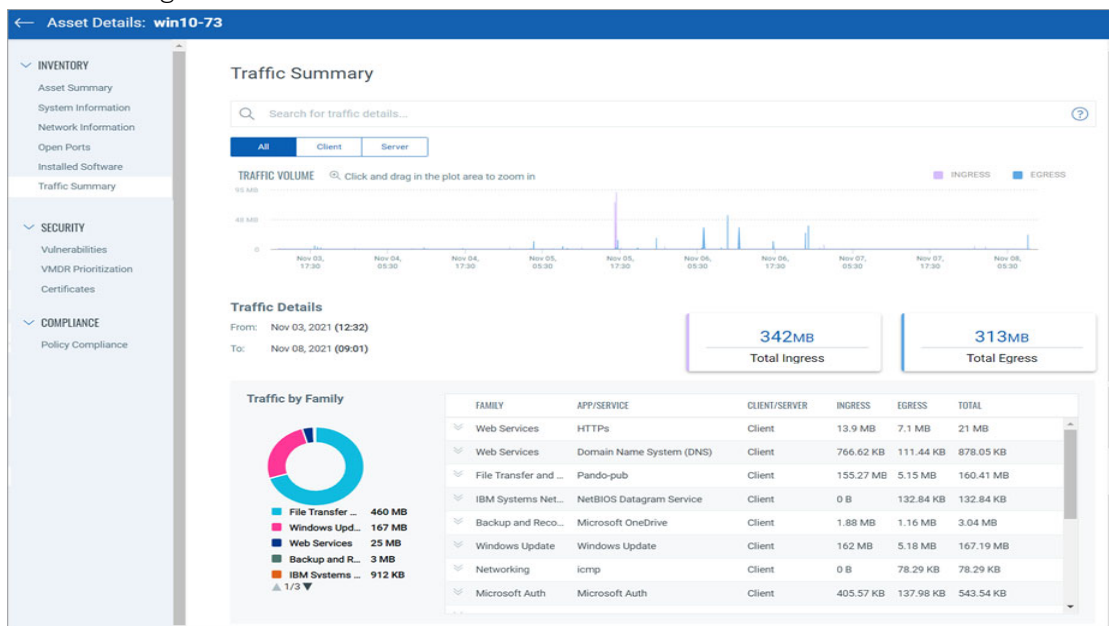
The Qualys Asset Inventory cloud app aggregates and correlates the data gathered by all Qualys sensors – Qualys Passive Sensors, the Qualys network scanners and the Qualys Cloud Agent – giving you a comprehensive, detailed inventory of all your hardware and software, as well as a multi-dimensional view of your global, hybrid IT environment.

What are the Benefits?

You get complete visibility into managed and unmanaged assets, including asset details like hostname, operating system, device manufacturer and model, open ports, network services and much more.



Passive Sensor analyzes existing network traffic without sending a single packet to the devices being discovered.



Get insights to the asset's network activity, with traffic summary categorized by ingress/egress, service type, and port/protocol.

Drill down to traffic between a source and destination. You get enterprise application identification (e.g. database) based on traffic pattern.

How it Works

The Network Passive Sensor (PS) is placed inside your network and takes snapshots of the data flowing over the network. It extracts metadata from these snapshots and sends them to the Qualys Cloud Platform for analysis. This allows us to catalog the assets by operating system and hardware.

- **Asset De-duplication With Managed Assets:**

If an asset discovered by the sensor is already known by active scanning or is reported by a cloud agent, then it is considered a managed asset and NPS de-duplicates the passively sensed asset with the managed asset using the Cloud Agent correlation ID, MAC address, hostname, or IP as a criteria (please refer to the below section for IP-based de-duplication criteria). A de-duplicated asset is listed in the managed inventory.

De-duplication uses the following criteria in the order of descending priority:

- De-duplication based on correlation ID works if passive sensor discovers correlation ID and the same is available for a managed asset. The way NPS learns the correlation ID is if gets a copy of the scan traffic when the Qualys scanner runs a VM scan of the asset containing a cloud agent and the scan profile has the QID that queries the asset for its correlation ID.

Note: The agent correlation ID is generated by agents installed on Windows and Linux hosts. VM scan also has an option to use the agent correlation ID to de-duplicate agent-collected data with the results of authenticated or unauthenticated scans.

- De-duplication uses MAC if asset is not de-duplicated using correlation ID.
- If MAC is also not known, then an exact match is necessary for hostname-based de-duplication. If the passive sensor senses "johndoe" as the hostname and the managed asset's hostname is reported with a domain name such as "johndoe.somedomain.org" or vice versa, the assets will not duplicate. In such cases, user can add domain names such as "somedomain.org" as input to NPS, for it to de-duplicate it with the managed asset. To add a domain, go to the **Sensors** tab and click **View Details** from the Quick Action menu of a sensor. Alternatively, you can click the sensor and go to the sensor details page > **General Settings** > **Add domain**. To learn more about configuring the domains, refer to the [Online Help](#).
- Finally, if neither of the above conditions are met, then NPS uses only the IP address to de-duplicate provided both managed and un-managed IPs are in the same network. For details on the need of the Network feature, refer to Appendix D, "Extending the Network Feature Section," of the Qualys [Network Passive Sensor Appliance User Guide](#). If user does not have "Network" in the subscription, NPS defaults to treating all IPs as a part of one global default network.

IP-only de-duplication uses additional IP configuration: dynamic (DHCP) and static IPs. An unmanaged asset with a static IP is immediately de-duplicated with the managed asset of the same IP. If the unmanaged asset has a dynamic IP assigned from the DHCP pool, the de-duplication with the managed asset of the same IP happens provided the timestamp of the managed scan and the timestamp of the asset seen by passive sensor are close to each other i.e. within a stipulated time period. This time period is the asset's DHCP lease period identified by PS or the IP inactivity time period if PS is unable to discover the DHCP lease

period in cases where DHCP flow is not seen on sniffing interface or the appliance is overloaded and drop the DHCP packet. The user can configure an IP subnet/range as static or dynamic at the time of configuring the internal asset configuration for the appliance.

The asset reported by passive sensor is listed in the unmanaged inventory provided:

1. Asset is not detected by an active scan
2. Asset is detected by active scan but not yet de-duplicated

• **De-duplication Within Unmanaged Assets:**

NPS de-duplicates assets within the unmanaged inventory based on MAC address, hostname or IP.

De-duplication uses the following criteria:

- Hostname-based de-duplication happens only for non-mobile devices or for hostnames not added to the exclusion list. Refer to the General Settings section of the Network Passive Sensor (NPS) Online Help for more details on adding hostnames to the exclusion list and why it is needed.
- NPS de-duplicates assets within the unmanaged inventory based on IP, when same IP is reported by multiple passive sensors, provided all sensors are part of the same network (Network subscription and configuration is needed only when the enterprise network has overlapping/same IP addresses). As a result, if more than one passive sensors are deployed in a network and are configured with the same IP addresses in the internal asset group, then NPS de-duplicates assets reported by different passive sensors if the IP address is the same and provided that MAC address is not learnt. IPs configured as static qualify for immediate de-duplication, whereas for IPs configured as DHCP, assets will be de-duplicated only if their timestamps are close enough – i.e. within IP inactivity time.

Note: If the user configure Network Passive Sensor (NPS) with an IP as static in one internal asset group and the same IP as DHCP in a different internal asset group, then NPS treats the IP as static.

In an enterprise having 2 subnets that have the same/overlapping IP addresses would need,

- a) to deploy 2 passive sensors, one for each network.
- b) would want to inventory assets uniquely within each subnet and not have the same IP (seen without MAC or hostname) reported by the 2 passive sensors, de-duplicate into one asset.

To do this, user must associate each sensor to its own network and also create network range tags that are a combination of network and IP ranges. A tag can be created in **VMDR > Assets > Asset Groups > New Asset Group** OR **CSAM > Tags > New Tag > Create tag**. Create a dynamic tag with the rule "IP Address in Range(s) + Network(s)".

To elaborate the above with an example, take the case of an enterprise has 2 branch offices in locations L1 and L2. Both locations have the same subnet allocated to Wifi network- say IP range IPn. Passive sensor NPS1 and NPS2 are 2 sensors deployed to sense subnet IPn in locations L1 and L2 respectively.

User must,

- a) Create 2 networks N1 and N2 for locations L1 and L2
- b) Configure NPS1 with network N1 and NPS2 with network N2
- c) Create tags T1 and T1 of type IP2+Network such that T1 = N1, IPn and T2= N2, IPn

The above configuration ensures that when same IP is reported by NPS1 and NPS2, 2 separate assets one in each network is created.

The following table summarizes the asset de-duplication criteria used in NPS:

Qualys Cloud Agent CorrelationID	Macs	IPs	Hostnames	Network	De-duplicate?
Same	Doesn't Matter	Doesn't Matter	Doesn't Matter	Doesn't Matter	Yes
Not Available	Same	Doesn't Matter	Doesn't Matter	Doesn't Matter	Yes
Not Available	Different	Doesn't Matter	Same	Doesn't Matter	Yes
Not Available	Different	Same	Different	Same	Yes, within IP inactivity
Not Available	Different	Same	Different	Different	No
Not Available	Not Available	Same	Not Available	Same	Yes, within IP inactivity
Not Available	Not Available	Same	Not Available	Different	No

Exclude Hostname from Asset de-duplication

User has an option to specify hostnames that NPS should exclude while de-duplicating assets using hostnames. NPS de-duplicates managed and unmanaged assets based on multiple conditions of which hostname is one.

To explain why a user may have to exclude some hostnames from being considered in de-duplication criteria, let us take one example which is a common scenario in Operational Technology (OT) network topologies. Consider an OT network having many industrial access level switches where each switch is connected to assets such as PLCs (Programmable Logic Controller), HMIs (Human Machine Interface), RTUs (Remote Terminal Unit), motion control drives etc. It is common in OT networks to only minimally configure the devices and leave the other configurable parameters unchanged. So, all the industrial switches could be minimally configured to have different IPs but their hostnames are unchanged and remain the same as the default configuration. Similarly for HMI devices as well. As a result, one common hostname is used by all switches and

another common one used by all HMI devices. To track each such device as an independent asset in the inventory, the user can add the common switch hostname and the common HMI hostname in the exclusion list provided by this feature.

The screenshot shows the 'Network Passive Sensor' configuration interface. The top navigation bar includes 'HOME', 'SENSORS', and 'CONFIGURATION'. The 'CONFIGURATION' section is active, with sub-tabs for 'Internal Assets', 'Excluded Assets', 'Monitor External Assets', and 'General Settings'. The 'General Settings' tab is selected, and the 'Exclusions' section is visible. The 'Exclusions' section has a description: 'Configure names that Qualys should exclude from hostname based asset de-duplication'. Below this is an 'Add Hostnames' section with a text input field labeled 'Enter Hostname' and an 'Add' button. There are also links for 'Clear Selection' and 'Remove Selected'. A table lists the added hostnames: 'HOSTNAMES' (with a checkbox), 'ASD', 'QWE', and 'example'. Each entry has an edit icon (pencil) and a delete icon (X). A 'Save' button is at the bottom of the table.

Sensor Deployment Options

Qualys Network Passive Sensor is available as both a physical and virtual appliance.

- Physical Appliance: 1Gbps, 4Gbps, and 10Gbps appliance
- Virtual Appliance: Support for VMware ESXi (6.0 and above) and Microsoft Hyper-V

Operational Mode: Out of band - fed by tap, span or packet broker

Centralized sensor management, including software updates, from the Qualys Cloud Platform for convenience.

Appliance Connectivity and Interfaces

The appliance has two types of interfaces: management interface and sniffing interface.

Management Interface

The management interface is used for connecting to the Qualys Cloud Platform and for streaming asset metadata to the Qualys Cloud Platform, as well as performing management and maintenance activities remotely from the Qualys UI.

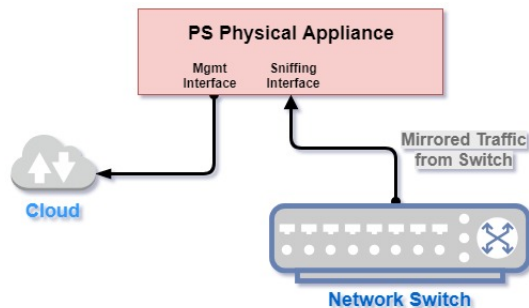
You'll assign an IP address to the management interface either statically or using DHCP. DHCP is enabled by default. Configuring the management interface is required for the Passive Sensor to have Internet connectivity and to connect to the Qualys Cloud Platform.

Sniffing Interface

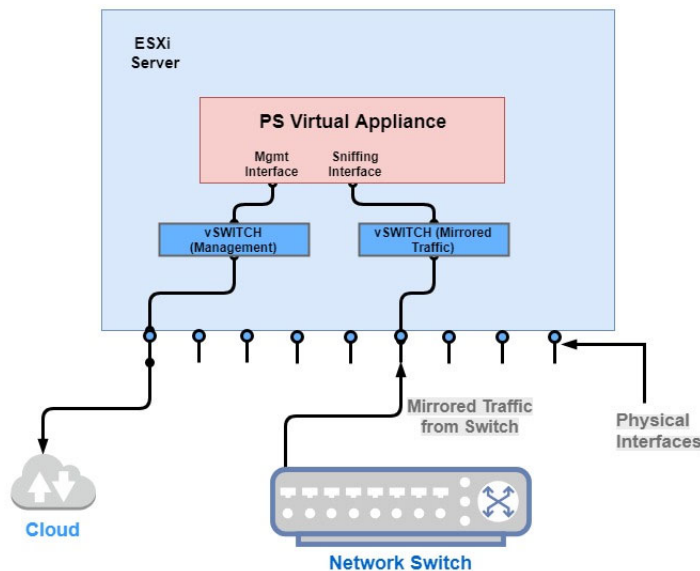
One or more traffic sniffing interfaces are used to receive mirrored traffic to the Network Passive Sensor. Once the traffic that needs to be monitored is identified: 1) Configure the switch that sees the traffic in question by mirroring the traffic to a port, 2) Connect that mirrored port to the passive sensor sniffing interface of the sensor, and 3) Enable “Promiscuous Mode” on respective vSwitch and port group.

You will not assign an IP address to the sniffing interface.

The following picture shows 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 cloud.



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 cloud.



Network Placement and Sensor Sizing

It's best to position passive sensors at points in the network that see maximum aggregate traffic. For effective traffic monitoring, passive sensors should be attached to tap/span ports of distribution switch/routers in the network.

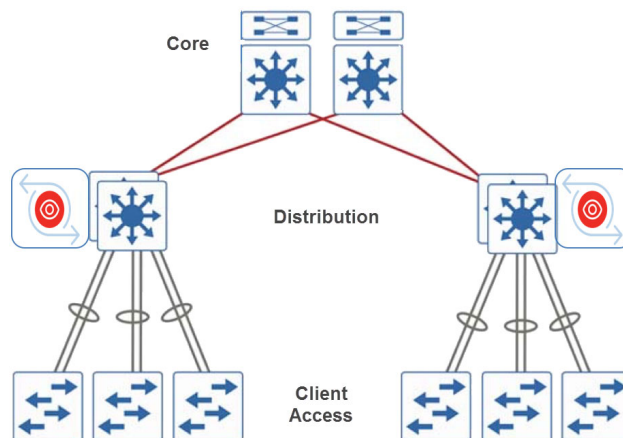
What size do you need?

You'll want to consider the traffic throughput at the deployment points, the need for accurate coverage of all assets and total count of all assets. Typically passive sensors with 1G interfaces would be sufficient for an aggregate traffic that does not exceed 900 Mbps from an average of up to 3,000 assets.

Where should you attach passive sensors?

Passive sensors attached to core switch/routers may not have visibility into the local traffic of the distribution switch, i.e. traffic between assets attached below the same distribution switch. Passive sensors attached to distribution switches will provide much better accuracy and visibility. Multiple passive sensors may have to be deployed depending on the network topology.

The following diagram shows passive sensors at the distribution layer. In this example, the traffic from all devices in the Client Access network gets aggregated at the distribution switches and traffic from the distribution switches gets aggregated at the core switch.



Quick Steps

You need to deploy the appliance on your network, generate a personalization code, and use the code to register the appliance with the Qualys Cloud Platform.

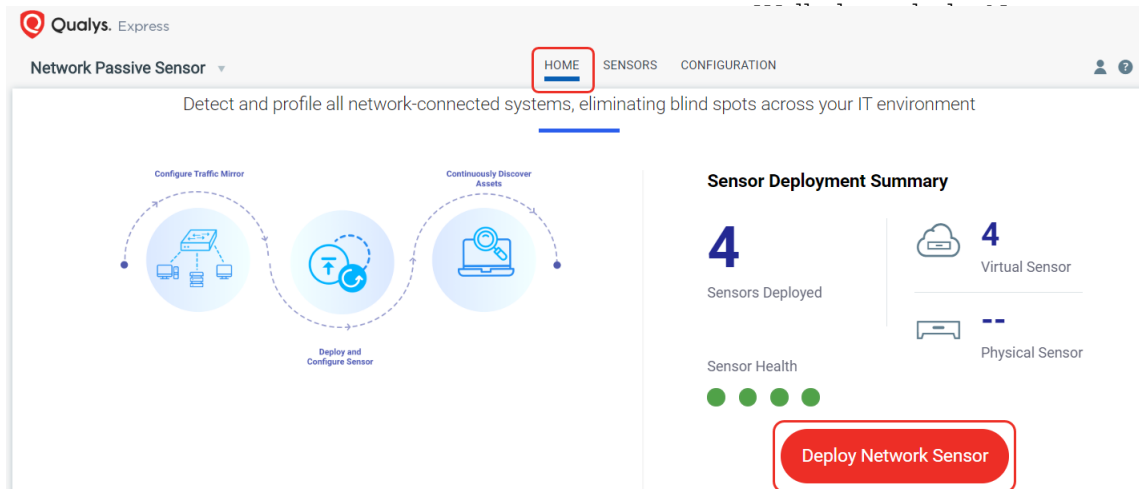
Before you Begin - Mirror the Traffic

You need to feed traffic to the sensor by mirroring the traffic (using physical tap or mirror port). Then connect the mirrored port to the sniffing interface of the sensor. This step is required in order to see discovered assets.

Network Passive Sensor supports mirror traffic of SPAN, RSPAN, and ERSPAN methods. For more information, refer to the [Deployment Guide](#).

Step 1 - Generate a Personalization Code

Each sensor needs a unique personalization code to register it with the Qualys Cloud Platform. Log into the Qualys UI and pick the **Network Passive Sensor** app. On the **Home** screen, choose **Deploy Network Sensor** OR on **Sensors** tab, choose **New Sensor** and pick **Physical Sensor** or **Virtual Sensor**.



Step 2 - Deploy and Register the Appliance

Add the appliance to your network and make network configuration settings.

Physical Appliance

Depending on your appliance variant (with LCD or without LCD), you can do your configurations using LCD interface for using remote console connected using serial port.

Configurations using LCD interface - Plug-in the physical appliance on your network. Then use the LCD display on the appliance to make network configuration settings (static IP, proxy). You'll also register the appliance using the personalization code copied from Step 1 by entering it using the LCD display on the appliance. Refer to the [Physical Appliance User Guide](#) for the detailed steps.

Configurations using serial port - Plug-in the physical appliance on your network. Then use PuTTY to connect using serial port and to display remote console for network configuration settings (static IP, proxy). You'll also register the appliance using the personalization code copied from Step 1 by entering it using the option in the remote console. Refer to the [Physical Appliance User Guide](#) for the detailed steps.

Virtual Appliance

Download the virtual appliance image from the New Sensor wizard or from Home > Deploy Network Sensor > Virtual Sensor in the Network Passive Sensor UI and deploy it in VMware ESXi or Microsoft Hyper-V. When you start up the new virtual machine a virtual console window appears where you'll make network configuration settings (static IP, proxy). You'll also register the appliance using the "Personalize this scanner" option in the console window. Refer to the [Virtual Appliance User Guide](#) for the detailed steps.

Step 3 - Configure Assets

Network Passive Sensor can see traffic flows between two types of IP addresses. These IP addresses can be internal (within your network) or external (outside your network).

You can configure how you want to categorize your assets discovered by the sensors while monitoring traffic flow. All these assets are listed in the **Assets** tab of **Global AssetView/CyberSecurity Asset Management**.

Assets can be defined as Internal Assets, Excluded Assets, and External Assets.

Internal Assets

To add internal assets, simply go to **Configuration > Internal Assets > Add**.

← Internal Assets

Internal Assets

Define the IP ranges within your network that you want to monitor. These IP addresses will be individually tracked for traffic analysis.

The passive sensor senses all the traffic that you have mirrored. However, by defining internal asset ranges, you choose the assets you want to monitor and report on.

Internal Asset Group/Network

Name *

ICS_test_group

Include the Following Sensors

Select Sensors

1 SENSOR SELECTED

Remove All

Test_Sensor

×

Do you want to inventory the assets? ?

☒ Yes ☐ No

Internal Asset IP Range

Default IP Ranges

☒ 192.168.0.0/16

☒ 172.16.0.0/12

☒ 10.0.0.0/8

Type

DHCP

Cancel

Save

Here, you define the IP ranges within your network you want to monitor. The assets discovered for these IP addresses will be individually inventoried and tracked for traffic analysis. You can use default IP ranges, IP range tags, or customized IP ranges options to define range of internal assets. NPS will inventory assets for the IP ranges configured in the Internal Asset IP Range when default option under Do you want to Inventory the assets is set to **Yes**.

Select **No** if you want to just monitor the traffic flows to/from the configured IP ranges but do not want to track them in asset inventory. You can always edit the sensor configuration later to add assets for the IP ranges to the inventory if you have selected No while registering virtual or physical sensors.

To complete the sensor setup and to start sensing assets you must define Internal Asset ranges. The passive sensor senses all the traffic that you have mirrored. However, by defining internal asset ranges, you choose the assets you want to monitor and report on.

1 - Default IP Ranges

This option defines internal assets discovered within default internal ranges for your network. Click **Select Sensors** to select sensor from the list of sensors for which you want to define internal asset.

Include the Following Sensors

Select Sensors

1 SENSOR SELECTED

Remove All

Test_Sensor

×

Do you want to inventory the assets? ?

☒ Yes ☐ No

Internal Asset IP Range

Default IP Ranges

☒ 192.168.0.0/16

☒ 172.16.0.0/12

☒ 10.0.0.0/8

Type

DHCP

Cancel

Save

2 - IP Range Tags

This option defines internal assets discovered with IP range tags. These are the dynamic tags created with 'IP Address In Range(s)' rule engine. Click **Select Sensors** to select sensor from the list of sensors for which you want to define internal asset. Click **Select IP Ranges** to select IP tags from the list of tags for which you want to define internal asset.

Include the Following Sensors

Select Sensors

Remove All

1 SENSOR SELECTED

Test_Sensor

×

Do you want to inventory the assets? ?
☒ Yes ☐ No

Internal Asset IP Range
IP Range Tags

Include the Following IP Tags

Select IP Ranges

TAGSIP RANGES

nov_tag110.113.231.21,10.113.231.38,10.113.231.71,10.113.231.73,10.113.231.77,1...

×

Type
DHCP

CancelSave

3- Custom IP Ranges

This option defines internal assets discovered with custom IP ranges. You can provide IP ranges for monitoring. Click **Select Sensors** to select sensor from the list of sensors for which you want to define internal asset.

Include the Following Sensors

Select Sensors

Remove All

1 SENSOR SELECTED

Test_Sensor

×

Do you want to inventory the assets? ?
☒ Yes ☐ No

Internal Asset IP Range
Custom IP Ranges

IP Ranges +
10.10.10.0/12

Type
DHCP

CancelSave

Excluded Assets

Here, you'll define the IP ranges or MAC addresses to be excluded from the inventory. The assets discovered for these addresses will be masked as Excluded in the traffic summary.

To add excluded assets, simply go to **Configuration > Excluded Assets > Add**.

The screenshot shows the 'Excluded Assets' configuration form. At the top, there is a blue header bar with a back arrow and the text 'Excluded Assets'. Below this, the form has a title 'Excluded Assets' followed by a descriptive paragraph: 'Define the IP or MAC addresses to be excluded from the inventory. The assets discovered for these addresses will be masked as "Excluded" in traffic summary.' The form contains two main sections. The first section is for 'Name', with a text input field and a 'Required' label. The second section is for 'Asset Type', with two radio buttons: 'IP Ranges' (selected) and 'MAC Address'. Below this is a text input field with the placeholder 'Enter an IP Range...' and a '+' icon. At the bottom of the form are 'Cancel' and 'Save' buttons.

Monitor External Assets

Here, you'll define the external sites you want to monitor. These sites will be reported individually for traffic summary however these will not be inventoried like the internal assets.

To add external assets, simply go to **Configuration > Monitor External Assets > Add**.

The screenshot shows the 'External Assets' configuration form. At the top, there is a blue header bar with a back arrow and the text 'External Assets'. Below this, the form has a title 'External Assets' followed by a descriptive paragraph: 'Define the external sites you want to monitor. These sites will be reported individually for traffic summary however; these will not be inventoried like the internal assets.' The form contains two main sections. The first section is for 'Name', with a text input field and a red asterisk indicating it is required. The second section is for 'Details', with a text input field containing the placeholder 'Enter an IP Address or a domain name' and an 'Add' button. At the bottom of the form are 'Cancel' and 'Save' buttons.

General Settings

General Settings tab consists of two sub tabs: General Configuration and Exclusion.

General Configuration

- You can help Qualys NPS to enhance the operating system and device prediction of the asset by providing fingerprint data.
- You can set up notifications for events like Driver Change Required, Reboot Required, and Asset Reporting Stopped to be sent to your email address.

You can see the latest events generated in the events section of the sensor details page.

EVENTS	COUNT	HOSTNAME	TYPE	TIMESTAMP RANGE
Driver Change Required	1	AUJ	Moderate	07 Sep 2023 08:56 am
Reboot Required	1	AUJ	Moderate	07 Sep 2023 08:52 am

Exclusion

You can exclude specific hostnames when merging unmanaged assets or merging them into managed assets.

General Configuration

Qualys NPS service utilizes the data gathered from traffic flows to predict the OS and hardware. NPS does not collect any user-specific sensitive data. It collects the protocol-specific data gathered from packet headers, which are transparently displayed to the customer in the asset's Raw Discovery Data (in the **CSAM/GAV > Asset Details > System Information > View Raw Information Data** section).

NPS service identifies patterns in this data to predict OS and device models. There is always a scope for improving pattern recognition to detect more OS and device models. Once consent is given, Qualys can collect the asset's metadata and utilize it to enhance predictions of OS and device models in future releases.

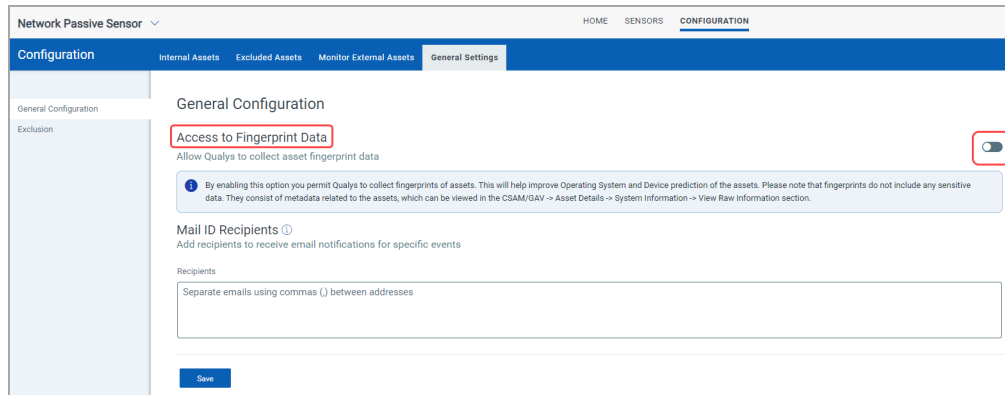
Follow these steps to configure the general settings.

- Navigate to **Configuration > General Settings > General configuration**.
- To give consent to Qualys to access the metadata, toggle Access to Fingerprint Data to allow access.

Go to the **Recipients** text box and add the e-mail. You can add multiple e-mails using comma separated.

Click **Save**

Once you add the recipients, they receive the events in their e-mail inbox.

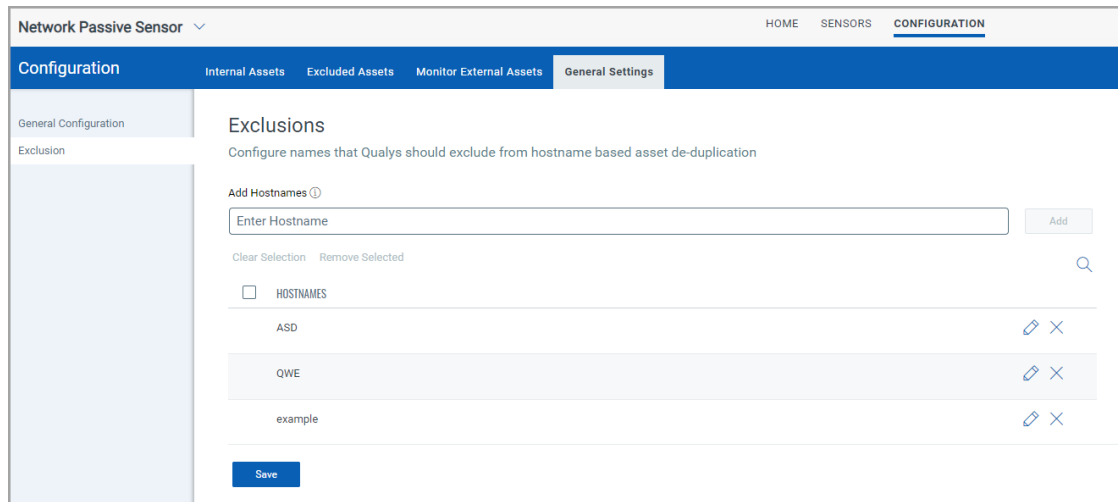


Exclusion

You can configure hostnames that need to be excluded while merging unmanaged assets or merging unmanaged assets into managed assets.

The hostnames provided here are case-insensitive. When a new hostname is added to the exclusion list, make sure first to purge the asset created for that hostname. Refer the following screenshot for configuring excluded hostnames.

Also, you can configure hostnames that need to be excluded while de-duplicating unmanaged assets or de-duplicating unmanaged assets into managed assets. The hostnames provided here are case-insensitive. When a new hostname is added to the exclusion list, make sure first to purge the asset created for that hostname. Refer to the following screenshot for configuring excluded hostnames.



Note: Contact [Qualys Customer Support](#) to get them deleted to avoid deduplication in the future.

Step 4- Check the status

Your sensor needs to successfully connect to the Qualys Cloud Platform to start discovering assets. The **Sensors** tab in the **Network Passive Sensor** UI shows the status for each sensor that's been added.

Once connected, the sensor starts reporting new discoveries. On the Sensors tab you can see the count for total assets discovered and assets discovered in the last 24 hours.

Network Passive Sensor

HOMESENSORSCONFIGURATION

Sensors

0Active Assets (7days)

0New Discoveries (24hrs)

FiltersNew Sensor

1 - 4 of 4

SENSOR	DEPLOY LOCATION	ACTIVE ASSETS (1 HOUR)	NETWORK UTILIZATION	CPU	RAM
<div><div></div><div>PS_AutoVirtual</div><div>Unregistered</div></div>	Pune	0	0	0	0
<div><div></div><div>PS-1</div><div>Unregistered</div></div>	Pune	0	0	0	0
<div><div></div><div>Test_Sensor</div><div>QPS-01G-0100-VM 1.3.3-8</div><div>Sensing</div></div>	Pune	0	0.03 Gbps/1.0 Gbps	19%	22%

Step 5- View Asset Details in Asset Inventory

Network Passive Sensor reports all discoveries to Qualys Asset Inventory, where discoveries are first checked against the existing list of managed assets. Assets that are already known by active scans or from cloud agents are considered managed assets. When such assets are found by the sensor, the asset data is correlated and de-duplicated. Assets that are previously unknown are considered unmanaged assets.

You can toggle your view between All, managed and unmanaged assets at any time.

CyberSecurity Asset Management						
Inventory						
184 Total Assets		Choose All, Managed, Unmanaged from here				
MANUFACTURER		TOP OPERATING SYSTEMS CATEGORIES				
Unidentified 123		Linux Unidentified Windows Network Oper... Mobile				
VMware 57		All Managed Unmanaged				
Cisco Systems 2		1 - 50 of 184				
LG 1		ASSET				
Palo Alto Networ... 1		CRITICALITY OPERATING SYSTEM HARDWARE LAST USER SOURCES MODULES TAGS				
		2 Linux Virtualized				
		First Foun... Last Seen: S...				

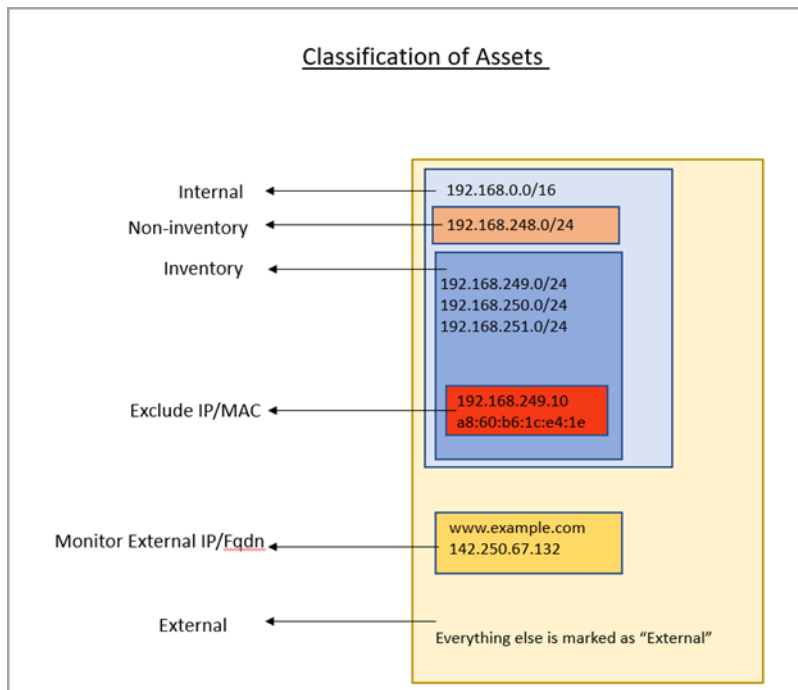
Classification of Assets in Passive Sensor

Passive sensor classifies IPs as internal and external for the purpose of asset inventory and traffic monitoring.

The area labelled “Internal” in the diagram below is the universe of IP ranges that exists within an enterprise and therefore worth building an asset inventory. Everything outside this range is “External” and not worth inventorying.

From a traffic monitoring perspective, PS tracks flows between assets in the inventoried IP range by 4-tuple. PS does not track individual IPs in the “External” range and attributes all external IPs to a single asset named “External”.

Following is a detailed explanation of how PS treats each class of IPs.



What is Inventory

PS uses IP addresses in this range to

- Create assets and inventory various asset attributes such as hostname, MAC address, protocol specific attributes, etc.
- Track traffic flows to/from these IPs to other all other IPs outside this range.

Assets with IPs in this range are listed under the CSAM inventory.

PS aggregates the traffic flows from an IP in the internal range to another IP in the internal range by 4-tuple of Source IP, Destination IP, Destination port, and TCP or UCP protocol. Appliance reports traffic flows at an interval of 5 minutes for new assets and at 30 minutes for asset updates.

The appliance aggregates multiple flows of the same tuple into one flow when reporting it in the 5- or 20-minutes reporting interval.

For example, if Asset A1 initiated HTTP flow to a webserver A2 multiple times within the 30 minutes interval, PS aggregates these flows and reports a single HTTP flow from A1 to A2 at reporting time.

How to Configure Inventoried IP Range

To configure an IP range/subnet as internal inventoried, select the appliance from the Passive Sensor Module listing and navigate to its details to edit the internal asset configuration. Here add the IP range. NPS will inventory assets for the IP ranges configured in the Internal Asset IP Range when default option under Do you want to Inventory the assets is set to **Yes**.

Select **No** if you want to just monitor the traffic flows to/from the configured IP ranges but do not want to track them in asset inventory. You can always edit the sensor configuration later to add assets for the IP ranges to the inventory.

← Internal Assets

Internal Assets

Define the IP ranges within your network that you want to monitor. These IP addresses will be individually tracked for traffic analysis.

The passive sensor senses all the traffic that you have mirrored. However, by defining internal asset ranges, you choose the assets you want to monitor and report on.

Internal Asset Group/Network

Name *

Subnet-A

Include the Following Sensors [Select Sensors](#)

1 SENSOR SELECTED [Remove All](#)

NPS-A

Do you want to inventory the assets? ?

☒ Yes ☐ No

Internal Asset IP Range

Custom IP Ranges

IP Ranges *

10.10.10.0/24

Type

DHCP

[Cancel](#) [Save](#)

What is Non-inventory

PS uses IP addresses in this range only for tracking traffic flows to other IPs in the inventory range and NOT for inventory purpose. Assets in this IP range do not show in the CSAM inventory. However, traffic flows to/from these assets are listed in the Network tab of CSAM and under the inventoried asset-centric traffic tab of CSAM.

How to Configure Non-Inventoried IP Ranges

To configure an IP range/subnet as internal non-inventoried, select the appliance from the Passive Sensor Module listing and navigate to its details to edit the internal asset configuration. Here add the IP range. NPS will inventory assets for the IP ranges configured in the Internal Asset IP Range when default option under Do you want to Inventory the assets is set to **Yes**.

Select **No** if you want to just monitor the traffic flows to/from the configured IP ranges but do not want to track them in asset inventory. You can always edit the sensor configuration later to add assets for the IP ranges to the inventory.

← Internal Assets

Internal Assets

Define the IP ranges within your network that you want to monitor. These IP addresses will be individually tracked for traffic analysis.

The passive sensor senses all the traffic that you have mirrored. However, by defining internal asset ranges, you choose the assets you want to monitor and report on.

Internal Asset Group/Network

Name *

Subnet-B

Include the Following Sensors

Select Sensors

1 SENSOR SELECTED

Remove All

NPS-A

×

Do you want to inventory the assets? ⓘ

☐ Yes ☒ No

Internal Asset IP Range

Custom IP Ranges

IP Ranges *

10.20.20.0/24

+

Type

DHCP

Cancel

Save

To review the configuration, check the last column “Inventoried”

Configuration

Internal Assets

Excluded Assets

Monitor External Assets

General Settings

☐

Actions (0)

Add

1 - 13 of 13

⏮ ⏪ ⏩ ⏭ ⚙

NAME	IP RANGE	SENSOR	TYPE	INVENTORIED
Subnet-A	10.10.10.0/24	NPS-B	DHCP	No
Subnet-A	10.10.10.0/24	NPS-A	DHCP	Yes
Subnet-B	10.20.20.0/24	NPS-A	DHCP	No
Subnet-B	10.20.20.0/24	NPS-B	DHCP	Yes

What is Excluded

If there is a need to not see some sensitive or confidential assets listed in the inventory, then the passive sensor allows the user to specify configuring IPs and/or MACs in the Excluded range.

PS excludes gathering all inventory information of the IPs/MACs added in this category/group. These assets do not show in the CSAM asset listing. In the traffic flows to/from these assets as seen in the traffic listing, the asset is seen as Excluded without any IP-address.

How to Configure Excluded IPs/MACs

To configure an IP / MAC as excluded, select the appliance from the Passive Sensor Module listing and navigate to its details to edit the Excluded Assets configuration.

Network Passive Sensor		
Configuration		
Internal Assets Excluded Assets Monitor External Assets General Settings		
<input type="checkbox"/> Actions (0) <button>Add</button>		
NAME	TYPE	IP RANGE
exclude-test-dns	IP	10.1.1.1
test-exclude	IP	10.1.1.1

Traffic summary representation for Excluded Assets:

curl 7 29 0		curl 7 29 0		Client	43.75 KB	12.98 KB	56.73 KB
TIMESTAMP	THIS ASSET (CLIENT)	FROM/TO	PROTOCOL	PORT	INGRESS	EGRESS	TOTAL
Mar 02 2022 13:42	10.1.1.1	Excluded	tcp	3128	6.06 KB	1.88 KB	7.94 KB
Mar 02 2022 13:42	10.1.1.1	Excluded	tcp	3128	37.69 KB	11.1 KB	48.79 KB

What is Monitored External

PS does not track IPs outside the inventoried and non-inventoried range and attributes them to one asset named External as explained earlier. However, the user may want to monitor traffic flows from internal assets to certain external IPs/FQDNs. For example, monitor the volume of traffic from internal assets to social media sites such as Facebook, Twitter, etc. PS provides a "Monitored External" configuration and uses FQDNs or IPs specified therein, to track traffic flows destined to an asset created per group. These assets do not show in the CSAM asset listing. In the traffic flows to/from these assets as seen in traffic listing, the asset is seen as External if FQDN was added or the actual IP, if IP was added".

How to Configure Monitor External FQDNs or IPs

Select the appliance from the Passive Sensor Module listing and navigate to its details to edit the External Assets configuration to add FQDN / IP in a group. The following screenshots shows 2 groups, each one with a unique name. PS will track traffic flows going to one of the 2 assets that represents each group.

Configuration		
Internal Assets Excluded Assets Monitor External Assets General Settings		
<input type="checkbox"/> Actions (0) <button>Add</button>		
NAME	DETAILS	
social-media	31	www.facebook.com
yahoo-website	www.yahoo.com	

Traffic summary representation of Monitor External Assets & External Assets:

FAMILY	APP/SERVICE	CLIENT/SERVER	INGRESS	EGRESS	TOTAL
Web Services	HTTPs	Client	10.59 MB	996.19 KB	11.57 MB

TIMESTAMP	THIS ASSET (CLIENT)	FROM/TO	PROTOCOL	PORT	INGRESS	EGRESS	TOTAL
Mar 02 2022 19:01	10.1	External	tcp	443	8.51 MB	109.11 KB	8.62 MB
Mar 02 2022 19:01	10.1	External	tcp	443	15.06 KB	2.14 KB	17.2 KB
Mar 02 2022 19:00	10.1	External	tcp	443	6.29 KB	1.04 KB	7.33 KB
Mar 02 2022 18:57	10.1	98.137.11.165	tcp	443	4 KB	3.22 KB	7.23 KB
Mar 02 2022 18:55	10.1	31.13.65.36	udp	443	40.9 KB	28.5 KB	69.4 KB

External Assets Traffic

Monitor External Assets Traffic

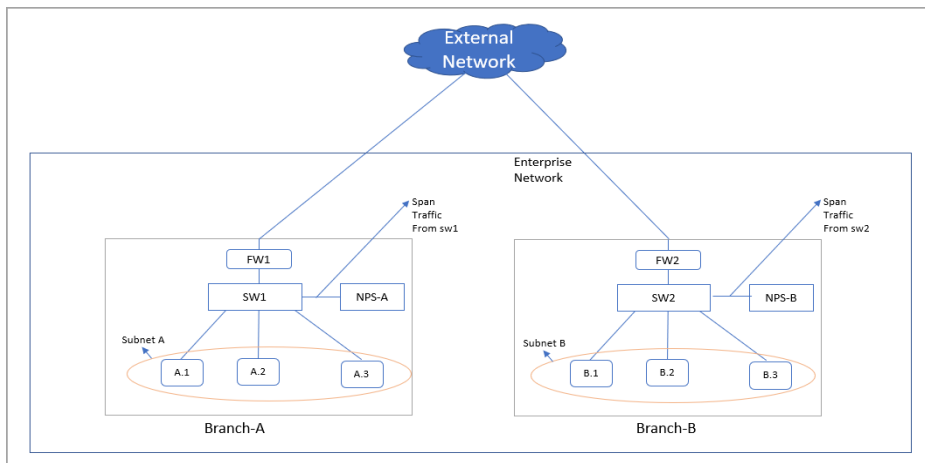
Best Practices

This section contains certain best practices to follow when configuring the internal assets in PS appliances.

1. Avoid configuring overlapping subnets as internal (inventoried) assets on more than one sensor appliance

In deployments that have more than one passive network sensor appliances registered with the same Qualys cloud account, it is recommended that the configuration of internal inventory network ranges should not overlap between the sensors.

To explain this better, let us consider a sample deployment that has 2 sensors deployed in different locations registered to the same account.



The enterprise network in the above scenario has 2 branches A and B. There are 2 sensors deployed one each in branch A and B. For the enterprise network subnets A and B together make up the range on IPs for internal assets that have to be inventoried. Assets A.1, A.2, and A.3 belong to subnet A and B.1, B.2, and B.3 belong to subnet B.

Now consider a case where there is intra branch traffic. Each of the sensors in branch A and B will "see" traffic flows from/to assets in subnets A to B.

For example, if A.1 were to initiate a flow to B.1, both sensors would sense this flow. If both sensors are configured with subnet A and B as the internal (inventoried) range, then both sensors will report assets A.1 and B.1 causing the same assets to be reported twice to Qualys cloud. This causes additional workload on the cloud services and this may result in delayed or missed updates of the assets or traffic flows as seen in the asset or traffic listing.

This workload multiplies if there are flows from each one of the assets in subnet A to B.1, such as A.1 to B.1, A.2 to B.1, and A.3 to B.1.

So, adding the same subnet into multiple sensors is inefficient and not a recommended configuration.

Desired/Recommended configuration: Detect assets in location specific subnets and provision a "non-inventoried" asset category

A recommended configuration to avoid duplicate processing on the cloud is to configure each sensor with a unique subnet as its inventoried range and add the other subnets internal to the organization as its internal non-inventoried range.

So in the above example, the sensor deployed in Branch A would only consider IPs of subnet A as the internal IPs and treat everything else as external. This means even subnet B which belongs to the universe on internal IPs of the organization would be considered external to the sensor in branch A. However, to track the inter-branch traffic flows so to know which asset in subnet A was talking to which asset in subnet B and vice-versa, it is recommended to add subnet B as internal (non-inventoried) range in sensor of location A. The passive sensor uses the non-inventoried range or IP to create assets whose attributes are not collected just as in the case of External assets but with a difference that its IP is recorded.

Similarly for the sensor in location B, configure subnet B as its internal inventoried range and subnet A as its internal non-inventoried range.

With the above configuration sensor in location A would report A.1, A.2, and A.3 as internal inventoried assets and B.1 as the non-inventoried assets. Similarly, the sensor in location B would report B.1 as its internal inventoried asset and A.1, A.2, and A.3 as its non-inventoried asset.

This configuration saves the PS services from the burden of additional processing. This also conserves the WAN bandwidth needed by sensors to report metadata to Qualys cloud as only one sensor reports the inventoried assets.

To summarize, the configuration of both passive sensors is as follows:

Passive Sensor Appliance Location	Internal (inventoried)	Internal (non-inventoried)
Branch A	Subnet A	Subnet B
Branch B	Subnet B	Subnet A

2. Avoid mirroring replicated IPs to a single appliance

In topologies, more common in OT networks, multiple smaller networks can have the same IP subnet. Each such replicated IP subnets has to be mirrored to a separate PS appliance. Avoid mirroring multiple such subnets to one appliance.

For example, consider a site with a yard having many cranes and each crane is a small network having exactly the same type of devices with the same IPs configured.

The overlapping IP address space in each crane can be handled by the Network feature which the customer can subscribe to. This feature allows the same subscription to uniquely identify IP within a network.

The Network feature is already supported in VM and PC modules. NPS uses the network feature by de-duplicating passively sensed unmanaged IPs/assets with managed assets belonging to the same Network. NPS exercises the network-based to de-duplicate assets only when it has neither MAC nor hostname information to uniquely identify the assets for de-duplication.

So here is what the configuration of PS appliance in each crane would look like

Crane #1

- Add Crane#1 IP range R1 in Asset Group AG1 in Network N1 in VM module
- Run policy compliance scan for the asset group AG1 in N1 in VM module
- Add NPS1 to Network N1 and configure NPS 1 to sense IP range R1 in N1

Crane #2

- Add Crane#2 IP range R2 in Asset Group AG2 in Network N2 in VM modules
- Run policy compliance scan for the asset group AG2 in N2 in the VM module
- Add NPS2 to Network N2 and configure NPS 2 to sense IP range R2 in N2

3. Add NATed IPs in the excluded list

PS does not yet support the capability to detect NATed devices. All assets behind NAT devices get masqueraded by the NATed IP and if PS sees this NATed IP, it will associate meta-data/attributes of all such devices to a single asset which has the Nated IP, making the asset very large, and these slow down the processing pipeline on the cloud. So, it is recommended to add such IPs as internal assets to be excluded.

4. Do not feed multiple copies of the same packet to the sensor

It is important that the TAPs or SPAN ports that feed the traffic copy to PS do not contain duplicate copies of the same packet. This will result in PS reporting incorrect volumes of traffic flow.

5. Backup and restore of PS VM image

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