Network Passive Sensor

Getting Started Guide

April 29, 2022

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

Table of Contents

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 PS continuously monitors all 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

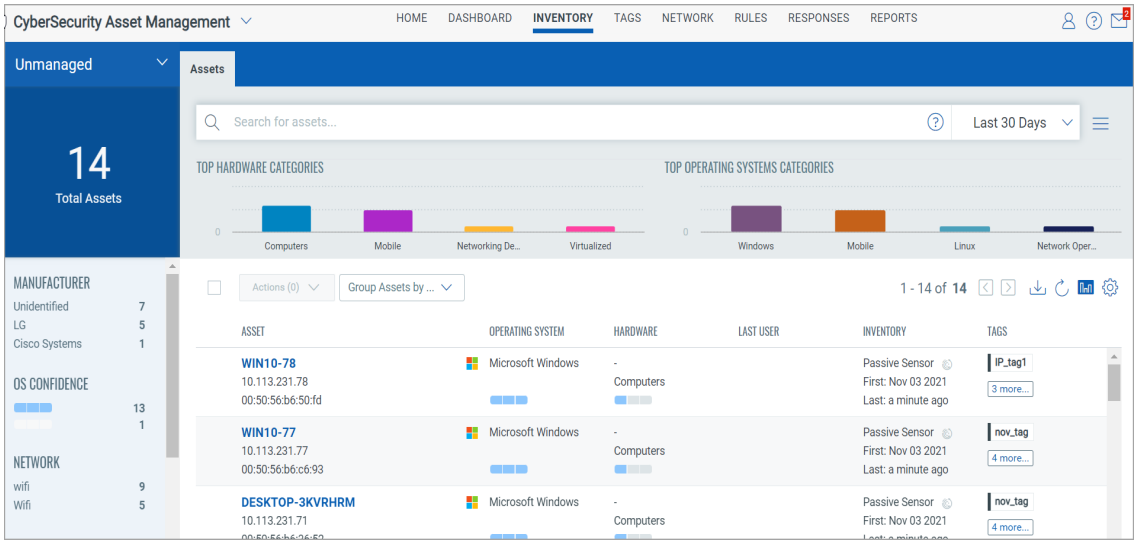
Qualys PS identifies assets that for different reasons can't be actively scanned or monitored with agents. That's often the case with assets like industrial equipment, IoT and medical devices.

Centralized control and visibility of assets

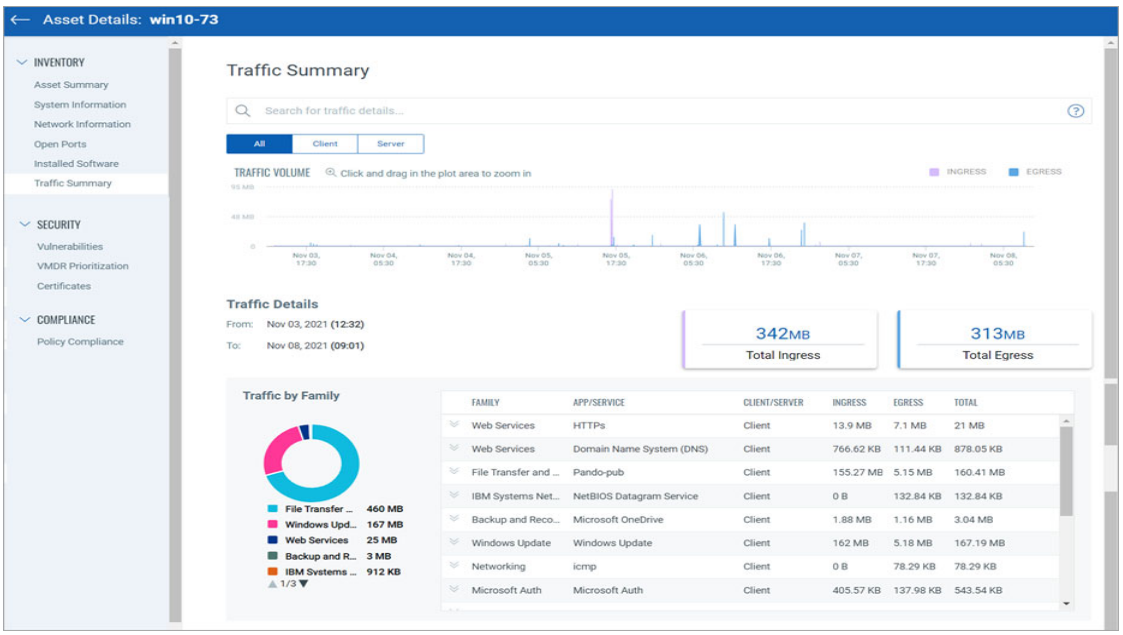
The Qualys Asset Inventory cloud app aggregates and correlates the data gathered by all Qualys sensors – Qualys Passive Sensors, the Qualys network scanners and the Qualys Cloud Agent – giving you a comprehensive, detailed inventory of all your hardware and software, as well as a multi-dimensional view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

What are the benefits?

You'll 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'll get enterprise application identification (e.g. database) based on traffic pattern.

How it works

The Network Passive Sensor 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 then catalog assets by operating system and hardware.

All assets discovered by Network Passive Sensor are reported to Qualys Asset Inventory where you can see information about them.

If an asset discovered by the sensor is already known by active scans or by cloud agent then it is considered a managed asset and the asset data is correlated and merged using MAC or hostname as a criteria. So, if the MAC or hostname of passively sensed asset matches with that of the managed asset, then two assets are merged and shown in the **Managed** inventory.

The hostname based merge relies on exact match. Hence, in the case where passive sensor sensed "johndoe" as the hostname and the managed assets' hostname is reported as "johndoe.somedomain.org" and vice-versa, the assets will not merge. The asset reported by the passive sensor is placed in the **Unmanaged** inventory, if

- it is not detected by active scan

- it is detected by active scan but not merged

Prior to PS 1.4.0.0, merging of managed and unmanaged assets was based on the MAC or hostname. From PS 1.4.0.0, the merge criteria is enhanced as follows:

• IP-only based merges provided the IPs of both managed and unmanaged assets belong to the same Network. For details refer to Appendix D- Extending the Network Feature section of the Qualys Network Passive Sensor Physical Appliance User Guide.

• IP-only based merges based on additional information of dynamic (DHCP) and static IPs. An unmanaged asset that has a static IP immediately qualifies for merge with the managed asset of the same IP. If un-managed asset has a dynamic IP assigned from the DHCP pool, the de-duplication with the managed asset of same IP will trigger provided, the last scan timestamp of managed asset is within the asset's DHCP lease period identified by PS. If DHCP lease period couldn't be determined by PS due to reasons like missing DHCP flow, then IP inactivity time is considered while merging.

- NPS uses MAC to merge if available, if not then hostname and lastly only IP.

The below table summarizes the asset merge criteria used in NPS:

Macs	IPs	Hostnames	Sensors	Merge?
Same	Doesn't Matter	Doesn't Matter	Doesn't Matter	Yes
Different	Doesn't Matter	Same	Doesn't Matter	Yes
Different	Same	Different	Same	Yes, within IP inactivity
Different	Same	Different	Different	No
Not Available	Same	Not Available	Same	Yes, within IP inactivity
Not Available	Same	Not Available	Different	No

Macs	IPs	Hostnames	Sensors	Merge?
Not Available	Same	Same	Doesn't Matter	Yes
Not Available	Same	Different	Same	Yes, within IP inactivity
Not Available	Same	Different	Different	No
Not Available	Different	Same	Same	Yes
Not Available	Different	Same	Different	Yes

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.

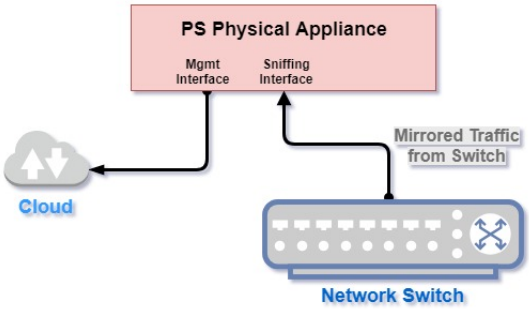
You'll assign an IP address to the management interface either statically or using DHCP. DHCP is enabled by default. Configuring the management interface is required for the Passive Sensor to have Internet connectivity and to connect to the Qualys Cloud Platform.

Sniffing Interface

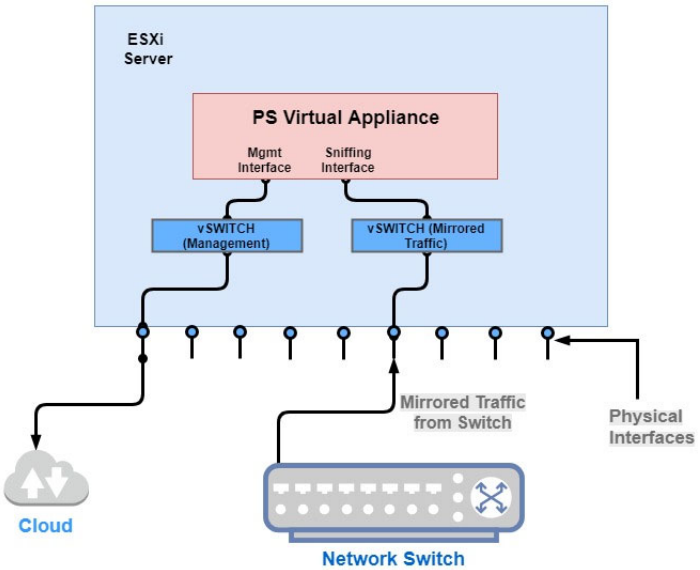
One or more traffic sniffing interfaces are used to receive mirrored traffic to the Network Passive Sensor. Once the traffic that needs to be monitored is identified: 1) Configure the switch that sees the traffic in question by mirroring the traffic to a port, 2) Connect that mirrored port to the passive 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.

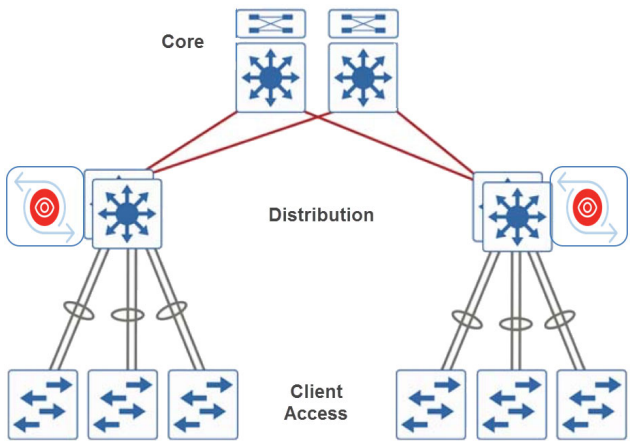
What size do you need?

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

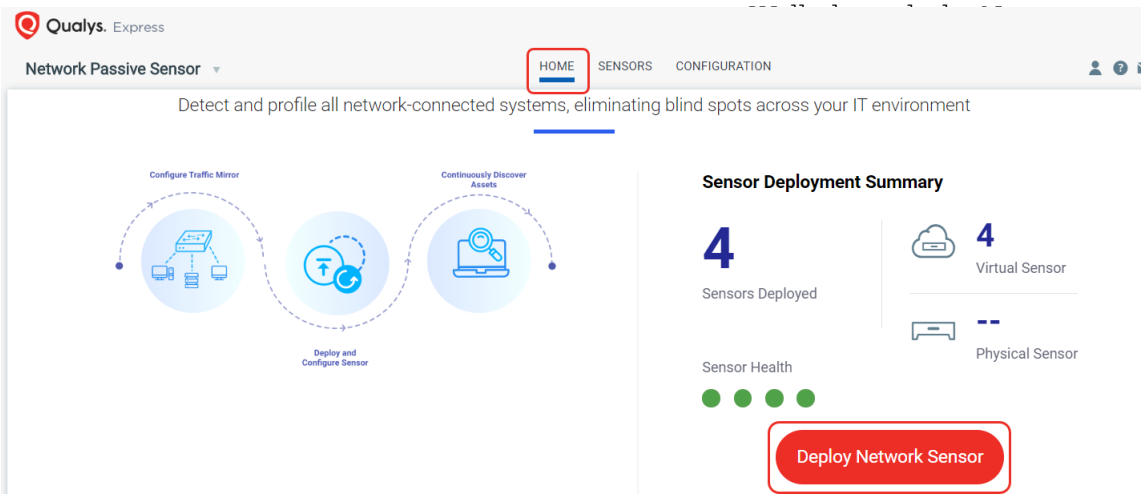
Before you begin - Mirror the traffic

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

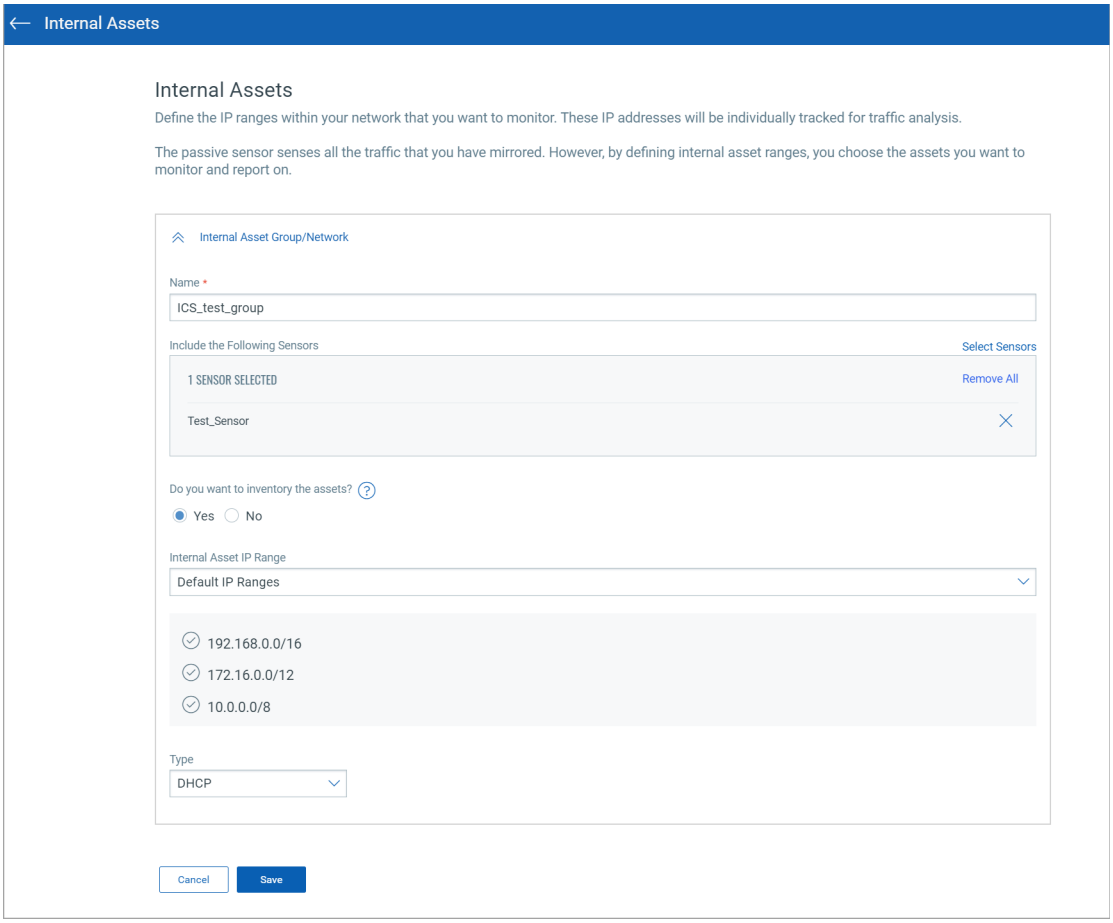
Network Passive Sensor can see traffic flows between two types of IP addresses. These IP addresses can be internal (within your network) or external (outside your network).

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**.

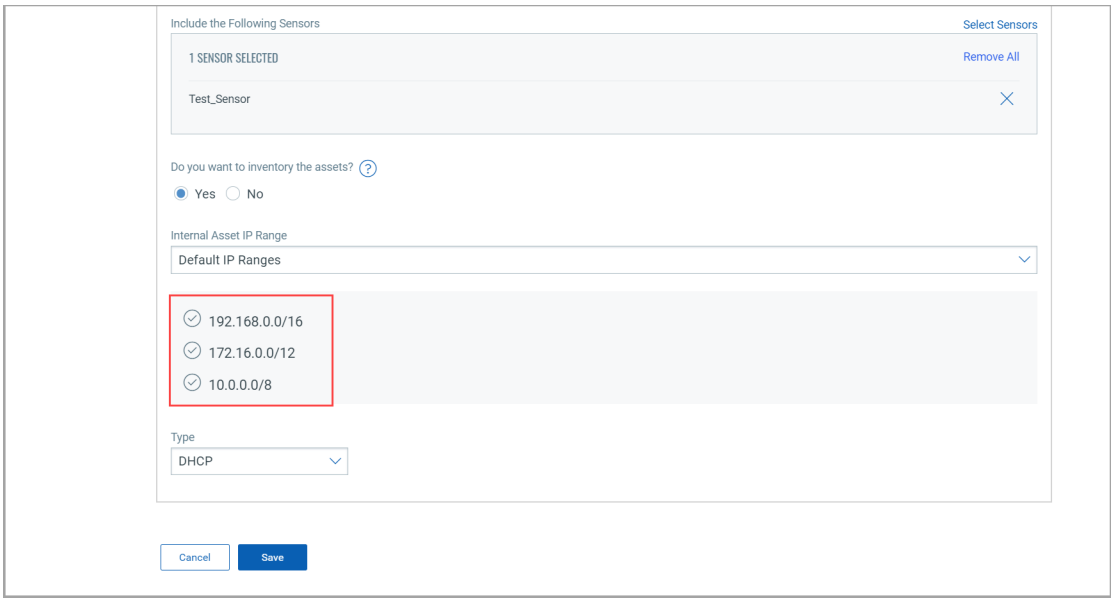


Here, you'll define the IP ranges within your network you want to monitor. The assets discovered for these IP addresses will be individually inventoried and tracked for traffic analysis. You can use default IP ranges, IP range tags, or customized IP ranges options to define range of internal assets. Select **Do you want to inventory the assets** check box for marking inventoried assets.

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.

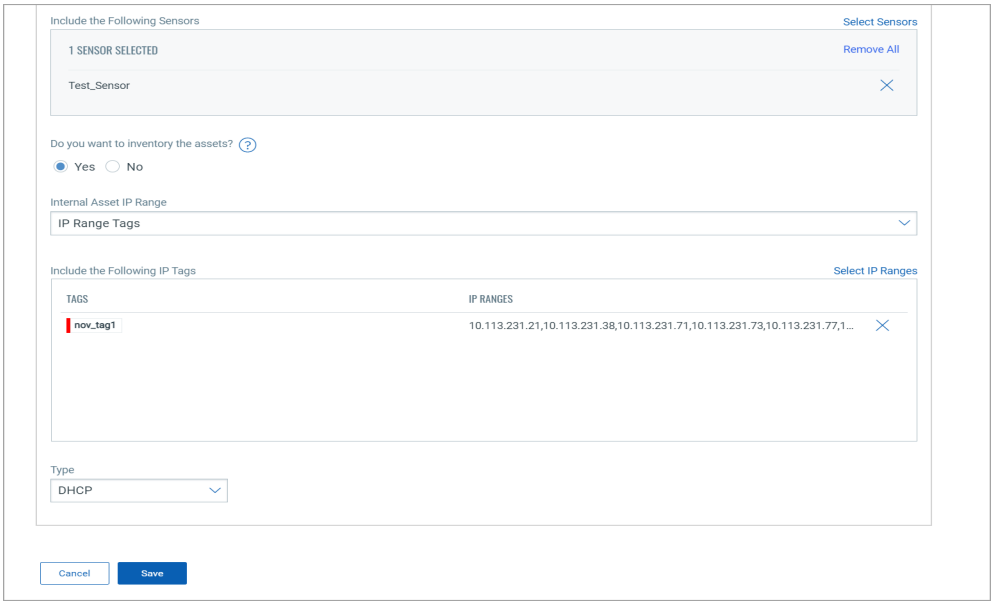
1 - Default IP Ranges

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.



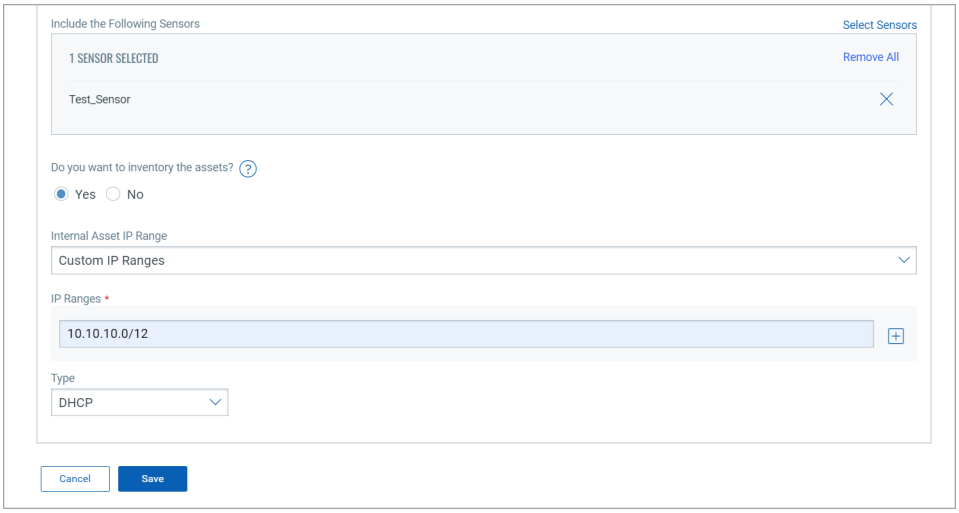
2 - IP Range Tags

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.



3- Custom IP Ranges

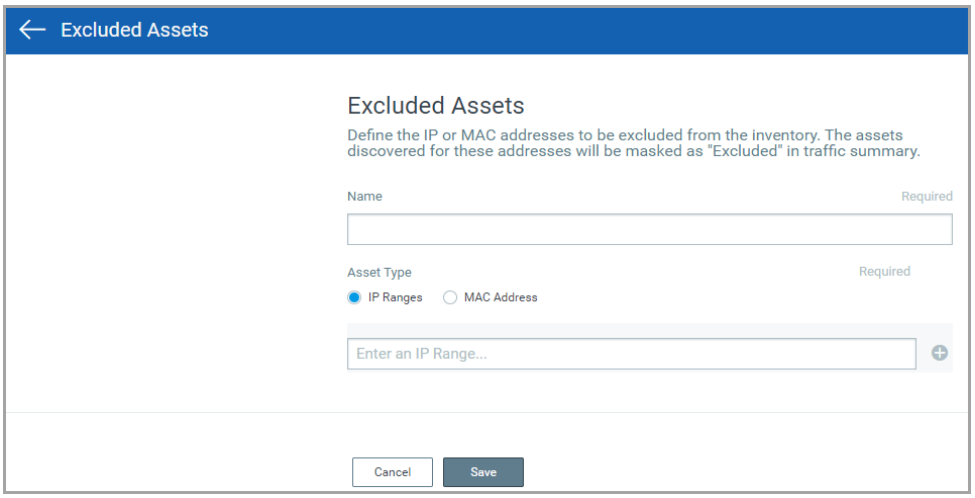
This option defines internal assets discovered with custom IP ranges. You can provide IP ranges for monitoring. Click **Select Sensors** to select sensor from the list of sensors for which you want to define internal asset.



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.

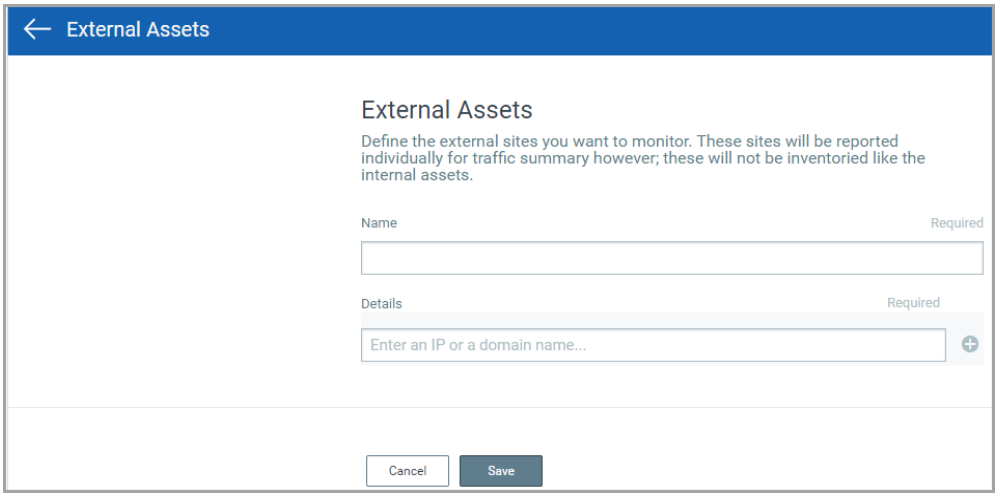
To add excluded assets, simply go to **Configuration** > **Excluded Assets** > **Add**.



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.

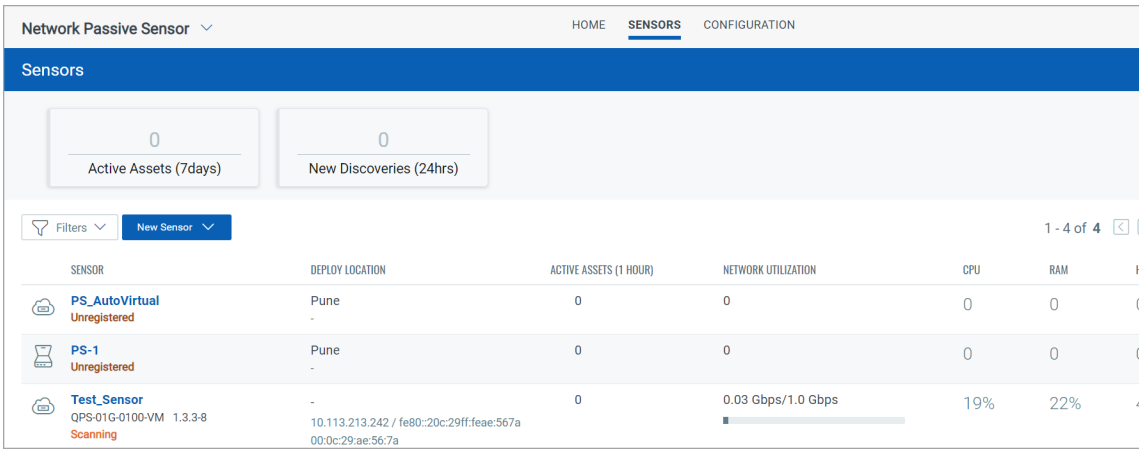
To add external assets, simply go to **Configuration** > **External Assets** > **Add**.



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.

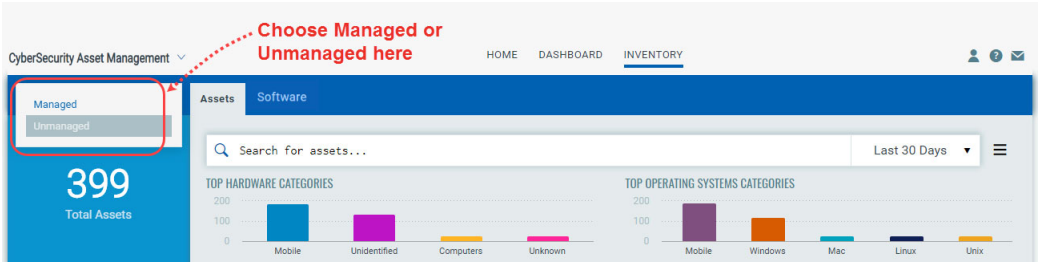
Once connected, the sensor will start reporting new discoveries. On the Sensors tab you'll see the count for total assets discovered and assets discovered in the last 24 hours.



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 merged. Assets that are previously unknown are considered unmanaged assets.

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



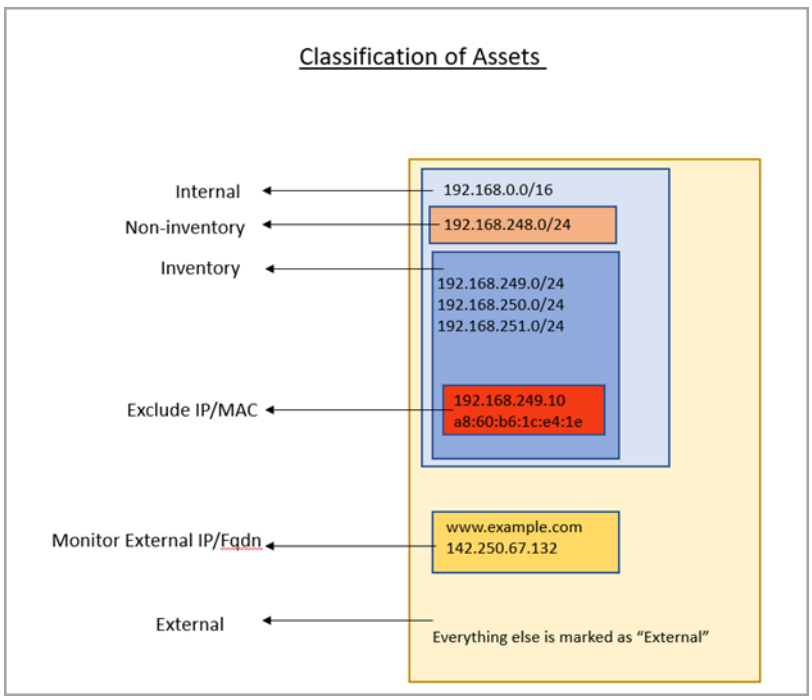
Classification of Assets in Passive Sensor

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, NPS tracks flows between assets in the inventoried IP range by 4-tuple. NPS 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 NPS treats each class of IPs.



What is Inventory

NPS uses IP addresses in this range to

a) Create assets and inventory various asset attributes such as hostname, MAC address, protocol specific attributes, etc.

b) 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.

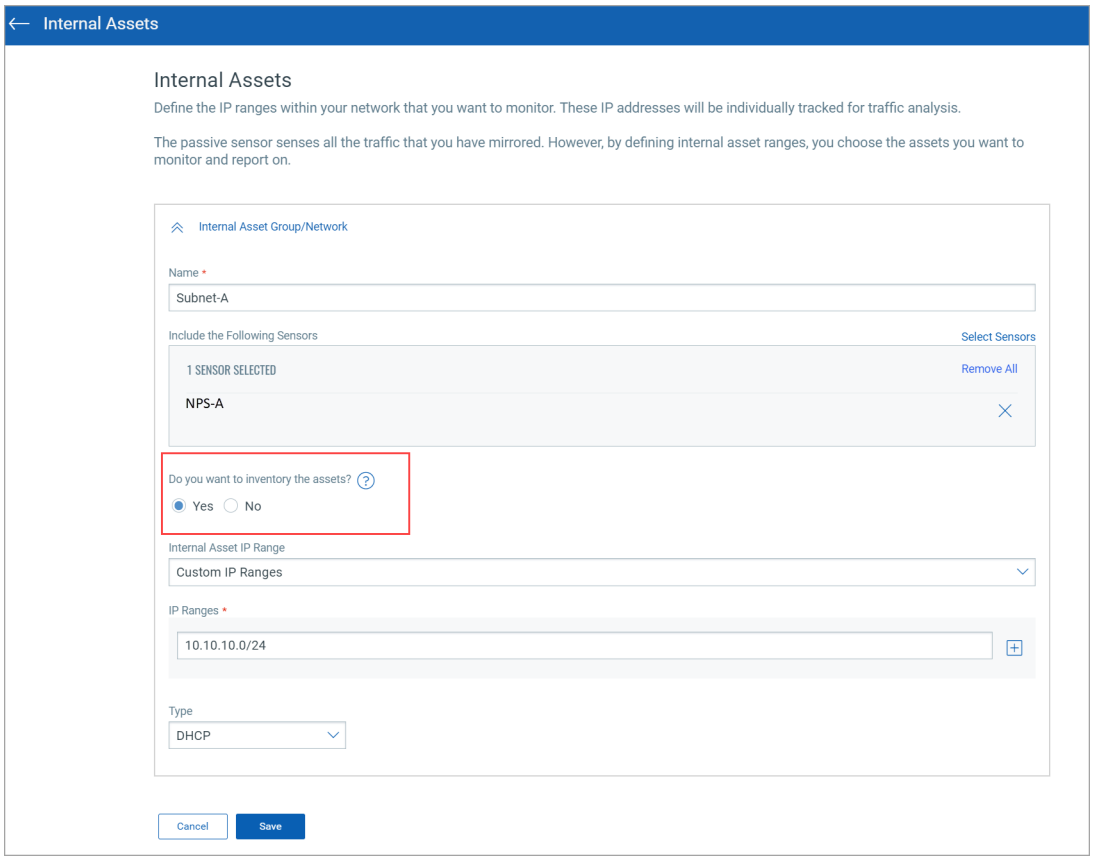
NPS aggregates the traffic flows from an IP in the internal range to another IP in the internal range by 4-tuple of Source IP, Destination IP, Destination port, and TCP or UCP protocol. Appliance reports traffic flows at an interval of 5 minutes for new assets and at 30 minutes for asset updates.

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, NPS 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 and set the radio button under "Do you want to inventory these assets?" to Yes.

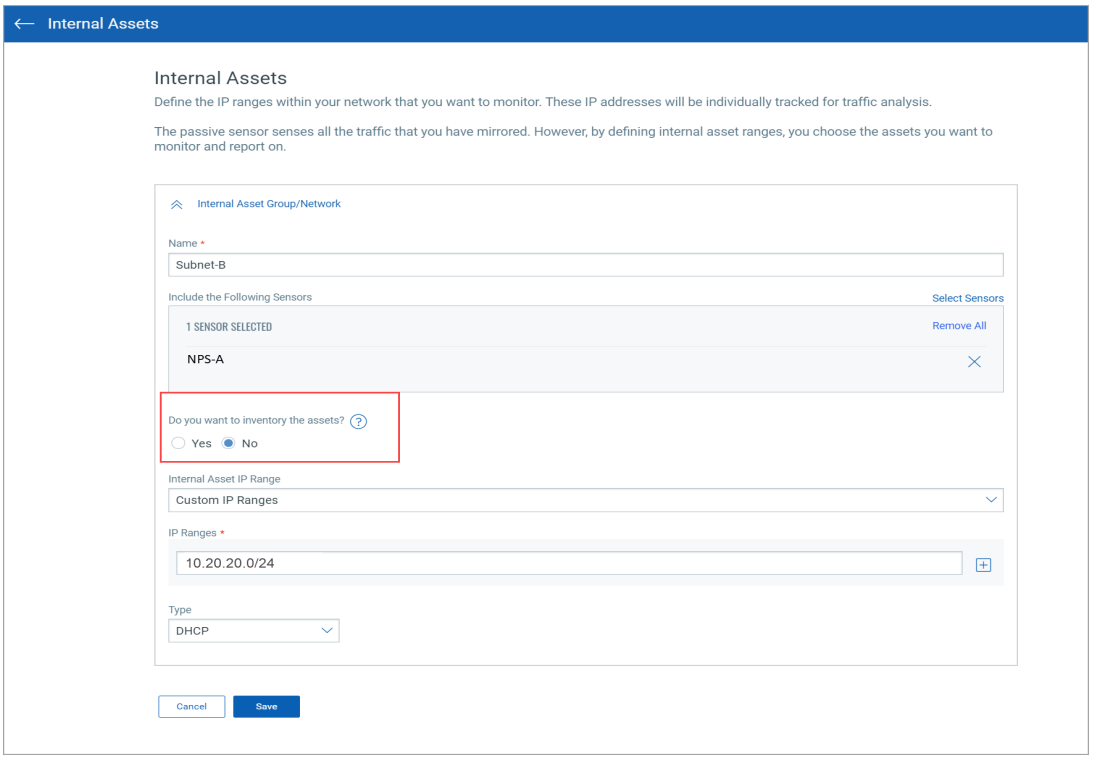


What is Non-inventory

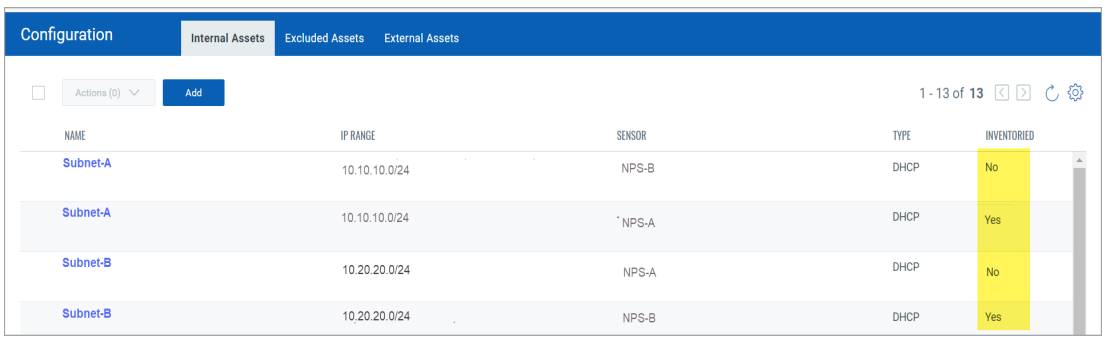
NPS uses IP addresses in this range only for tracking traffic flows to other IPs in the inventory range and NOT for inventory purpose. Assets in this IP range do not show in the CSAM inventory. However, traffic flows to/from these assets are listed in the Network tab of CSAM and under the inventoried 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 and set the radio button under "Do you want to inventory these assets?" to No.



To review the configuration, check the last column "Inventoried"



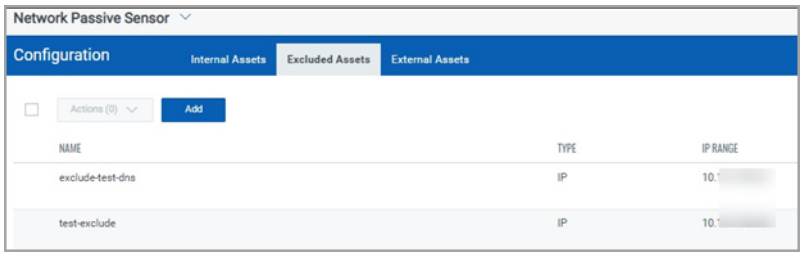
What is Excluded

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.

NPS 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.



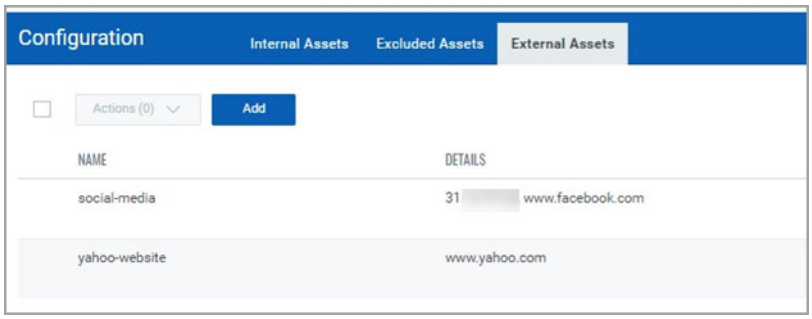
Traffic summary representation for Excluded Assets:

What is Monitored External

NPS 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. NPS 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. NPS will track traffic flows going to one of the 2 assets that represents each group.



Traffic summary representation of Monitor External Assets & External Assets:

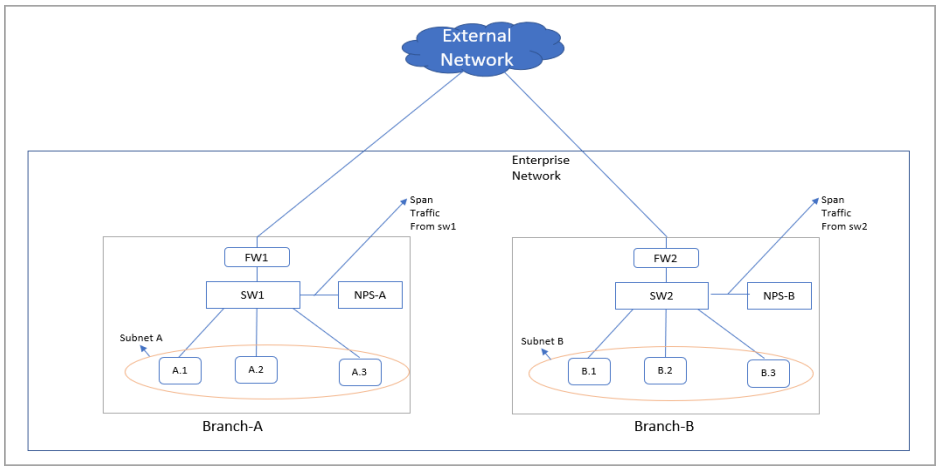
Best Practices

This section contains certain best practices to follow when configuring the internal assets in NPS 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 NPS 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 and is part of the PS 1.4.0.0 release. 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 merge 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**

NPS 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 NPS 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 NPS services on Qualys cloud account retains the sensor configuration and applies it to the appliance on reboot.