Network Passive Sensor
Virtual Appliance User Guide

September 17, 2021
Table of Contents

About this Guide ............................................................................................................. 4

Welcome to Qualys Network Passive Sensor ............................................................... 5

Network requirements / configuration .............................................................................. 5
Get Started .......................................................................................................................... 5
  Mirror the traffic .............................................................................................................. 6
  Step 1 - Download Virtualization Image ...................................................................... 6
  Step 2 - Generate Personalization Code ..................................................................... 6
  Step 3 - Deploy Virtualization Image ......................................................................... 7
  Step 4 - Register the Virtual Appliance .................................................................... 18
  Step 5 - Check the Status ......................................................................................... 18
Configure Assets .............................................................................................................. 20

Network Configurations ......................................................................................... 25

  Configure Static IP Address .................................................................................... 25
  Proxy Configuration .................................................................................................. 26

Appendix .................................................................................................................... 27

  Virtual Network Passive Sensor (PS) Appliance Packet Throughput Based on Resources 27
  Virtual Network Passive Sensor (PS) Throughput Capacity Based on Hardware ............ 27
  Adding/Removing Sniffing Interfaces from Virtual Appliance ..................................... 31
About this Guide

Welcome to Qualys Cloud Platform! In this guide, we’ll show you how to set up your virtual appliance for Qualys Network Passive Sensor.

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 a founding member of the Cloud Security Alliance (CSA).

For more information, please visit www.qualys.com.

Contact 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 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.

Virtual Appliance is available with 1 Gbps max throughput.

It’s easy to set up a virtual appliance. We’ll help you with the steps.

Network requirements / configuration

<table>
<thead>
<tr>
<th>Bandwidth</th>
<th>Minimum recommended bandwidth connection of 1 Megabits per second (Mbps) to the Qualys Cloud Platform for a network containing around 10,000 assets.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance Access</td>
<td>The Network Passive Sensor must be able to reach certain infrastructure located on the Qualys Cloud Platform where your Qualys account is located. The local network must be configured to allow outbound HTTPS (port 443) access to the Internet, so that the Network Passive Sensor can communicate with the Qualys Cloud Platform. Tip: Log into your account and go to Help &gt; About to see the Qualys Cloud Platform URLs.</td>
</tr>
<tr>
<td>DHCP or Static IP</td>
<td>By default the Network Passive Sensor is pre-configured with DHCP. If configured with a static IP address, be sure you have the IP address, netmask, default gateway and primary DNS.</td>
</tr>
<tr>
<td>Proxy Support</td>
<td>The Network Passive Sensor includes Proxy support with or without authentication. Proxy-level termination (as implemented in SSL bridging, for example) is not supported. SOCKS proxies are not supported.</td>
</tr>
</tbody>
</table>

Get Started

Network Passive Sensor will start discovering assets on your network once you complete the setup. It takes just a couple of minutes. It’s important that you complete the steps in the order shown.
Welcome to Qualys Network Passive Sensor
Get Started

Mirror the traffic
You need to feed traffic to the appliance by mirroring the traffic (using physical tap or
mirror port). Connect the mirrored port to the sniffing interface of the appliance. 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 - Download Virtualization Image
1) Log in to the Qualys UI and select Network Passive Sensor from the app picker.
2) On the Home tab, scroll down and click Deploy Network Sensor.
3) From the Sensors tab, go to New Sensor > Virtual Sensor and then click Download link
from Deploy Image step of the New Virtual Sensor wizard. For VMware ESXi, you can
download the image (OVA file) to your local system. For Hyper-V, you can download zip file
of the Hyper-V image. Click I Agree from Review and Agree to Virtual Scanner License
popup. The image download will start.

Step 2 - Generate Personalization Code
You’ll need a unique personalization code to register your appliance with the Qualys
Cloud Platform. Follow these steps to generate a personalization code:
1) Log in to the Qualys UI and select Network Passive Sensor from the app picker.
2) On the Sensors tab, go to New Sensor > Virtual Sensor to register a new sensor.
3) In the New Virtual Sensor wizard, provide a name for your sensor and the location.
Click the Generate Code button. Copy the code and keep it handy. You’ll need it later.
4) Click Next to go to the Installation screen. If you have not downloaded image from
Home screen, you’ll be able to download it form there.
5) Click Next to go to the Define Internal Assets screen. 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
or use customized IP ranges. Select Inventory these assets check box for marking
inventoried assets. You’ll be able to apply existing tags to these assets. To configure
internal, external and excluded type of assets, refer Configure Assets.
6) Click Finish to complete the registration steps. A pop up will be shown with Sensor not
connected text. Now complete the next steps and the sensor status will change once
registration is successful in Step 4 - Register the Virtual Appliance.
Step 3 - Deploy Virtualization Image

You can deploy the image on the VMware ESXi or Microsoft Hyper-V. VMware ESXi or Microsoft Hyper-V monitors the network activity without any active probing of the device in order to detect the active assets on the network. It identifies the key device attributes that help the web services on the cloud to catalog the devices into operating system/hardware.

Deployment on VMware ESXi

ESXi server requirements: VMware ESXi 6.0 or later, 50 GB HDD, 16 GB Memory, Octa-Core Processor

Follow these steps to deploy an image on ESXi server:

1) Login to your ESXi Server, and go to Virtual Machines > Create/Register VM. It will open New Virtual Machine wizard.

2) For creation type, choose Deploy a virtual machine from an OVF or OVA file.
3) Click **Next** and enter a name for your virtual machine. Select or drag/drop the virtual sensor image you downloaded in **Step 1 - Download Virtualization Image**.

4. Click **Next** and select the destination datastore for the virtual machine configuration files and all of the virtual disks.
5. Click **Next** to go to the **Deployment Options** page. The OVA file creates a VM with two interfaces - Management and Sniffing.
The Management interface is required to connect the virtual appliance to the Qualys Cloud Platform. Make sure the Management interface is connected to the pre-configured port group having WAN or Internet connectivity.

The Sniffing interface is used by the appliance to inspect the traffic. Make sure the Sniffing interface is connected to the pre-configured port group having TAP/TUN interface. Also make sure that “Promiscuous Mode” is enabled on respective vSwitch and port group.

Following screen shows typical vSwitch topology with port group settings.
6. Click **Next** and review the settings configured earlier. Click **Finish** and wait for some time to complete the virtual appliance deployment using OVA.

7. Once the deployment is complete, open the virtual appliance console by selecting the VM and navigating to **Console > Open browser console**. Wait while the VM boots up.
8) There are some network configuration settings (static IP, proxy) you’ll need to set before proceeding to the next step. Complete Network Configurations.

**Deployment on Microsoft Hyper-V**

Hyper-V server requirements: Microsoft Hyper-V 2012 R2 or later, 50 GB HDD, 16 GB Memory, Octa-Core with total 14 GHz dedicated CPU Clock Processor

Follow these steps to deploy an image on Hyper-V server:

1) Login to your Hyper-V Server and go to **Start > Server Manager > Tools > Hyper-V Manager**. Right-click your Hyper-V host and select **New > Virtual Machine...**

2) For Specify Name and Location, provide the name that will be displayed on Hyper-V Manager and select the location where virtual machine will be stored.

3) For Specify Generation, select the appropriate generation (recommended - Generation 1) for the virtual machine.

4) For Assign Memory, provide appropriate memory (RAM) for the virtual machine. Minimum recommended RAM is 16384 MB.

5) For Configure Networking, select appropriate virtual switch with Internet connectivity so that the network adapter on the sensor can use a virtual network for communication with Qualys cloud platform.

6) For Connect Virtual Hard Disk, select “Use an existing virtual hard disk” and provide the location of the .vhdx file (Unzip the zip file downloaded in Step 1 - Download Virtualization Image to obtain the virtual hard disk file. As an example, unzip qPS-1.0.0-1-vhdx.zip to obtain the virtual hard disk qPS-1.0.0-1-disk1.vhdx).

7) Click **Next** and review Summary. Click **Finish** and your virtual machine is ready. Following screen shows the deployment configurations.
8) Select the virtual machine (just created) and navigate to Settings. Change default number of virtual processors to 8.
9) Make sure that “Automatic Stop Action” the VM is set to “Turn off the virtual machine” and apply changes.

10) Navigate to Virtual Switch Manager and create a new virtual network switch > Select type of switch as External.
11) Give a name to the virtual switch, e.g., “test_switch”.

12) Select the appropriate external physical NIC interface to connect the virtual switch from the drop-down menu.

13) Uncheck the option **Allow management operating system to share the network adapter**.

14) Click OK
15) In Powershell, execute the following commands:
- Set the port feature property to the virtual switch created.
  
  ```powershell
  $portFeature = Get-VMSystemSwitchExtensionPortFeature -FeatureName "Ethernet Switch Port Security Settings"
  $portFeature.SettingData.MonitorMode = 2
  Add-VMSwitchExtensionPortFeature -ExternalPort -SwitchName test_switch -VMSwitchExtensionFeature $portFeature
  ```
- Configure the port monitor mode.
  ```powershell
  $portFeature.SettingData.MonitorMode = 2
  ```
- Use the same switch name as defined earlier
  ```powershell
  Add-VMSwitchExtensionPortFeature -ExternalPort -SwitchName test_switch -VMSwitchExtensionFeature $portFeature
  ```

16) Select the virtual machine and go to Settings.
17) Go to **Add Hardware** > Select **Network Adapter** > Click **Add** > Click **OK** to add new network adapter in Hyper-V.

18) Select the second Network Adapter tab from the drop-down > Select the newly created virtual switch (**test_switch**).
19) Go to **Advanced Features** > Select **Destination** from Mirroring Mode drop-down in Port Mirroring Section.

20) Power on the VM.

21) There are some network configuration settings (static IP, proxy) you’ll need to set before proceeding to the next step. Complete **Network Configurations**.

**Step 4 - Register the Virtual Appliance**

1) Open the Virtual Appliance console by selecting the VM and then navigating to **Console** > Open browser console.

2) Choose the **Personalize this scanner** option.

3) Enter your 14 digit personalization code which you generated in **Step 2 - Generate Personalization Code**.
4) Click **Submit** and wait for the confirmation message **Appliance registration completed successfully**. Check that the status on the console is Registered.

5) Once your appliance successfully registers to the Qualys Cloud Platform, you’ll start seeing appliance with status as paused.

**Step 5 - Check the Status**

Log in to the Qualys UI and select **Network Passive Sensor** from the application picker. Navigate to the **SENSORS** tab to view list of sensors in your account and their status.

You’ll see the status for each appliance in the list: Paused, Scanning or Not Connected. If the status is **Paused**, you can view details for the appliance, reboot the appliance, start scanning, delete assets and deregister. If the status is **Scanning**, you can view details and pause scanning.
If the status is **Not Connected**, you can view details for the appliance.

**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 IT Asset Inventory** module.

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

**Internal Assets**

To add internal assets, simply go to **Configuration > Internal Assets > Create New**.
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 Inventory these 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 - Use Default Internal 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 - Use 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 Tags** to select IP tags from the list of tags for which you want to define internal asset.
3- Custom 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.
Network Configurations

You’ll need to complete certain network configuration settings under Set up Network. This is where you’ll enable and configure the management interface of the appliance.

These configurations are described:

Configure Static IP Address
Proxy Configuration

Configure Static IP Address

If the core group to which Management interface is connected has DHCP server, then you can view the Management Network Configurations with Show option. If DHCP is not on your network, you must enable the Virtual Sensor with a static IP address using the STATIC IP option. One of these configurations is required.

To enable a static IP address, follow these steps:

1) Go to the Set up Network menu option and press Enter to continue.
2) Press Space Bar to select Static IP option and choose OK.
3) Provide parameters for Static IP configuration:
   - IP address - Enter the static IP address.
   - Netmask - Enter the desired netmask value.
   - Gateway - Enter the gateway IP address.
   - DNS1 - Enter the IP address for the primary DNS server.
   - DNS2 - Enter the IP address for the secondary DNS server. This entry is optional.
4) Choose Submit and press Enter. Wait for some time and you’ll see a confirmation message for successful configuration of network settings.
Network Configurations
Proxy Configuration

Proxy Configuration

If the Virtual Sensor is behind a Proxy server, you need to enable a Proxy configuration using the Enable Proxy menu option. Authentication (Basic) of the Virtual Sensor connection to your Proxy server can be enabled by configuring the Proxy user and password fields.

The Virtual Sensor uses Secure Sockets Layer (SSL) protocol (HTTPS) to secure its connection to the Qualys web application, in a similar way that a web browser does to a secure web server. If the Qualys connection must pass through a Proxy server, then you must enable the Proxy option on the Virtual Sensor. This configuration re-directs Qualys outbound connections through the Proxy server.

Your Proxy server must be configured to tunnel or pass through the SSL session to the Qualys web application. This ensures a secured end-to-end connection. SSL bridging or tunnel termination must not be configured in your Proxy server when supporting the Virtual Sensor.

To configure Proxy support, follow these steps:

1) Go to the Set up Network menu option.

2) Choose Proxy Configuration and press Enter to continue.

3) Select Enable Proxy and click OK.

4) When the Enter the proxy server details prompt appears, provide the proxy server parameters:

   - Proxy IP Address - Enter the Proxy server’s IP address.
   - Proxy Port - Enter the port number assigned to the Proxy server.

5) Click Next to select the authentication type from NoAuth, BasicAuth and NTLMAuth. If you select authentication type as BasicAuth or NTLMAuth, you need to provide user name and password.

   - Proxy User - Enter the user name for Proxy authentication. If authentication is not enabled at the Proxy level, leave the entry field blank.
   - Proxy Password - Enter the password for Proxy authentication. If authentication is not enabled at the Proxy level, leave the entry field blank.
Appendix

**Virtual Network Passive Sensor (PS) Appliance Packet Throughput Based on Resources**

The Virtual Network Passive Sensor (PS) appliances auto-scaling capability starts automatically at the boot time to calculate how much packet throughput it can handle.

The delta increase in the throughput depends on the additional dedicated resources made available to the appliance. The resources include the CPU clock, the type of CPU, and the type of RAM in the VM appliance system.

To handle continuous traffic, the CPU GHz must be allocated in a dedicated manner. The estimated maximum throughput is visible on the sensor details page. The throughput may vary depending on the dedicated nature of the resources and the type of traffic visible to the sensor.

**Virtual Network Passive Sensor (PS) Throughput Capacity Based on Hardware**

The calculation of ThroughPut is directly dependent on the CPU resources attached to the VM appliance. However, it is strongly advised to increase memory resources as per your requirement.

With each two additional CPU cores added to the appliance, an additional LB pipe will be added, followed by an additional DPI-AEC instance pair entry that will get added in the respective DB table. When these different CPU cores are removed, a corresponding number of LB pipes are also reduced, and DPI-AEC instance pair DB entries are also be removed.

**Comparison Chart**

Utilize hardware at the best possible level to leverage the Qualys (PS) appliance effectively.

<table>
<thead>
<tr>
<th>Capacity (MBps)</th>
<th>RAM (GB)</th>
<th>CPU Core</th>
</tr>
</thead>
<tbody>
<tr>
<td>500</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>750</td>
<td>12</td>
<td>6</td>
</tr>
<tr>
<td>1000</td>
<td>16</td>
<td>8</td>
</tr>
<tr>
<td>1250</td>
<td>18</td>
<td>10</td>
</tr>
<tr>
<td>1500</td>
<td>20</td>
<td>12</td>
</tr>
<tr>
<td>1750</td>
<td>22</td>
<td>14</td>
</tr>
<tr>
<td>2000</td>
<td>24</td>
<td>16</td>
</tr>
</tbody>
</table>

**CPU core specification**: Intel(R) Xeon(R) CPU @ 2.30GHz  
**RAM specification**: RAM DDR4 2133
**Note:** In the above chart, for an appliance expected to process more than 1000Mbps traffic, a minimum of 2 GB RAM is mandatory with the addition of every 2 CPU cores. However, we strongly recommend to provide 4GB RAM with the addition of every 2 CPU cores to ensure smooth functionality of Qualys NPS appliances.

**Virtualization Platform:** VMware ESXi 6.7.0

The data is generated under the best-conditioned environment, and the result might vary according to your setup.

**Throughput capacity per 2 core is also dependent on CPU frequency as follows:**
- If CPU Frequency is less than 1.5GHz, then per DPI instance, throughput value will be 150MBps (<1.5GHz = 150MBps).
- If CPU Frequency is between 1.5GHz - 2.0GHz, then per DPI instance, throughput value will be 200MBps (1.5GHz - 2.0GHz = 200MBps).
- If CPU Frequency is more than 2.0GHz, then per DPI instance, throughput value will be 250MBps (>=2.0GHz = 250MBps).

**How to Modify Hardware Resources for VM Deployed on the ESXi Server**

1. Go to **System Shutdown** option and press **Enter** to shutdown the appliance via console.

2. Click **Edit**.
Appendix

3. Increase the **CPU** cores and **Memory** as per your throughput requirements and click **Save** to save your configuration.

4. Click **Power ON** to start your appliance.

---

**How to Modify Hardware Resources for VM Deployed on the HyperV Server**

1. Follow Step 1 same as mentioned above.

2. Select the virtual machine and go to **Settings**. Modify the **CPU** cores and **Memory** as per your throughput requirements > Click **Apply** to apply the changes > Click **OK** to save your configuration.
3. **Power ON** the VM.
Adding/Removing Sniffing Interfaces from Virtual Appliance

Network Passive Sensor (PS) now supports an aggregated/bonded sniffing interface. A virtual interface aggregates multiple physical interfaces allowing the appliance to add one or more sniffing interfaces.

How to Add Sniffing Interface to the PS Appliance Deployed on the ESXi Server

1. Go to the **System Shutdown** option and press **Enter** to shutdown the appliance via console.

2. Click **Edit**
3. Click **Add Network Adapter** for adding new sniffing interface.

4. Select appropriate port group > Select the adapter type **VMXNET 3** > Click **Save** to save your configuration.

5. **Power on** the VM.
**How to Remove Sniffing Interface to the PS Appliance Deployed on the ESXi Server**

1. Follow the Step 1 and Step 2 same as mentioned above.
2. Remove the newly added interface and click **Save** to save the configuration.

3. **Power on** the VM.

**How to add Sniffing Interface to the PS Appliance Deployed on the HyperV Server**

1. Go to the **System Shutdown** option and press **Enter** to shutdown the appliance via console.

**Note**: A virtual switch that views the mirrored network traffic should be connected to the newly created interface.

[Click here](#) to follow steps 10 to 20 in the Deployment on Microsoft Hyper-V section to create a virtual switch and add a new sniffing interface to it.
How to Remove Sniffing Interface to the PS Appliance Deployed on the HyperV Server

1. Go to the System Shutdown option and press Enter to shutdown the appliance via console.

2. Select the virtual machine and go to Settings > Select the Network Adapter tab that needs to be removed > Click Remove > Click Apply > Click OK to remove the network adapter.