COPYRIGHT
Copyright © 2019 McAfee, LLC

TRADEMARK ATTRIBUTIONS
McAfee and the McAfee logo, McAfee Active Protection, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundstone, McAfee LiveSafe, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, True Key, TrustedSource, VirusScan are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

LICENSE INFORMATION
License Agreement
NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.
Contents

Preface ............................ 7
  About this guide ................................... 7
  Audience ................................... 7
  Conventions .................................. 7
  Find product documentation ................. 8

1 About Cloud and Data Center Security ......... 9

2 Virtual IPS Sensor deployment ..................... 11
  Virtual Sensors - advantages .................. 13
  Virtual IPS Sensor models ..................... 13
  Requirements for deploying Virtual Sensors ......................... 14
  Considerations ................................... 15
    Supported modes for Virtual Sensor ............ 15
    Features supported by a Virtual Sensor ........ 15
    Features not supported by Virtual Sensors .......... 17
  Deploying Virtual IPS Sensors on VMware ESX Server ................. 17
    Install Virtual Sensors ..................... 18
    Deployment scenarios for Virtual IPS Sensors ............ 41
    Verify the deployment ..................... 78
  Deployment of Virtual IPS Sensors on KVM ................. 78
    Access KVM ................................ 79
    Install the Virtual IPS Sensor on KVM ............ 79
    Troubleshooting scenarios .................... 91
    Uninstall the Virtual IPS Sensor from KVM .......... 92
  Add the Virtual Sensor in the Manager ............. 93
  Manage Licenses ................................ 94
  Generate the License Compliance report ............ 97

Network Security Platform for VMware NSX

3 IPS for virtual networks using Intel Security Controller ............. 103
  Securing virtual networks with Intel Security Controller .................. 103
    Security challenges in an SDDC ................. 104
    How Intel Security Controller secures virtual networks ............. 105
    Advantages of Intel Security Controller .................. 107
    Virtual IPS Sensors deployed through Intel Security Controller .......... 107
  Deploying next generation IPS service to a virtual network .................. 108
    Terminology ................................ 109
    Components involved in IPS service ............ 111
    High-level steps to implement a security service ............ 113
    How the IPS service works .................... 115
    Requirements for deploying IPS service ............ 118
    Considerations ................................ 119
    Prepare an ESXi host for NSX ................. 121
Define an IP address pool for virtual security appliances .................................................. 122
Define virtualization connectors ...................................................................................... 126
Define manager connectors .............................................................................................. 130
Manage software images for virtual security appliances .................................................. 132
Manage distributed appliances ......................................................................................... 138
Jobs and tasks .................................................................................................................. 150
Create a security group in VMware NSX ....................................................................... 154
Create a security policy in VMware NSX ....................................................................... 158
Apply a security policy to a security group in VMware NSX ........................................... 161
Configure virtual security system to fail-close or fail-open .............................................. 164
Manager functions regarding IPS service deployment ..................................................... 168
Troubleshooting tips and FAQs regarding IPS service ..................................................... 177

Network Security Platform for Amazon Web Services

4  Securing your Amazon Web Services (AWS) datacenter ........................................ 181

Network Security Platform for the public cloud ............................................................. 181
AWS Terminologies .......................................................................................................... 182
Components of Network Security Platform for AWS ..................................................... 183
How Network Security Platform functions to protect public cloud infrastructure ....... 183
Configuration flow ............................................................................................................ 184
Packet flow in Network Security Platform ..................................................................... 184
High Availability of vNSP solution ................................................................................ 186
Manager Disaster Recovery (MDR) for Managers ......................................................... 186
Controller High Availability (HA) ................................................................................. 187
Considerations ................................................................................................................ 189
Requirements to deploy Network Security Platform in AWS environment ................. 192
Create IAM roles and policies ......................................................................................... 196
User data for establishing trust ...................................................................................... 197
Manage Licenses ............................................................................................................. 198
Virtual IPS Sensor Model to secure the public cloud ..................................................... 201
Generate the License Compliance report ........................................................................ 202
Telemetry ........................................................................................................................ 204
Telemetry for vNSP Clusters ......................................................................................... 205
Workflow for deploying Network Security Platform in AWS ....................................... 206
High-level steps for configuring Network Security Platform in AWS environment .... 206
Install the Network Security Manager .......................................................................... 208
Configure a vNSP Controller ......................................................................................... 213
Launch the vNSP Controller AMI instance ................................................................ 219
Create a vNSP Cluster .................................................................................................... 222
Create a protected group ............................................................................................... 226
Launch the Virtual IPS Sensor AMI instance ............................................................... 229
Download the Virtual Probe ......................................................................................... 234
Install the Virtual Probe ............................................................................................... 235
View summary details of a selected vNSP Cluster ....................................................... 236
Uninstall the Virtual Probe ........................................................................................... 238
Jumbo frame parsing ...................................................................................................... 238
Auto scaling of Sensors to improve traffic throughput .................................................... 241
Virtual IPS Sensors auto scaling in AWS ..................................................................... 241
Configuration of Sensors to protect Web Servers with an Elastic Load Balancer (ELB) .. 242
vNSP cluster configuration ............................................................................................ 242
Create an auto scaling group for Virtual IPS Sensors in AWS ..................................... 243
View the Virtual IPS Sensors launched in a vNSP cluster ........................................... 256
Viewing alerts detected by vNSP cluster ..................................................................... 256
Features not supported .................................................................................................. 257
Best Practices ................................................................................................................ 257
Preface

This guide provides the information you need to configure, use, and maintain your McAfee product.

Contents

- About this guide
- Find product documentation

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience. The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.
- **Users** — People who use the computer where the software is running and can access some or all of its features.

Conventions

This guide uses these typographical conventions and icons.

- **Italic** — Title of a book, chapter, or topic; a new term; emphasis
- **Bold** — Text that is emphasized
- **Monospace** — Commands and other text that the user types; a code sample; a displayed message
- **Narrow Bold** — Words from the product interface like options, menus, buttons, and dialog boxes
- **Hypertext blue** — A link to a topic or to an external website

- **Note:** Extra information to emphasize a point, remind the reader of something, or provide an alternative method
- **Tip:** Best practice information
- **Caution:** Important advice to protect your computer system, software installation, network, business, or data
- **Warning:** Critical advice to prevent bodily harm when using a hardware product
Find product documentation

On the ServicePortal, you can find information about a released product, including product documentation, technical articles, and more.

Task
1. Go to the ServicePortal at https://support.mcafee.com and click the Knowledge Center tab.
2. In the Knowledge Base pane under Content Source, click Product Documentation.
3. Select a product and version, then click Search to display a list of documents.
About Cloud and Data Center Security

Cloud computing and virtualization have begun to play a huge role in the IT infrastructure and scalability of an organization’s business. However, while the terms virtualization and cloud are used almost interchangeably, it is important to note the distinction that this guide makes between the two terms. Virtualization is the technology that separates the physical infrastructure to create dedicated resources. It separates compute environments from the actual physical hardware thereby allowing servers, workstations, storage, and other systems to be independent of the hardware layer. Virtualization is the foundation on which Cloud computing is based and Cloud computing is the delivery of shared computing resources as a service or on-demand through the Internet. For better readability, it might simply be referred to as the "cloud" in this guide.

Early adoption of the cloud can provide organizations with an opportunity to transform their business models and gain a competitive edge. Cloud environments are generally the most cost-effective solutions compared to conventional on-premise environments both in the short and the long term. Measurable benefits such as lower costs, greater agility, and better resource utilization have spurred initial adoption. Cloud computing is comprised of two specific deployment models which are described here:

- **Public cloud** refers to cloud infrastructure that is managed by a business, academic or government organization or a combination of these. All infrastructure and data reside on the premises of the cloud provider. Public cloud models have all your data and applications residing on the cloud provider's servers. The primary advantage of the public cloud model is the ease to deploy. Any individual or business can sign up for advanced services on the cloud with just a credit card. Obtaining such services without the public cloud would require expensive and time-consuming resources to be set up within your organization network.

- **Data center** refers to cloud computing that delivers the same benefits of public cloud such as scalability and self-service provisioning but through a proprietary architecture. However, while public cloud deployments serve multiple clients or organizations, data centers (they might sometimes be known as private clouds) serve only one organization. Data center deployments keep data and applications within your control so that they do not have to be stored and operated from a third-party organization's infrastructure. From this description, it would seem that security is not a challenge in a data center deployment. However, because data center deployments require new deployments for resource pooling and elastic scalability, it is prone to security challenges that must be anticipated and planned for.

McAfee Network Security Platform is a full featured next-generation IPS solution ready for the unique demands of cloud environments. It is an intelligent security solution that discovers and blocks sophisticated threats in the network with unmatched speed, accuracy, and simplicity. Combined with network virtualization and security platforms. Network Security Platform delivers best-in-class enterprise security against sophisticated attacks on virtual infrastructures. You are able to deploy it as a standalone Virtual IPS Sensor to monitor both east-west and north-south traffic or as a service that is orchestrated across a software defined data center.

The following type of solutions are available:
• Standalone Virtual IPS Sensor, a virtual instance of the physical IPS Sensor, can be deployed on hypervisors and used to monitor traffic between virtual machines.

• Cluster solution which comprises several Virtual IPS Sensors that are clustered in a single appliance and orchestrated in a data center using a tool such as Intel® Security Controller. The cluster can be used to deploy IPS as a service in environments that use network virtualization software such VMware NSX.

**Standalone and distributed IPS appliances**

In a standalone Virtual IPS deployment, any number of Virtual IPS Sensor can be installed per hypervisor. Each Virtual IPS Sensor is managed separately through the Network Security Manager (Manager). You can have different policies configured for each Virtual IPS Sensor. Maintenance and troubleshooting of each Virtual IPS Sensor is also carried out individually.

In the distributed solution, a logical container contains several Virtual IPS Sensors within itself. The container is known as Virtual Security System and, unlike Virtual IPS Sensors, the Virtual Security System appears in the Manager as a single device with several instances of the Virtual IPS Sensors. The Virtual Security System is orchestrated using Intel Security Controller and is managed through VMware NSX. When a security policy is applied to a Virtual Security System, all instances of the Virtual IPS Sensor within it are updated with the same policy. Each Virtual IPS Sensor is configured similarly but functions independently of the other and provides security to the specific host it is deployed on. Maintenance and troubleshooting of a Virtual Security System involves managing one device in the Manager. For example, when you apply a configuration update to one Virtual Security System appliance, all Virtual IPS Sensor instances contained in it are updated with the same configuration. Such centralized management of several instances of the Virtual IPS Sensor proves beneficial in deploying a scalable security solution across your data center.

In subsequent chapters, we will look at both these deployment models and the various environments in which they can each be deployed.

This section describes the various models and the virtualization environments in which they can be deployed.

<table>
<thead>
<tr>
<th>Virtual IPS Sensor model</th>
<th>Supported virtualization environment</th>
<th>Type of solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS-VM600</td>
<td>VMware ESX and KVM</td>
<td>Standalone</td>
</tr>
<tr>
<td>IPS-VM100</td>
<td>VMware ESX and KVM</td>
<td>Standalone</td>
</tr>
<tr>
<td>IPS-VM100-VSS</td>
<td>VMware NSX</td>
<td>Distributed</td>
</tr>
</tbody>
</table>
Enterprises are moving towards virtual IT infrastructures such as private and public cloud, virtual data centers for servers, and virtual machines for clients. Security requirements for a virtual network might vary vastly when compared to physical networks. For example, monitoring of peer-to-peer traffic and access control in a virtual network have their own challenges. Based on the network architecture and security requirements, virtual security products are required to protect virtual IT infrastructures. Even for physical networks, virtual security products can bring in savings in terms of cost and space.

A Virtual IPS Sensor (Virtual Sensor) is McAfee’s virtual next-generation IPS product. It is a virtual instance of the NS-series Sensor software, which you can install as a virtual appliance on a VMware ESX server. You do not require the Sensor hardware to deploy a Virtual Sensor. Though primarily designed to protect virtual networks, you can deploy a Virtual Sensor to protect physical networks as well.

In this document, the terms Virtual IPS Sensor and Virtual Sensor are interchangeably used.

The Virtual IPS Sensor is available as an OVA image. Open Virtualization Format (OVF) is an open standard across various virtualization platforms, for packaging and distributing the software to be run on virtual machines. An OVF virtual machine consists of a folder containing virtual machine files and a file describing them. An Open Virtualization Appliance (OVA) file is a single compressed file that contains the contents of an OVF folder.

Similar to a physical Sensor, you use a Manager to configure and manage Virtual Sensors. This Manager can be installed on a physical server or on a virtual machine. Also, you can use the same Manager to manage both virtual and physical Sensors including heterogeneous Sensor environments.

A Virtual Sensor supports most of the features that are supported by a physical Sensor. Except for the fact that you deploy Virtual Sensors in a virtual environment, the process of configuring and managing them is similar to that of physical Sensors. Virtual Sensors also function similar to their physical counterparts when it comes to protecting your networks. With the added advantage of being a virtual instance, you can deploy a Virtual Sensor to protect various network architectures. Some of the common scenarios are covered in this document.

You install a Virtual Sensor in an VMware ESX server. Then, you can deploy this Virtual Sensor to inspect traffic between:

- Virtual machines (VMs) on this ESX server.
- VMs on different ESX servers and the VMs on this host.
• Physical machines and the VMs on this ESX servers.
• Physical networks wherein this ESX server is inline.

Figure 2-1  Virtual Sensor deployment

To use the information in this document, familiarity with the following might be required:
• Administration of VMware ESXi hosts including virtual networks within VMware ESXi hosts.
• Management of guest virtual machines.
• Installation, configuration, and management of Network Security Sensor and Manager.

Contents
- Virtual Sensors - advantages
- Virtual IPS Sensor models
Virtual Sensors - advantages

The following are the advantages of Virtual Sensors:

- As with any virtual technology, Virtual Sensors too bring in savings in terms of space, cost of the appliance, maintenance costs, power to run the appliances, power for air-conditioning, and so on.

- Virtual Sensors enable inspection of traffic that never leave an ESX server. Also, you can implement security policies, (Exploit, DoS, Firewall, Advanced Malware policies) on this traffic.

- Virtual Sensors are very easy and quick to deploy. Therefore, they can scale up to any rapid expansions of your virtual network.

- You can deploy Virtual Sensors without any physical access to the ESX server.

- Though protecting virtual networks has its unique challenges, there is no compromise on security with respect to Virtual Sensors. It protects networks similar to a physical Sensor, including features such as application identification and visualization, Firewall policies, Advanced Malware policies and so on. Also, just like physical Sensors, a Virtual Sensor can integrate and communicate with other McAfee products.

- Based on factors such as the size of your network and network architecture, it is possible to use Virtual Sensors to protect both your virtual and physical networks.

- You can use the same Manager as a single-point-of-control for managing your physical and Virtual Sensors.
  - Provides the flexibility of using virtual, physical, or a mixture of virtual and physical Sensors to protect your networks.
  - Managing Sensors is simplified and centralized.
  - You can define the security policies to both virtual and physical networks at one place. So, the task of defining and implementing security policies for the virtual networks still rests with your security experts.
  - Provides a consolidated view of the threat information from both virtual and physical Sensors.
  - Enables consistent and consolidated report generation for all your networks.

  This Manager can also be installed on a VM.

- Virtual Sensors are self-contained with respect to protecting your networks. That is, there is no requirement for any third-party applications to protect virtual or physical networks.

- Virtualization of virtual ports is available. That is, you can virtualize the interfaces of a physical Sensor by creating sub-interfaces based on VLAN or CIDR. Following the same procedure, you can create sub-interfaces of the monitoring ports of a Virtual Sensor.

Virtual IPS Sensor models

The table describes the available Virtual IPS Sensor models.
### Requirements for deploying Virtual Sensors

This section discusses the server requirements for deploying Virtual Sensors.

#### VMware ESX server requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtualization software</td>
<td>VMware ESX 5.0 and later.</td>
</tr>
<tr>
<td>CPU</td>
<td>• Intel Xeon processor 5000 series or higher.</td>
</tr>
<tr>
<td></td>
<td>• Minimum required processor speed is 1 GHz; recommended is 2 GHz or more.</td>
</tr>
<tr>
<td></td>
<td>• 3 or 4 logical CPU cores based on the Virtual Sensor model.</td>
</tr>
<tr>
<td></td>
<td>• Minimum 4 Ethernet ports; recommended is 6 (More Ethernet ports enable you to use</td>
</tr>
<tr>
<td></td>
<td>that many Ethernet port pairs as monitoring port pairs.)</td>
</tr>
</tbody>
</table>

#### Other requirements

- To install the Virtual Sensor, that is to deploy the OVA file, you need VMware vCenter Server. Using the VMware vSphere Client to deploy the Virtual Sensor OVA file is not recommended. For subsequent management of your VMware ESXi server, you might use VMware vSphere Client.

  > The procedures explained in this document were documented using VMware vCenter Server Version: 5.1.0.10100 Build 1123965 and VMware vSphere Web Client Version 5.1.0 Build 1063329.

- Network Security Manager 8.1.x or later installed on a virtual or physical machine.

- You require one license per Virtual Sensor. The license is also specific to the Virtual Sensor model you purchased. Make sure you have secured the required number of licenses from McAfee.

- You must exclude the Virtual Sensor from VMware Distributed Resource Scheduler (DRS).

- Do not install VMware tools for a Virtual Sensor.
For optimal and predictable performance follow these guidelines.

- You must configure each Virtual Sensor VM to execute on as many cores as required for the Sensor model by assigning CPU affinity to the VM. For example, an IPS-VM100 VM must be affinitized to 3 logical cores.

- No other virtual machines running on the same ESXi host can be allowed to share the CPU cores that are assigned to a Virtual Sensor virtual machine. For example, if there are 16 CPU cores on a ESX server, the Virtual Sensor VM can be affinitized to the first 3 CPUs. All other VMs running on the same ESX server must be excluded from using the first 3 CPUs by affinitizing them to use the remaining CPUs on the host.

**Considerations**

Review this section and its sub-sections before you deploy a Virtual Sensor.

- Based on how you deploy the Virtual Sensor, you might have to re-configure some of the vSwitches on your VMware ESXi host.

- Currently, Virtual Sensors are not VMware vMotion aware. That is, you cannot move a Virtual Sensor between VMware ESXi hosts. You must manually deploy the Virtual Sensor in the other VMware ESXi hosts.

- Currently, Virtual Sensor deployment involves only standard vSwitches and not distributed vSwitches.

- You need an Active Fail-Open kit to deploy Sensor monitoring ports in fail-open mode. This is applicable to scenarios where the Virtual Sensor is between two physical network devices. For inline inspection of traffic to virtual machines, only fail-closed mode is applicable.

- Currently, failover-deployment of Virtual Sensors is not supported.

Under test conditions, it is observed that it takes less than a minute for a Virtual Sensor to restart and become fully operational again. This factor mitigates the risk of significant network disruption due to inline Virtual Sensor monitoring ports going down. It is recommended to deploy Active Failopen Kit to avoid network disruption due to a restart of Virtual Sensor.

**Supported modes for Virtual Sensor**

You can deploy a Virtual Sensor in the following modes:

- SPAN mode.
- Inline fail-closed mode.
- For inline fail-open mode, you must use an external Active Fail-Open Bypass Kit.

**Features supported by a Virtual Sensor**

The following are the list of features supported by Virtual Sensors.

**Table 2-1 Supported features**

<table>
<thead>
<tr>
<th>Feature name</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS policies for exploit attacks</td>
</tr>
<tr>
<td>IPS policies and DoS policies for detection of DoS attacks</td>
</tr>
<tr>
<td>DNS DoS protection</td>
</tr>
<tr>
<td>Reconnaissance policies</td>
</tr>
<tr>
<td>Feature name</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Quarantine (automatic, through IPS policies, Attack Log, and from the Quarantine page within the Analysis tab)</td>
</tr>
<tr>
<td>MDR</td>
</tr>
<tr>
<td>Virtual Sensor monitoring ports based on CIDR and VLAN</td>
</tr>
<tr>
<td>Snort custom attack definitions</td>
</tr>
<tr>
<td>McAfee custom attack definitions</td>
</tr>
<tr>
<td>Protection of Web application servers</td>
</tr>
<tr>
<td>Advanced Traffic Inspection</td>
</tr>
<tr>
<td>Inspection of Q in Q traffic</td>
</tr>
<tr>
<td>Layer 2 passthru mode is supported but implemented differently when compared to physical Sensors</td>
</tr>
<tr>
<td>Layer 7 data collection</td>
</tr>
<tr>
<td>SYN cookie protection</td>
</tr>
<tr>
<td>ARP spoofing protection</td>
</tr>
<tr>
<td>IP spoofing protection</td>
</tr>
<tr>
<td>Virtualization of monitoring ports using VLANs and CIDRs (VIDS)</td>
</tr>
<tr>
<td>MPLS traffic inspection</td>
</tr>
<tr>
<td>IPv6 traffic inspection</td>
</tr>
<tr>
<td>IPv6 support for the management port</td>
</tr>
<tr>
<td>Inspection of tunneled traffic including GRE tunneled traffic</td>
</tr>
<tr>
<td>HTTP response scanning</td>
</tr>
<tr>
<td>Inspection of double VLAN tagged traffic</td>
</tr>
<tr>
<td>Monitoring Sensor performance</td>
</tr>
<tr>
<td>Synchronization of Sensor clock using an NTP server</td>
</tr>
<tr>
<td>Display Sensor CLI audit log events in the Manager</td>
</tr>
<tr>
<td>TACACS+ user in audit logs</td>
</tr>
<tr>
<td>Secure Transfer of Files from Sensor CLI</td>
</tr>
<tr>
<td>Application Identification and Visualization</td>
</tr>
<tr>
<td>Firewall policies</td>
</tr>
<tr>
<td>Advanced Traffic inspection</td>
</tr>
<tr>
<td>SmartBlocking of attacks including use of IP Reputation to augment SmartBlocking</td>
</tr>
<tr>
<td>Integration with McAfee GTI for IP reputation and file reputation. This includes protection from high-risk hosts.</td>
</tr>
<tr>
<td>Connection Limiting policies</td>
</tr>
<tr>
<td>Inspection of X-Forwarder-For Header Information. Reputation lookup and quarantine of client IP addresses in the XFF header.</td>
</tr>
<tr>
<td>Layer 7 Data Collection</td>
</tr>
<tr>
<td>Stateless Firewall access rules</td>
</tr>
<tr>
<td>Simulated Blocking</td>
</tr>
<tr>
<td>Latency monitor</td>
</tr>
<tr>
<td>Capture data packets (packet capture)</td>
</tr>
<tr>
<td>Granular access control for CLI commands (for TACACS users)</td>
</tr>
</tbody>
</table>
Table 2-1 Supported features (continued)

<table>
<thead>
<tr>
<th>Feature name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Malware policies including integration with McAfee Advanced Threat</td>
</tr>
<tr>
<td>Defense and NTBA Appliances</td>
</tr>
<tr>
<td>Advanced callback activity including Bot Command and Control server activity</td>
</tr>
<tr>
<td>detection</td>
</tr>
<tr>
<td>Network forensics</td>
</tr>
<tr>
<td>Passive device profiling</td>
</tr>
<tr>
<td>Web server protection against DoS attacks</td>
</tr>
<tr>
<td>Traffic prioritization</td>
</tr>
<tr>
<td>Netflow export to NTBA</td>
</tr>
<tr>
<td>Integration with McAfee® Endpoint Intelligence Agent (McAfee EIA)</td>
</tr>
<tr>
<td>Sensor autorecovery — Since a Virtual IPS Sensor cannot depend on its software</td>
</tr>
<tr>
<td>to go to layer2 during recovery, the traffic is interrupted until all</td>
</tr>
<tr>
<td>applications are restarted and the Sensor is back to GOOD health.</td>
</tr>
</tbody>
</table>

After you deploy a Virtual Sensor, the process of configuring and managing it is similar to that of a physical Sensor. Therefore, refer to the corresponding section for information on how to configure the supported features.

Features not supported by Virtual Sensors

The following are the list of features that are not supported by Virtual Sensors.

Table 2-2 Features not supported

<table>
<thead>
<tr>
<th>Feature name</th>
</tr>
</thead>
<tbody>
<tr>
<td>TAP mode</td>
</tr>
<tr>
<td>SSL decryption</td>
</tr>
<tr>
<td>Sensor failover</td>
</tr>
<tr>
<td>Cloud threat detection</td>
</tr>
<tr>
<td>Traffic prioritization with application content</td>
</tr>
</tbody>
</table>

Deploying Virtual IPS Sensors on VMware ESX Server

To deploy Virtual IPS Sensors, you must first install the Virtual IPS Sensors and establish trust with a Manager. After trust is established, you can deploy the Virtual IPS Sensor for protecting your networks. How you configure the Virtual IPS Sensor, however, depends on the network architecture and your security needs.

The following is a high-level procedure that you can consider to install and subsequently deploy a Virtual IPS Sensor:

1. Verify your VMware ESX server meets the hardware and software requirements. See Requirements for deploying Virtual Sensors on page 14.

2. Install the Virtual IPS Sensors and establish a trusted communication channel between the Virtual IPS Sensors and a Manager. See Install Virtual Sensors on page 18.

3. Determine how you want to deploy the Virtual IPS Sensor and configure it accordingly. See Deploying Virtual IPS Sensors on VMware ESX Server on page 17.
Install Virtual Sensors
Before you can deploy a Virtual Sensor to protect your network, you must install the Virtual Sensor and establish trust between the Virtual Sensor and the Manager.

The following are the high-level steps to install a Virtual Sensor:

1. Identify the network to which you want to place the Virtual Sensor and the Manager. Accordingly, identify the vSwitch and the port group for the management port and the Manager. You can use the default switch port group of vSwitch0, which is VM Network, to connect the Sensor management port. However, if required, you can also create a vSwitch to connect the management port. To create a vSwitch for management port connectivity, see Create a standard vSwitch for the management port on page 18.

2. For every Virtual Sensor that you plan to deploy, import the required licenses in the Manager. See Manage Licenses on page 25.

3. Add the Virtual Sensor in the Manager. See Add the Virtual Sensor in the Manager on page 29.

4. Install the Virtual Sensor and establish trust with the Manager. See Install Virtual Sensors on page 18.

Create a standard vSwitch for the management port

Before you begin
To create a vSwitch, you might be required to connect an additional physical NIC on the ESX.

After you install the Virtual Sensor, you need a standard vSwitch to which you connect the management port of the Virtual Sensor. If you have installed the Manager on the same ESX, you can connect it to this switch as well. When you create a standard vSwitch, ESX creates a default port group for this vSwitch.

Task
1. Connect an additional physical NIC on the ESX to the adjacent physical switch.
   This is required for the vSwitch that you are creating.

2. Log on to the ESX as the root user in VMware vSphere Web Client.
3 In the vSphere Home tab, select Hosts and Clusters.

4 Select the required ESX server and select Manage | Networking | Virtual switches.
5 Click on the **Add host networking** icon.

6 For **Select connection type**, as an example select **Physical Network Adapter** and click **Next**.

Selecting the connection type depends on your network design and requirements. For example, if the Manager is installed on a physical machine, then you must select physical network adapter. If not the Sensor and the Manager cannot communicate. If the Manager is installed on a virtual machine and you plan to use the same vSwitch for both the Sensor management port and the Manager, then you might choose **Virtual Machine Port Group for a Standard Switch**. For the scenarios explained in this document, select **Physical Network Adapter**.

7 For **Select target device**, select **New standard switch**, the required number of ports, and then click **Next**.
8 For Create a Standard Switch step, click Add adapters icon.

9 In the Add Physical Adapters to the Switch dialog box, select the required network adapter and click OK. Make sure that a physical NIC corresponding to the network adapter you selected is connected to the network.
10 Verify the properties of the selected adapter and click **Next** and then select **Finish**.
The vSwitch that you created is listed in the **Virtual switches** section.

11 Add the required switch port groups for the vSwitch that you created; select that vSwitch and then click on the **Add host networking** icon.
12 In the Select connection type step, select **Virtual Machine Port Group for a Standard Switch** and then click Next.

13 In the Select target device step, select **Select an existing standard switch** and make sure the vSwitch that you created is selected. Then click Next.

14 In the Network Label field, enter the required name for the default port group that the wizard creates for the switch.
   You can modify Network Label later. For easier management, you can name it as **Management Port Group**.

15 Optionally, in VLAN ID field, select **All (4095)** and select Next.
   If required, you can specify the required VLAN ID as per your network configuration.
16 Review the details displayed in the **Ready to complete** step and click **Finish**.
This vSwitch is now listed with the switch port group that you created.

<table>
<thead>
<tr>
<th>Switch</th>
<th>Discovered Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSwitch1</td>
<td>–</td>
</tr>
<tr>
<td>vSwitch2</td>
<td>–</td>
</tr>
<tr>
<td>vSwitch3</td>
<td>–</td>
</tr>
</tbody>
</table>

Standard switch: vSwitch3 (Management Port Group)

17 Move the mouse over the physical adapter and click on it.

Standard switch: vSwitch3 (Management Port Group)
18 Click on the **Edit adapter speed** icon.

19 Verify if the **Configured Speed, Duplex** is set to **Auto negotiate**.

For other property values, you can leave them with the default values.

**Manage Licenses**

Licenses are required to add vNSP Clusters. These licenses can either be individual .jar files, or they can be bundled together and provided to you in the form of a .zip file. Each license supports a pre-defined number of Virtual IPS Sensors, and this number is specific to the license file you have procured.

- There is no limit on the number of license files you can add to the Manager.
- The license files do not expire.

The Manager periodically compares the number of Virtual IPS Sensors supported by your licenses with the installed number of Virtual IPS Sensors. You are compliant as long as the number of Virtual IPS Sensors in your Manager does not exceed the total number of Virtual IPS Sensors allowed across all licenses. For example, if you have two licenses, one which allows 5 and the other which allows 10 Virtual IPS Sensors, you are compliant as long as you have no more than 15 Virtual IPS Sensors in this Manager.
If there are not enough licenses added to the Manager, a fault is raised accordingly.

The **Licenses** page in the Manager displays your compliance, and maintains the count for Virtual IPS Sensors and Virtual Probes. This page also displays and allows you to add and remove individual licenses.
Task

1. In the Manager, select Manager | <Admin Domain Name> | Setup | Licenses.

2. The Summary section displays the overall compliance, the number of Virtual IPS Sensors along with the maximum number allowed, and the number of Virtual Probes in use.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall License Status</td>
<td>Overall compliance which can either be Compliant or Non-compliant. If the Virtual IPS Sensor count is within the maximum limit defined in the license, the overall state is displayed as Compliant with a green icon preceding it. If the Virtual IPS Sensor count exceeds the maximum limit, the overall state is displayed as Non-Compliant with a red icon preceding it.</td>
</tr>
<tr>
<td>Total Virtual Sensors</td>
<td>Number of Virtual IPS Sensors in use along with the maximum number</td>
</tr>
<tr>
<td>Total Virtual Probes</td>
<td>Number of Virtual Probes in use</td>
</tr>
</tbody>
</table>

Figure 2-2 Licenses Page

<table>
<thead>
<tr>
<th>License</th>
<th>Added</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key 5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
If the overall license status is **Compliant**, the tool tip for Total Virtual Sensors displays that no additional licenses are required. However, if the overall license status is **Non-Compliant**, the tool tip for Total Virtual Sensors indicates that additional number of licenses are required for compliance.

<table>
<thead>
<tr>
<th>Summary</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall License Status:</td>
<td>Compliant</td>
</tr>
<tr>
<td>Total Virtual Sensors:</td>
<td>2 in use (33 allowed)</td>
</tr>
<tr>
<td>Total Virtual Probes:</td>
<td>3 in use</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Summary</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall License Status:</td>
<td>Non-Compliant</td>
</tr>
<tr>
<td>Total Virtual Sensors:</td>
<td>2 in use (1 allowed)</td>
</tr>
<tr>
<td>Total Virtual Probes:</td>
<td>3 in use</td>
</tr>
</tbody>
</table>

3 The **Individual Licenses** section displays the details of each license imported into the Manager.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td><strong>Key</strong> – Key of the license file</td>
</tr>
<tr>
<td></td>
<td><strong>Generated</strong> – Date when the license file was generated</td>
</tr>
<tr>
<td></td>
<td><strong>Customer</strong> – Customer for whom the license file was generated</td>
</tr>
<tr>
<td></td>
<td><strong>Grant ID</strong> – The McAfee Grant ID of the corresponding customer</td>
</tr>
<tr>
<td>Virtual Sensors Allowed</td>
<td>Maximum number of Virtual IPS Sensors allowed for the selected license</td>
</tr>
<tr>
<td>Added</td>
<td><strong>Time</strong> – Date in &lt;mmm-yy&gt; format, and time when the license was added</td>
</tr>
<tr>
<td></td>
<td><strong>By</strong> – Name of the user who added the license</td>
</tr>
<tr>
<td>Comment</td>
<td>Enables you to add your comment per license file that is imported. Double-click in the <strong>Comment</strong> field and enter your comment. Click outside this field and your comment is automatically saved.</td>
</tr>
</tbody>
</table>
4 To import licenses into the Manager, click **Add License**. Click **Browse** to locate the license, and then click **OK**. The successful addition of a license is displayed at the top of the page.

5 To remove a license, select the license you want to remove from the **Individual Licenses** section, and click **Remove**.
   In the pop-up window, click **OK** to remove the selected license or **Cancel** to return to the **Licenses** page.

6 Click **Save as CSV** to export license information in the .csv format. The default CSV file name is **NsmLicenseList.CSV**.

**Add the Virtual Sensor in the Manager**

**Before you begin**
You have a Manager version 8.1.7.x or later either on a virtual or a physical machine.

You can add the Virtual Sensor in the Manager and specify a shared secret key. You can use a Manager installed on a VM or on a physical server.
Task
1. In the Manager select Devices | <Admin Domain Name> | Global | Add and Remove Devices.

2. Click New.

3. Specify at least the Device Name, Device Type, and Shared Secret.
   - Select IPS Sensor as the Device Type.
   - You must use the same Device Name and Shared Secret when you deploy the Virtual Sensor.

4. Click Save.

Figure 2-3 Virtual Sensors added in a Manager

For more information on deleting a configured Sensor, see topic Delete a Sensor from the Manager, section How to replace a Sensor, chapter Troubleshooting in the McAfee Network Security Platform IPS Administration Guide.

Install the Virtual Sensor

Before you begin
- The Virtual Sensor installation file is a .ova file. Make sure this file is accessible from your client machine.
- Standard vSwitches and switch port groups are available for the Sensor management port and monitoring ports that you plan to use. Consider that you are installing IPS-VM100, which has one management port, one response port, and 4 monitoring ports. Currently you plan to deploy ports 1-2 in inline mode between 2 vSwitches. You do not plan to use ports 3 and 4 for now. For this example, make sure you have the following:
  - Standard vSwitch with switch port group for the management port. The Sensor must be able to communicate with the Manager through this switch port group.
  - Two standard vSwitches with switch port groups for monitoring port 1 and 2. That is, the Sensor will act as a bridge between these two vSwitches with port pair 1-2 inline between these two vSwitches.
  - Different dummy switch port groups for the Sensor ports that you do not plan to use now — response port and monitoring ports 3 and 4.
  - You have added the Virtual Sensor in the Manager.
**Task**

1. Log on to the ESX as the root user in VMware vSphere Web Client.

2. In the vSphere Home tab, select Hosts and Clusters.
3 Navigate to the required node such as a resource pool, right-click, and select **Deploy OVF Template**.

![Image of deploying OVF Template](image)

4 Click **Browse** and locate the `.ova` file.

![Image of selecting file](image)
5 Review the details and click **Next**.

In the **Name** field, enter a name for the Sensor and also select the corresponding datacenter. Preferably enter the same name that you entered when adding the Sensor in the Manager.
7 From the Select virtual disk format list, select Thin Provision.

8 In the Setup networks section, select the switch port groups for the corresponding Sensor ports.
   - For example scenario 2 for example, assign VNSP Client Port for monitoring port 1 and VNSP Server Port for monitoring port 2.
   - Assign temporary, non-functional switch port groups to the unused Sensor ports, that is the response port and ports 3 and 4 (for scenario 2). You select a functional switch port group for the response port when you configure the Virtual Sensor for IDS (SPAN).

   ![Warning]

   You must never assign the same port group to peer monitoring ports. For example, monitoring ports 3 and 4 must not be assigned the same port group. If you do, it results in a loop within the ESX.

   - For the management port, assign the port group belonging to the vSwitch that you created for the Sensor management port. This switch port group must enable communication with the Manager server.

   ![Warning]

   Within the same Virtual Sensor, no Source (monitoring port or the response port) should have the same Destination (switch port group) as that of the Sensor management port.

9 In the Customize template page, specify the Sensor setup details.
a. Enter the same Sensor name that you specified in the Manager.

b. Optionally, enter the IPv4 address for the Sensor.
   You can specify IPv4, IPv6, or both type of IP addresses to the Sensor.

c. If you had specified an IPv4 address, specify the subnet mask for the IPv4 address that you provided.

d. If you had specified an IPv4 address, specify the default gateway for the IPv4 address.
   This is mandatory if the Sensor needs to communicate outside its network. For example, the Manager could be on a different subnet.

e. Optionally, specify an IPv6 address to the Sensor.

f. If you had specified an IPv6 address, specify the default gateway for the IPv6 address.

g. Specify the IPv4 or IPv6 address of the hypervisor such as VMware ESX server on which you are deploying the Virtual Sensor.

h. Specify the Manager’s primary IPv4 or IPv6 address.
   To specify the Manager’s secondary IP address, use the `set manager secondary ip` command in the Sensor CLI after the Sensor is installed.

i. Specify the shared secret key and also confirm it by re-entering.

j. Click Next.
10 Review the configuration that you specified, select **Power on after deployment**, and then click **Finish**.

Click **Back** and make changes, if required. Note that the Sensor setup details that you entered are listed under **Properties**.

11 After the Virtual Sensor is installed, open an SSH client session to logon to the Sensor.
Alternatively, you can click **Launch Console** in the vSphere Web Client.
In the Sensor CLI, enter admin and admin123 as the login name and password respectively.

Use the status CLI command to check if trust is established with the Manager and if signature set is present in the Sensor.

If the signature set is not present, you can deploy the signature set from the Deploy Pending Changes page of the Manager.

Configure CPU affinity for Virtual Sensors

Before you begin
You have installed the Virtual Sensor.

For optimal and predictable performance of Virtual Sensors, you must follow the below guidelines.

• You must configure each Virtual Sensor VM to execute on as many cores as required for the Sensor model by assigning CPU affinity to the VM. For example, an IPS-VM100 VM must be affinitized to 3 logical cores.

• No other virtual machines running on the same ESXi host can be allowed to share the CPU cores that are assigned to a Virtual Sensor virtual machine. For example, if there are 16 CPU cores on a ESX server, the Virtual Sensor VM can be affinitized to the first 3 CPUs. All other VMs running on the same ESX server must be excluded from using the first 3 CPUs by affinitizing them to use the remaining CPUs on the host.

Task
1. Use the shut CLI command to shutdown the Virtual Sensor and also make sure in the VMware vSphere Web Client that the Virtual Sensor is powered off.

2. Log on to the ESX as the root user in VMware vSphere Web Client.
3 In the vSphere Home tab, select Hosts and Clusters.
Under the corresponding ESX, select the required Virtual Sensor and select **Edit virtual machine settings**.
In the **Edit Settings** dialog, click **CPU**.

6. From the **HT Sharing** drop-down, select the required option.

HT sharing means hyperthreaded core sharing.

- **None** — For best, optimal, and predictable performance, McAfee recommends this option.
- **Internal** — Better, less optimal, and less predictable performance is expected with this option.
- **Any** — Normal performance, which is less optimal than **Internal** and sometimes even unpredictable is expected with this option.

For the description of these options and to know the difference between them, refer to VMware documentation.
7 In the **Scheduling Affinity** text box enter the logical CPU affinities for the Virtual Sensor.

<table>
<thead>
<tr>
<th>HT Sharing (*)</th>
<th>Internal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling Affinity (*)</td>
<td>Hyperthreading Status:</td>
</tr>
</tbody>
</table>

The string that you enter depends on the Virtual Sensor model. For example, IPS-VM600 uses 4 logical CPU cores. So, in the snap above, 5-8 indicates processors 5, 6, 7, and 8.

8 Click **OK**.

9 Power on the Virtual Sensor in VMware vSphere Web Client.

**Deployment scenarios for Virtual IPS Sensors**

There are subsections that describe some scenarios for you to understand various deployment options. These scenarios are examples used for the sake of explanation; they might not exactly match real or typical network architectures. You can use the scenarios to determine the Virtual IPS Sensor deployment process for your network. As a VMware ESX administrator, your must identify a process that requires the least amount of changes to your network architecture and configuration.

The following is a high-level procedure that you can consider to deploy a Virtual IPS Sensor:

1 Determine how you want to deploy the Virtual IPS Sensor. You can review the scenarios discussed in the subsections. When deciding the deployment type, you can factor in:
   - The kind of protection that your network requires. For example, whether you need to place monitoring ports in inline mode against SPAN mode.
   - How to deploy the Virtual IPS Sensor with the least changes to your VMware ESX configuration.

2 Follow the procedural information provided for the corresponding scenario.
   a Evaluate your VMware ESX deployment and identify the vSwitches that need to be modified and those that need to be created.
   b Evaluate the port groups that can be used and the ones that need to be created.
   c Identify the vSwitches and port groups for the Sensor monitoring ports.
   d Identify the vSwitches and port groups for the clients and servers that you need to protect.

3 Verify if the deployment is functioning as expected. See *Verify the deployment* on page 78.

**Scenario 1: Inspection of traffic between virtual machines in SPAN mode**

This scenario involves using a SPAN monitoring port to inspect traffic between virtual machines on the same ESX. Similar to the SPAN mode deployment of a physical Sensor, the SPAN mode deployment of a Virtual IPS Sensor is also simple and non-intrusive.
Scenario description before Virtual IPS Sensor deployment

- The servers are installed on guest VMs on the ESX.
- These servers are connected to a standard vSwitch, vSwitch0.
- vSwitch0 has a physical adapter, which is connected to networks outside the ESX.

![Scenario before Virtual IPS Sensor deployment](image)

Figure 2-4  Scenario before Virtual IPS Sensor deployment

Scenario description after Virtual IPS Sensor deployment

- In vSwitch0 create a new switch port group set in promiscuous mode.
- The Virtual IPS Sensor is deployed on the ESX.
- Consider that the Manager is installed on a VM connected to vSwitch1.
- In this scenario, the Manager is connected to the management port of the Virtual IPS Sensor through vSwitch1. This vSwitch1 has a physical adapter vmnic1. So, you can access the Manager and the Sensor from outside the ESX.
- Monitoring port 1 of the Virtual IPS Sensor is in SPAN mode. This is connected to the promiscuous switch port group in vSwitch0. Therefore, a copy of all the packets of vSwitch0 are sent to port 1 for intrusion detection.

![Scenario after Virtual IPS Sensor deployment](image)

Figure 2-5  Scenario after Virtual IPS Sensor deployment
Scenario 1: High-level steps for Virtual Sensor deployment

This section assumes the following for deploying the Virtual Sensor for scenario 1.

- The ESX server meets the requirements as discussed in Requirements for deploying Virtual Sensors on page 14.
- You have the privileges on the ESX server to add and modify vSwitches and port groups.
- You have installed the Virtual Sensor and established trust with the Manager successfully. As an example in this scenario, the management port is connected to vSwitch1.
- As an example, this section uses the IPS-VM100 Virtual Sensor to explain the deployment.
- This scenario involves only a Sensor monitoring port deployed in SPAN mode.
- This section uses only the vSphere Client for configurations on the ESX.

**Task**

1. Modify vSwitch0 to create a switch port group in promiscuous mode.
   - Refer to Modify an existing standard vSwitch for a monitoring port on page 64. Subsequently, you assign this switch port group to the SPAN port.

2. Modify vSwitch0 to create a switch port group.
   - Subsequently, you assign this switch port group to the Sensor response port.

3. Configure the SPAN port on the Virtual Sensor in the Manager.
   - a. Click the Devices tab.
   - b. Select the domain from the Domain drop-down list.
   - c. In the left pane, click the Devices tab.
   - d. Select the device from the Device drop-down list.
   - e. Select Setup | Physical Ports.
   - f. Double-click on monitoring port 1 and then from the Mode drop-down, select SPAN or Hub.
   - g. Click OK.
   - h. Click Save in the Monitoring Port Details panel.
   - i. Select Deploy Pending Changes and in the Deploy Pending Changes page select Configuration & Signature Set for the required Virtual Sensor and click Update.

4. Assign the switch port groups you created in steps 1 and 2 to the Sensor SPAN port and the response port respectively.
   - See Specify the switch port groups for monitoring ports on page 70.

5. Verify if you have deployed the Virtual Sensor correctly and whether it is inspecting traffic.
   - Refer to Verify the deployment on page 78.

Scenario 2: Inline inspection of traffic between virtual machines

This scenario involves inspecting the traffic between virtual machines on the same ESX.
Scenario description before Virtual Sensor deployment

- The clients and servers belong to the same subnet (10.10.10.x).
- The clients and servers are connected to different virtual machine port groups within the same standard vSwitch (vSwitch0).
- For the sake of this discussion, assume that the clients and servers have no access from outside the ESX. That is, there is no physical NIC associated with vSwitch0.

![Diagram of Scenario before Virtual Sensor deployment]

**Figure 2-6 Scenario before Virtual Sensor deployment**

Scenario description after Virtual Sensor deployment

- Two more standard vSwitches (vSwitch1 and vSwitch2) are now added.
- The Virtual Sensor is deployed on the ESX.
- In this scenario, the Manager is installed on a VM connected to vSwitch2.
- In this scenario, the Manager is connected to the management port of the Virtual Sensor through vSwitch2. This vSwitch2 has a physical adapter vminc0. So, you can access the Manager and the Sensor from outside the ESX.
- The monitoring port pair 1-2 of the Virtual Sensor is inline between the client and server.
The client and the monitoring port 1 are connected to two different port groups within vSwitch0. The port group to which the monitoring port is connected is set to promiscuous mode.

Similarly, the server and monitoring port 2 are connected to two different port groups within vSwitch1. Any traffic from the client to the server is inspected by the monitoring port pair 1-2.

---

**Scenario 2: High-level steps for Virtual Sensor deployment**

This section assumes the following for deploying the Virtual Sensor for scenario 2.

- The ESX server meets the requirements as discussed in [Requirements for deploying Virtual Sensors on page 14](#).
- You have the privileges on the ESX server to add and modify vSwitches and port groups.
- You have installed the Virtual Sensor and established trust with the Manager successfully. As an example in this scenario, the management port is connected to vSwitch2.
- As an example, this section uses the IPS-VM100 Virtual Sensor to explain the deployment.
- This scenario involves only a Sensor monitoring port pair deployed in inline fail-closed mode.
- This section uses only the vSphere Client for configurations on the ESX.

**Task**

1. Create vSwitch1 for connecting Sensor monitoring port 2 and the 10.10.10.16 server.
   Refer to [Create a standard vSwitch for a monitoring port on page 54](#).

2. Modify vSwitch0 to connect monitoring port 1.
   Refer to [Modify an existing standard vSwitch for a monitoring port on page 64](#).

3. Assign the corresponding switch port group (promiscuous mode) that you created in step 1 to monitoring port 2.
   See [Specify the switch port groups for monitoring ports on page 70](#).

4. Change the switch port group for the 10.10.10.16 server such that it is now connected to vSwitch1.
5 Assign the corresponding switch port group (promiscuous mode) that you created in step 2 to monitoring port 1.

   See Specify the switch port groups for monitoring ports on page 70.

6 Verify if you have deployed the Virtual Sensor correctly and whether it is inspecting traffic.

   Refer to Verify the deployment on page 78.

**Scenario 3: Inspection of traffic to virtual servers**

This scenario involves inspecting the traffic going to and coming out of virtual servers installed on an ESX. In this deployment, the Sensor monitoring port acts as a gateway to the protected servers.

**Scenario description before Virtual Sensor deployment**

- The servers are installed on guest VMs on the ESX.
- These servers are connected to a standard vSwitch, vSwitch0.
- vSwitch0 has a physical adapter, which is connected to networks outside the ESX.

![Figure 2-8 Scenario before Virtual Sensor deployment](image)

**Scenario description after Virtual Sensor deployment**

- Two more standard vSwitches (vSwitch1 and vSwitch2) are now added.
- The Virtual Sensor is deployed on the ESX.
- The Manager is installed on a VM connected to vSwitch2.
- The management port of the Virtual Sensor is connected to vSwitch2. This virtual switch has a physical adapter. So, you can access the Manager and the Sensor from outside the ESX.
- The monitoring port pair 1-2 of the Virtual Sensor is inline between external network through vmnic0 and the server farm on the ESX.
The servers and the monitoring port 1 are connected to two different port groups in vSwitch0. The port group to which the monitoring port is connected is set to promiscuous mode.

Monitoring port 2 is connected to vSwitch1, which is in turn connected to external network through vmnic0. Therefore, any traffic to the servers from the outside network is inspected by the port pair 1-2.

Note that the monitoring port 1 is connected to a promiscuous switch port group on vSwitch0. Therefore, the Sensor will inspect traffic between Server 1 and Server 2 as well though it is not inline. Effectively this is as if monitoring port 1 is in SPAN mode. To avoid the Sensor from inspecting the traffic between the servers, define ACLs on the Sensor accordingly.

Figure 2-9  Scenario after Virtual Sensor deployment

Scenario 3: High-level steps for Virtual Sensor deployment

This section assumes the following for deploying the Virtual Sensor for scenario 3.

- The ESX server meets the requirements as discussed in Requirements for deploying Virtual Sensors on page 14.
- You have the privileges on the ESX server to add and modify vSwitches and port groups.
- You have installed the Virtual Sensor and established trust with the Manager successfully. As an example in this scenario, the management port is connected to vSwitch2.
- As an example, this section uses the IPS-VM100 Virtual Sensor to explain the deployment.
- This scenario involves only a Sensor monitoring port pair deployed in inline fail-closed mode.
- This section uses only the vSphere Client for configurations on the ESX.

Task

1. Create a standard vSwitch for connecting Sensor monitoring port 2 with the external network through vmnic0. For this scenario, consider it is vSwitch1.
   Refer to Create a standard vSwitch for a monitoring port on page 54.
   Make sure this vSwitch has a physical adapter and that this is connected to the corresponding external switch.

2. Modify vSwitch0 to connect monitoring port 1 and the virtual servers.
   For this scenario, you need not change the switch port group for the virtual servers. Create a new switch port group for monitoring port 1. Refer to Modify an existing standard vSwitch for a monitoring port on page 64.

3. Assign the corresponding switch port group (promiscuous mode) to the monitoring ports.
See Specify the switch port groups for monitoring ports on page 70.

- The switch port group that you created in step 1 (vSwitch1) must be assigned to monitoring port 2.
- The switch port group that you created in step 2 (vSwitch0) must be assigned to monitoring port 1.

4 Verify if you have deployed the Virtual Sensor correctly and whether it is inspecting traffic.

Refer to Verify the deployment on page 78.

**Scenario 4: Inspection of traffic between physical machines**

In addition to virtual networks, you can use the Virtual Sensor to protect physical networks as well. This is typically used in very large networks, where space might be a constraint to install multiple physical Sensors.

**Scenario description before Virtual Sensor deployment**

- The clients and servers are connected to different physical switches.
- For the sake of simplicity, assume that the client and servers are on the same VLAN.
- The two switches are connected through their trunk ports. Since all the machines are assumed to be on the same VLAN, no routing is required.

![Figure 2-10 Scenario before Virtual Sensor deployment](image)

**Scenario description after Virtual Sensor deployment**

- The trunk ports of the two switches are connected two physical NICs on the ESX.
- These NICs are connected to two different vSwitches, which are in turn connected to monitoring port pair 1-2.
• vSwitch2 is used to connect the management port, which in turn is connected to a Manager on a physical machine.

• The monitoring port pair 1-2 of the Virtual Sensor is now inline between the client and the server.

---

**Scenario 4: High-level steps for Virtual Sensor deployment**

This section assumes the following for deploying the Virtual Sensor for scenario 4.

• The ESX server meets the requirements as discussed in Requirements for deploying Virtual Sensors on page 14.

• You have the privileges on the ESX server to add and modify vSwitches and port groups.

• You have installed the Virtual Sensor and established trust with the Manager successfully. As an example in this scenario, the management port is connected to vSwitch2.

• As an example, this section uses the IPS-VM100 Virtual Sensor to explain the deployment.

• This scenario involves only a Sensor monitoring port pair deployed in inline fail-closed mode.

• This section uses only the vSphere Client for configurations on the ESX.

**Task**

1. Connect the trunk port of Physical switch 1 and Physical switch 2 to two different physical NICs on the ESX.

2. Create two standard vSwitches for connecting Sensor monitoring ports 1 and 2.

   Refer to Create a standard vSwitch for a monitoring port on page 54. Both these switches need physical adapters. For this scenario, vSwitch0 must be assigned a physical adapter that is connected to Physical switch 1. Similarly, vSwitch1 must be assigned a physical adapter that is connected to Physical switch 2.
3 Create a switch port group in vSwitch0, which corresponds to the trunk port on Physical switch 1.
   a Log on to the ESX as the root user in VMware vSphere Web Client.

![Login to VMware vSphere Web Client](image1.png)

b In the vSphere Home tab, select Hosts and Clusters.

![vSphere Home tab](image2.png)
c  Select the required ESX server and select Manage | Networking | Virtual switches | vSwitch0.

d  Click on Add host networking icon for vSwitch0.
e For **Select target device**, select **Select an existing standard switch** and make sure vSwitch0 is selected.

f In the **Network Label** field, enter a name. For example, enter *Physical Client Port*.

g In the **VLAN ID (Optional)** field, select **All (4095)** because this switch port group corresponds to the trunk port of a physical switch.

h Click **Next** and then **Finish**.

i Under **Standard switch: vSwitch0 (VM Network)**, click on the switch port group that you created. In this example, it is *Physical Client Port*. 
j With the switch port group selected, click on the Edit Settings icon for the switch port group.

![Edit Settings dialog](image)

k In the Edit Settings dialog, select the Security tab and make sure the fields are set with the following values and click OK.

- **Promiscuous mode** — Accept. This is set to accept because traffic related to all the hosts connected to Physical switch 1 is involved.
- **MAC Address Changes** — Reject.
- **Forged Transmits** — Accept.

4 Use the previous step to create a similar switch port group in vSwitch1. This corresponds to the trunk port on Physical switch 2.

5 Assign the switch port group that you created in step 3 to monitoring port 1. See Specify the switch port groups for monitoring ports on page 70.
6 Assign the switch port group that you created in step 4 to monitoring port 2.
   See Specify the switch port groups for monitoring ports on page 70.
   Make sure the monitoring port 1 is connected to the corresponding port group (VNSP100-PG-Port1) on
   vSwitch0 and the monitoring port 2 is connected to the corresponding port group (VNSP100-PG-Port2) on
   vSwitch1. Both these port groups must have their VLAN ID as All (4095). This is required since the monitoring
   ports are connected to trunk ports of the physical switches.

7 Verify if you have deployed the Virtual Sensor correctly and whether it is inspecting traffic.
   Refer to Verify the deployment on page 78.

Create a standard vSwitch for a monitoring port

**Before you begin**
If you require external access to VMs connected to this switch, you will be required to connect an
additional physical NIC on the ESX to a physical switch.

You connect monitoring ports to standard vSwitches. When you create a standard vSwitch, ESX creates a default
port group for this vSwitch. Each monitoring port in a Virtual Sensor must be connected to different port
groups.

**Task**
1 Optionally, connect an additional physical NIC on the ESX to the adjacent physical switch.
   In scenario 4, for example, you must connect an additional NIC to the corresponding physical switch.

2 Log on to the ESX as the root user in VMware vSphere Web Client.

![Login to VMware vSphere Web Client](image)
3 In the vSphere Home tab, select Hosts and Clusters.

4 Select the required ESX server and select Manage | Networking | Virtual switches.
5 Click on the **Add host networking** icon.

![Add host networking icon](image)

6 In the **Select connection type** section, select the required connection type and click and click **Next**.

Selecting the connection type depends on your network design and requirements. If the VMs that will be connected to this switch do not need access outside the ESX then you might select **Virtual Machine Port Group for a Standard Switch**. However, for requirements as in scenario 4, it is mandatory to select **Physical Network Adapter**. Consider that you now select **Virtual Machine Port Group for a Standard Switch**.

![Select connection type](image)

7 For **Select target device**, select **New standard switch**, the required number of ports, and then click **Next**.

![Select target device](image)
8 Based on your network requirements, click on the **Add adapters** icon and select the corresponding physical network adapter. Then click **Next**.

![Add adapters icon](image)

9 In the **Network Label** field, enter the required name for the default port group that the wizard creates for the switch.

   You can modify **Network Label** even later. For easier management, name this as `VNSP100-PG-Port1` for example.

10 In **VLAN ID**, select **All (4095)** and select **Next**.

![Connection settings](image)
11 Click Finish.
This vSwitch is now listed under Virtual Switches in the Networking tab.

12 Select the vSwitch that you created, move the mouse over its physical adapter, and click on it.

Diagram of vSwitch 3 and its physical adapter.
13 Click on the **Edit adapter speed** icon.

For other property values, you can leave them with the default values.

14 Verify if the **Configured Speed, Duplex** is set to **Auto negotiate**.
15 Modify the security properties of the vSwitch.
   a  Select the vSwitch and click on the Edit settings icon.

   ![Virtual switches](image)

   b  Select Security and make sure the fields are set to the values mentioned and then click OK.
      • Promiscuous mode — Reject.
      • MAC Address Changes — Reject.
      • Forged Transmits — Accept.

16 Modify the security settings of the default port group.
   It is assumed that you will use this port group to connect the monitoring port of a Sensor.
   a  Move the mouse over the default port group and click on it.
      The switch port group is now selected.

   ![vSwitch4](image)
b  Click on the **Edit settings** icon for the switch port group.

c  Click **Properties** and modify the Network Label if required.

d  Make sure **VLAN ID** is set to **All (4095)**.
   This switch port group must receive all VLAN traffic similar to a trunk port.

e  Click **Security**, select the **Override** check box next to **Promiscuous Mode** and then select **Accept** from the drop-down.
   This is mandatory for the port group that you will use for any Sensor monitoring port.

17  Create a new port group for the other VMs in this vSwitch.
For example, in scenario 2, this is the port group that you will use for the 10.10.10.16 server.

Skip this step for scenario 4.

a  Select the corresponding vSwitch and click on the **Add host networking** icon.

b  In the **Select connection type** step, select **Virtual Machine Port Group for a Standard Switch** and then click **Next**.

c  In the **Select target device** step, select **Select an existing standard switch** and make sure the vSwitch that you created is selected. Then click **Next**.
d  In the **Network Label** field, enter the required name for the default port group that the wizard creates for the switch.

You can modify **Network Label** later. For easier management, you can name it as **Server Port**.

e  In the **VLAN ID (Optional)** field, you can specify the required VLAN. For scenario 1, for example, select **None (0)** and click **Next** and then **Finish**.

**None (0)** means that the traffic is not tagged with a VLAN.

f  Move the mouse over the switch port group and click on it.

The switch port group is now selected.
Click on the **Edit settings** icon for the switch port group.

In the **Security** tab, make sure the fields are set with the following values and click **OK**.
- **Promiscuous mode** — Reject.
- **MAC Address Changes** — Reject.
- **Forged Transmits** — Accept.

Click **OK** to close the **Edit settings** dialog.

**Modify an existing standard vSwitch for a monitoring port**

If you plan to connect a monitoring port to an existing vSwitch, you might have to modify some of the configuration. For example, in scenario 2, you need to modify virtual switch 1 to connect it to monitoring port 1.

**Task**

1. Log on to the ESX as the root user in VMware vSphere Web Client.
2 In the vSphere Home tab, select Hosts and Clusters.

If the page takes time to render, click on the page-refresh icon at the top.

3 Select the required ESX server and select Manage | Networking | Virtual switches.
4 Select the required vSwitch and click on its **Edit settings** icon.

5 Select **Security** and make sure the fields are set to the values mentioned and then click **OK**.
   - **Promiscuous mode** — Reject.
   - **MAC Address Changes** — Reject.
   - **Forged Transmits** — Accept.

6 Modify the port group that you are using for the VMs in this switch.
For example, in scenario 2, this is the port group that you use for the 10.10.10.15 client.

a Move the mouse over the required port group and click on it.
The switch port group is now selected.

b Click on the Edit settings icon for the switch port group.

c Click Properties and modify the Network Label if required.
For example, change it to Client Port.

d In the VLAN ID (Optional) field, you can specify the required VLAN. For the scenarios in this section, select None (0).
e Click **Security** and make sure the fields are set with the following values and click **OK**.

- **Promiscuous mode** — **Reject**.
- **MAC Address Changes** — **Reject**.
- **Forged Transmits** — **Accept**.

<table>
<thead>
<tr>
<th>Properties</th>
<th>Promiscuous mode</th>
<th>MAC address changes</th>
<th>Forged transmits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Reject</td>
<td>Reject</td>
<td>Accept</td>
</tr>
<tr>
<td>Traffic shaping</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Teaming and failover</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7 Create a port group to connect the monitoring port of a Sensor.

a Select the corresponding vSwitch and click on the **Add host networking** icon.

b In the **Select connection type** step, select **Virtual Machine Port Group for a Standard Switch** and then click **Next**.
c In the **Select target device** step, select **Select an existing standard switch** and make sure the vSwitch that you created is selected. Then click **Next**.

![Select target device](image)

---

d In the **Network Label** field, enter the required name. For example, enter VNSP Client Port.

e Make sure VLAN ID is set to All (4095), click **Next** and then **Finish**.

![Network Label](image)

---

f Move the mouse over the switch port group and click on it. The switch port group is now selected.

![Switch port group](image)
**g** Click on the **Edit settings** icon for the switch port group.

![Edit settings icon](image)

**h** In the Security tab, select **Override** next to **Promiscuous mode** and then select **Accept** from the drop-down. Click **OK** when done.

This is mandatory for the port group that you will use for any Sensor monitoring port.

![Security tab](image)

---

**Specify the switch port groups for monitoring ports**

When you install the Virtual Sensor, you select the switch port group for the required Sensor ports. No two port must be connected to the same switch port group to prevent loopback. As a precaution, the monitoring and response ports are disconnected by default.

As a good practice, assess the vSwitches and the switch port groups that you would require. Then you can create them in your ESX before you begin installing the Virtual Sensor. You can also create the dummy switch port groups for the ports that you do not plan to deploy.
The first two network adapters correspond to the management port and the response port respectively. The remaining adapters correspond to the monitoring ports. The following graphic shows the mapping between network adapters and the Sensor ports for IPS-VM100.

![Diagram showing network adapter to Sensor port mapping](image)

**Figure 2-12 Network adapter to Sensor port mapping**

The left side is the Virtual Machine Properties dialog that you can access in the vSphere client for a Virtual Sensor. To access the Virtual Machine Properties dialog, select the Virtual Sensor in the vSphere client and then select *Edit virtual machine settings*. The right side of the graphic shows the *Physical Ports* page in the Manager for a Virtual Sensor.

In case of IPS-VM600, network adapters 3 through 8 correspond to the monitoring ports in the same order. Network adapters 1 and 2 correspond to the management port and the response port respectively.

**Task**

1. Log on to the ESX as the root user in VMware vSphere Web Client.
2 In the vSphere Home tab, select Hosts and Clusters.

3 Under the corresponding ESX, select the required Virtual Sensor.
   You can view the network adapters corresponding to the Sensor ports in the VM Hardware section. The current status of these adapters is also displayed.
4 Click **Edit Settings** in the **VM Hardware** section.

5 In the **Edit Settings** dialog, select **Connected** check box for the required network adapters (Sensor ports) and click **OK**.

In the **VM Hardware** section, you can verify that these network adapters are now connected.

**Deploying Virtual Sensor monitoring ports in inline fail-open mode**

**Before you begin**

Before you deploy monitoring ports in inline fail-open mode, make sure the Sensor is functioning as expected with the same ports in inline fail-closed mode.
If a Virtual Sensor receives traffic from a physical network device, then you can deploy an inline pair in inline fail-open mode. Consider a scenario, wherein the Virtual Sensor inspects traffic between virtual machines as shown (scenario 4).

![Diagram showing network setup with Virtual Sensor](image)

**Figure 2-13 Scenario, wherein the Virtual Sensor inspects traffic between virtual machines**

The monitoring port pair 1-2 is inline between physical switches 1 and 2. By default, inline monitoring ports of a Virtual Sensor are in the fail-closed mode. The network between the client and the server is broken under any of the following conditions:

- Link failure in either port 1 or 2.
- Power or application failure in the Virtual Sensor.
- Either vSwitch0 or vSwitch1 is down.
- Link failure in either vmnic0 or vmnic1.
- The ESX server is down.
To mitigate the risk of network breakdown due to these conditions, you can deploy the monitoring port 1-2 in fail-open mode. Fail-open operation for the monitoring ports of a Virtual Sensor, require the use of an external copper bypass switch.

- Only McAfee-certified 10/100/1000 external Copper active fail-open bypass kits are supported.
- Installing the active fail-open bypass kit involves a brief network downtime.

Figure 2-14  Scenario, wherein the active fail-open bypass kit is installed

Task

1. Install the 10/100/1000 external Copper active fail-open bypass kit and power it on (with dual power sources).
   Refer to McAfee Network Security Platform Copper Active Fail-open Bypass Kit Guide for information.

2. Disconnect the trunk port of Physical switch 1 from vmnic0, and connect the trunk port to the port marked A in the bypass kit.

3. Similarly, disconnect the trunk port of Physical switch 2 from vmnic1, and connect the trunk port to the port marked B in the bypass kit.

4. Connect the port marked 1 to vmnic0 and the port marked 2 to vmnic1.

5. In the Manager, set the port in inline fail-open active mode.
   a. Click the Devices tab.
   b. Select the domain from the Domain drop-down list.
   c. In the left pane, click the Devices tab.
   d. Select the device from the Device drop-down list.
   e. Select Setup | Physical Ports.
   f. Double-click on the required port and select Inline Fail Open – Active in the Mode field.
g Confirm and then click Save.

• In the Sensor CLI, run the `show intfport <port number>` command and verify that Fail-Open Switch shows **PRESENT** and Fail-Open Port shows **INLINE**.

• When the Sensor is operating, the switch is **on** and routes all traffic directly through the Virtual Sensor.

![Figure 2-15 Routing when Sensor is operating](image-url)
When the Sensor fails, the switch automatically shifts the Virtual Sensor to a bypass state: in-line traffic continues to flow through the network link, but is no longer routed through the Sensor.

![Figure 2-16 Routing when Sensor fails](image)

When a monitoring port goes down, its status in the Manager is shown as *unknown*. A critical-fault message is also generated. This message is cleared when the monitoring port pair is back inline.

If the monitoring port is down or if the Sensor goes into layer 2 bypass mode, the fail-open bypass kit turns on and the traffic bypasses the Sensor. If you run the `show intfport <port number>` command, the Fail-Open Port field displays **BYPASS**.
• If the Sensor layer 2 bypass mode, the **Fail-Open Port** field, displays **LAYER2_BYPASS**.

• Once the Sensor resumes normal operation, the bypass switch returns to the **off** state, again enabling in-line monitoring.

For the details of how the external Copper active fail-open bypass kit works, see the **10/100/1000 Copper Active Fail-open Bypass Kit Guide**.

6 You can also configure the bypass switch to operate in tap mode.

• See **10/100/1000 Copper Active Fail-open Bypass Kit Guide** for information.

• There is no specific configuration in the **Physical Ports** page in the Manager for tap mode. The configuration is only in the bypass switch.

• When the bypass switch is in tap mode, and you run `show intfport <port number>` command, the **Fail-Open Port** field displays **TAP**.

### Verify the deployment

You can use the following information to verify if you have deployed the Virtual Sensor correctly and if it is inspecting traffic.

**Task**

1 Make sure the Sensor management port and the Manager server and reachable to each other.

2 On the Sensor CLI, use the status and show commands to see if trust is established, the channels are up, and if the Sensor is in good health.

3 On the Manager Dashboard, check the **System Health** monitor to verify if the Sensor is active.

4 In the Manager, select **Devices** | **<Admin Domain Name>** | **Devices** | **<Device name>** | **Setup** | **Physical Ports** and check if the monitoring ports and up.

5 Verify if the client and server are reachable from one another.

6 Send a sample attack from the client to the server, for example root.exe, and check if an alert is raised in the Attack Log with the correct details.

7 After you deploy a Virtual Sensor, the process of configuring and managing it is similar to that of a physical Sensor. Therefore, refer to the corresponding section for information. For example, the procedures related to virtualization of monitoring ports is similar to that of physical ports. For information on how to create sub-interfaces out of the monitoring ports of a Virtual Sensor, see Chapter **How to understand virtualization**, McAfee Network Security Platform IPS Administration Guide.

---

**Deployment of Virtual IPS Sensors on KVM**

To deploy Virtual IPS Sensors on KVM, make sure you have installed KVM on a Linux operating system such as Ubuntu 14.04. Through the Linux operating system, install the Virtual IPS Sensor and establish trust with a Manager. Once you have established trust, the Virtual IPS Sensor is ready to be configured to protect your network. How you configure the Virtual IPS Sensor, however, depends on the network architecture and your security needs.
The following is a high-level procedure that you can consider to install and subsequently deploy a Virtual IPS Sensor:

**Task**

1. Verify your KVM server meets the hardware and software requirements. See Requirements for deploying Virtual Sensors on page 14.

2. Install the Virtual IPS Sensor and establish a trusted communication channel between the Virtual IPS Sensor and a Manager.

3. Determine how you want to deploy the Virtual IPS Sensor and configure it accordingly. There are several method to deploy the Virtual IPS Sensor on KVM. In this document, we provide you some samples. You will be provided with the QCOW image which is the Virtual IPS Sensor image.

**Tasks**

- **Access KVM on page 79**

**Access KVM**

This section describes the steps that can be used to access KVM hypervisor on your Ubuntu 14.04 server.

**Task**

1. Install Ubuntu 14.04 on the server and configure the required network interfaces.

   - It is recommended that you configure at least two network interfaces.

2. Launch Putty and login to the Ubuntu 14.04 server using its IP address.

3. Install KVM on the Ubuntu 14.04 server. For more information, refer to the KVM Installation documentation.

4. Once you have installed KVM, you can begin deploying your Virtual IPS Sensor using:
   - Virtual Machine Manager console - enables you to configure and manage your virtualization host, networking, and storage resources. It allows you to create and deploy virtual machines and services on private clouds that you manage.

5. You can check the status of your Virtual IPS Sensor by using the `virsh` command line. The `virsh` command line interface tool is used for managing guest virtual machines and the hypervisor.
   - `virsh list` - lists the Virtual IPS Sensors that are installed on KVM
   - `virsh console <vmips name>` - allows you to access the Virtual IPS Sensor

**Install the Virtual IPS Sensor on KVM**

Before you can deploy a Virtual IPS Sensor to protect your network, you must install the Virtual IPS Sensor on KVM, and establish trust between the Virtual IPS Sensor and the Manager.

The following are the high-level steps to install a Virtual IPS Sensor:

1. Identify the network on which you want to place the Virtual IPS Sensor and the Manager.

2. Install the Virtual IPS Sensor and establish trust with the Manager.

3. Add the Virtual IPS Sensor in the Manager. See Add the Virtual Sensor in the Manager on page 29.

4. For every Virtual IPS Sensor that you plan to deploy, import the required licenses in the Manager. See Manage Licenses on page 25.
Sample 1: Install a Virtual IPS Sensor through the command prompt

Before you begin

Before you begin to deploy the Virtual IPS Sensor through the KVM command line interface (CLI), decide whether you want to use Open vSwitches or Linux bridges for traffic flow.

You can choose to deploy the Virtual IPS Sensor through the CLI in KVM using either Open vSwitches or Linux bridges depending on your requirements. Depending on which Sensor model you have decided to use, you will require:

- Six Open vSwitches or Linux bridges to connect the six interfaces of the IPS-VM100
- Eight Open vSwitches or Linux bridges to connect the eight interfaces of the IPS-VM600

These devices are used as:

- One management bridge – Used for communication between the KVM management interface and the Virtual IPS Sensor management port
- One response bridge – Used by the response port of the Virtual IPS Sensor to take response actions during an attack (for example, a TCP reset is sent to an attacker IP address through the response port which closes the session with the attacker and the target)
- Monitoring bridges – Used by the Virtual IPS Sensor to inspect traffic. These ports can be deployed in line or in SPAN mode. Each monitoring port requires one bridge or Open vSwitch — the IPS-VM100 has four monitoring ports and the IPS-VM600 has six monitoring ports.

Let us illustrate this sample deployment mechanism through a IPS-VM100 Sensor.

**Task**

1. Begin by creating bridges or switches.

   In this illustration, we will name the bridges and switches br1 through br6.

   - If you are using Open vSwitch, use the `ovs-vsctl` command.

     ```bash
     ovs-vsctl add-br br1
     ovs-vsctl add-br br2
     ...
     ovs-vsctl add-br br6
     ```

   - If you are using a Linux bridge, use the `brctl` command.

     ```bash
     brctl addbr br1
     brctl addbr br2
     ...
     brctl addbr br6
     ```

2. Create an XML file using the sample provided in the section, Sample XML file on page 81.

3. Place the XML file in a convenient location, in the Linux server, where it can be accessed and modified.

4. Edit the XML file by `vi default-vm100.xml` command.

   For this illustration, we have chosen to create bridges instead of Open vSwitches. The modified XML file resembles the same below.

5. Replace the bridge IDs with the bridge IDs you provided while creating the bridges.
6 Create the virtual machine.

**General syntax**

```
virsh define <XML file name>
```

**Sample syntax**

```
virsh start default-vm100.xml
```

If the operation is successful, you see a message that reads **Domain docvmips100 defined from default-vm100.xml.**

7 Start the Virtual IPS Sensor image up.

**General syntax**

```
virsh start <instance name>
```

**Sample syntax**

```
virsh start docvmips100
```

If this is successful, you see a message that reads **docvmips600 started.**

8 Initialize the Virtual IPS Sensor service.

**General syntax**

```
virsh console <instance name>
```

**Sample syntax**

```
virsh console docvmips100
```

If this is successful, you see a message that reads **Connected to domain docvmips100.**

9 Use the default credentials to log on to the Virtual IPS Sensor.

Default credentials to all Sensors are:

- **Username:** admin
- **Password:** admin123

The Virtual IPS Sensor setup begins.

**Sample XML file**

A sample of the XML file required for your deployment is provided below. We consider deployment of an IPS-VM100 for which the parameters considered in the illustration are:

- Number of CPUs required is 3
- Memory require is 4 GB
- Six bridges are required for which customizable bridge IDs
  - `vmips_mgmt_br` is the Management bridge
  - `resp_br` is the Response bridge
  - `mon_br3` through `mon_br6` are Monitoring bridges
- NIC type is virtio
• Hard disk emulation is IDE

• Path of the file along with the filename is /home/doc/sensorsw_vm100_83714.qcow

```xml
<domain id="2" type="kvm">
  <name>vmips</name>
  <memory unit="KiB">4194304</memory>
  <currentMemory unit="KiB">4194304</currentMemory>
  <vcpu placement="static">3</vcpu>
  <resource>
    <partition>/machine</partition>
  </resource>
  <os>
    <type arch="x86_64" machine="pc-1.0">hvm</type>
    <boot dev="hd" />
  </os>
  <features>
    <acpi />
    <apic />
    <pae />
  </features>
  <clock offset="utc" />
  <on_poweroff>destroy</on_poweroff>
  <on_reboot>restart</on_reboot>
  <on_crash>restart</on_crash>
  <emulator>/usr/bin/kvm</emulator>
  <disk device="disk" type="file">
    <driver name="qemu" type="qcow2" cache='none'/>
    <source file="/home/doc/sensorsw_vm100_83714.qcow" size="10G"/>
    <target bus="ide" dev="hda" />
    <alias name="ide0-0-0" />
    <address bus="0" controller="0" target="0" type="drive" unit="0" />
  </disk>
  <controller index="0" type="scsi">
    <alias name="scsi0" />
    <address bus="0x00" domain="0x0000" function="0x0" slot="0x07" type="pci" />
  </controller>
  <controller index="0" type="ide">
    <alias name="ide0" />
    <address bus="0x00" domain="0x0000" function="0x1" slot="0x01" type="pci" />
  </controller>
  <controller index="0" type="usb">
    <alias name="usb0" />
    <address bus="0x00" domain="0x0000" function="0x2" slot="0x01" type="pci" />
  </controller>
  <controller index="0" model="pci-root" type="pci">
    <alias name="pci0" />
  </controller>
  <interface type="bridge">
    <source bridge="vmips_mgmt_br" />
    <virtualport type="openvswitch" />
    <target dev="vnet0" />
    <model type="virtio" />
    <alias name="net0" />
  </interface>
  <interface type="bridge">
    <source bridge="mon_br1" />
    <virtualport type="openvswitch"/>
    <target dev="vnet1" />
    <model type="virtio" />
    <alias name="net1" />
  </interface>
  <interface type="bridge">
    <source bridge="resp_br" />
    <virtualport type="openvswitch" />
    <target dev="vnet2" />
    <model type="virtio" />
</domain>
```
Sample 2: Install a Virtual IPS Sensor through the KVM user interface

Another way to install the Virtual IPS Sensor on KVM is using the KVM user-interface.
Task
1. Log on to the Linux server user interface using the IP address and the credentials.
2. Go to the Virtual Machine Manager.
   If you have any instances running, you see these instances listed in this window.

3. Click the icon to create a new virtual machine.
   The wizard window appears.
4. Enter a name for the Virtual IPS Sensor, choose the appropriate option to find the installer image from the list, and click Forward.
   Since we have the image in another location, we select Import existing disk image.
   Clicking Forward brings you to step 2 where you must select:
   • the path where the image file is located
   • type of OS
5. From the **OS type** drop-down list, select Linux.

6. From the **Version** drop-down list, select Generic kernel.

7. Browse to the location where the Virtual IPS Sensor image is located and select the QCOW image. We recommend that you place the software image in a folder other than the root folder.

8. Click **Forward**.

We come to step 3 in the deployment where you must select the memory and CPU requirements for the Virtual IPS Sensor.
9 Manually enter the **Memory (RAM)** required and number of **CPUs** required.

For memory and CPU requirements of each Virtual IPS Sensor model refer the section, **Requirements for deploying Virtual Sensors** on page 14.

10 Click **Forward**.

We come to step 4 of the wizard where you opt whether to customize the configuration before installation. You can also review your settings in the previous steps.

11 Select the **Customize configuration before install** checkbox.

12 Expand the **Advanced options** tab.

a Click the **Virtual network** drop-down and select **Specify shared device name**.

This option is meant to specify a shared device which facilitates communication with the Virtual IPS Sensor management port. The **Bridge name** field appears.

b Enter **vr1** which is the shared management bridge to which all Virtual IPS Sensor management interfaces connect with in this illustration.
Make sure the rest of the settings are configured as shown in the list below. For this illustration, these were default settings.

1. Select the **Set a fixed MAC address** checkbox and make sure a MAC address is seen.
2. From the **Virt Type** drop-down list make sure kvm is selected.
3. From the **Architecture** drop-down list, make sure x86_64 is selected.
4. From the **Firmware** drop-down list, make sure Default is selected.

**Click Finish.**

You are routed to the next step in the deployment where you can review your entire configuration tab-by-tab.

You will also need to verify some of the settings in these tabs.

13. To verify and modify appropriate settings:

   a. Click the **Disk 1** tab.
   1. Expand the **Advanced** options tab.
   2. From the **Disk bus** drop-down list, select IDE since other formats are not supported.
3 From the **Storage format** drop-down list, select qcow2.

4 Click **Apply** to confirm your changes.

---

**b** Click the **NIC** tab.

1 From the **Device model** drop-down list, select virtio.
   
   You can also select e1000 but we recommend selecting virtio for best results.

2 Click **Apply** to confirm your changes.

**c** Click **Add Hardware**.

The **Add New Virtual Hardware** wizard appears. We require additional NICs (beyond the management NIC) for a Virtual IPS Sensor to function normally.

1 Click on the **Network** tab.

2 From the **Host device** drop-down list, select **Specify a shared device name**.
   
   The **Bridge name** field appears.

3 Enter **vr2** which is the first bridge that we are creating manually.
4. From the Device model drop-down, select virtio.

5. Click Finish.

   A new NIC with a MAC address appears in the menu on the left. The MAC address in the menu refers to that of the Virtual IPS Sensor interface.

\[d\] Repeat step c to create another four NICs since we are about to deploy a IPS-VM100.

   If you want to deploy a IPS-VM600, create seven NICs in addition to the first NIC that appears in the menu. The difference between the number NICs required for each model is because the IPS-VM100 has four monitoring ports whereas the IPS-VM600 has six monitoring ports.

14. Click Begin Installation.

   Creation of the Virtual IPS Sensor virtual machine begins. This process take a few minutes. After installation of the Virtual IPS Sensor, you are routed to the login prompt for the Virtual IPS Sensor CLI which displays the name of the instance you chose in step 1 of the wizard.

15. Provide default credentials for the Virtual IPS Sensor and set it up like you would any other Network Security Platform IPS Sensor.

   After you complete setup of the Virtual IPS Sensor, you are able to assign it to a Manager. Managing the Virtual IPS Sensor through the Manager is the same as managing any other Sensor.
Sample 3: Install a Virtual IPS Sensor using a command

Before you begin

Before you begin to deploy the Virtual IPS Sensor through the KVM command line interface (CLI), you must decide whether you want use Open vSwitches or Linux bridges for traffic flow.

You can choose to deploy the Virtual IPS Sensor through the CLI in KVM using either Open vSwitches or Linux bridges depending on your requirements. Depending on which Sensor model you have decided to use, you will require:

- Six Open vSwitches or Linux bridges to connect the six interfaces of the IPS-VM100
- Eight Open vSwitches or Linux bridges to connect the eight interfaces of the IPS-VM600

These devices are used as:

- One management bridge – Used for communication between the KVM management interface and the Virtual IPS Sensor management port
- One response bridge – Used by the response port of the Virtual IPS Sensor to take response actions during an attack (for example, a TCP reset is sent to an attacker IP address through the response port which closes the session with the attacker and the target)
- Monitoring bridges – Used by the Virtual IPS Sensor to inspect traffic. These ports can be deployed in line or in SPAN mode. Each monitoring port requires one bridge or Open vSwitch — the IPS-VM100 has four monitoring ports and the IPS-VM600 has six monitoring ports.

These steps illustrate a sample deployment mechanism of a IPS-VM600 Sensor using a command in the KVM command line interface.

Task

1. Begin by creating bridges or switches.

   In this illustration, we will name the bridges br1 through br8.

   - If you are using Open vSwitch, use the `ovs-vsctl` command.

     ```
     ovs-vsctl add-br br1
     ovs-vsctl add-br br2
     ...
     ovs-vsctl add-br br8
     ```

   - If you are using a Linux bridge, use the `brctl` command.

     ```
     brctl addbr br1
     brctl addbr br2
     ...
     brctl addbr br8
     ```
2 Open the string provided in the block below, in a notepad editor such as Notepad++, to install your Virtual IPS Sensor.

Strings for both Virtual IPS Sensor models, IPS-VM100 and IPS-VM600, are provided.

**IPS-VM100**

```text
virt-install --name=<instance_name> --ram=4096 --arch=x86_64 --vcpus=3 --os-type=linux --import --disk path=/home/doc/sensoraw_vm100_83714_temp2.qcow,bus=ide,size=6,format=qcow2 --network bridge:mgmt_br,model=virtio --network bridge:mon_br1,model=virtio --network bridge:resp_br,model=virtio --network bridge:mon_br2,model=virtio --network bridge:mon_br3,model=virtio --network bridge:mon_br4,model=virtio
```

**IPS-VM600**

```text
```

3 Edit the parameters mentioned below depending on your setup.

- **Instance name**: This is the name of the Virtual IPS Sensor instance also referred to in the Sensor CLI as Sensor name. It must be unique since it will be the same name that reflects in the Manager.
- **Bridge IDs**: These must match the bridge that you provided while creating the bridges using the `brctl addbr` command in KVM.
- **Disk path**: This is the path of the QCOW file within the Linux file system.

4 Log on to the Linux CLI using your credentials.

5 Copy the string from the notepad editor and paste it in the CLI.

If this is successful, installation of the Virtual IPS Sensor begins. After the installation is complete the Virtual IPS Sensor comes to the `setme login` prompt. Setting up the Virtual IPS Sensor from this point is the same as setting up any other Sensor.

### Troubleshooting scenarios

While deploying the Virtual IPS Sensor you need make sure that vital parameters required to bring it up are mentioned as per requirements. The parameters along with their requirements that are critical for the deployment are:

- **CPU**: IPS-VM100 - 3 | IPS-VM600 - 4
- **Memory (RAM)**: IPS-VM100 - 4096 MB (4 GB) | IPS-VM600 - 6144 MB (6 GB)
- **NIC type**: virtio
- **Number of bridges**: IPS-VM100 - 6 | IPS-VM600 - 8

#### Errors you will see if any of these parameters are incorrect

When any of the parameters above are configured incorrectly, the command prompt displays errors which enable you to correct the problem. The errors along with the messages that you receive are mentioned in this section. All screenshots in this section use an IPS-VM100 to illustrate. Similar errors messages appear if you attempt to deploy the IPS-VM600 with incorrect parameters.
### Uninstall the Virtual IPS Sensor from KVM

This section describes the steps required to uninstall your Virtual IPS Sensor from KVM.

#### Sample 1: Uninstall a Virtual IPS Sensor through the command prompt

To uninstall the Virtual IPS Sensor from KVM, you must undefine the domain that deployed for the instance and then remove the instance itself.

**Task**

1. Log on to the Linux server through a hyperterminal client such as PuTTY.
2. Run the `virsh undefine <XML file name>` command.
   
   If the operation is successful, you see Domain `<XML file name>` is undefined.
3. Run the `virsh destroy <instance name>` command.
   
   If the operation is successful, you see Domain `<instance name>` is destroyed.
   
   You can now reuse the bridges to deploy another instance of a Virtual IPS Sensor.

#### Sample 2: Uninstall a Virtual IPS Sensor through the KVM user interface

Another way to remove the Virtual IPS Sensor in KVM is through the KVM user interface.

---

<table>
<thead>
<tr>
<th>Incorrect parameter</th>
<th>Error</th>
</tr>
</thead>
</table>
| Number of CPUs required is provided incorrectly | ![Resource Status](image1)  
VM100 requires 3 CPU Cores. Detected 2 cores. !!!  
Configure correct parameters, Delete and Re-deploy the NSP-Sensor !!! |
| Memory allocated is other than the required memory | ![Resource Status](image2)  
VM100 requires 4GB memory. Detected 3GB memory. !!!  
Configure correct parameters, Delete and Re-deploy the NSP-Sensor !!! |
| NICs created are not virtio type of NICs | ![Resource Status](image3)  
Either Network Driver for interface-5 (eth5) is not VIRTIO or doesn't exist. !!!  
Configure correct parameters, Delete and Re-deploy the NSP-Sensor !!! |
| Number of NICs created is fewer than the required number | ![Resource Status](image4)  
VM100 requires 6 Network interfaces. Detected 5 network interfaces. !!!  
Configure correct parameters, Delete and Re-deploy the NSP-Sensor !!! |
Task
1 Log on to the Linux server user interface using the IP address and the credentials.

2 Go to the Virtual Machine Manager.
   All instances you are running are listed in this window.

3 Right-click the instance that you want to remove and click Delete.
   The Delete option is greyed out until a virtual machine is shut down. To shut down the Virtual IPS Sensor, log on to the Sensor CLI and use the `shutdown` command.
   After you click Delete, you are prompted to choose whether you want to delete the instance from the list or from the disk.

4 Select either of the options and remove the Virtual IPS Sensor.

Add the Virtual Sensor in the Manager

Before you begin
You have a Manager version 8.1.7.x or later either on a virtual or a physical machine.

You can add the Virtual Sensor in the Manager and specify a shared secret key. You can use a Manager installed on a VM or on a physical server.

Task
1 In the Manager select Devices | <Admin Domain Name> | Global | Add and Remove Devices.

2 Click New.
3 Specify at least the Device Name, Device Type, and Shared Secret.
   • Select IPS Sensor as the Device Type.
   • You must use the same Device Name and Shared Secret when you deploy the Virtual Sensor.

4 Click Save.

Figure 2-17 Virtual Sensors added in a Manager
For more information on deleting a configured Sensor, see topic Delete a Sensor from the Manager, section How to replace a Sensor, chapter Troubleshooting in the McAfee Network Security Platform IPS Administration Guide.

Manage Licenses
Licenses are required to add vNSP Clusters. These licenses can either be individual .jar files, or they can be bundled together and provided to you in the form of a .zip file. Each license supports a pre-defined number of Virtual IPS Sensors, and this number is specific to the license file you have procured.

- There is no limit on the number of license files you can add to the Manager.
- The license files do not expire.

The Manager periodically compares the number of Virtual IPS Sensors supported by your licenses with the installed number of Virtual IPS Sensors. You are compliant as long as the number of Virtual IPS Sensors in your Manager does not exceed the total number of Virtual IPS Sensors allowed across all licenses. For example, if you have two licenses, one which allows 5 and the other which allows 10 Virtual IPS Sensors, you are compliant as long as you have no more than 15 Virtual IPS Sensors in this Manager.

If there are not enough licenses added to the Manager, a fault is raised accordingly.

The Licenses page in the Manager displays your compliance, and maintains the count for Virtual IPS Sensors and Virtual Probes. This page also displays and allows you to add and remove individual licenses.
Task

1. In the Manager, select Manager | <Admin Domain Name> | Setup | Licenses.

2. The Summary section displays the overall compliance, the number of Virtual IPS Sensors along with the maximum number allowed, and the number of Virtual Probes in use.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall License Status</td>
<td>Overall compliance which can either be Compliant or Non-compliant. If the Virtual IPS Sensor count is within the maximum limit defined in the license, the overall state is displayed as Compliant with a green icon preceding it. If the Virtual IPS Sensor count exceeds the maximum limit, the overall state is displayed as Non-Compliant with a red icon preceding it.</td>
</tr>
<tr>
<td>Total Virtual Sensors</td>
<td>Number of Virtual IPS Sensors in use along with the maximum number</td>
</tr>
<tr>
<td>Total Virtual Probes</td>
<td>Number of Virtual Probes in use</td>
</tr>
</tbody>
</table>

Figure 2-18 Licenses Page
If the overall license status is **Compliant**, the tool tip for Total Virtual Sensors displays that no additional licenses are required. However, if the overall license status is **Non-Compliant**, the tool tip for Total Virtual Sensors indicates that additional number of licenses are required for compliance.

### Summary

<table>
<thead>
<tr>
<th>Overall License Status:</th>
<th>Compliant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Virtual Sensors:</td>
<td>2 in use (33 allowed)</td>
</tr>
<tr>
<td>Total Virtual Probes:</td>
<td>3 in use</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Overall License Status:</th>
<th>Non-Compliant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Virtual Sensors:</td>
<td>2 in use (1 allowed)</td>
</tr>
<tr>
<td>Total Virtual Probes:</td>
<td>3 in use</td>
</tr>
</tbody>
</table>

3 The **Individual Licenses** section displays the details of each license imported into the Manager.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>Key – Key of the license file</td>
</tr>
<tr>
<td></td>
<td>Generated – Date when the license file was generated</td>
</tr>
<tr>
<td></td>
<td>Customer – Customer for whom the license file was generated</td>
</tr>
<tr>
<td></td>
<td>Grant ID – The McAfee Grant ID of the corresponding customer</td>
</tr>
<tr>
<td>Virtual Sensors Allowed</td>
<td>Maximum number of Virtual IPS Sensors allowed for the selected license</td>
</tr>
<tr>
<td>Added</td>
<td>Time – Date in &lt;mmm-yy&gt; format, and time when the license was added</td>
</tr>
<tr>
<td></td>
<td>By – Name of the user who added the license</td>
</tr>
<tr>
<td>Comment</td>
<td>Enables you to add your comment per license file that is imported. Double-click in the Comment field and enter your comment. Click outside this field and your comment is automatically saved.</td>
</tr>
</tbody>
</table>
4 To import licenses into the Manager, click **Add License**. Click **Browse** to locate the license, and then click **OK**. The successful addition of a license is displayed at the top of the page.

5 To remove a license, select the license you want to remove from the **Individual Licenses** section, and click **Remove**.

   In the pop-up window, click **OK** to remove the selected license or **Cancel** to return to the **Licenses** page.

   You cannot delete the last license file from the Manager if at least one vNSP Cluster is defined in the Manager. When you attempt to delete the last license, an error message is displayed and deletion is prevented.

6 Click **Save as CSV** to export license information in the .csv format. The default CSV file name is NsmLicenseList.CSV.

---

**Generate the License Compliance report**

You can generate a Virtual IPS Sensor Compliance Report to know if you are compliant with the maximum number of Virtual IPS Sensors allowed by your licenses. The report also lists the licenses added to the Manager and the Virtual IPS Sensors currently managed by it.
Task

1. In the Manager, go to **Manager | <Admin Domain Name> | Reporting | Configuration Reports | Licenses.**

2. Select the required option from the **Output Format list**, and click **Submit.**

   Virtual IPS Sensor Compliance Report is available only for the Admin Domain in the Manager.

---

**Figure 2-19 Compliance report**

---

**Figure 2-20 Non compliance report**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall License Status</td>
<td>Current overall compliance status of the number of Virtual IPS Sensors</td>
</tr>
<tr>
<td>Total Virtual Sensors</td>
<td>Number of Virtual IPS Sensors that are in use and the maximum number allowed</td>
</tr>
<tr>
<td>Total Virtual Probes</td>
<td>Number of Virtual Probes in use</td>
</tr>
<tr>
<td>Report Generation Time</td>
<td>Date in <code>&lt;yyyy-mm-dd&gt;</code> format, and time at which the report was generated</td>
</tr>
<tr>
<td>License</td>
<td>Key - Key of the license file</td>
</tr>
<tr>
<td></td>
<td>Generated - Date when the license file was generated</td>
</tr>
<tr>
<td></td>
<td>Customer - Customer for whom the license file was generated</td>
</tr>
<tr>
<td></td>
<td>Grant ID - McAfee Grant ID of the corresponding customer</td>
</tr>
</tbody>
</table>

**Option Definition**

- **Overall License Status**: Current overall compliance status of the number of Virtual IPS Sensors
- **Total Virtual Sensors**: Number of Virtual IPS Sensors that are in use and the maximum number allowed
- **Total Virtual Probes**: Number of Virtual Probes in use
- **Report Generation Time**: Date in `<yyyy-mm-dd>` format, and time at which the report was generated
- **License**: Key - Key of the license file, Generated - Date when the license file was generated, Customer - Customer for whom the license file was generated, Grant ID - McAfee Grant ID of the corresponding customer
<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Sensors Allowed</td>
<td>Total number of Virtual IPS Sensors that can be managed for the added license files</td>
</tr>
</tbody>
</table>
| Added                  | **Time** - Date in <mmm-yy> format, and time at which the license file was added to the Manager  
|                        | **By** - Name of the user who added the license file                       |
| Comment                | Enables you to add your comment per license file that is imported. Double-click in the Comment field and enter your comment. Click outside this field and the your comment is automatically saved. |
| Managed Virtual IPS Sensors | # - Row number  
|                        | **Name** - Name of the Virtual IPS Sensor  
|                        | **Model** - Model number of the Virtual IPS Sensor  
|                        | **Cloud Cluster / VSS** - Name of the vNSP Cluster to which the corresponding Virtual IPS Sensor belongs |
Virtual IPS Sensor deployment
Generate the License Compliance report
Network Security Platform for VMware NSX

Chapter 3  IPS for virtual networks using Intel Security Controller
IPS for virtual networks using Intel Security Controller

If your Manager version is later than 8.3.7.35, you can integrate McAfee® Network Security Platform with Intel Security Controller to provide next-generation IPS service for software-defined datacenters (SDDC).

This section provides the following information:

• An overview of Intel Security Controller and how it collaborates with McAfee Network Security Platform and NSX to provide IPS service to SDDCs.
• Detailed procedures to deploy next-generation IPS for virtual networks using Intel Security Controller.
  To deploy IPS service to SDDCs, you configure Intel Security Controller, Manager, and NSX. To configure NSX, you need vCenter web client.

This section assumes the following:

• You have installed and set up Intel Security Controller virtual appliance. For information, see the latest Open Security Controller Product Guide.
• For information on installing and configuring VMware NSX, refer to VMware documentation.
• For information on installing and configuring the virtual infrastructure, refer to the corresponding documentation. For example, for VMware virtual infrastructure, refer to VMware documentation.

Limited information on how to set up and configure a VMware-based SDDC is provided in Intel Security Controller Product Guide. However, this information is designed only for setting up test environments. For production environments and details of VMware functionalities, you must refer to VMware documentation.

Contents

- Securing virtual networks with Intel Security Controller
- Deploying next generation IPS service to a virtual network

Securing virtual networks with Intel Security Controller

Intel® Security Controller (henceforth, referred to as Intel Security Controller) is a centralized platform to enable software-defined security for software-defined datacenters (SDDC). Intel Security Controller provides a common set of management services, acting as a broker between the security solutions and the virtual infrastructure. You can use Intel Security Controller to provide service such as next-generation Intrusion Prevention System (IPS) virtual infrastructures.

Intel Security Controller integrates with a hypervisor and a networking provider to provide security solutions as a service to your virtual networks. Using Intel Security Controller as a liaison between the security service and its associated components, and the virtualization providers, you are able to provide security services for virtual networks.
To illustrate this, consider a virtual environment that uses VMware vCenter* and VMware ESXi* as its hypervisor and VMware NSX* as its Software Defined Network (SDN) controller to deploy security services on virtual infrastructure.

![Software Defined Data Center](image)

**Figure 3-1 Intel Security Controller solution overview - current virtualization environment supported**

Intel Security Controller is a virtual appliance that you install on an ESXi host. It provides a Java*-based web application for configuration and management. You can deploy Intel Security Controller on existing virtual infrastructure without any configuration changes to those virtual networks.

As the above illustration shows you can also deploy security services on OpenStack* environments.

**Contents**

- Security challenges in an SDDC
- How Intel Security Controller secures virtual networks
- Advantages of Intel Security Controller
- Virtual IPS Sensors deployed through Intel Security Controller

**Security challenges in an SDDC**

Consider a large-scale SDDC consisting of hundreds of hosts aggregated under multiple clusters. Virtualization provides flexibility and agility to its users, wherein they can spin up virtual machines (VMs). Users can spin up isolated logical networks as easily as one can spin up VMs. All these possibilities require no changes in the physical networking configuration. When multiple users spin up new networks and move working VMs across physical boxes in such a large-scale data center, security is threatened.
To match with the capabilities of virtualization solutions, Intel Security Controller can seamlessly, non-intrusively, and non-disruptively integrate security services with existing virtualized environments. This enables network security services to keep pace with the speed, agility, and scalability of virtualization features and solutions.

**How Intel Security Controller secures virtual networks**

To understand how Intel Security Controller can orchestrate security for virtual networks, consider a VMware-based SDDC as illustrated here. For the sake of explanation, this SDDC is shown to contain only a few ESXi hosts.

Two ESXi hosts are clustered together. A few Windows VMs are connected to a distributed vSwitch that spans across these two ESXi hosts. VMware vCenter and NSX are installed on a third ESXi host in the same data center but outside the cluster. With vMotion*, you can move the VMs between host-1 and host-2.

![Figure 3-2 An example SDDC](image-url)
Consider a datacenter in which you want to implement a security service function (security service) using Intel Security Controller. This illustration shows next-generation IPS.

![Diagram of SDDC with IPS service through Intel Security Controller]

**Figure 3-3  SDDC with IPS service through Intel Security Controller**

To deploy a security service, some of the generic tasks you need to complete are:

1. Install the Intel Security Controller virtual appliance in an ESXi host outside the cluster in which you want to deploy the security service.

2. Select a security manager for managing these security appliances. Consider that you are using an existing security manager, which is managing other security appliances in your network. Only minimal user intervention is required to install these security appliances. Discovery and establishment of trust with the corresponding security manager is automatic.

3. Deploy the security service to an ESXi cluster such that when you select an ESXi cluster, the security service is available to all VMs on the corresponding ESXi hosts. In this example, there is only one cluster. Intel Security Controller collaborates with vCenter and NSX such that virtual security is automatically deployed in every host in the selected cluster.

4. In NSX, create security groups containing the objects you want to protect in the cluster. For example, you can select the cluster itself or the distributed switch port group. Then the security service is available for all VMs corresponding to the selected object. In this example, VMs 1 through 4 are selected for IPS service. So traffic related to these VMs is subjected to next-generation IPS analysis. In effect, if VM1 communicates with VM2, traffic does not exit the host. However, the security service inspects such traffic.
Notes:

- Even if you migrate one of the protected VMs to a different host, the same security service is automatically provided to that VM.

- If you add a host to the cluster, you must make sure that network virtualization components are installed on the host as part of host preparation through NSX. Then, an instance of the security service is automatically installed on that host. Trust is also automatically established, by way of exchange or a password or a certificate key, between this instance of the security service and the corresponding security manager.

- Consider that you select the distributed switch port group (dSwitchPortGroup) as the object to be protected. Then any new VM added to this switch port group is automatically subjected to IPS (or other security service).

Advantages of Intel Security Controller

- Intel Security Controller facilitates simple, seamless, non-intrusive, and non-disruptive security service integration with an existing virtualized environment.

- The best-in-class security solutions available to your physical networks are available to your virtual networks as a software-based service.

- Regarding securing virtual networks, Intel Security Controller can cope with the flexibility, scalability, and agility of virtualization solutions. After you deploy a security service, your virtual networks are protected with minimal user-intervention as they scale up.

- When you deploy an IPS service, you can use your current security manager and those security policies for the SDDC.

- You do not need to change your physical or virtual network architecture to provide a security service to your virtual networks.

- Provides visibility of intra-VM traffic (east-to-west) for security.

- Under test conditions, Intel Security Controller did not impact functionality or performance of virtualization solutions.

Virtual IPS Sensors deployed through Intel Security Controller

When you implement IPS service using Intel Security Controller, it involves the deployment of a type of virtual IPS Sensors. These virtual IPS Sensors are referred to as Virtual Security Systems. A Virtual Security System is to some extent similar to the regular Virtual IPS Sensors, such as the IPS-VM100 Sensor.
Table 3-1  Differences between Virtual IPS Sensors and Virtual Security Systems

<table>
<thead>
<tr>
<th>Virtual IPS Sensors</th>
<th>Virtual Security Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>You manually install Virtual IPS Sensor and establish trust with the Manager. Sensor shared secret key is required to establish trust.</td>
<td>Sensor deployment and trust establishment is automatic. Intel Security Controller orchestrates the deployment and trust establishment. Sensor shared secret key is not relevant. Post deployment of Virtual Security System instances, if necessary, you can re-establish trust between the Manager and a specific Virtual Security System instance from the Intel Security Controller web application.</td>
</tr>
<tr>
<td>Each Virtual IPS Sensor is an individual entity.</td>
<td>A Virtual Security System is a container object for its instances. That is, if your ESXi cluster consists of two ESXi hosts, a virtual Sensor is deployed in each host. These two virtual Sensors are the instances of one Virtual Security System. So, the Virtual Security System is the logical container of these two virtual Sensors. The virtual Sensors (or instances of a Virtual Security System) are the appliances, which inspect traffic. Each Virtual Security System instance is an individual entity. However, these instances are managed as one Virtual Security System. This is similar to how a Manager manages a Sensor failover pair. Therefore, the same security policies and other configuration are applied to the instances of a Virtual Security System.</td>
</tr>
<tr>
<td>The scope of Virtual IPS Sensors is limited to the host in which it is deployed.</td>
<td>Virtual Security System caters to the entire cluster. You can upgrade or downgrade the software version of the Virtual Security System instances in the cluster. Also, when you deploy the changes from the Manager, the changes are deployed to the Virtual Security System instances in the cluster.</td>
</tr>
<tr>
<td>Virtual IPS Sensors work with standard virtual switches and standard switch port groups only.</td>
<td>Virtual Security System instances work with distributed virtual switches and distributed switch port groups only.</td>
</tr>
<tr>
<td>Virtualization features such as vMotion and DRS are not supported.</td>
<td>Next-generation IPS service is available to a VM regardless of where it is located in the data center. Also, the IPS configuration applied on that VM does not change because the VM is now in a different ESXi host. DRS has no impact on how a Virtual Security System function.</td>
</tr>
<tr>
<td>Inline and SPAN are supported.</td>
<td>Only inline is supported.</td>
</tr>
<tr>
<td>Inline deployment might require changes to your standard virtual switches. So, it might involve a brief network downtime.</td>
<td>No changes to distributed switches, port groups, or physical network configuration are required.</td>
</tr>
<tr>
<td>Depending on the model, a virtual management port, a virtual response port, and a number of virtual monitoring ports are visible in the Manager.</td>
<td>The virtual ports are not exposed.</td>
</tr>
</tbody>
</table>

Deploying next generation IPS service to a virtual network

In the current release, Intel Security Controller supports only next-generation IPS to be deployed as a service to your virtual networks. When you deploy the IPS service, the traffic from and to the protected VMs are subjected to inline inspection by a Virtual IPS Sensor. If a VM is the source of malicious traffic, the Virtual Sensor takes the configured response action.
One Virtual Sensor is installed per ESXi host. The Manager that you specified in the Security Manager Connector manages all these Virtual Sensors. These Virtual Sensors are configured similarly but function independently. That is, these Virtual Sensors provide IPS to their respective ESXi hosts but implement the same IPS and other IPS configuration.

To deploy the Virtual IPS Sensors, Intel Security Controller integrates with NSX. This integration also ensures that the relevant traffic is routed through the Virtual Sensor for inspection.

The IPS service makes available all relevant next-generation IPS features for your dynamic virtual networks. Deploying the IPS service is non-intrusive and non-disruptive even though the Virtual Sensors are deployed in inline mode only. Scaling up or changing your virtual networks do not warrant any kind user-intervention to your IPS service deployment. Also, any change to the IPS configuration is automatically applied to all Virtual Sensors. Intel Security Controller does not take any action directly but orchestrates the actions by its integration with ESX, vCenter, Manager, and the Virtual Sensors.

Contents
- Terminology
- Components involved in IPS service
- High-level steps to implement a security service
- How the IPS service works
- Requirements for deploying IPS service
- Considerations
- Prepare an ESXi host for NSX
- Define an IP address pool for virtual security appliances
- Define virtualization connectors
- Define manager connectors
- Manage software images for virtual security appliances
- Manage distributed appliances
- Jobs and tasks
- Create a security group in VMware NSX
- Create a security policy in VMware NSX
- Apply a security policy to a security group in VMware NSX
- Configure virtual security system to fail-close or fail-open
- Manager functions regarding IPS service deployment
- Troubleshooting tips and FAQs regarding IPS service

Terminology
To configure Intel Security Controller to act as a broker, you first define the building blocks. You then use these building blocks to configure Intel Security Controller so that it can act as a broker between the virtualization provider and security solutions.

- Virtualization connector — In this building block, you define the virtualization provider entities. You must confirm that the virtualization provider is accessible to Intel Security Controller.
  - For VMware, you define the IP address and administrator logon credentials for NSX and vCenter.
  - For OpenStack, you must make sure to define administrator credentials to Keystone, which is the OpenStack user-interface.

- Appliance instances — The virtual security appliances, which intercept the traffic from the VMs.
  For IPS, Virtual Sensors are the security appliance instances, which are referred to as Virtual Security System instances.
• Security service manager connector (Manager connector) — In this building block, you define the management console for managing the security appliances. For IPS, you define the Manager IP address and the root admin logon credentials, which will manage the Virtual Sensors installed in the hosts. For firewall, you define the Security Management Console (SMC) IP address and the API authentication key.

• Security service function (security service) — This component refers to the security service you intend to deploy such as next-generation IPS or next-generation firewall. You can use the Service Function Catalog page to upload corresponding software images for further deployment through Intel Security Controller.

• Distributed appliances — A distributed appliance, associates the security solution and the virtualization solution. That is, you define a distributed appliance using the virtualization connectors and security manager connector as building blocks. In a distributed appliance, you specify the following:
  • One security manager connector.
  • The model and version of the security appliance.
    For IPS, this is the version and model of the virtual Sensors, which are later deployed in the ESXi hosts.
    For firewall, this is the version of the VMware vCenter compatible image of
  • One or more virtualization connectors.
  • For each virtualization connector, you must select a Manager admin domain. The security appliances are managed under the specified admin domain. In the case of IPS, if you select My Company (root admin domain), all virtual Sensors are managed under My Company in the Manager. In case of firewall, select shared domain in SMC to view the managed devices.

**Figure 3-4 Distributed appliance**

• Virtual system: A virtualization connector associated with a manager domain is a virtual system. The most common example of a virtual system is the Virtual Security System for IPS and Virtual Security System container for firewall. A Virtual Security System is the logical container object for all deployed virtual security service functions or Virtual Security System instances.
- Intel Security Controller agents: Security services deployed through Intel Security Controller have the following agents.
  - Control Path Agent: This agent is responsible for communication between the security services and the security manager.
  - Data Path Agent: This agent makes sure the traffic from the VMs are routed through the security service for inspection in case of VMware. The data path agent does not manage traffic for OpenStack.
- Job and tasks: Some of the actions that you perform in Intel Security Controller are treated as jobs and tasks. The high-level action is treated as a job. For example, synchronizing a distributed appliance is a job. A job might consist of a number of tasks. That is, a job can be broken down into tasks. For example, if synchronizing a distributed appliance is the job, checking the manager connector and validating existing NSX components are some of the tasks. When all tasks are completed successfully, the corresponding job is complete.

Jobs and tasks enable you to easily track and troubleshoot your actions in Intel Security Controller. When you trigger a job, the state, status, start time, completed time, and so on are displayed for the job as well as its component tasks.

### Components involved in IPS service

The following are the components directly related to IPS service provided through Intel Security Controller:

- Manager: This is the Network Security Manager which manages all the Virtual Sensors deployed through Intel Security Controller. You provide the IP address and admin logon credentials when you define the Security Manager Connector. When you deploy the IPS Service, Intel Security Controller ensures that the installed Virtual Sensors automatically establish trust with the specified Manager.
  
  There is no shared secret key configuration required on Virtual Sensors and Manager.

  Once trust is established, these Sensors and the Manager communicate similar to the regular Sensors. Currently, you cannot use Managers that are part of an Manager Disaster Recovery (MDR) pair to manage the Virtual Sensors deployed through Intel Security Controller.

- Virtual IPS Sensor deployed through Intel Security Controller: The Virtual IPS Sensor deployed through Intel Security Controller for the most part are similar to the regular Virtual IPS Sensors. However, these Sensor images are slightly modified to exchange communication with Intel Security Controller. Therefore, you cannot install the regular Virtual Sensors through Intel Security Controller; you must use the specific Virtual Sensor images for Intel Security Controller. Once these Sensors are deployed and trust established with the Manager, these Sensors function similar to the regular Virtual Sensors.

  The Virtual Sensors deployed through Intel Security Controller support all the relevant features similar to the regular Virtual Sensors.

- ESX Agent: In vCenter, the Virtual IPS Sensors deployed through Intel Security Controller are grouped under a resource pool called ESX Agents. This resource pool is created under the cluster for which you deploy IPS service. It is recommended that you do not attempt to change the settings for these Sensors grouped in the ESX Agent resource pool.

- Security Group in NSX: This is a group of VMware objects for which the IPS service is provided. For example, if you include a distributed port group, the Virtual IPS Sensor monitors traffic related to all the VMs connected to this distributed port group. Similarly, if you select a cluster, the Virtual IPS Sensor monitors traffic related to all the VMs in the cluster. You define this security group through vCenter.

- Security Policy in NSX: You define this policy in NSX using the vCenter web client. You define the required security services in a security policy. Then you apply this policy to a security group in NSX (described above).
A security policy has three sections:

- Guest introspection services - You define the VM-level security services such as anti-virus, vulnerability management, data security, and so on in this section. These features are native to NSX and not provided through Intel Security Controller. So, this section is not relevant for IPS service.

- Firewall rules - You define a set of ACL rules to regulate the traffic coming in and going out of the corresponding security group. This firewall feature is a native feature of NSX and not a service provided through Intel Security Controller. So, this section is not relevant for IPS service.

- Network Introspection Services - This section relates to services such as IPS and IDS through external solutions. So, you define the details related to IPS service in this section and apply it to the required security group.

In the security policy, you specify the following:

- You must select the required distributed appliance from the security name list. The distributed appliances that you defined in Intel Security Controller are listed under service name in vCenter.

- Security profile. These are the IPS policies that are currently defined in the corresponding Manager. When you create a distributed appliance, Intel Security Controller collects the IPS policy names from the Manager specified in the Security Manager Connector. Intel Security Controller provides this list of policies to NSX, which is listed under Profile in vCenter. So, the IPS policies in the Manager are the same as that of security profiles in NSX/vCenter.

- Source and destination of traffic based on which the selected security profile (IPS policy) must be applied. This option is to enable you to specify the inbound or outbound direction.

You can select the same profile (IPS policy) for both inbound and outbound or specify different policies.

- Policy groups in the Manager: The policy group in the Manager is the collection of next-generation IPS policies defined in the Manager. For example, a policy group contains definitions for exploit attacks, recon attacks, DoS attacks, advanced malware, and firewall access rules. When you create a distributed appliance, Intel Security Controller provides these policy groups from the Manager to NSX. Then, vCenter displays this list under security profile when you configure network introspection services in the security policy in NSX.
High-level steps to implement a security service

Any security service through Intel Security Controller is a collaboration between vCenter, NSX, the security service manager, and the virtual security service appliances that orchestrated by Intel Security Controller. To illustrate what this means, consider an SDDC as shown here. Assume that you want to provide a security service such as IPS or firewall to VMs 1 through 4. vCenter and NSX are up and running on ESXi-3.

![An example of SDDC](image-url)
The following are the high-level steps for configuring the security service using Intel Security Controller. There are multiple orders by which you can complete this configuration. The steps provided here are in the recommended order.

1. When you deploy the security service to a cluster, Intel Security Controller collaborates with NSX to install a virtual security service appliance in each host of that cluster. Each of these virtual security service appliances needs a management port IP address. In this example, there are two hosts in the cluster which means that you need two IP addresses for the management ports of these appliances.

   You define a pool of IP addresses in the NSX Manager. For each IP address pool, you also define the required network details such as the default gateway and DNS server IP addresses.

   The number of IP addresses in an IP address pool depends on the number of ESXi hosts that you plan to include in the corresponding cluster. You must also factor in the ESXi hosts that you might add to the cluster in future. When you add ESXi hosts to the cluster after deploying a security service, NSX automatically installs an instance of the virtual security service appliance in those ESXi hosts. NSX needs an IP address to assign to these virtual appliances. Consider that the cluster for which you plan to provide the security service currently has two ESXi hosts. However, you plan to include 5 more ESXi hosts later on. Though two IP addresses are currently sufficient, you need 5 more for the ESXi hosts that you plan to add.

2. Complete the following configuration in Intel Security Controller.

   a. Create a virtualization connector by providing the IP address and logon credentials for NSX and vCenter. You can create as many virtualization connectors as you require. For example, you want to provide the same security service to multiple clusters managed by different vCenters. Then create virtualization connector for each vCenter. The same security policies are applied to all hosts in all these clusters when you implement the security service.

      In this example, one virtualization connector is sufficient since there is only one cluster managed by one vCenter. See Define virtualization connectors on page 126.

   b. Create a manager connector by providing its IP address and admin logon credentials. See Define manager connectors on page 130.

   c. Define the virtual security service appliance in Intel Security Controller and import the required security service function images into Intel Security Controller. See Change the software version of security appliances on page 134.

   d. Create a distributed appliance using the virtualization connectors, manager connector, and the required virtual security service image from the previous 3 steps. When you associate a virtualization connector with a security manager domain, a Virtualization System is created in Intel Security Controller.

   e. Deploy the Virtualization Systems that you created in the previous step in the relevant clusters. If there are multiple clusters that you want to protect, you must deploy the Virtualization System separately for each cluster. Then, Intel Security Controller collaborates with the corresponding vCenter and NSX to deploy Virtual Sensors in each ESXi host in the specified cluster. See Deploy virtual systems on page 140.
3 Complete the following configuration in NSX using vCenter web client.
   a NSX needs to know the IP addresses of the VMs to be protected for it to route the traffic for the network introspection service (that is, to the Virtual Security System instances). For NSX to know the IP addresses, VMware tools must be running on the VMs. If VMware tools is not running, you must include the IP addresses of such VMs in a security group. Before you create the security group, create an IP set object containing the IP addresses of VMs on which VMware tools is not running.
   b In the Networking & Security tab of vCenter, create a security group and add the VMs that you want to protect. In our example, you include VMs 1 through 4 in the security group. See Create a security group in VMware NSX on page 154.
   c Create a security policy and in the Network Introspection Services step, select the corresponding distributed appliance and the security service policy for both inbound and outbound traffic. The distributed appliances are listed as Service Name and the security service policies are listed as Profiles in vCenter. See Create a security policy in VMware NSX on page 158.
      Apply the security policy that you created in the previous to the policy group created in step 1. See Apply a security policy to a security group in VMware NSX on page 161.

4 Complete the following in the security service manager.
   a Log on to the security service manager and verify whether the Virtual Security System is listed in the appropriate device list.
   b Check the status of the Virtual Security System in the security service manager. Also, in case of IPS, verify whether a signature set is present. If not, take appropriate measures to provide one. For example, in IPS, you must deploy pending changes to the Virtual Security System from the Devices tab. The pending changes are automatically updated to all individual Virtual IPS Sensors of that Virtual Security System.
   c If necessary, log on to the CLI of the virtual security service appliance and view the configuration.

5 To verify successful deployment, send sample attack traffic from one of the protected VMs and check if an alert is displayed in the security service manager.

6 By default, Virtual Security System instances are deployed in fail-open mode. You can configure a Virtual Security System to fail-close if necessary. See Configure virtual security system to fail-close or fail-open on page 164.

How the IPS service works
When you deploy a Virtual System from Intel Security Controller, NSX creates one Virtual Sensor per host in the specified cluster. This Virtual Sensor provides IPS service for the protected VMs in that host.

1 When you create a security manager connector in Intel Security Controller (step 2-2 in High-level steps to implement a security service on page 113), Intel Security Controller gathers the policy group names from the Manager and provides them to NSX. This is how the Manager policy groups are available for you to select when you add a network introspection service in a security policy in NSX.

2 As described in step 2-3 in High-level steps to implement a security service on page 113, you import the required Virtual Sensor software images into Intel Security Controller. Intel Security Controller provides these image files to NSX to install the Virtual Sensors in the ESXi hosts.

3 When you create the Virtualization System, you select the Manager admin domain. Intel Security Controller uses this information to align the Virtual Sensors under the selected admin domains in the Manager.
When you deploy the Virtualization System, Intel Security Controller orchestrates the installation of the Virtual Sensors in the corresponding ESXi hosts through NSX. The following actions are also completed automatically.

Figure 3-7  SDDC with IPS service through Intel Security Controller

- Intel Security Controller creates the corresponding Virtual Security Sensor objects in the Manager and under the selected admin domain. Recall that a Virtual Security Sensor is the logical container in the Manager for the deployed Virtual Sensors. Virtual Security Sensor is comparable to the Sensor failover object created in the Manager when you pair up Sensors for failover. Virtual Security Sensor in the Manager is the equivalent of Virtual Systems in a Distributed Appliance in Intel Security Controller.

- The Virtual Sensors automatically establish trust with the Manager specified in the Security Manager Connector.

- The internal monitoring ports are automatically configured for operation.

- When you create or delete a new policy group in the Manager, Intel Security Controller automatically updates NSX so the changes reflect in NSX as well.

- When you add an ESXi host to the cluster, NSX automatically installs the Virtual Sensor on this new ESXi host and aligns the Virtual Sensor under the corresponding admin domain in the Manager.

- If you change the IPS configuration, you must deploy the changes to the Virtual Security Sensor. Intel Security Controller makes sure that these changes are deployed in all Virtual Sensors of that Virtual Security Sensor.

In our example, VMs 1 to 4 are included in the security group of NSX. That is, these are VMs for which IPS service is provided currently. If VM1 communicates with VM2, NSX directs this traffic to pass through the inline Virtual Sensor on ESXi-1. Any traffic originating from or destined to VMs 1 to 3 pass through this Virtual Sensor.
Consider VM1 communicates with VM4, which is on ESXi-2. The Virtual IPS Sensor on ESXi-1 applies the outbound policy group on this traffic before it exits out of the host. When it reaches ESXi-2, the Virtual Sensor on this host applies the inbound policy group before forwarding it. So, if both these Virtual Sensors detect an attack in this traffic, they raise separate alerts in the Manager. The corresponding Virtual Sensors take the required response action as configured in the policies.

The Virtual Sensor does not receive the traffic if two VMs not belonging to the security group communicate with each other.
Requirements for deploying IPS service

Make sure that you meet the following requirements before you deploy IPS service using Intel Security Controller.

- The hosts must be running on ESXi version 5.5 or later.

- You can deploy IPS service only at a cluster level. So, make sure that you have clustered the hosts for which you want to provide IPS service. You must create a cluster even if you want to deploy IPS service to only one host.

- You have VMware vCenter version 5.5 or later installed (corresponding to the ESXi version).

- You have VMware NSX version 6.1 or later installed.

- All hosts in the clusters have network virtualization components installed (Host Preparation).

- Intel Security Controller requires distributed virtual switches of version 5.5. Standard virtual switches are not supported.

- If the corresponding clusters contain more than one ESXi host, you must set up an NFS datastore for those clusters. In case of clusters with more than one ESXi hosts, the Virtual Sensors are installed only in NFS datastores. If a cluster contains only one ESXi host, a VMFS datastore will suffice.

- You have Manager 8.2.7.23 or later installed.

- You have imported the Virtual Sensor software images into Intel Security Controller.
• Intel Security Controller can communicate with the vCenter, NSX, and the Manager.
• VMware tools must be running on the protected VMs. This enables the NSX (NetX) APIs to redirect traffic to the Virtual Sensor on the host. If VMware tools are not installed on the VMs, an alternative is to create a grouping object based on IP sets in NSX. Then, you must add this grouping object in the security group.

Considerations
Review the following before you deploy IPS service using Intel Security Controller.

• Because Intel Security Controller currently supports only IPv4 addressing, the Manager, IP pool for Virtual Security Systems, NSX, and vCenter Server must all have an IPv4 address. Also, the products with which you plan to integrate the Virtual Security System instances must also have an IPv4 address.
• MDR is not supported currently. So, you cannot use a Manager, which is part of an MDR.
• Only inline mode is supported. You configure inline fail-open and fail-close modes not on the Sensor but through an NSX mechanism.
• Failover of Virtual Security System instances is not supported.
• IPS-VM100-VSS Virtual Security System model is similar to the IPS-VM100 Virtual IPS Sensor with respect to Sensor performance and capacity values. See the Network Security Platform Best Practices Guide for performance and capacity values of IPS-VM100.

IPS features - supported
The following are the list of IPS features supported by Virtual Security Systems in this release:

• Inline fail-open and fail-close are through an NSX mechanism
• To apply the policies, you must use Policy Groups in the Manager
  • IPS policies
  • Advanced Malware policies
  • Inspection Options policies
  • Connection Limiting policies
  • Firewall policies
• Quarantine (automatic, through IPS policies as well as manual from the Attack Log). In addition, quarantine through security tags of NSX is also supported.
• Snort custom attack definitions
• McAfee custom attack definitions
• Protection of Web application servers
• Advanced Traffic Inspection
• Layer 2 passthru mode is supported but implemented differently when compared to physical Sensors
• Layer 7 data collection
• MPLS traffic inspection
• IPv6 traffic inspection
• HTTP response scanning
• Inspection of double VLAN tagged traffic
• Synchronization of Sensor clock using an NTP server
• Display Sensor CLI audit log events in the Manager
• TACACS+ user in audit logs
• Secure Transfer of Files from Sensor CLI
• Application Identification and Visualization
• Advanced Traffic inspection
• SmartBlocking of attacks including use of IP Reputation to augment SmartBlocking
• Integration with McAfee GTI for IP reputation and file reputation. This includes protection from high-risk hosts.
• Inspection of X-Forwarder-For Header Information. Reputation lookup and quarantine of client IP addresses in the XFF header.
• Stateless Firewall access rules
• Granular access control for CLI commands (for TACACS users)
• Advanced callback detection including Bot Command and Control server activity detection
• Web server protection against DoS attacks
• Integration with McAfee Endpoint Intelligence Agent (McAfee EIA)
• Sensor autorecovery is done through a VM recovery feature.
• Syn cookie
• Latency monitor
• Traffic prioritization
• IP fragmentation flood
• Inspection of tunneled traffic including GRE tunneled traffic
• Passive device profiling
• Attacks using evasion techniques – supported but some combinations may not be detected.

**IPS features - not supported**
The following are the list of IPS features not supported by Virtual Security Systems in this release:

• Inspection of SSL traffic
• Capture data packets (packet capture) in file mode (that is, sending the captured files to the Manager or to an SCP server).
• DNS spoof protection feature (to prevent DDoS attacks)
• Simulated blocking
• MDR

  **Note:** If a Virtual Security System is added in a Manager, you cannot create an MDR pair with that Manager. If the Manager is already part of an MDR, Virtual Security System cannot be deployed using this Manager.

• Correlation of attacks
• DoS learning and DoS threshold
• Jumbo frames are passed without attack detection.
• Monitoring Sensor performance

Prepare an ESXi host for NSX

Before you begin
• You have successfully installed and configured the NSX Manager.
• You have admin privileges in the vCenter Server.

To protect the VMs through Intel Security Controller and NSX, you must prepare the ESXi host of those VMs. You use the Networking & Security options in the vCenter Server Web Client to prepare an ESXi host.

Task
1 Log on to vCenter Server Web Client with administrator privileges.
2 Select Home | Networking & Security | Installation | Host Preparation.
3 Select the required NSX Manager.
4 Click Install for the required cluster or ESXi host.

![NSX Manager](image)

Installation of network virtualization components on vSphere hosts

<table>
<thead>
<tr>
<th>Clusters &amp; Hosts</th>
<th>Installation Status</th>
<th>Firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td>DRS</td>
<td>Install</td>
<td>Not Enabled</td>
</tr>
</tbody>
</table>

5 Click Yes to proceed with the installation.

![Install](image)

Are you sure you want to continue with the install?

Yes  No

You can monitor the progress of the task.
The installation status column shows if the task completed successfully.

![Installation](image)

If the host preparation task fails, restart the corresponding ESXi hosts and repeat the task.

Define an IP address pool for virtual security appliances

If you have installed NSX, you can define the IP pool for the virtual security appliances. Along with the IP addresses, you also define other network settings such as the default gateway IP address and the subnet mask.

Currently, Intel Security Controller supports only IPv4 addresses. So, the IP pool must contain IPv4 addresses only.
**Task**

1. Log on to vSphere* Web Client as the root user.

2. In the vSphere Home tab, select Networking & Security.


---

**Figure 3-8 Select networking & security**

**Figure 3-9 Select NSX Managers**
4 Select the NSX Manager in which you want to define the IP pool and then select Manage | Grouping Objects | IP Pools.

Figure 3-10 Select IP pools
5 Click + to add an IP pool.

6 In the Add IP Pool window, enter the details and click OK.

Table 3-2 Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a relevant name for the IP pool.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Enter the IP address of the default gateway for the IP addresses. After you create the IP pool, you cannot modify the default gateway IP address.</td>
</tr>
<tr>
<td>Prefix Length</td>
<td>Enter the network prefix length of the IP addresses.</td>
</tr>
<tr>
<td>Primary DNS</td>
<td>Enter the IP address of the primary or the preferred DNS server for the IP addresses.</td>
</tr>
<tr>
<td>Secondary DNS</td>
<td>Optionally, enter the IP address of the secondary DNS server.</td>
</tr>
<tr>
<td>Static IP Pool</td>
<td>Enter the range of valid IPv4 addresses. Make sure there is no IP address clash. That is, the IP addresses in the IP pool must not have been assigned to a network object or already included in a different IP pool.</td>
</tr>
</tbody>
</table>
IPS for virtual networks using Intel Security Controller
Deploying next generation IPS service to a virtual network

Table 3-2  Option definitions (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>Click to save the settings and create the IP pool.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Click to close the dialog box without saving the changes.</td>
</tr>
</tbody>
</table>

Figure 3-11  Add IP pool

The summary view displays the count of IP addresses in an IP pool and the count of addresses in use.

Figure 3-12  Summary view

Define virtualization connectors

Before you begin

- To add a virtualization connector, you must have already uploaded the SDN controller plugins based on your virtualization environments. For more information, refer to Manager plugins.

You are able to define virtualization connectors from the Intel Security Controller web application.
**Task**

1. In the Intel Security Controller web application, select **Setup | Virtualization Connectors**. The Virtualization Connector page displays the currently available virtualization connectors.

   ![Virtualization Connector page](image)

   **Table 3-3 Option definitions**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the virtualization connector record.</td>
</tr>
<tr>
<td>Type</td>
<td>Virtualization provider which you mention when you create the virtualization connector. VMware and OpenStack are the supported types.</td>
</tr>
<tr>
<td>Controller IP</td>
<td>IP address of the virtual security controller such as SDN controller.</td>
</tr>
<tr>
<td>Provider IP</td>
<td>IP address of the virtualization provider server. Clicking the hyperlink provided for the IP address opens the login screen of the virtualization provider.</td>
</tr>
</tbody>
</table>

   Certain virtualization providers are configured on specific ports of the server. You are required to enter the port at the end of the URL.

2. Take one of the following actions:

   To create a new virtualization connector, click **Add** and enter the options in the **Add Virtualization Connector** dialog.

   ![VMware virtualization connector](image)  ![OpenStack virtualization connector](image)
Table 3-4 Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name that enables you easily identify a virtualization connector record.</td>
</tr>
</tbody>
</table>
| Type    | Virtualization provider from the list of currently supported providers. You are provided with two options:  
• VMware  
• OpenStack |
| Cancel  | Closes the dialog without saving the changes. |
| OK      | Closes the dialog box with the changes saved to the Intel Security Controller database. A warning displays if Intel Security Controller is unable to connect to virtualization provider using the IP address and credentials. You can still create the virtualization connector. However, if you use this virtualization connector in a distributed appliance, you cannot delete the distributed appliance or virtualization connector record.  
If you are using NSX and delete a virtualization connector, Intel Security Controller deletes the related data from NSX. So, if Intel Security Controller is unable to log on to the NSX defined in the virtualization connector, the task of deleting the virtualization connector fails. |

**VMWare**

<table>
<thead>
<tr>
<th>NSX</th>
<th>IPv4 address of VMware NSX Manager Virtual Appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>IPv4 address of VMware NSX Manager Virtual Appliance.</td>
</tr>
<tr>
<td>User Name</td>
<td>Logon name of an admin user.</td>
</tr>
<tr>
<td>Password</td>
<td>Corresponding password.</td>
</tr>
</tbody>
</table>

**vCenter**

<table>
<thead>
<tr>
<th>IP</th>
<th>IPv4 address of VMware vCenter with which the NSX management service is connected.</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Root admin user name of the vCenter.</td>
</tr>
<tr>
<td>Password</td>
<td>Corresponding password.</td>
</tr>
</tbody>
</table>

**OpenStack**

<table>
<thead>
<tr>
<th>SDN Controller</th>
<th>[Optional] SDN controllers allow network programming capability in which the control plane and data plane are separated. You are able to steer or redirect traffic from the virtual machines to the inspection device, depending on the SDN controller you are using.</th>
</tr>
</thead>
</table>
| Type           | SDN controller that is used by your virtual network. An SDN controller replaces the control plane of underlying hardware and replaces it with software thereby removing the dependancy on hardware type. Select from the list of currently supported providers. You are provided with the following options:  
• NSC (Network Security Controller) – A simple SDN controller used primarily to redirect traffic. It does not offer service function chaining, failure policy support, and off-box redirection.  
• MIDO_NET* – An full-service SDN controller developed by Midokura*.  
• NONE – Intel Security Controller can operate in a deployment-only mode in which it will not redirect traffic. Instead, your virtual network has its own infrastructure to redirect traffic. The only requirement is for the switching device to add an identifier which notifies the security service about which policy is to be used during traffic inspection. |
| IP  | IPv4 address of the SDN controller. |
Table 3-4 Option definitions (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Username of the SDN controller.</td>
</tr>
<tr>
<td>Password</td>
<td>Password of the SDN controller.</td>
</tr>
<tr>
<td>Keystone IP</td>
<td>Enter the IPv4 address of the tenant environment in OpenStack.</td>
</tr>
<tr>
<td>Admin Tenant Name</td>
<td>Name of the admin tenant that is used in OpenStack.</td>
</tr>
<tr>
<td></td>
<td>This tenant must have sufficient privileges to query and perform all operations and must have to access other tenants in the environment.</td>
</tr>
<tr>
<td>User Name</td>
<td>Username of the administrator.</td>
</tr>
<tr>
<td>Password</td>
<td>Password of the administrator.</td>
</tr>
<tr>
<td>Show Advanced Settings</td>
<td>(Optional) Clicking this button opens the Advanced Settings pop-up, which provides you the ability to configure RabbitMQ* settings.</td>
</tr>
<tr>
<td></td>
<td>If these settings are not configured correctly you will lose the dynamic capabilities of Intel Security Controller.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Communication OpenStack and Intel Security Controller is over secure HTTP channels.</td>
</tr>
<tr>
<td>RabbitMQ User Name</td>
<td>Username of the RabbitMQ application. The default username is guest.</td>
</tr>
<tr>
<td>RabbitMQ Password</td>
<td>Password of the RabbitMQ application. The default password is guest.</td>
</tr>
<tr>
<td>RabbitMQ Port</td>
<td>Dedicated port for communication with the RabbitMQ application. The default port used is 5672.</td>
</tr>
</tbody>
</table>

3 To edit a virtualization connector record, select the record and click **Edit**.

You cannot change the **Type**. After you complete making the changes, click **OK** to save the changes.

It is highly recommended that you do not change the IP addresses of the virtualization connector servers (the SDN and the virtualization provider) after deployment of virtual security system instances.

4 To delete a virtualization connector record, select the record and click **Delete**.

If the virtualization connector you want to delete is used in a distributed appliance, you must first delete the distributed appliance record. To delete a distributed appliances record, see Deleting a distributed appliance in VMware on page 147.
Define manager connectors

**Before you begin**

- To add a manager connector, you must have already uploaded the manager plugins based on your virtualization environments. For more information, refer to Manager plugins.

You are able to configure manager connectors from the Intel Security Controller web application.

**Task**

1. In the Intel Security Controller web application, select **Setup | Manager Connectors**.

The Manager Connector page appears, displaying currently available manager connectors.

![Manager Connector page](image)

**Figure 3-16 Manager Connector page**

**Table 3-5 Option definitions**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Manager Connector</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Name of the manager connector record.</td>
</tr>
<tr>
<td>Type</td>
<td>Security service manager type which you select when you create the manager connector.</td>
</tr>
<tr>
<td>Host</td>
<td>IP address of the security service manager server. Clicking the hyperlink provided for the IP address opens the login screen of the security service manager.</td>
</tr>
<tr>
<td>Last Job Status</td>
<td>Status of the most recent job. Clicking the hyperlink provided for the job ID, routes you directly to the Jobs page with tasks for the specific job displayed in the Tasks pane.</td>
</tr>
<tr>
<td><strong>Policies</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Name of the policy in the security service manager. Initially all default policies from the security service manager are linked with Intel Security Controller. Different default policies are linked depending on the security service manager it is deployed in.</td>
</tr>
<tr>
<td>Domain</td>
<td>Name of the domain from which the policies are linked in the security service manager</td>
</tr>
</tbody>
</table>
2 Take the appropriate action:
   To create a new manager connector, click Add and enter the options in the Add Manager Connector dialog.

   Figure 3-17 Add manager connector

   Table 3-6 Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name, which enables you easily identify a manager connector record.</td>
</tr>
<tr>
<td>Type</td>
<td>Based on the type of security service, select the manager connector type. The selected type requires an IP address and method of authentication. The method of authentication can either be a username and password or an API key. Username depends on the requirement of the management client. An API key is a 24-character alphanumeric authentication key that is randomly generated when you configure the API Client in the Management Client.</td>
</tr>
<tr>
<td>IP</td>
<td></td>
</tr>
<tr>
<td>User Name</td>
<td>Demo</td>
</tr>
<tr>
<td>Password</td>
<td>*********</td>
</tr>
</tbody>
</table>

   Cancel Click to close the dialog without saving the changes.
   OK Click to close the dialog box with the changes saved to the Intel Security Controller database. When you click OK, all the admin domains and policy groups available in the Manager are sent to Intel Security Controller.

3 To edit a manager connector record, select the record and click Edit.
   You cannot change the Type. After you complete making the changes, click OK to save the changes. A job is started and the job number is displayed at the right-side bottom of the Manager Connector page. You can monitor the progress of this job in the Jobs page.

   It is highly recommended that you do not change the IP address of the security manager after deployment of the virtual security system instances.

4 To delete a manager connector record, select the record and click Delete.
   If the manager connector you want to delete is used in a distributed appliance, you must disassociate the manager connector from the distributed appliances before you delete the manager connector. Alternatively, you can delete the distributed appliance record. To delete a distributed appliances record, see Deleting a distributed appliance in VMware on page 147.

5 To synchronize any changes with the manager connectors, click Sync.
   When there are any policy updates made in the security appliance manager, you can trigger manual synchronization to update the changes in the manager connector. A new information pop-up appears notifying you that the job has begun along with the job number. After the synchronization is complete, the Last Job Status for that instance changes from RUNNING to PASSED or FAILED depending on the result.
Manage software images for virtual security appliances

To provide a security service, Intel Security Controller orchestrates the installation of the corresponding virtual security appliance on designated hosts. Or in the case of virtualization connectors such as OpenStack, go a step further and provides you the ability to create security groups with such tenants or virtual machines. For this, it is essential to follow this sequence of steps for the reasons explained beside the step:

1. Import relevant software images into Intel Security Controller – Software images imported to Intel Security Controller will be used to deploy security service on designated assets which can be located on any of the supported virtual environments.

2. Create a distributed appliance, in Intel Security Controller – This is where you specify the model and software version combination for that security service.

   For security service function such as IPS, you select the virtual security system model and software version, manager connector, and virtualization connector.

When you later deploy either of the security services, the SDN controller installs the corresponding model and software version of the security appliance in each designated instance.

You use the Service Function Catalog page in Intel Security Controller to import software images for security appliances. When you import a particular software image, the model and version information are automatically populated. You can import multiple software image versions for each virtual security appliance model. You can then upgrade or downgrade the software image for deployed appliances.

Define the service function catalog

Before you begin

- You have admin rights in the Intel Security Controller web application.
- The .zip file containing the virtual security appliance software image is available from your endpoint.

You use the Service Function Catalog page to manage the software for security service deployments.

You can manage the security function catalog by importing the required software images corresponding to that model.

After you add software images to the security function catalog, you are able to select a specific image for each virtualization system at the time when you create distributed appliances. For existing distributed appliances, you are able to modify the choice of software image for that security service. You are also able to also downgrade the software image in the same manner.
The **Service Function Catalog** page provides information about the existing security service deployments. You can view information or delete the security service deployments.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>Displays the name of the security service Manager</td>
</tr>
<tr>
<td>Model</td>
<td>Displays the type of Manager</td>
</tr>
<tr>
<td>Manager Type</td>
<td>Displays the Manager software version installed</td>
</tr>
<tr>
<td>Manager Software Version</td>
<td>Displays the Manager software version installed</td>
</tr>
<tr>
<td>Software Version</td>
<td>Displays the software version of the security service installed</td>
</tr>
<tr>
<td>Software</td>
<td>Displays the software version of the security service installed</td>
</tr>
<tr>
<td>Virtualization Type</td>
<td>Displays the name of the type of virtualization deployed</td>
</tr>
<tr>
<td>Image Name</td>
<td>Name of the security service image installed</td>
</tr>
</tbody>
</table>

**Task**

1. In the Intel Security Controller web application, select **Setup | Service Function Catalog**.
2. Click **Auto Import** in the **Model** section.

The **Auto Import Appliance Software Version** pop-up appears.
3 In this pop-up, click **Choose File** and select the zipped virtual security system image file.

4 Click **OK** to begin uploading this file.

You cannot edit any records for a model.

![Auto Import Appliance Software Version](image)

Figure 3-20 Auto Import File Select Pop-up

A progress bar appears providing the status of the file upload. At the end of the upload, it validates the image file before applying it.

**Change the software version of security appliances**

**Before you begin**

- Using the security function catalog, you have successfully imported the required software image in Intel Security Controller web application. Importantly, make sure that you specified the software version of the image correctly. See Define the service function catalog on page 132.

- You have the required access to deploy security services in NSX.

Before or after deploying a security service, you might want to change the software version of the corresponding security appliances. For example, after you deploy IPS or firewall service, you might want to upgrade the software image of the virtual security system instance. Alternatively, you can downgrade to an earlier version as well.
After you import the required software images in the security function catalog of Intel Security Controller, you can change the image to the required version.

- After you change the version of security appliances, you must resolve installation status of the service deployment in NSX. NSX then deletes the current security appliances from the datastore and installs the version that you selected. It is evident that security appliances are not actually upgraded or downgraded but replaced with new instances installed with a selected software version. For OpenStack, all these functions are automatically replaced during upgrade or downgrade. You have to check the Jobs/Tasks status to make sure that the process is complete without failures.

- In case of some security service functions such as IPS, the security service manager is unaware that the existing instances of the virtual security system are deleted and new ones are installed. The security service manager considers that the version of the virtual security systems has changed and trust is re-established. The name of virtual security system and the instances remain unchanged in the security service manager. The IP addresses assigned to the deployed security appliances also remain unaffected.

- After you change the software version, you must resolve the installation status of the corresponding service deployment in NSX.

- Until the new instances of the security appliances are fully up and running, the security service is suspended.

- Because security appliances are installed and not upgraded or downgraded, you can switch to a different version regardless of the current functional state of the appliances.

**Task**

1. In the Intel Security Controller web application, select Setup | Distributed Appliances.

2. Select the required distributed appliance record and click Edit.

3. In the Edit Distributed Appliance dialog box, select the required security model-version combination from the Service Function Definition drop-down list and click OK.

![Figure 3-21 Select the required version for the security appliance](image-url)

IPS for virtual networks using Intel Security Controller
Deploying next generation IPS service to a virtual network

McAfee Network Security Platform 9.1
4 Review the warning message and click **OK** to proceed with the version change.

![Upgrade Warning Message](image)

**Figure 3-22 Upgrade message**

> Warning messages disappear from the screen automatically if you move your mouse or click a key on your keyboard. However, they remain on the screen if you do not perform either of these actions.

For OpenStack, once you select **OK**, a job is triggered. This job is responsible for new image deployment and no further action is required from the user.

NSX stops the corresponding virtual security appliances to install the selected version of the security appliances. So the installation status of the virtual security appliances is now **Failed**.

![Installation Status](image)

**Figure 3-23 Installation status of service deployment**

5 Log on to vCenter and resolve the installation status for the corresponding service.

The status on this will be one of four possibilities:

- **Unknown** – No information is available.
- **Down** – Includes an error message about the health of the security service. The most relevant indicators in this context are **Discovery** and **Inspection-Ready**. When the status is Down, it implies that both indicators are **False** and that you must investigate your deployment.
- **Warning** – Implies that the security service discovery was complete, but is not inspection-ready.
- **Up** – Implies that both indicators are positive.
6 After the **Installation Status** turns to **Succeeded** and the **Service Status** displays **Up**, deploy the configuration changes to the virtual security system from the Manager.

![Figure 3-24 Installation status of service deployment](image)

When you deploy the configuration changes, the Manager pushes the signature set to the virtual security system instances.

7 When you deploy configuration changes, the **Propagating Manager File...** job is triggered in Intel Security Controller. Select **Status** | **Jobs** and make sure that **Propagating Manager File...** job is passed.

![Figure 3-25 Propagating Manager File....](image)

If the **Propagating Manager File....** job fails, deploy the configuration changes again from the Manager.

8 In the security manager, make sure the virtual security system and its member instances are connected and up-to-date.

9 Select **Status** | **Appliance Instances** and make sure the **Discovered** and **Inspection-Ready** for the corresponding appliances are **true**. If not, the security service function is suspended.

![Figure 3-26 Appliance instances status](image)
Manage distributed appliances

**Before you begin**

- The required virtualization connectors, the manager connector, and the security-appliance image file are available in Intel Security Controller.
- VMware vCenter, NSX Manager, and the Manager are all up and reachable to Intel Security Controller.

You manage distributed appliances from the Intel Security Controller web application.

**Task**

1. In the Intel Security Controller web application, select **Setup | Distributed Appliances**.

The **Distributed Appliances** page appears, displaying available distributed appliances.

![Figure 3-27 Distributed Appliances page](image-url)
To create a new distributed appliance, click **Add** and enter the options in the **Add Distributed Appliance** dialog.

![Add Distributed Appliance dialog box](image)

**Figure 3-28 Add Distributed Appliance dialog box**

**Table 3-7 Option definitions**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a relevant name for the distributed appliance record.</td>
</tr>
<tr>
<td>Manager Connector</td>
<td>Select the manager connector for the distributed appliance. For IPS, select the manager connector that refers to a Network Security Manager.</td>
</tr>
<tr>
<td></td>
<td>For firewall, select the manager connector that refers to the SMC.</td>
</tr>
<tr>
<td>Service Function Definition</td>
<td>Select a corresponding security appliance. This list of security appliances is from the security function catalog. So if you are unable to find a specific appliance definition, add it in the appliance catalog.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Click to select a particular virtualization connector.</td>
</tr>
<tr>
<td>Virtualization Connector</td>
<td>This is the list of all added virtualization connectors. You can select multiple virtualization connectors. However, there is only one manager connector per distributed appliance. That is, you can map multiple virtualization connectors with one manager connector. If you select a virtualization connector, which is already selected in a different distributed appliance, that virtualization connector is automatically disassociated from the earlier distributed appliance.</td>
</tr>
<tr>
<td>Type</td>
<td>This is the virtualization provider corresponding to a virtualization connector.</td>
</tr>
</tbody>
</table>
Table 3-7 Option definitions (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager Domain</td>
<td>This is the list of admin domains from the security manager which you specified in the corresponding manager connector.</td>
</tr>
<tr>
<td></td>
<td>• When you select the manager connector, Intel Security Controller displays the current admin domains from the corresponding security manager.</td>
</tr>
<tr>
<td></td>
<td>• When you select an admin domain, Intel Security Controller creates the Virtualization System under this admin domain in the security manager.</td>
</tr>
<tr>
<td></td>
<td>This is called as VSS in the Manager and is the logical container of the Virtual Sensors installed in each ESXi host. A VSS is similar to a failover Sensor object in the Manager.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Click to close the dialog without saving the changes.</td>
</tr>
<tr>
<td>OK</td>
<td>Click to close the dialog with the changes saved to the Intel Security Controller database.</td>
</tr>
<tr>
<td></td>
<td>When you create a manager connector, all the admin domains and policy groups available in the Manager are sent to Intel Security Controller.</td>
</tr>
<tr>
<td></td>
<td>So, when you click OK while creating the distributed appliance, Intel Security Controller gathers the current policy groups from the Manager and provides this list to the NSX Manager. This is how the Network Security Platform policy groups are available in the vCenter as profiles. You select these profiles when you create a security policy in vCenter.</td>
</tr>
<tr>
<td></td>
<td>You cannot edit if the distributed appliance record is deleted. This is indicated by the status mentioned in the Deleted column for a record.</td>
</tr>
</tbody>
</table>

• To delete a distributed appliances record, see Deleting a distributed appliance in VMware on page 147.

3 To edit a distributed appliance record, select the record and click Edit.

4 A job is started and the job number is displayed at the right-side bottom of the Distributed Appliances page. You can monitor the progress of this job in the Jobs page.

You cannot change the Name, the Manager Connector, and the Manager Domain options. After you complete making the changes, click OK to save the changes.

Tasks
• Deploy virtual systems on page 140
• Maintaining virtual appliance instances on page 144
• Deleting a distributed appliance in VMware on page 147

Deploy virtual systems

Before you begin
• You have created the distributed appliance successfully.
• VMware vCenter, NSX Manager, and the security manager are all up and can be reached by Intel Security Controller.
• If the cluster contains more than one ESXi host, you must set up an NFS datastore to deploy the virtual systems. In case of clusters with more than one ESXi host, virtual security service appliances are installed only in NFS datastores. If a cluster contains only one ESXi host, a VMFS datastore will suffice.
• You have prepared the ESXi hosts in the cluster for NSX.
You have created a distributed switch port group for the virtual security service appliance management ports. Through this switch port group, the virtual security service appliance must be able to communicate with the security manager, Intel Security Controller, NSX, and vCenter Server.

You have created the IP address pool to assign IP addresses for the virtual security service appliance management ports.

When you create a distributed appliance, a virtual system (virtual security system) record is automatically created. The virtual security system is visible in the security service manager, in Intel Security Controller, and in NSX as a security service. You can then deploy the virtual system as a security service from NSX.

When you deploy a virtual system, Intel Security Controller collaborates with vCenter, NSX, and the security manager to deploy the virtual security appliance in all hosts (hypervisors). In the case of IPS service, for example, NSX installs a virtual security system instance (a virtual IPS Sensor) in each ESXi host of the cluster. These virtual security system instances are automatically assigned network details and have established trust with the security manager.

**Task**

1. In the Intel Security Controller web application, select **Setup | Distributed Appliances**.

   The **Distributed Appliances** page displays the currently available distributed appliances.

   ![Distributed Appliances page](image)

   **Figure 3-29 Distributed Appliances page**

2. Select the required distributed appliance you created and ensure the following.

   - The **Last Job Status** shows **Passed**.
   - The virtual system is created and listed in the **Virtual Systems** section of the page.

3. In the security manager, make sure that the virtual system is automatically added.

4. Log on to vSphere Web Client as the root user.
5 In the vSphere Home tab, select Networking & Security | Installation | Service Deployments.

![Image of vSphere home page with Networking & Security highlighted](image_url)

**Figure 3-30 vSphere home page**

6 From the NSX Manager list, select the required NSX Manager.

7 Click **+** to create a service deployment.

   The **Deploy Network & Security Services** wizard opens.

8 In the **Select services & schedule** step, select the service named after the distributed appliance you created. For example, if the distributed appliance you created is *DA_N_America*, the corresponding service is *Intel IPS DA_N_America*.

![Image of Deploy Network & Security Services wizard](image_url)

**Figure 3-31 Select services & schedule**

9 If you want to deploy the virtual system now, select **Deploy now** and then click **Next**. Else, select the date and time for deployment and then click **Next**.
In the Select clusters step, select the required data center and the cluster, for which you want to provide IPS service.

Figure 3-32  Select clusters

In the Select storage step, select the required datastore.

If the corresponding cluster contains more than one ESXi host, you must select an NFS datastore.

Figure 3-33  Select storage

In the Configure management network page, the record containing the selected service and cluster is displayed. Complete the following in Configure management network step.

Figure 3-34  Configure management network

a From the Network drop-down list, select the distributed switch port group which the virtual security service appliances must use for management data. That is, the virtual security service appliance management port uses the switch port group you select here.

b From the IP assignment drop-down list, select the IP address pool which you configured and then click Next.

In the Ready to complete step, review the configuration and click Finish.

Depending on the number of ESXi hosts and your network infrastructure, it takes some minutes for the virtual security service appliances to be deployed.
14 Make sure that the Installation Status shows up as Succeeded and Service Status shows up as Up in the Installation page.

![Figure 3-35 Installation page](image)

15 In the security manager, deploy all changes to make sure the individual virtual security service appliances are updated.

16 Select the virtual system name based on the distributed appliance name and then select the appropriate option to view summary information about it.

Recall that one virtual security service appliance is automatically deployed per ESXi host in the cluster.

17 In Intel Security Controller, select Status | Appliance Instances.

The deployed virtual security system instances (security appliances) are listed. Make sure the state of Discovered and Inspection-Ready are True.

![Figure 3-36 Deployed virtual security system instances](image)

**Maintaining virtual appliance instances**

When you create a distributed appliance, you enable the required virtualization connectors in the distributed appliance. For every enabled virtualization connector, Intel Security Controller creates a virtual security system (virtual system) by default. In case of IPS, this virtual system in the distributed appliance corresponds to the virtual system in the SMC.

A virtual system is assigned a name by assigning a sequentially increasing number to the name of the distributed appliance. When you deploy this virtual system on the required cluster, NSX automatically installs a virtual security appliance in each ESXi host of the cluster. In the case of IPS and firewall services, a virtual security appliance corresponds to the virtual security system instance, that is the virtual IPS Sensor installed in each ESXi host.
After you deploy the virtual security system, you can view and maintain deployed virtual appliances from the **Appliance Instances** page of Intel Security Controller.

**Task**

1. In Intel Security Controller, select **Status | Appliance Instances.**

![Figure 3-37  Appliance instances](image)

The **Appliance Instances** page lists all the virtual appliances that are currently deployed.

2. Select an appliance instance and click **Agent Status** to view the details of the Intel Security Controller agents running on the appliance. Most of these details are also visible in the security manager.
   - **Refresh** — Refreshes the **Intel Security Controller Agent(s) Status Window.**
   - **Close** — Closes the **Intel Security Controller Agent(s) Status Window.**
   - **Name** — Name assigned to the virtual security system.
   - **IP:**
     - For VMware — The IP address assigned to the management port of the virtual appliance. This IP address is randomly assigned from the IP pool, which you specified when you deployed the security service.
     - For OpenStack:
       - **Local IP** — The IP address that is assigned to the virtual appliance within OpenStack.
       - **Public IP** — IP address assigned to a virtual appliance that is accessible from an external network.
   - **V. Server**— IP address of the virtualization provider or hypervisor server.
   - **Intel Security Controller IP** — The IP address of Intel Security Controller.
   - **Manager IP** — The IP address of the corresponding Manager, which manages the appliance. In the case of IPS service for example, it is the IP address of the Network Security Manager.
   - **Version** — The version of the Control Path Agent (CPA) on the appliance.
   - **Agent time** — The time as per CPA’s clock.
   - **Uptime** — Indicates how long the CPA is up and running.
   - **CPA PID** — Unique ID for the CPA.
   - **DPA PID** — Unique ID for the Data Path Agent (DPA) running on the appliance.
   - **DPA Info** — The version details of the DPA.
   - **DPA Stats** — Displays the number of packets received, transmitted, dropped, and so on by the appliance.
   - **Discovered** — Displays true or false which are corresponding values that suggest whether the instance of the security service is discovered or not.
   - **Inspection Ready** — Displays true or false which are corresponding values that suggest whether the instance of the security service is available for deployment and configuration or not.
3 Click Sync to manually synchronize changes by selecting the required appliance instance. The most common scenario in which you will use this is if an automatic update fails. Such an update is initiated if you change network settings of Intel Security Controller or change the password of the default agent user name. Intel Security Controller agents in the virtual security system instances (appliances) are updated automatically. If the default update fails, use the manual sync option.

When you click Sync, a Syncing Intel Security Controller Agent(s) job is triggered.

4 To upgrade Intel Security Controller agents in the virtual security system instances (appliances), select an appliance instance and click Upgrade Agent. An Upgrade Intel Security Controller Agent(s) job is triggered.

5 If the Discovered state of an appliance is false, select the appliance and click Appliance Re-authentication to re-authenticate the appliance with the corresponding manager.

In the case of IPS service or firewall service, the virtual security system instance re-establishes trust with the security service Manager when you click Appliance Re-authentication.

For firewall, perform re-authentication only when the status of the virtual security system container node is white in SMC.

In some situations, there might be a slight delay before the Discovered state turns to true. One such example is when you just deploy a security service in NSX. In such cases, wait for the state to change instead of clicking Appliance Re-authentication again.

6 Select an appliance instance and click Download Agent Log to save log files related to the appliance. Either use the log files for troubleshooting or share it with your sales partner to investigate further.

7 To filter the displayed records, enter or select a value in the required column headers and press the Enter key.

Table 3-8 Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name assigned to each virtual appliance by default. The name consists of numeric ID appended to the virtual security system name. For example, if DA_N_America_6_7 is the name, DA_N_America_6 is the name of the virtual security system and 7 is the numeric ID appended to give the virtual appliance a unique name.</td>
</tr>
<tr>
<td>IP-Address</td>
<td>IP address assigned to the management port of the virtual appliance. This IP address is randomly assigned from the IP pool, which you specified when you deployed the security service.</td>
</tr>
<tr>
<td>Discovered</td>
<td>Indicates if an appliance is discovered by the manager managing that appliance. If this is false for an appliance, click Appliance Re-authentication to trigger re-authentication with the corresponding manager. In case of IPS, the discovered state is true if the output of the status command for the appliance indicates the following: • Trust is established with the security manager. • Alert and log channels are up.</td>
</tr>
<tr>
<td>Inspection-Ready</td>
<td>Indicates that the appliance is ready for traffic. As an example, the inspection-ready state in IPS is True if the output of the status command indicates the following: • Signature file is present in the virtual security system instance. • System is initialized. • System health is good.</td>
</tr>
</tbody>
</table>
Table 3-8 Option definitions (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Status</td>
<td>Timestamp of when Intel Security Controller last checked on the virtual appliance. This time is as per the Intel Security Controller system clock.</td>
</tr>
<tr>
<td>Agent Version</td>
<td>Intel Security Controller agent on the virtual security system instance. This agent handles the management traffic between the appliance and the corresponding manager.</td>
</tr>
<tr>
<td>V.Server</td>
<td>IP address of the virtualization (ESXi) server on which the virtual appliance is installed.</td>
</tr>
<tr>
<td>V.Connector</td>
<td>Unique name of the corresponding virtualization connector that you mentioned when you configured that connector. Clicking the hyperlink provided for the virtualization connector of any of the agents, routes you directly to the list of virtualization connectors in the Virtualization Connectors page.</td>
</tr>
<tr>
<td>Manager</td>
<td>Unique name of the corresponding manager connector that you mentioned when you configured that connector. Clicking the hyperlink provided for the manager of any of the agents, routes you directly to the list of manager connectors in the Manager Connectors page.</td>
</tr>
<tr>
<td>Distributed Appliance</td>
<td>Unique name of the corresponding distributed appliance that you mentioned when you configured that appliance. Clicking the hyperlink provided for the distributed appliance of any of the agents, routes you directly to the list of distributed appliances in the Distributed Appliances page.</td>
</tr>
<tr>
<td>Model</td>
<td>Model number of the security appliance as mentioned in the Service Function Catalog page.</td>
</tr>
<tr>
<td>Version</td>
<td>Software version of the security appliance as mentioned in the Service Function Catalog page.</td>
</tr>
</tbody>
</table>

Deleting a distributed appliance in VMware

Before you begin
1. You have access rights to uninstall service deployments in NSX.
2. The details you provided in the virtualization connectors and manager connector used in the corresponding distributed appliance are valid.

Since distributed appliance information is not stored in OpenStack, you can directly delete a distributed appliance in the Intel Security Controller web application.

When you successfully delete a distributed appliance, the corresponding virtual security system instances (ESX agents) are deleted. Therefore, it results in the termination of the security service provided by these virtual security system instances.

To delete a distributed appliance, you must first sequentially delete the related objects in NSX as explained in this section.
Task

1. In the vSphere Home tab, select Networking & Security | Installation | Service Deployments.

2. Select the corresponding service deployment and click ✗.

![Service Deployment Table]

3. Select Delete now or schedule the deletion and click OK.

   Depending on your configuration, it might take several minutes to uninstall the service deployment. This process deletes the virtual security system instances (ESX agents), implying the security service is terminated.

4. Select Service Composer | Security Policies and then select the NSX Manager.

5. Select the security policy used in the deleted IPS or NGFW service deployment and click 📷.

   The security groups to which you assigned the security policy are displayed in pop-up window.

6. Deselect all the security groups to which you assigned the security policy and click OK.


8. Select the corresponding service definition and click the edit icon.

   You can identify the service definition by the name of the distributed appliance you want to delete.
Select Service Instances.

![Service instances](image1)

**Figure 3-38 Service instances**

Select the instance, which is displayed.

![Select the instance](image2)

**Figure 3-39 Select the instance**

The corresponding service profiles are listed on the right side.

**Service Profiles**

![Service profiles](image3)

**Figure 3-40 Service profiles**

Select and delete all the service profiles one by one.

Select the service instance and delete the service instance.

The corresponding security policy in NSX is automatically deleted.

In the Networking & Security pane, select Service Definitions.
14 Delete the corresponding service definition.

   Locate the service definition based on the name of the distributed appliance you want to delete. This
   completes the deletion of the related objects in NSX.

15 In Intel Security Controller web application, select Setup | Distributed Appliances.

16 Select the distributed appliance and click Delete.
   • Deleting the distributed appliance, deletes the service definition in NSX.
   • After the distributed appliance deletes successfully, you can delete the corresponding manager
     connector and virtualization connector, if required.

Jobs and tasks

Certain actions you perform in Intel Security Controller are tracked as jobs. When you start a job, it triggers one
or more background activities in Intel Security Controller. These background activities are tracked as tasks of
that job. Therefore, a job is completed only when all its tasks are successfully completed.

Jobs and tasks enable easy tracking and troubleshooting. For example, if a job failed, you just have to look at
the failed task to locate the stage at which the job failed. If a job is running for a long time, you can troubleshoot
by looking at the task at which the processing is stuck.

Intel Security Controller triggers a job, when you take any of the following actions:
   • Create, edit, synchronize, or delete a manager connector.
   • Create, edit, synchronize, or delete a distributed appliance.
   • Synchronize appliance instances.
   • Appliance instance re-authentication.
   • Upgrade the software for an appliance instance.
   • Modify the password of the default users.

Viewing jobs and tasks

You can view the jobs and the corresponding tasks in the Jobs page.

Task

1 In the Intel Security Controller web application, select Status | Jobs.
The jobs are listed in the top pane of the page. When you click on a job, the corresponding tasks are listed in the bottom pane.

All time stamps displayed in the Jobs page are according to Intel Security Controller system time. You can use the `show clock` command or the Manage | Server | Summary page to check the current date and time on Intel Security Controller. To change the system time, use the `set time` and `set timezone` commands.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Graph</td>
<td>Click to see a graphical representation of the order of tasks for the selected job.</td>
</tr>
<tr>
<td>Abort</td>
<td>Click if you do not need a job to be processed any further or remove it from the processing queue.</td>
</tr>
<tr>
<td></td>
<td>Even when you abort a job, the entries for all tasks of that job are created; task IDs are assigned for all tasks; job ID is assigned for the job.</td>
</tr>
<tr>
<td>ID</td>
<td>This is a system-assigned unique ID to each job. This ID is assigned in a sequential order.</td>
</tr>
<tr>
<td>Name</td>
<td>This is a system-defined name to a job. The name of the connector is appended at the end of the name. For example, if you delete a distributed appliance named example_DA, the name assigned for this job is Delete Distributed Appliance 'example_DA'.</td>
</tr>
<tr>
<td>Objects</td>
<td>Unique name of the distributed appliance executing that job. Clicking the hyperlink provided routes you directly to the list of distributed appliances in the Distributed Appliances page.</td>
</tr>
</tbody>
</table>
Table 3-9  Option definitions in the Jobs pane (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State</strong></td>
<td>Indicates the current state of the job. The following are the possible values:</td>
</tr>
<tr>
<td>• <strong>NOT_RUNNING</strong> — indicates that Intel Security Controller started the job but is unable to complete the process.</td>
<td></td>
</tr>
<tr>
<td>• <strong>QUEUED</strong> — indicates that the job is in the queue to be processed. For example, there might be too many concurrent jobs being processed and the jobs in the queue are processed as soon as system resources are available.</td>
<td></td>
</tr>
<tr>
<td>• <strong>RUNNING</strong> — indicates that the job is now being processed.</td>
<td></td>
</tr>
<tr>
<td>• <strong>COMPLETED</strong> — indicates that Intel Security Controller completed processing the job. However, check the status of the job to see if the job was completed successfully.</td>
<td></td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>Indicates the result for a job. The following are the possible values:</td>
</tr>
<tr>
<td>• <strong>FAILED</strong> — indicates that one or more the tasks of that job failed. So, Intel Security Controller is unable to complete the job successfully.</td>
<td></td>
</tr>
<tr>
<td>• <strong>PASSED</strong> — indicates that all tasks of the job are completed successfully. Hence, the jobs are also completed successfully.</td>
<td></td>
</tr>
<tr>
<td>• <strong>ABORTED</strong> — A user clicked Abort to stop processing the job further.</td>
<td></td>
</tr>
<tr>
<td><strong>Started</strong></td>
<td>The time stamp of when the job is started. This is empty for jobs which processing never started. For example, if you aborted jobs, which are queued for processing, this time stamp is empty.</td>
</tr>
<tr>
<td><strong>Completed</strong></td>
<td>The time stamp of when the job is completed regardless of the job Status. The Completed time stamp is available only for those jobs, which are in completed State. Regarding Status, the completed time stamp is displayed for all failed, passed, and aborted jobs. In case of failed and passed jobs, this time stamp indicates when the last task was completed. In case of aborted jobs, this time stamp indicates when a user aborted the job.</td>
</tr>
<tr>
<td><strong>Failure Reason</strong></td>
<td>Displays the reason for the failure of the job</td>
</tr>
<tr>
<td><strong>Queued</strong></td>
<td>The time stamp of when a user started the action. If Intel Security Controller processes the job as soon as it is triggered, this time stamp is the same as that of the Started time stamp.</td>
</tr>
<tr>
<td><strong>Submitted By</strong></td>
<td>Name of the user who initiated the job.</td>
</tr>
</tbody>
</table>

When you click Job Graph, a graphical representation of the order and dependency of tasks displays. The tasks are color-coded to indicate their status.

• Green indicates the task succeeded.
• Yellow indicates the task is in progress. Not shown if the task is in different state.
• Red indicates the task failed.
• Gray indicates that the task is skipped.
• White indicates that the task is aborted or not yet scheduled.
• Orange indicates that the task is scheduled for execution.
• Light Blue indicates that there are predecessor tasks and only some of them are currently completed.
• Magenta arrow head indicates all tasks (not just its predecessors) before this task must be successfully completed.
• Black arrow head normal indicates allow task to start execution when any of its predecessors succeed.

• Black arrow head empty indicates all predecessor tasks must be in a completed state.

![Job graph](image)

Figure 3-42 Job graph

2 Click a job to view its tasks.

**Table 3-10 Option definitions in the Tasks pane**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order</td>
<td>Indicates the sequence in which the tasks are executed.</td>
</tr>
<tr>
<td>Name</td>
<td>This is a system-defined name to a task. The name of the relevant connector is appended at the end for some of the tasks.</td>
</tr>
<tr>
<td>Objects</td>
<td>Unique name of the distributed appliance executing that task. Clicking the hyperlink provided routes you directly to the list of distributed appliances in the Distributed Appliances page.</td>
</tr>
<tr>
<td>State</td>
<td>Indicates the current state of the job. The following are the possible values:</td>
</tr>
<tr>
<td></td>
<td>• NOT_RUNNING — indicates that Intel Security Controller started the task but is now aborted.</td>
</tr>
<tr>
<td></td>
<td>• QUEUED — indicates that the task is in the queue to be processed. For example, there might be too many concurrent tasks being processed and the tasks in the queue are processed as soon as system resources are available.</td>
</tr>
<tr>
<td></td>
<td>• PENDING — indicates that there are predecessor tasks and only some of them are currently completed.</td>
</tr>
<tr>
<td></td>
<td>• RUNNING — indicates that the task is now being processed.</td>
</tr>
<tr>
<td></td>
<td>• COMPLETED — indicates that Intel Security Controller completed processing the task. However, check the status of the task to see if it was completed successfully.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates the result for a task. The following are the possible values:</td>
</tr>
<tr>
<td></td>
<td>• FAILED — indicates that the task failed. So, Intel Security Controller is unable to complete the job successfully.</td>
</tr>
<tr>
<td></td>
<td>• SKIPPED — indicates that Intel Security Controller skipped this task and proceeded to the next task. When a prerequisite task fails, the current task is skipped.</td>
</tr>
<tr>
<td></td>
<td>• PASSED — indicates that the task is completed successfully.</td>
</tr>
<tr>
<td></td>
<td>• ABORTED — indicates that the task was started but a user clicked Abort to stop processing the job further.</td>
</tr>
<tr>
<td>Started</td>
<td>The time stamp of when the task is started. This is empty for tasks which never started.</td>
</tr>
<tr>
<td>Completed</td>
<td>The time stamp of when the task is completed regardless of the job Status. The Completed time stamp is available only for those tasks, which are in completed State.</td>
</tr>
</tbody>
</table>

Regarding Status, the completed time stamp is displayed for all failed, passed, skipped, and aborted tasks. In case of failed and passed tasks, this time stamp indicates when the task was completed. In case of aborted jobs, this time stamp indicates when a user aborted the job. In case of skipped tasks, this time stamp indicates when a task was skipped.
Table 3-10 Option definitions in the Tasks pane (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error</td>
<td>Displays the reason for failed tasks.</td>
</tr>
<tr>
<td>Predecessors</td>
<td>Indicates the Order number of one or more tasks, which must be completed to complete this task. Click Job Graph to see the graphical representation of the order in which tasks are executed.</td>
</tr>
<tr>
<td>ID</td>
<td>This is a system-assigned unique ID to each task. This ID is assigned in a sequential order and is unique across jobs.</td>
</tr>
</tbody>
</table>

3 Use the following options to change the display in the jobs and tasks pane.

- The page automatically shows the updated content. If necessary, you can click in the jobs or the tasks pane.
- To change the order of the columns in the jobs or tasks pane, click on a column header and drag it to where you want in the pane.
- Click on a column header to sort the records in the ascending or descending order. For example, click on the Order column in the tasks pane to display the records in descending order, that is, the last task is displayed first and the first task is displayed last.
- To filter the records, enter or select the values in the required columns and press the Enter key. All records containing the specified values are listed. For example, enter distributed appliance Name column and select Failed in the Status column to view the failed jobs with the Failure Reason related to distributed appliances. Follow a similar procedure to filter records in the tasks pane.

![Figure 3-43 Filter records in the Jobs page](image)
- To remove the filters, delete the search strings and selections from the columns and press Enter on your keyboard.

Create a security group in VMware NSX

In an NSX Manager, you create a security group and then include the required VMs in that group. Then you can apply an NSX security policy to this security group, the corresponding security service is provided to those VMs included in the security group.

If VMware tools is not running on the VMs, you must include those VMs in the security group and also create an IP set containing the IP addresses of those VMs and include that IP set in the security group. The steps for creating an IP set object is under “Group objects based on IP sets.”
Task
1. Log on to vSphere Web Client as the root user.
2. In the vSphere Home tab, select Networking & Security.

![vSphere home page](image)

Figure 3-44 vSphere home page


![Service composer](image)

Figure 3-45 Service composer

4. From the NSX Manager list, select the NSX Manager in which you want to define the security group.

5. Click ![button] to create a security group.
6 In the New Security Group wizard, enter a meaningful name and, if required, a description, then click Next.

![New Security Group wizard](image1)

**Figure 3-46 New security group**

7 Select Select objects to include.

![Select objects to include](image2)

**Figure 3-47 Select objects to include**

8 From the Object Type drop-down list, select the object based on which you want to include VMs.
For example, if you select distributed port group in this list, the distributed port groups currently defined in the data center are listed. When you select a distributed port group, all the VMs connected to this port group are included in the security group.

- You can also base the inclusion on multiple object types. For example, you can select a few distributed switch port groups and some VMs.

- For VMs on which VMware tools is not running, you must include them in the security group. Also, you must create an IP set object and include that IP set in the security group. To include the IP set, select **IP Sets** from the **Object Type** list.

Consider that you selected **Virtual Machine** from the **Object Type** drop-down list.

9. Select the required objects (in our example, VMs) and click to move them under **Selected Objects**. Then click **Next**.

10. If you want to exclude any VMs, click **Select objects to exclude** in the **New Security Group** wizard. This is similar to how you included VMs based on objects. For example, you want to include all the VMs connected to a distributed switch port group except for 5 server VMs. Then, you can include the distributed switch port group in step 3 of **New Security Group** wizard and exclude only those 5 VMs in step 4.

11. Click **Ready to complete**, review the objects included and those excluded. Then click **Finish** to create the security group.

The security group you created is listed in the **Security Groups** tab for the corresponding NSX Manager.
Create a security policy in VMware NSX

In an NSX Manager, you create a security policy, which you can apply to a security group in NSX. This security policy contains the security profile to be applied on the VMs included in that security group.

For example, in the case of IPS service, you select the IPS policy group as a security profile in a security policy of NSX. Then, when you apply this security policy to a security group, a Virtual Sensor uses this IPS policy group to inspect traffic related to the protected VMs.

**Task**

1. Log on to vSphere Web Client as the root user.
2. In the vSphere *Home* tab, select *Networking & Security*.
4. From the *NSX Manager* list, select the NSX Manager in which you want to define the security policy.
5. Click 🖍️ to create a security policy.
6  In the **New Security Policy** wizard, enter a meaningful name and, if required, a description and click **Next**.

![New Security Policy](image)

**Figure 3-52 New security policy**

7  Select **Network Introspection Services** and click ![add icon] to add a network introspection service.

All products that currently integrate with Intel Security Controller are network introspection services.

For the security services to work as expected, you must add two network introspection services. One introspection service is for inbound traffic to the security group. The second one is for the outbound traffic from the security group.
8 In the Add Network Introspection Service dialog, enter the required options and click OK.

**Figure 3-53 Add network introspection service**

![Add Network Introspection Service dialog](image)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a relevant name for the inbound or outbound security service. Consider you are adding the outbound first.</td>
</tr>
<tr>
<td>Service Name</td>
<td>This is the list of relevant distributed appliances defined in Intel Security Controller. In a distributed appliance, specify the virtualization connector which, in turn, contains the NSX Manager IP address. The Service Name list contains the distributed appliances in which the current NSX Manager is referenced.</td>
</tr>
<tr>
<td>Profile</td>
<td>This is the list of security policies defined in the security service manager. In a distributed appliance, specify the security manager. Based on the Service Name (distributed appliance) you selected, the security policies are displayed here.</td>
</tr>
<tr>
<td>Source</td>
<td>Click Change... and select Policy’s Security Groups because this security service is for outbound traffic from the security group. Click OK.</td>
</tr>
<tr>
<td>Destination</td>
<td>Click Change... and select Any because this security service is meant for outbound traffic from the security group. Click OK.</td>
</tr>
<tr>
<td>OK</td>
<td>Click OK to create the outbound security service.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Click to close the dialog box without saving the changes.</td>
</tr>
</tbody>
</table>
Follow a similar procedure to create the inbound security service.

- You can opt for the same Profile or choose another.
- You must select Any for Source and Policy’s Security Groups for Destination.

Figure 3-54 Policy’s security groups

Select Ready to complete, review the configuration, and click Finish to create the security policy.

Figure 3-55 Ready to complete

The security policy you created is listed in the Security Policies tab for the corresponding NSX Manager.

Apply a security policy to a security group in VMware NSX

Before you begin
Make sure you have created the required security groups and the security policies in the NSX Manager.
In an NSX Manager, you create a security policy, which you can apply to a security group. This creates the association between security groups and security policies.

**Task**

1. Log on to vSphere Web Client as the root user.

2. In the vSphere **Home** tab, select **Networking & Security**.

   ![vSphere Web Client](image)

   **Figure 3-56** vSphere home tab

3. Select **Service Composer** | **Security Policies**.

   ![Service Composer](image)

   **Figure 3-57** Service composer

4. From the **NSX Manager** list, select the corresponding NSX Manager.
5  Select the security policy you want to apply and click 🎨.

![Image of Service Composer window with Security Policies tab selected.](image)

**Figure 3-58  NSX manager**

6  Select the security groups on which you want to apply the security policy and click **OK**.

![Image of Select the security groups dialog box.](image)

**Figure 3-59  Select the security groups**
You can view the details in the Security Policies tab.

![Security policies](image1.png)

**Figure 3-60  Security policies**

**Configure virtual security system to fail-close or fail-open**

When you successfully install the security service, the Virtual Security System instances are deployed in fail-open mode by default. You can configure the Virtual Security System instances to run in fail-close or fail-open mode. Similar to any other configuration, the fail-close or fail-open setting of a Virtual Security System applies to all its instances.

The fail-open or fail-close configuration is implemented through an NSX mechanism. The solution uses an attribute in the service definitions of NSX to implement fail-open or fail-close configuration.

**Task**

1. In the vSphere Home tab, select Networking & Security | Service Definitions.
2. Select the corresponding service definition and click the edit icon.
   
   You can identify the service definition by the name of the distributed appliance.
3. Select Service Instances.
   
   ![Service instances](image2.png)

   **Figure 3-61  Service instances**
4 Select the instance, which is displayed.

**Figure 3-62  Select the instance**

The corresponding service profiles are listed on the right side.

**Service Profiles**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Image" /> Intel IPS da_na_56_Default ...</td>
<td>AutoCreated Default Set</td>
</tr>
<tr>
<td><img src="image2.png" alt="Image" /> Intel IPS da_na_56_Default ...</td>
<td>AutoCreated Default Set</td>
</tr>
<tr>
<td><img src="image3.png" alt="Image" /> Intel IPS da_na_56_Default ...</td>
<td>AutoCreated Default Set</td>
</tr>
</tbody>
</table>

**Figure 3-63  Service profiles**
5 Double-click on the service profile, which you have used in the network introspection service of the applied security policy.

Consider that you selected the Default Client and Server Protection (IDS IPS) profile in the inbound and outbound network introspection service (as shown below).

![Figure 3-64  Edit network introspection service](image)

Double-click on Default Client and Server Protection service profile.

![Figure 3-65  Select the service profile](image)

6 Select the **Failure Policy** attribute and click **Edit**.

![Figure 3-66  Failure policy attribute](image)
By default, the **Failure Policy** attribute's fail-open key is set to true. This means the Virtual Security System instance fail-opens in case of a failure. Set the value to false, if you want the Virtual Security System instance to fail-close.

![Edit attributes](image1.png)

**Figure 3-67 Edit attributes**

In the **Edit attributes** dialog box, select **Publish changes to underlying service profile** and click **OK**.

Select the attribute and click **Publish**.

![Select publish](image2.png)

**Figure 3-68 Select publish**

Repeat the process if you used different profiles for inbound and outbound network introspection services.
Manager functions regarding IPS service deployment

In the context of IPS service through Intel Security Controller, you use the Manager to perform the following tasks:

• Define the Manager admin domains, which should manage the Virtual Security System and the member instances. You can select the required domain for each Virtualization System in a distributed appliance. Then, the virtual security system is created under the domain you selected in the distributed appliance.

• Create a policy group containing the security policies for next-generation IPS. For example, the policy group can contain an IPS policy, Advanced Malware policy, and Firewall policy. When you deploy the IPS service, Intel Security Controller collaborates with vCenter and NSX to ensure the Virtual Security System instances use the selected policy group for traffic inspection.
  • For a Virtual Security System, the policy assignment is only through a policy group. That is, you cannot assign IPS policy, Firewall policy, and so on separately. To access the Policy Groups page, select Policy | <Admin Domain Name> | Intrusion Prevention | Objects | Policy Groups.
  • For the Virtual Security System, you assign the policy groups that you create in the Manager through the security policies of NSX. That is, you cannot assign the policy group to a Virtual Security System instance or its interface through the Manager.

• When you create a new policy group, Intel Security Controller makes sure that the security policies in NSX are updated accordingly. The Syncing Appliance Manager Connector <manager connector name> job is triggered in Intel Security Controller.

• **Important note on renaming or deleting policy groups in the Manager:** Recall that the policy groups in the Manager are automatically available as service profiles and profile configurations in NSX. So, when you delete even an unused policy group in the Manager or rename a policy group, you must manually delete the service profile and profile configuration in NSX. Else the subsequent manager-connector sync and distributed-appliance sync jobs fail.
  1 In the Networking & Security pane, select Service Definitions.
  2 Select the corresponding service definition and click the edit icon.
  3 Select Service Instances.
4 Select the instance, which is displayed.

5 Delete the service profile corresponding to the policy group you renamed or deleted in the Manager.

6 In the Networking & Security pane, select Service Definitions.

7 Select the corresponding service definition and click the edit icon.

8 Delete the profile configuration corresponding to the policy group you renamed or deleted in the Manager.

- View details of the deployed Virtual Security System instances. For example, you can view the VMware ESXi servers on which the Virtual Security System instances are installed, the IP addresses of the Virtual Security System instances, and so on. See View summary details of a selected vNSP Cluster on page 169.

- Use the Manager to deploy configuration changes, signature sets, and so on for the Virtual Security System instances.

- For information on how to change the policy group assigned to virtual security system instances, see Assign policy groups to virtual security systems on page 171.

- If you want to modify an attack definition, deploy configuration changes from the Manager after you modify the attack definition. For example, if you use the Default Prevention policy in the policy group. If you modify any attack definition in Default Prevention, deploy the configuration changes to the virtual security system.

- View the alert and other details sent by the Virtual Security System instances.

**View summary details of a selected vNSP Cluster**

You might want to view the details of vNSP Cluster instances in the Manager.
Task

1. In the Manager, select Devices | <Admin Domain Name> | Devices | <vNSP Cluster> | Summary.

   The device Summary page displays.

   ![Figure 3-69 Summary details of a virtual security system](image)

   **Table 3-12 Option definitions**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Displays whether there are pending changes to be deployed to the virtual security system or if it is up to date. Green indicates that the system is up to date and blue indicates that there are pending changes to be deployed.</td>
</tr>
<tr>
<td>Device Type</td>
<td>The type of device. For example, vNSP Cluster.</td>
</tr>
<tr>
<td>vNSP Controller</td>
<td>Displays the name of the vNSP Controller.</td>
</tr>
<tr>
<td>Controller Software</td>
<td>Displays the vNSP Controller image version that is currently installed.</td>
</tr>
<tr>
<td>Virtual Probe Software</td>
<td>Displays the Virtual Probe image version that is currently installed.</td>
</tr>
<tr>
<td>Member Sensor Software</td>
<td>Displays the Sensor software version that is currently installed.</td>
</tr>
<tr>
<td>Member Sensors Name</td>
<td>Display the status and name of the Sensor instance.</td>
</tr>
<tr>
<td>Protections</td>
<td>Displays the Software, Signature set, and Callback Detector versions of the Sensor.</td>
</tr>
<tr>
<td>Last Deployment</td>
<td>The time stamp of when pending changes were deployed last.</td>
</tr>
<tr>
<td>Software</td>
<td>Displays the version of the Sensor and status and version of the Virtual Probe.</td>
</tr>
<tr>
<td>Monitoring Port IP</td>
<td>The Monitoring Port IP address configured for the Sensor.</td>
</tr>
<tr>
<td>Management Port</td>
<td>The network settings of Virtual IPS Sensor.</td>
</tr>
<tr>
<td>Last Reboot</td>
<td>The time stamp of when a Virtual IPS Sensor instance was last restarted.</td>
</tr>
</tbody>
</table>

2. To update the vNSP Cluster details, click Edit Cluster.

   You can edit the Description and the Sensor the vNSP Cluster is associated with.

3. To view details of a managed endpoint:
   a. Select Endpoint Actions | View Managed Endpoints.

4. To download Virtual Probe, select Virtual Probe Actions | Download Probe Installer for: <vNSP Cluster Name> | <OS> Virtual Probe.
5 To restart the Sensor, click Member Sensor Actions | Reboot.

6 To run a diagnostic trace for the Sensor, click Member Sensor Actions | Run diagnostics.

7 To export the Sensor software information in the form of a .csv file, click Save as CSV.

**Assign policy groups to virtual security systems**

**Before you begin**

You have created the required policy group in the Manager.

You might want to apply a different policy group to the deployed instances of a virtual security system.

**Task**

1 Log on to vSphere Web Client as the root user.

2 In the vSphere Home tab, select Networking & Security.

3 Select Service Composer | Security Policies.

4 From the NSX Manager list, select the corresponding NSX Manager.

5 Select the required security policy and click 

6 Select Network Introspection Services.

7 Select the required network introspection service and click the edit icon.
8 From the **Profile** drop-down list, select the required policy group and then click **OK**.

![Edit Network Introspection Service](image)

- **Name:** SP_EngrAut_Out_01
- **Description:** Outbound security policy for Engineering Automation; version 01.
- **Action:** Redirect to service
  - Do not redirect
- **Service Name:** Intel IPS da_na_04
- **Profile:**
  - Intel IPS da_na_04_PG_EgrAut_01 (IDS IPS)
  - Intel IPS da_na_04_Copy of PG_EgrAut_02 (IDS IPS)
  - Intel IPS da_na_04_Default Client and Server Protection (IDS IPS)
- **Source:** Intel IPS da_na_04_PG_EgrAut_01 (IDS IPS)
- **Destination:** Intel IPS da_na_04_PG_EgrAut_03 (IDS IPS)

> Either source or destination selection (or both) must be "Policy's Security Groups".

![Figure 3-70 Select the policy group in NSX](image)

9 **Click Finish.**

In Intel Security Controller, the **Syncing Service Profile** job is triggered for every network introspection service that you change. Make sure this job passes successfully.

![Jobs](image)

<table>
<thead>
<tr>
<th>ID</th>
<th>NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>136</td>
<td>Syncing Service Profile 'Intel IPS da_na_04_PG_EgrAut_03' Policy</td>
</tr>
<tr>
<td>135</td>
<td>Syncing Service Profile 'Intel IPS da_na_04_PG_EgrAut_01' Policy</td>
</tr>
</tbody>
</table>

![Figure 3-71 Job for synchronizing change in policy group](image)

You do not require to deploy configuration changes from the Manager.

**Quarantine endpoints using NSX features**

**Before you begin**

You have the required access to create security groups and security policies in NSX.
In case of alerts detected by Virtual Security System instances, you can use the native Quarantine feature to quarantine the source endpoint of an attack. You can also use the security tags and security policies in NSX to quarantine the source or the target endpoint of an attack.

To quarantine endpoints using NSX features, you tag the source or destination VM in alert from the Attack Log. In NSX, create a security group, which dynamically includes VMs tagged in the Attack Log. To this group, you assign a security policy, which effectively quarantines the tagged VM.

**Notes:**
- The Quarantine feature of IPS and the security tags of NSX are exclusive to each other.
- In case of security tags, currently you can only quarantine endpoints from the Attack Log. You cannot enable quarantine through security tags in the attack definitions.
- Currently, there is no indication in the Attack Log that an endpoint is tagged.
- Currently, to release an endpoint from quarantine, you must manually remove the tag in NSX.

This section uses an example to explain how to quarantine endpoints using security tags and security policies in NSX.

**Task**

1. In NSX, create a security group to dynamically include tagged VMs.
   - In vCenter web client, select **Home | Networking & Security | Service Composer | Security Groups**.
   - In the **Service Composer** page, select the NSX Manager from the drop-down list.
   - Click ![Create Security Group](image) to create a security group.
   - Enter a relevant name and description.
   - In the **Define dynamic membership** step, select **any** for **Match**.
   - In **Criteria Details**, select **Security Tag** and **Equals to** in the first two drop-down.
   - In the text box, exactly enter **Intel Security Controller-Quarantine**. The Manager assigns **Intel Security Controller-Quarantine** as the tag. So, you must also exactly enter this string for a tagged VM to be included in this security group.

   ![Membership criteria 1](image)

   **Figure 3-72 Adding criteria to include tagged VMs**

   - Click **Finish**.

2. In NSX, create a security policy to quarantine VMs tagged as **Intel Security Controller-Quarantine**.
   - In the **Securities Policies** tab of **Service Composer** page, click ![Create Security Policy](image) to create a security policy.
   - Enter a relevant name and description and proceed to step 3, **Firewall Rules**.
c  Add a firewall rule to allow traffic to the VM hosting the remediation portal.
   For Source, select Policy’s Security Groups. For Destination select the security group, which contains the VM hosting the remediation portal.

   ![New Firewall Rule](image1)

   **Figure 3-73  Rule to allow traffic to remediation portal**

   d  Add the last rule, which blocks all traffic.

   ![New Security Policy](image2)

   **Figure 3-74  Rule to block all traffic**

   e  Click Finish.
3 Apply the security policy from the previous step to the security group created in step 1.
   a In the **Securities Policies** tab of **Service Composer** page, select the relevant security policy and click OK.
4 Select the relevant security group and click **OK**.
5 Tag a VM from the Attack Log.
   a Select an alert and click **Other Actions**.
   b Go to **Tag Endpoint | via Intel Security Controller**.
   c Select either the source IP address or the destination IP address.
      The **Tag Virtual Endpoint via Intel Security Controller** pop-up opens.
      The endpoint and VSS server is detected by default.
   d Select the tag from the **Tag to Assign** drop-down list.
   e Click **Tag**.
      A successfully tagged message is displayed.
      
      Only the default tags are available for tagging the endpoint.
6 Confirm tagging in NSX.
   a In vCenter web client, select **Home | Networking & Security | Networking & Security Inventory | NSX Managers**.
   b Select the relevant NSX Manager and then select **Manage | Security Tags**.
   c Click on the **VM Count** for **Intel Security Controller-Quarantine**.

![Figure 3-75 VM Count for ISC-Quarantine](image)

*Figure 3-75 VM Count for ISC-Quarantine*
You can also check the current virtual machines included in the corresponding security group.
7 If required, release a VM from quarantine.
   To release a VM from quarantine, you must remove the **Intel Security Controller-Quarantine** tag for the VM.
   a In vCenter web client, select **Home | Networking & Security | Networking & Security Inventory | NSX Managers**.
   b Select the relevant NSX Manager and then select **Manage | Security Tags**.
Select Intel Security Controller-Quarantine and click.

Deselect the check box for the VMs you want to release from quarantine.

Figure 3-76  Release VMs from quarantine
Troubleshooting tips and FAQs regarding IPS service

How to make sure the IPS service is deployed successfully?

1. The installation status is succeeded and service status is up in the Installation page of NSX.

2. In NSX, you have created the security policy with network introspection services for inbound and outbound.

3. In NSX, you have applied the security policy to the security group.

4. The status is true for DISCOVERED and INSPECTION-READY in the Appliances Instances page of Intel Security Controller web application.

5. In the Manager, select Devices | <Admin Domain Name> | Devices | <Virtual Security System name> and make sure the Virtual Security System is up-to-date and all the member instances are connected.

I have made sure IPS service is deployed successfully. However, the Sensor is not detecting attack traffic?

• Make sure your deployment meets all the requirements mentioned in Requirements for deploying IPS service on page 118.

• Make sure you have included the protected virtual machines correctly in the security group. See Create a security group in VMware NSX on page 154.

• Make sure you have configured the security policy as described in Create a security policy in VMware NSX on page 158. Especially, make sure you have selected the correct policy group in the Profile list when you add the network introspection service.

• In the Manager, make sure the attack you are testing is enabled in the corresponding policy group.

How do I change a current policy applied on the Virtual Security System instances?

• Consider that you want to apply the same policy group but apply a different IPS policy. Then, select the required IPS policy in the policy group in the Manager.

• To change the applied policy group, do the following:
  1. In NSX, select Service Composer | Security Policies.
  2. Edit the required security policy and select Network Introspection Services.
  3. Edit the inbound or outbound network introspection service to select the required policy group from the Profile drop-down list.

If indicated in the Manager, deploy the configuration changes to the Virtual Security System instances.

I only want to inspect traffic in either inbound or outbound.

You must define network introspection services in NSX for both inbound and outbound. To not inspect outbound traffic for example, apply a policy group with the Default DoS and Reconnaissance Only policy selected for IPS and none for the other policies.

Unable to delete a distributed appliance record in Intel Security Controller

You must delete the related objects in NSX before you can delete a distributed appliance record. See Deleting a distributed appliance in VMware on page 147.

Manager connector sync and distributed appliance sync jobs fail or What happens if I rename or delete a policy group in the Manager?

See Important note on renaming or deleting policy groups in the Manager in Manager functions regarding IPS service deployment on page 168.
IPS for virtual networks using Intel Security Controller
Deploying next generation IPS service to a virtual network
Network Security Platform for Amazon Web Services

Chapter 4  Securing your Amazon Web Services (AWS) datacenter
Chapter 5  Upgrade AWS components
Chapter 6  Use case scenarios
Chapter 7  Failure of components
Chapter 8  Troubleshooting scenarios
Chapter 9  CLI commands for AWS
Securing your Amazon Web Services (AWS) datacenter

Cloud Computing provides a simple way to access servers, storage, databases and a broad set of application services over the Internet. Cloud Computing providers such as Amazon Web Services (AWS) own and maintain the network-connected hardware required for these application services, while you provision and use what you need via a web application. Network Security Platform can currently be deployed in the AWS environment.

The vNSP solutions consists of the Network Security Manager and the Virtual IPS Sensor. Functionality of each of these components are as follows:

- **Network Security Manager** — It is the same web based user interface that is used to manage the Virtual IPS Sensor and Virtual Security System. You can create and manage policies against attacks detected by the Sensors.
- **Virtual IPS Sensor** — This is the Network Security Sensor that protects the network against harmful attacks. It inspects the traffic and generates alerts in the Network Security Manager in case of attacks.

**Contents**
- Network Security Platform for the public cloud
- How Network Security Platform functions to protect public cloud infrastructure
- High Availability of vNSP solution
- Considerations
- Virtual IPS Sensor Model to secure the public cloud
- Generate the License Compliance report
- Telemetry
- Workflow for deploying Network Security Platform in AWS
- Auto scaling of Sensors to improve traffic throughput
- Features not supported
- Best Practices
- Usage guidelines

**Network Security Platform for the public cloud**

Network Security Platform for the public cloud is a scalable, enterprise-class solution that provides real-time threat protection to your public cloud infrastructure. Elastic Compute Cloud by AWS enables you to deploy your virtual machines and host applications on the public cloud.

Network Security Platform for AWS is a solution that protects instances in AWS environment from threats arising from outside the network or within.
AWS Terminologies

For detailed descriptions of AWS components and terminology, refer the AWS Documentation. This section is intended to be a glossary of some frequently used AWS-specific terms within this document and not to substitute for AWS Documentation.

**Availability Zone** — A distinct location within a region that is insulated from failures in other Availability Zones, and provides inexpensive, low-latency network connectivity to other Availability Zones in the same region.

**Region** — A named set of AWS resources in the same geographical area. A region comprises at least two Availability Zones.

**Amazon Virtual Private Cloud (Amazon VPC)** — A web service for provisioning a logically isolated section of the AWS cloud where you can launch AWS resources in a virtual network that you define. You control your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

**AWS EC2** — A web service that enables you to launch and manage Linux/UNIX and Windows server instances in Amazon's data centers.

**Amazon Machine Image (AMI)** — An encrypted machine image stored in Amazon Elastic Block Store (Amazon EBS) or Amazon Simple Storage Service. AMIs are like a template of a computer's root drive. They contain the operating system and can also include software and layers of your application, such as database servers, middleware, web servers, and so on.

**Instance** — A copy of an Amazon Machine Image (AMI) running as a virtual server in the AWS cloud.

**Security Groups** — A named set of allowed inbound network connections for an instance (security groups in Amazon VPC also include support for outbound connections). Each security group consists of a list of protocols, ports, and IP address ranges. A security group can apply to multiple instances, and multiple groups can regulate a single instance.

**Elastic Load Balancer** — A web service that improves an application's availability by distributing incoming traffic between two or more EC2 instances.

Elastic Load Balancing offers the Classic Load Balancer that routes traffic based on either application or network level information. The Classic Load Balancer is ideal for simple load balancing of traffic across multiple EC2 instances.

**Key Pairs** — A set of security credentials that you use to prove your identity electronically. A key pair consists of a private key and a public key.

**Elastic IP address** — A fixed (static) IP address that you have allocated in Amazon EC2 or Amazon VPC and then attached to an instance. Elastic IP addresses are associated with your account, not a specific instance. They are elastic because you can easily allocate, attach, detach, and free them as your needs change. Unlike traditional static IP addresses, Elastic IP addresses allow you to mask instance or Availability Zone failures by rapidly remapping your public IP addresses to another instance.

**Clusters** — A logical grouping of container instances that you can place tasks on.

**Auto scaling groups** — Auto Scaling groups is a collection of EC2 instances that maintains the correct number EC2 instances to handle the load for application.

**CloudWatch** — Amazon CloudWatch monitors the AWS resources and the applications run on AWS in real time. CloudWatch collects and tracks metrics, which are variables that can be measured for resources and applications. The CloudWatch alarms send notifications or automatically makes changes to the resources being monitored based on rules defined.
Components of Network Security Platform for AWS

In order to deploy Network Security Platform in AWS environment, you require the following components:

**Network Security Manager** software has a web-based user interface for configuring and managing Network Security Platform. Users connect to the Manager server from a supported client using a supported browser. The Manager functions are configured and managed through a GUI application which includes complementary interfaces for alerts, system status, system configuration, report generation, and fault management. The Manager is deployed directly in the AWS environment. It acts as a single pane of glass to manage Sensors deployed in the cloud.

**Virtual IPS Sensor** is McAfee's next-generation IPS product. The Virtual IPS Sensor is provided to you as an Amazon Machine Instance which can be deployed to protect assets in the AWS environment.

**vNSP Controller** is the central enforcement point for all network and security policies. It is a centralized manager that controls all Virtual Probes installed on the instances in the AWS environment. It can be configured in the Network Security Manager.

- **vNSP Cluster** — is a collection of Virtual IPS Sensors that inspect traffic directed to them by the virtual machines.
- **Protected group** — is a collection of virtual machines that redirect their traffic to a vNSP Cluster for inspection.

**McAfee Virtual Probes** are installed on all instances that need to be secured by the Virtual IPS Sensor. The Virtual Probe intercepts all traffic before it reaches its destination and then forwards it to the Virtual IPS Sensor for scanning.

---

How Network Security Platform functions to protect public cloud infrastructure

To protect your virtual machines in the AWS environment, the following components of Network Security Platform are deployed:

- Network Security Manager
- vNSP Controller
- Virtual IPS Sensor
- McAfee Virtual Probe

We assume that you have configured your VPCs and Availability Zones in line with your organization’s requirement.

When traffic flows to a virtual machine, the Virtual Probe installed in the virtual machine intercepts traffic and forwards it to the Virtual IPS Sensor for inspection in IPS mode. The Sensor then scans the traffic for any malicious activity. If there is no threat, the traffic is returned back to the virtual machine. If a threat is found, depending on the response action configured, the Sensor will either black hole the traffic or return the traffic after generating an alert in the Network Security Manager. In IDS mode of deployment, the Virtual Probes intercept the traffic in the same way as in IPS mode, but instead of forwarding traffic to the Sensors and receiving it back, only a copy of the traffic is forwarded to the Sensors. The original traffic continues to be processed by the virtual machine. The illustration shows you the basic IPS mode deployment of Network Security Platform in an AWS environment.
Configuration flow

Following is configuration process after the deployment of the cloud solution components:

1. The Network Security Manager is deployed first. All the other components then establishes communication with the Network Security Manager.

2. vNSP Controller is launched as an instance in AWS which first establishes trust with the Network Security Manager.

3. The Virtual IPS Sensor is also launched as an instance in AWS which establishes trust with the Network Security Manager as well as the vNSP Controller.

4. The Virtual Probe is deployed last on the virtual machines to be protected. The Probe through the Controller establishes a TCP tunnel with the Sensor to direct the traffic for inspection. Network Security Manager communicates with the Probe through the Controller.

Packet flow in Network Security Platform

Ingress packet

When a packet arrives at the interface, it is first checked to see if the packet is directed from a Sensor tunnel after inspection or to an application. If it is from a Sensor tunnel, the packet is already inspected and hence directed to the application. If the packet is to an application, then the packet should be inspected and hence the Probe checks for any Sensor to which it can redirect the traffic for inspection through the TCP tunnel. The
Sensor inspects the traffic as per the configuration. The packet after inspection is forwarded to the Sensor tunnel to be directed back to the application. If there is no Sensor available, a fail-open state is established where the packet is forwarded to the application without inspection.

**Egress packet**

When an application sends a packet, it is intercepted and sent to the Probe. The Probe sends the packet to the Sensor over TCP tunnel for inspection. After inspection, the Sensor sends the packet back to the Probe over TCP tunnel, which is sent out on the interface. If there are no Sensors, a fail-open state is established and the packet is sent out on an interface without inspection.
Packet flow in Sensor

A packet is received by the Sensor over the tunnel interface. The original packet is extracted by the Sensor and used for inspection. Based on the attack action configured in the Sensor, the packet is either blocked or directed to the Probe to be forwarded. The connection is blocked by dropping the packet and sending a TCP reset from the Sensor that resets the connection.

Figure 4-3 Packet flow in Sensor

High Availability of vNSP solution

The Virtual Network Security Platform solution provides various means to enable seamless traffic inspection. The main components within the solution are provided with failover functionality where when an instance of the component fails, the other instance of the component takes over the operation. This way the traffic is inspected without any interruption.

Manager Disaster Recovery (MDR) for Managers

The Manager Disaster Recovery (MDR) for Network Security Managers provides the ability to inspect traffic through the concept of an active and standby Manager which avoids any downtime. MDR for Virtual Sensors uses the same concept as an MDR which manages the hardware appliances. The MDR pair includes a Primary Manager and a Secondary Manager. One Manager is in Active state and the other in Standby state. When one of the Manager is not reachable, the other Manager becomes active which allows the Sensor to parse the traffic without any disruption.

The Managers communicate with each other through heartbeat which sends the health status of the Manager to each other. The heartbeat is sent at a pre-defined time interval.
The Virtual IPS Sensor sends alerts to both the Managers. Hence when the Secondary Manager becomes active, alerts generated when the Primary was active will be available in the Secondary Manager as well. Policies, clusters, and protected groups configured in the Primary Manager are replicated in the Secondary Manager as well. Once the Primary Manager becomes active again, data from the Secondary Manager are updated in the Primary Manager.

For more information on MDR, see the topic Manager Disaster Recovery (MDR) in the McAfee Network Security Platform Manager Administration Guide.

Controller High Availability (HA)

The Controller High Availability (HA) provides a failover mechanism where one of the Controller is always active and reachable. In a Controller HA pair, one Controller is in **Active** mode and the other Controller is in **Standby** mode. The Controller that completes registration first with the Network Security Manager becomes **Active**. The second Controller after registration with the Network Security Manager will be in **Standby** mode. The Controller HA pair uses elastic IP address for deployment to establish trust with the Network Security Manager. You can install the Virtual Probe and establish communication with the Controller even when one of the Controller in a Controller HA pair is active and available.

When the active Controller in the HA pair is down or not reachable, the standby Controller becomes **Active**. You can manually swap the Controller HA roles between active and standby. You can also create a Controller HA pair directly or change a standalone Controller to HA pair. When you convert a Controller HA pair to standalone Controller, the standby Controller de-registers from the Manager. You should manually delete the standby Controller instance in the AWS console.
In case of Controller HA with MDR Managers, the Controllers first tries to register with the Primary Manager. If the Primary Manager is in standby mode or is not reachable, then the Controllers register with the Secondary Manager. Once the Primary Manager is active again, you should retrieve the Controller configuration from the Secondary Manager manually.

**Figure 4-5  Controller High Availability**

McAfee recommends you to deploy the Controller in an auto scaling group in AWS with the size specified as 2. This way when one of the Controller instance is terminated or unrecoverable, the auto scaling group launches another instance of the Controller thus providing high availability for the Controller.
Considerations

Review this section and its sub-sections before you deploy a Virtual Sensor in the AWS environment.

Network Security Manager server requirements

The following table lists the 9.1 Manager/Central Manager windows server requirements:

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Minimum required</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Any of the following:</td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2 Standard or</td>
<td>Standard Edition operating</td>
</tr>
<tr>
<td></td>
<td>Enterprise Edition, English operating</td>
<td>system</td>
</tr>
<tr>
<td></td>
<td>system, SP1 (64-bit) (Full Installation)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2 Standard or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enterprise Edition, Japanese operating</td>
<td></td>
</tr>
<tr>
<td></td>
<td>system, SP1 (64-bit) (Full Installation)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 Standard Edition</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Server with a GUI) English operating</td>
<td></td>
</tr>
<tr>
<td></td>
<td>system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 Standard Edition</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Server with a GUI) Japanese operating</td>
<td></td>
</tr>
<tr>
<td></td>
<td>system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 Datacenter Edition</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Server with a GUI) English operating</td>
<td></td>
</tr>
<tr>
<td></td>
<td>system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 Datacenter Edition</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Server with a GUI) Japanese operating</td>
<td></td>
</tr>
<tr>
<td></td>
<td>system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 Standard Edition</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Server with a GUI) English operating</td>
<td></td>
</tr>
<tr>
<td></td>
<td>system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 Datacenter Edition</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Server with a GUI) English operating</td>
<td></td>
</tr>
<tr>
<td></td>
<td>system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2016 Standard Edition</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Server with a GUI) English operating</td>
<td></td>
</tr>
<tr>
<td></td>
<td>system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2016 Datacenter Edition</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Server with a GUI) English operating</td>
<td></td>
</tr>
<tr>
<td></td>
<td>system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Only X64 architecture is supported.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Memory</th>
<th>8 GB</th>
<th>&gt;16 GB</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Supports up to 3 million</td>
<td>Supports up to 10 million alerts in</td>
</tr>
<tr>
<td></td>
<td>alerts in Solr.</td>
<td>Solr.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CPU</th>
<th>Server model processor</th>
<th>Same</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>such as Intel Xeon</td>
<td></td>
</tr>
</tbody>
</table>

| Disk space  | 100 GB                      | 300 GB or more                          |
### Table 4-1 Virtual machine requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Any of the following:</td>
<td>Windows Server 2016 Standard Edition operating system</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2 Standard or Enterprise Edition, English operating system, SP1 (64-bit) (Full Installation)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2 Standard or Enterprise Edition, Japanese operating system, SP1 (64-bit) (Full Installation)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 Standard Edition (Server with a GUI) English operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 Standard Edition (Server with a GUI) Japanese operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 Datacenter Edition (Server with a GUI) English operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 Datacenter Edition (Server with a GUI) Japanese operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 Standard Edition (Server with a GUI) English operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 Datacenter Edition (Server with a GUI) Japanese operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2016 Standard Edition (Server with a GUI) English operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2016 Standard Edition (Server with a GUI) Japanese operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2016 Datacenter Edition (Server with a GUI) English operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2016 Datacenter Edition (Server with a GUI) Japanese operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Only X64 architecture is supported.</td>
<td></td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB</td>
<td>&gt;16 GB</td>
</tr>
<tr>
<td></td>
<td>Supports up to 3 million alerts in Solr.</td>
<td>Supports up to 10 million alerts in Solr.</td>
</tr>
<tr>
<td>Virtual CPUs</td>
<td>2</td>
<td>2 or more</td>
</tr>
<tr>
<td>Disk Space</td>
<td>100 GB</td>
<td>300 GB or more</td>
</tr>
</tbody>
</table>
## Network Security Manager client requirements

The following are the system requirements for client systems connecting to the Manager application:

<table>
<thead>
<tr>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operating system</strong></td>
<td></td>
</tr>
<tr>
<td>• Windows 8, English or Japanese</td>
<td>Windows 10, English or Japanese</td>
</tr>
<tr>
<td>• Windows 8.1, English or Japanese</td>
<td></td>
</tr>
<tr>
<td>• Windows 10, English or Japanese</td>
<td></td>
</tr>
<tr>
<td>The display language of the Manager client must be the same as that of the Manager server operating system.</td>
<td></td>
</tr>
<tr>
<td><strong>RAM</strong></td>
<td></td>
</tr>
<tr>
<td>2 GB</td>
<td>4 GB</td>
</tr>
<tr>
<td><strong>CPU</strong></td>
<td></td>
</tr>
<tr>
<td>1.5 GHz processor</td>
<td>1.5 GHz or faster</td>
</tr>
<tr>
<td><strong>Browser</strong></td>
<td></td>
</tr>
<tr>
<td>• Internet Explorer 11</td>
<td>• Internet Explorer 11</td>
</tr>
<tr>
<td>• Mozilla Firefox</td>
<td>• Mozilla Firefox 20.0 or later</td>
</tr>
<tr>
<td>• Google Chrome (App mode in Windows 8 is not supported)</td>
<td>• Google Chrome 24.0 or later</td>
</tr>
<tr>
<td>To avoid the certificate mismatch error and security warning, add the Manager web certificate to the trusted certificate list.</td>
<td>In Mozilla Firefox version 52 or Google Chrome version 42 and above, the NPAPI plug-in is disabled by default.</td>
</tr>
</tbody>
</table>
McAfee Virtual Probe Operating System compatibility

<table>
<thead>
<tr>
<th>Minimum required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
</tr>
<tr>
<td>Any of the following:</td>
</tr>
<tr>
<td>• 32-bit Red Hat Enterprise Linux (RHEL) 6.x</td>
</tr>
<tr>
<td>• 64-bit Red Hat Enterprise Linux (RHEL) 6.x, 7.x</td>
</tr>
<tr>
<td>• 32-bit CentOS 6.x</td>
</tr>
<tr>
<td>• 64-bit CentOS 6.x, 7.x</td>
</tr>
<tr>
<td>• 6.x SUSE Linux Enterprise Server (SLES) 10.3, 10.4, 11.2 openSUSE 10.3, 12.2.</td>
</tr>
<tr>
<td>• 32-bit Ubuntu Server 12.04, 14.04</td>
</tr>
<tr>
<td>• 64-bit Ubuntu Server 12.04, 14.04, 16.04</td>
</tr>
<tr>
<td>• 32-bit Amazon Linux 2014.09</td>
</tr>
<tr>
<td>• 64-bit Amazon Linux 2016.09, 2017.03, 2017.09</td>
</tr>
<tr>
<td>• Windows Server 2008 R2 Standard or Enterprise Edition, English operating system, SP1 (64-bit) (Full Installation)</td>
</tr>
<tr>
<td>• Windows Server 2008 R2 Standard or Enterprise Edition, Japanese operating system, SP1 (64-bit) (Full Installation)</td>
</tr>
<tr>
<td>• Windows Server 2012 Standard Edition (Server with a GUI) English operating system</td>
</tr>
<tr>
<td>• Windows Server 2012 Standard Edition (Server with a GUI) Japanese operating system</td>
</tr>
<tr>
<td>• Windows Server 2012 R2 Standard Edition (Server with a GUI) English operating system</td>
</tr>
<tr>
<td>• Windows Server 2012 R2 Standard Edition (Server with a GUI) Japanese operating system</td>
</tr>
<tr>
<td>• Windows Server 2012 R2 Datacenter Edition (Server with a GUI) English operating system</td>
</tr>
<tr>
<td>• Windows Server 2012 R2 Datacenter Edition (Server with a GUI) Japanese operating system</td>
</tr>
<tr>
<td>• Windows Server 2016 Standard Edition (Server with a GUI) English operating system</td>
</tr>
<tr>
<td>• Windows Server 2016 Standard Edition (Server with a GUI) Japanese operating system</td>
</tr>
<tr>
<td>• Windows Server 2016 Datacenter Edition (Server with a GUI) English operating system</td>
</tr>
<tr>
<td>• Windows Server 2016 Datacenter Edition (Server with a GUI) Japanese operating system</td>
</tr>
</tbody>
</table>

Requirements to deploy Network Security Platform in AWS environment

The following table lists the requirements to deploy Network Security Platform in the AWS environment.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Purpose</th>
<th>Privileges/ Other requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS GUI access</td>
<td>To launch Network Security Platform AMIs and</td>
<td>Privilege: Admin</td>
</tr>
<tr>
<td></td>
<td>configure setup</td>
<td></td>
</tr>
<tr>
<td>AWS access key and secretkey</td>
<td>To establish communication between the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Security Manager and AWS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>environment</td>
<td></td>
</tr>
<tr>
<td>Windows Server 2008 R2 /</td>
<td>To install the Network Security Manager by</td>
<td>RDP: Credentials with</td>
</tr>
<tr>
<td>2012 R2 / 2016</td>
<td>running setup.exe</td>
<td>admin access</td>
</tr>
<tr>
<td>vNSP Controller AMI</td>
<td>To install vNSP Controller</td>
<td></td>
</tr>
<tr>
<td>NSP instance AMI</td>
<td>To install Virtual IPS Sensor</td>
<td></td>
</tr>
</tbody>
</table>
The AWS user requires the following minimum permission to create access and secret keys to be used in the Network Security Manager:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "ec2:DescribeInstances",
            "ec2:DescribeTags",
            "ec2:DescribeVpcs",
            "ec2:DescribeSubnets",
            "ec2:DescribeAddresses",
            "ec2:AssociateAddress",
            "ec2:DisassociateAddress"
          ],
         "Resource": ["*"
          ]
      }
   ]
}
```

The following table lists the vNSP solution components requirements to deploy Network Security Platform in the AWS environment.

<table>
<thead>
<tr>
<th>Component</th>
<th>AWS Instance Type</th>
<th>Software Requirements</th>
<th>Network Requirements</th>
<th>Other Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Security Manager</td>
<td>m4.xlarge</td>
<td>Windows 2012 R2 Server</td>
<td>1 Network Interface (management subnet)</td>
<td>The instance should be EBS-optimized.</td>
</tr>
<tr>
<td>vNSP Controller</td>
<td>c4.xlarge</td>
<td>vNSP Controller AMI</td>
<td>1 Network Interface (management subnet)</td>
<td>The instance should be EBS-optimized.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Elastic IP is optional for a standalone Controller and is mandatory for Controller HA.</td>
<td></td>
</tr>
<tr>
<td>Virtual IPS Sensor</td>
<td>c4.xlarge</td>
<td>NSP instance AMI</td>
<td>2 Network Interfaces (primary: management subnet, second: data subnet)</td>
<td>Internet access is required to access AWS APIs.</td>
</tr>
<tr>
<td>Protected VM Instances</td>
<td>Any</td>
<td>Customer Supplied</td>
<td>1 or more (see deployment) Use public IP address or NAT gateway to access Controller EIP</td>
<td>• Networking performance less than or equal to 500 Mbps.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• No overlapping CIDR blocks across protected VPCs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• VPC peering required for the data subnet.</td>
</tr>
</tbody>
</table>
The following table lists the ports for security group settings required to deploy Network Security Platform in the AWS environment. For more information about ports used by Network Security Platform, see [KB59342](#).

<table>
<thead>
<tr>
<th>Component</th>
<th>Direction</th>
<th>Ports</th>
<th>Purpose</th>
<th>Source/ Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Security Manager</td>
<td>Inbound rules</td>
<td>8501, 8502, 8503, 8506, 8507, 8508</td>
<td>TCP port used for Sensor to Manager communication using a private IP address.</td>
<td>Virtual IPS Sensor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8504, 8509</td>
<td>TCP ports used for proprietary file transfer between the Manager and the Sensor using a private IP address.</td>
<td>Virtual IPS Sensor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>443</td>
<td>TCP port used for the following connections:</td>
<td>Virtual IPS Sensor, vNSP Controller, protected VM instance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• To connect to the Internet</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• To connect the Manager to the Virtual IPS Sensor (private IP address), vNSP Controller (public IP address if the Controller has elastic IP and private IP address), and protected VM instance (private IP address)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• For accessing the web UI of the Manager</td>
<td></td>
</tr>
<tr>
<td>Outbound Rules</td>
<td></td>
<td>8500</td>
<td>UDP port at the Sensor for SNMP channel using a private IP address.</td>
<td>Virtual IPS Sensor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>443</td>
<td>TCP port used for the following connections:</td>
<td>vNSP Controller, Secondary Manager (MDR)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• To connect the Manager to the vNSP Controller using public IP address if the Controller has elastic IP address and private IP address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• For peer Manager communication in case of Manager Disaster Recovery (MDR) using a private IP address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• To access AWS console.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>22</td>
<td>TCP port used for SSH (management subnet for either public or private IP address).</td>
<td>vNSP Controller</td>
</tr>
<tr>
<td>Both inbound and outbound</td>
<td></td>
<td>3389</td>
<td>TCP port to connect to the Manager using Remote Desktop Protocol (RDP).</td>
<td>---</td>
</tr>
<tr>
<td>Component</td>
<td>Direction</td>
<td>Ports</td>
<td>Purpose</td>
<td>Source/Destination</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------</td>
<td>-------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>vNSP Controller</td>
<td>Inbound</td>
<td>443</td>
<td>TCP port used by vNSP Controller for the following connections: • Manager communication using either public or private IP address • Sensor management using private IP address and public IP address if elastic IP is used. Use a NAT Gateway IP address if Sensor is connected using a private IP address. • Protected VM instances communication using private IP address and public IP address. Use a NAT Gateway IP address if the instance is connected using a private IP address.</td>
<td>Network Security Manager, Virtual IPS Sensor, protected VM instance</td>
</tr>
<tr>
<td></td>
<td>Outbound</td>
<td>443</td>
<td>TCP port used for both vNSP Controller to Manager communication and vNSP Controller to Sensor management using public and private IP address.</td>
<td>Network Security Manager, Virtual IPS Sensor</td>
</tr>
<tr>
<td></td>
<td>Both</td>
<td>3306</td>
<td>TCP port for data synchronization between vNSP Controllers when deployed in high availability mode.</td>
<td>---</td>
</tr>
<tr>
<td>Virtual IPS Sensor</td>
<td>Inbound</td>
<td>8500</td>
<td>UDP port at the Sensor for SNMP channel using a private IP address.</td>
<td>Network Security Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(management)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Outbound</td>
<td>8501, 8502, 8503, 8504, 8506, 8507, 8508, 8509 (management)</td>
<td>TCP port used for Sensor to Manager communication (management subnet using a private IP address).</td>
<td>Network Security Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9797</td>
<td>TCP port used by the protected VM instances to communicate with the Sensor using a private IP address.</td>
<td>Protected VM instance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(data)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protected VM</td>
<td>Inbound</td>
<td>No ports required for inbound data.</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>Instances</td>
<td>Outbound</td>
<td>No ports required for outbound data.</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Direction</td>
<td>Ports</td>
<td>Purpose</td>
<td>Source/Destination</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------</td>
<td>-------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Outbound rules</td>
<td></td>
<td>9797</td>
<td>TCP port used by the protected VM instances to communicate to the Sensor using a private IP address.</td>
<td>Virtual IPS Sensor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>443</td>
<td>TCP port used by the protected VM instance to connect vNSP Controller (public and private IP address) and the Manager (private IP address).</td>
<td>Network Security Manager, vNSP Controller</td>
</tr>
</tbody>
</table>

Create IAM roles and policies

An IAM role is similar to a user, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, a role does not have any credentials (password or access keys) associated with it. Instead, if a user is assigned to a role, access keys are created dynamically and provided to the user.

The AWS user requires the following minimum permission to create IAM roles:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ec2:DisassociateAddress",
        "ec2:DescribeInstances",
        "ec2:DescribeAddresses",
        "ec2:DescribeTags",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:AssociateAddress",
        "ec2:DescribeInstanceStatus"
      ],
      "Resource": "*"
    }
  ]
}
```

For more information on creating an IAM role, see the section IAM Roles.

Create an IAM role to attach the second interface to Virtual IPS Sensor and auto scaling groups

The Virtual IPS Sensor requires two interface, one for communication with the Network Security Manager for management and the other with the endpoints to inspect the traffic. If only one interface has been added during the launch of a Sensor instance, create the following IAM policy to automatically add the monitoring interface to the Sensor upon first boot. AWS allows you to assign a second interface only if you have the following rights enabled for your account:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1489796792000",
      "Effect": "Allow",
      "Action": [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ]
    }
  ]
}
```
User data for establishing trust

User data is defined in AWS to establish trust between the Manager and Controller or Manager and Sensor.

User data update to establish trust between Manager and vNSP Controller

Following is the JSON formatted data transferred to the instance to establish trust between the Network Security Manager and the Virtual IPS Sensor:

```
{
    "Primary NSM IP":"10.x.x.x", "Controller Name":"controller_name", "Controller Shared Key":"passphrase"
}
```

When using an MDR pair, provide the following user data:

```
{
    "Primary NSM IP":"10.x.x.x", "Secondary NSM IP":"10.x.x.x", "Controller Name":"controller_name", "Controller Shared Key":"passphrase"
}
```

If you are upgrading the Controller from version 3.5.3 to 3.6.1, you have to stop the Controller instance and update the user data according to the new format.

User data to define Network Security Manager for AWS auto scaling groups

Following is the script to establish trust between the Network Security Manager and the Virtual IPS Sensor:

```
{"Primary NSM IP":"10.x.x.x", "Cluster Name":"C1", "Sensor Shared Key":"xxx123", "dataSubnet": "subnet-b1da179d", "dataSecurityGroups": "sg-08731277" }
```

For an MDR pair with auto scaling groups, provide the following user data to establish the trust:

```
{"Primary NSM IP":"10.x.x.x", "Secondary NSM IP":"10.x.x.x", "Cluster Name":"C1", "Sensor Shared Key":"xxx123", "dataSubnet": "subnet-b1da179d", "dataSecurityGroups": "sg-08731277" }
```

Table 4-2  User data parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary NSM IP</td>
<td>IP address of the primary Manager</td>
</tr>
<tr>
<td>Secondary NSM IP</td>
<td>IP address of the secondary Manager</td>
</tr>
<tr>
<td>Controller Name</td>
<td>Name of the Controller defined in the Manager</td>
</tr>
<tr>
<td>Controller Shared Key</td>
<td>Shared secret key of the Controller provided in the Manager</td>
</tr>
<tr>
<td>Cluster Name</td>
<td>Name of the Cluster in the Manager where the auto scale group will be launched</td>
</tr>
<tr>
<td>Sensor Shared Key</td>
<td>Shared secret key to establish trust with the Sensor.</td>
</tr>
<tr>
<td>dataSubnet</td>
<td>Subnet where the monitoring interface will be launched</td>
</tr>
<tr>
<td>dataSecurityGroups</td>
<td>Security group to which the auto scale group is assigned to</td>
</tr>
</tbody>
</table>
Manage Licenses

Licenses are required to add vNSP Clusters. These licenses can either be individual .jar files, or they can be bundled together and provided to you in the form of a .zip file. Each license supports a pre-defined number of Virtual IPS Sensors, and this number is specific to the license file you have procured.

- There is no limit on the number of license files you can add to the Manager.
- The license files do not expire.

The Manager periodically compares the number of Virtual IPS Sensors supported by your licenses with the installed number of Virtual IPS Sensors. You are compliant as long as the number of Virtual IPS Sensors in your Manager does not exceed the total number of Virtual IPS Sensors allowed across all licenses. For example, if you have two licenses, one which allows 5 and the other which allows 10 Virtual IPS Sensors, you are compliant as long as you have no more than 15 Virtual IPS Sensors in this Manager.

If there are not enough licenses added to the Manager, a fault is raised accordingly.

The Licenses page in the Manager displays your compliance, and maintains the count for Virtual IPS Sensors and Virtual Probes. This page also displays and allows you to add and remove individual licenses.
Task

1. In the Manager, select Manager | <Admin Domain Name> | Setup | Licenses.

2. The Summary section displays the overall compliance, the number of Virtual IPS Sensors along with the maximum number allowed, and the number of Virtual Probes in use.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall License Status</td>
<td>Overall compliance which can either be Compliant or Non-compliant. If the Virtual IPS Sensor count is within the maximum limit defined in the license, the overall state is displayed as Compliant with a green icon preceding it. If the Virtual IPS Sensor count exceeds the maximum limit, the overall state is displayed as Non-Compliant with a red icon preceding it.</td>
</tr>
<tr>
<td>Total Virtual Sensors</td>
<td>Number of Virtual IPS Sensors in use along with the maximum number</td>
</tr>
<tr>
<td>Total Virtual Probes</td>
<td>Number of Virtual Probes in use</td>
</tr>
</tbody>
</table>

Figure 4-6 Licenses Page
If the overall license status is **Compliant**, the tool tip for Total Virtual Sensors displays that no additional licenses are required. However, if the overall license status is **Non-Compliant**, the tool tip for Total Virtual Sensors indicates that additional number of licenses are required for compliance.

<table>
<thead>
<tr>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall License Status:</td>
</tr>
<tr>
<td>Total Virtual Sensors:</td>
</tr>
<tr>
<td>Total Virtual Probes:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall License Status:</td>
</tr>
<tr>
<td>Total Virtual Sensors:</td>
</tr>
<tr>
<td>Total Virtual Probes:</td>
</tr>
</tbody>
</table>

3. The **Individual Licenses** section displays the details of each license imported into the Manager.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| License         | **Key** – Key of the license file  
**Generated** – Date when the license file was generated  
**Customer** – Customer for whom the license file was generated  
**Grant ID** – The McAfee Grant ID of the corresponding customer |
| Virtual Sensors Allowed | Maximum number of Virtual IPS Sensors allowed for the selected license |
| Added           | **Time** – Date in <mmm-yy> format, and time when the license was added  
**By** – Name of the user who added the license |
| Comment         | Enables you to add your comment per license file that is imported. Double-click in the **Comment** field and enter your comment. Click outside this field and your comment is automatically saved. |
4 To import licenses into the Manager, click **Add License**. Click **Browse** to locate the license, and then click **OK**. The successful addition of a license is displayed at the top of the page.

5 To remove a license, select the license you want to remove from the **Individual Licenses** section, and click **Remove**.

In the pop-up window, click **OK** to remove the selected license or **Cancel** to return to the **Licenses** page.

6 Click **Save as CSV** to export license information in the .csv format. The default CSV file name is NsmLicenseList.CSV.

---

**Virtual IPS Sensor Model to secure the public cloud**

<table>
<thead>
<tr>
<th>Model</th>
<th>Maximum Sensor throughput</th>
<th>Number of monitoring ports</th>
<th>Management port</th>
<th>Logical CPU Cores</th>
<th>Memory required</th>
<th>Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS- VM100-VSS</td>
<td>550 Mbps</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>Minimum 4 GB</td>
<td>8 GB</td>
</tr>
</tbody>
</table>
Generate the License Compliance report

You can generate a Virtual IPS Sensor Compliance Report to know if you are compliant with the maximum number of Virtual IPS Sensors allowed by your licenses. The report also lists the licenses added to the Manager and the Virtual IPS Sensors currently managed by it.
**Task**

1. In the Manager, go to Manager | <Admin Domain Name> | Reporting | Configuration Reports | Licenses.

2. Select the required option from the Output Format list, and click Submit.

   Virtual IPS Sensor Compliance Report is available only for the Admin Domain in the Manager.

---

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall License Status</td>
<td>Current overall compliance status of the number of Virtual IPS Sensors</td>
</tr>
<tr>
<td>Total Virtual Sensors</td>
<td>Number of Virtual IPS Sensors that are in use and the maximum number allowed</td>
</tr>
<tr>
<td>Total Virtual Probes</td>
<td>Number of Virtual Probes in use</td>
</tr>
<tr>
<td>Report Generation Time</td>
<td>Date in &lt;yyyy-mm-dd&gt; format, and time at which the report was generated</td>
</tr>
<tr>
<td>License</td>
<td>Key - Key of the license file</td>
</tr>
<tr>
<td></td>
<td>Generated - Date when the license file was generated</td>
</tr>
<tr>
<td></td>
<td>Customer - Customer for whom the license file was generated</td>
</tr>
<tr>
<td></td>
<td>Grant ID - McAfee Grant ID of the corresponding customer</td>
</tr>
</tbody>
</table>
### Telemetry

Telemetry enables McAfee Network Security Platform to send attributes such as alert data details, alert data summary, general setup, feature usage, and system faults. This report is sent to the McAfee GTI server for further analysis. Sending information through telemetry about each of these attributes to McAfee is optional.

**Configure Telemetry**

The GTI page in the Manager displays, and allows you to exercise control over the information that you send to McAfee. Each attribute in the GTI section can be enabled or disabled using the radio buttons provided against it.

**Task**

1. In the Manager, select **Manager | <Admin Domain Name> | Integration | GTI**.

2. On the right under **Send?**, select the **Yes** or **No** radio buttons against the respective category.

3. In the **Technical Contact Information** section, provide your contact information to McAfee Labs.
In the Test GTI Lookup section, enter an IP address to check its reputation. This is used to check whether communication with the GTI server is established.

You can capture telemetry information for your selected attributes by clicking Show Me What I’m Sending. Clicking this link creates a PDF file which displays the information that is sent to McAfee.

For more information about the attributes, refer McAfee Network Security Platform Installation Guide.

### Telemetry for vNSP Clusters

Telemetry is required as long as you have defined one or more vNSP clusters. Telemetry is automatically enabled when the first vNSP Cluster is defined in the Manager. This is indicated by the vNSP Cluster Usage attribute on the GTI page becoming read-only.

The following vNSP cluster information is sent to McAfee daily at 00:00 hour.

- Name and grant ID associated with each virtual sensor license
- Overall license compliance status
- Total number of allowed virtual sensors
- Total number of virtual sensors currently in use with vNSP clusters
- Total number of virtual probes currently in use with vNSP clusters
- Maximum number of virtual probes used
- Manager version

Telemetry data is not sent if the Manager is unable to establish connection with the McAfee GTI server. In this case, the following actions cannot be performed on Virtual IPS Sensors in AWS environment.

- Deploy pending changes
- Automatic updating of signature sets and callback detectors
**Deploy Pending Changes**

When you make configuration changes, you must apply the changes to your devices. In the Manager, you can deploy these changes to all devices in the admin domain from the Global tab. The navigation path for this is Devices | <Admin Domain Name> | Global | Deploy Pending Changes. Under the Deploy column, select the check boxes for respective devices, and click Deploy.

For more information about deploying pending changes to your devices, refer *McAfee Network Security Platform Manager Administration Guide*.

When the Manager is not connected to the internet, all check boxes for deployment are disabled, and a tool tip displays the message **Pending changes cannot currently be deployed to this device either because a license is required or the Manager is unable to send telemetry data to McAfee.**

When deployment of pending changes to the Virtual IPS Sensors is prevented, the Manager validates the connectivity every 60 minutes. If a connection with the McAfee GTI server is established, configuration changes to the Virtual IPS Sensors will be automatically enabled.

You can manually validate connectivity to the McAfee GTI server by clicking Test Connection in the Manager | <Admin Domain Name> | Integration | GTI page.

**Workflow for deploying Network Security Platform in AWS**

This section provides information about the deployment of Network Security Platform to protect your instances in AWS environment.

**High-level steps for configuring Network Security Platform in AWS environment**

We assume that your VPCs and Availability Zones are configured in line with your organization's requirement. The Virtual IPS Sensor can be installed in the same VPC as your virtual machines or in a separate VPC. Before installing the Manager, ensure that you have selected the appropriate region in the AWS console.

For recommendations on the various deployment options, see the topic **Best Practices** on page 257.

This section provides the high-level steps for deploying Network Security Platform in AWS environment.

1. Install the Network Security Manager (Virtual/On-premises).
2. In the Network Security Manager, create a vNSP Controller.
3 Launch the vNSP Controller AMI.

4 In the Network Security Manager, create a vNSP cluster, and configure the Protected Groups for the vNSP Cluster.

5 In the AWS console,
   a Launch a Virtual IPS Sensor instance using the template AMI.
   b Create the customized AMI, and use it to launch a second instance of the Virtual IPS Sensor.

6 From the Network Security Manager, download the Virtual Probe which is specific to the OS of the machine that is to be protected.

7 Install the probe in the instances that are to be protected.
Install the Network Security Manager

The Network Security Manager is installed on a virtual machine in the AWS environment or on-premises.
If you have the Manager behind a firewall, you need to update your firewall rules accordingly such that ports are open for the Manager to communicate with Sensors and the vNSP Controller. For more information on ports used by the Manager to communicate with Sensors and vNSP Controllers, see the section Requirements to deploy Network Security Platform in AWS environment on page 192.

For more information on installing the Network Security Manager, see the McAfee Network Security Platform Installation Guide.

**Attach a second interface to recover the Manager**

The Network Security Manager instance in AWS can be recovered in case of a failure. To recover the Manager, you should define a second interface while launching the Manager instance. In case of the Manager failure, you can attach the interface you defined while launching the new Manager instance. This helps retain the Sensor configuration as the same IP address is used for Sensor-Manager communication. You first have to create a network interface and then attach it to the Manager instance.

> For an MDR pair, you should define two interfaces and attach it to both the Managers.

**Create a network interface**

To create a network interface, perform the following steps:

1. In the AWS console, go to Services | EC2.
2. In the left pane under the NETWORK & SECURITY section, click Network Interfaces.
3. In the Network Interfaces page, click Create Network Interface.
4. Enter the following details and click Yes, create:
   - Description: Enter a name or description for the interface.
   - Subnet: Select the subnet in which the Network Security Manager is launched.
   - Private IP: The IP address is assigned automatically based on the availability in the subnet. Alternatively, you can also define the IP address for the interface.
   - Security groups: Select the same security group that is defined assigned to the Network Security Manager.

**Table 4-3  Option definitions**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter a name or description for the interface.</td>
</tr>
<tr>
<td>Subnet</td>
<td>Select the subnet in which the Network Security Manager is launched.</td>
</tr>
<tr>
<td>Private IP</td>
<td>The IP address is assigned automatically based on the availability in the subnet. Alternatively, you can also define the IP address for the interface.</td>
</tr>
<tr>
<td>Security groups</td>
<td>Select the same security group that is defined assigned to the Network Security Manager.</td>
</tr>
</tbody>
</table>

![Create Network Interface](image)

**Figure 4-9 Create an interface**
Attach a network interface

To attach the second interface to the Network Security Manager, perform the following steps:

1. In the AWS console, go to Services | EC2.
2. In the left pane under the INSTANCES section, click Instances and select the Network Security Manager instance.
3. Click Actions | Networking | Attach Network Interface.
4. Enter the following details and click Attach:

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance ID</td>
<td>Displays the ID of the Network Security Manager instance.</td>
</tr>
<tr>
<td>Network Interface</td>
<td>Select the network interface you created for the Manager.</td>
</tr>
</tbody>
</table>

Figure 4-10  Attach the interface to the Manager

If you attach another network interface to your instance, your current public IP address is released when you restart your instance. Learn more about public IP addresses.
Recover the Manager

When you launch a new instance of the Network Security Manager, you have to select the network interface during the installation process. The IP address attached with this new interface is available in the Description tab for the Manager. Enter the IP address of the Manager which is connected through the interface in the pre-installation summary step during Manager installation.

Configure MDR for AWS cloud

First, you must configure MDR separately on both the Primary and Secondary Managers:

**Task**

1. Select Manager | `<Admin Domain Name>` | Setup | MDR.

   - MDR for AWS cloud does not support IPv6 addresses.

   - The Manager supports a maximum of three IP addresses during MDR configuration. The Manager assumes that all the IP addresses are bound to the same host name.

2. Fill in the following fields:
Table 4-5 Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role of this Manager</td>
<td>Select <strong>Primary</strong> to use this Manager as the active Manager, or <strong>Secondary</strong> to use this Manager as the standby.</td>
</tr>
<tr>
<td>Use Out-of-Band (OOB) Manager-to-Manager Communication?</td>
<td>• Yes to use separate interfaces for Manager-Manager and Manager-Sensor communication.</td>
</tr>
<tr>
<td></td>
<td>• No to use the same interface for Manager-Manager and Manager-Sensor communication.</td>
</tr>
<tr>
<td>Peer IP for Manager-to-Manager Communication</td>
<td>This option appears if you selected the option <strong>Yes</strong> in Use Out-of-Band (OOB) Manager-to-Manager Communication?. Enter the IP address of the Peer Manager that you want to use for Manager-Manager communication.</td>
</tr>
<tr>
<td></td>
<td>If you set Use Out-of-Band (OOB) Manager-to-Manager Communication? to Yes in the Primary Manager, then set this option as Yes in your Secondary Manager as well. A mismatch in this option setting between the Primary and Secondary Manager pair will result in an MDR configuration failure.</td>
</tr>
<tr>
<td>Peer IP for Manager-to-Sensor Communication</td>
<td>Enter the IP address of the peer Manager that is used for communication with the Sensor.</td>
</tr>
<tr>
<td>MDR Pair Shared Secret</td>
<td>The same shared secret key must be entered on both Managers for MDR creation to be successful. Enter a minimum of eight characters and use no special characters.</td>
</tr>
<tr>
<td>Confirm MDR Pair Shared Secret</td>
<td>Re-enter the same shared secret key.</td>
</tr>
<tr>
<td>Downtime Before Switchover</td>
<td>Enter the downtime in minutes before the switch to the Secondary Manager occurs. Downtime before switchover should be between 1-10 minutes. This field is disabled if the Role of this Manager of Manager is set to Secondary.</td>
</tr>
</tbody>
</table>

3 Click **Finish** to confirm your changes.

When you click **Finish** and your peer Manager’s MDR settings are not yet configured, then Network Security Platform displays a warning to remind you to configure the peer Manager MDR settings.

You can configure only **IPv4 address** for Manager-Sensor communication as given in the following scenarios:

- If a Sensor is connected to Manager over an IPv4 network, or you want to add a Sensor from the IPv4 network to the Manager, then you need to enter the **IPv4 address** of the peer Manager.

- When Use Out-of-Band (OOB) Manager-to-Manager Communication is set to No, Peer IP for Manager-to-Sensor Communication is used for both Manager-Manager and Manager-Sensor communication.

- When Use Out-of-Band (OOB) Manager-to-Manager Communication is set to Yes, Peer IP for Manager-to-Sensor Communication is used only for Manager-Sensor communication.

You need to use the Peer IP for Manager-to-Sensor Communication while establishing trust between the Sensor and Manager. Ensure that your peer Manager is configured to use the same IP address as selected from the Dedicated Interface list during the Peer Manager installation. If mis-configured, Network Security Platform generates an error message to prompt you to enter the correct IP address. For more information on Sensor communication Interface, see McAfee Network Security Platform Installation Guide.
Configure a vNSP Controller

Before you begin

Ensure that you have the following details:

• Access and Shared keys provided to you during the creation of your AWS account
• Information about the region of your cloud environment

To set up communication between the Manager and the Controller server you have to configure the vNSP Controllers in the Manager.
Task

1. In the Manager, select Devices | <Admin Domain Name> | Global | vNSP Controllers.

The vNSP Controllers page appears and displays the vNSP Controllers that are currently available.

<table>
<thead>
<tr>
<th>Column</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller Name</td>
<td>Displays the name of the vNSP Controller.</td>
</tr>
<tr>
<td>Mode</td>
<td>Displays the mode in which the Controller is deployed.</td>
</tr>
<tr>
<td></td>
<td>Standalone — Single Controller instance is deployed.</td>
</tr>
<tr>
<td></td>
<td>High-Availability — Two Controller instances are deployed, one as active and the other as standby.</td>
</tr>
<tr>
<td>Service IP Address</td>
<td>Displays the elastic IP address assigned to the Controller. If an elastic IP address is not assigned in case of a standalone Controller, then the private IP address used for communication between the Controller and the Manager is displayed.</td>
</tr>
<tr>
<td>Instances</td>
<td>Displays the name or the IP address of the Controller Server. The icon before the Controller IP address displays the status of the Controller. The status can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>Online</td>
</tr>
<tr>
<td></td>
<td>Disconnected</td>
</tr>
<tr>
<td></td>
<td>Connected but Service Offline</td>
</tr>
<tr>
<td>Controller/Probe Software</td>
<td>Displays the software version of the vNSP Controller and the Virtual Probe.</td>
</tr>
<tr>
<td>HA Role</td>
<td>Displays if the Controller is in Active mode or Standby mode.</td>
</tr>
<tr>
<td>Tunnel Network</td>
<td>Displays the subnet used for secure communication by the vNSP Controller, Virtual IPS Sensors, and the Virtual Probes. The subnet should be a CIDR other than an underlay network and the IP address should not be used anywhere in the network. You can use the Automatic Private IP Addressing (APIPA) scheme to assign the IP address. The APIPA address CIDR is 169.254.0.0/16.</td>
</tr>
<tr>
<td>Cloud Environment</td>
<td>Type — Displays the name of the cloud service provider.</td>
</tr>
<tr>
<td></td>
<td>Region — Indicates the region in which your vNSP Controller resides.</td>
</tr>
<tr>
<td></td>
<td>Access Key — Displays the access key for the selected cloud environment. Access key allows the Manager to access AWS programmatically.</td>
</tr>
<tr>
<td>Last Updated</td>
<td>Time — Displays the time when the vNSP Controller was last updated.</td>
</tr>
<tr>
<td></td>
<td>By — Displays the user who modified the vNSP Controller.</td>
</tr>
<tr>
<td>Column</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>Comment</td>
<td>Displays additional information for the vNSP Controller.</td>
</tr>
<tr>
<td></td>
<td>Refresh the status of all the Controllers using the refresh icon provided at the top of the page.</td>
</tr>
</tbody>
</table>

Figure 4-13  vNSP Controllers

To create a new vNSP Controller, click `+`. The Controller Details panel appears which allows you to provide credentials for the cloud environment, the IP address, and the corresponding subnet details of the vNSP Controller.
Enter the required details:

### Table 4-6 Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller Name</td>
<td>Enter a unique name for the Controller.</td>
</tr>
<tr>
<td></td>
<td>The name can contain up to 64 alphanumeric (upper or lower case letters and numbers) characters, spaces, including commas, hyphens, underscores, and periods. The name must not begin with a special character.</td>
</tr>
<tr>
<td>Mode</td>
<td>Select the deployment mode for the Controller as <strong>Standalone</strong> or <strong>High-Availability</strong>.</td>
</tr>
<tr>
<td>Custom Service IP Address</td>
<td>Select the checkbox if you want to assign an elastic IP address for a standalone Controller.</td>
</tr>
<tr>
<td>Service IP Address</td>
<td>Enter the elastic IP address through which the Controller communicates with the Virtual Probes. This field appears for a standalone Controller only if you selected <strong>Custom Service IP Address</strong>. This field is mandatory for a HA pair.</td>
</tr>
<tr>
<td>HA Timeout (minutes)</td>
<td>Enter the time period for which the standby Controller has to wait before switching to active mode. This field appears only if you selected <strong>High-Availability</strong> mode.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter a secret key for the Controller.</td>
</tr>
<tr>
<td>Confirm Shared Secret</td>
<td>Re-enter the secret key for the Controller.</td>
</tr>
<tr>
<td>Tunnel Network</td>
<td>Select the subnet for communication between the Virtual IPS Sensors, Controller, and Virtual Probes. The subnet has to be in IPv4 CIDR block format. Use a CIDR block that is not used in any VPC. This subnet is used for private communication and should not be used anywhere else in the network. The subnet should be a CIDR other than an underlay network and the IP address should not be used anywhere in the network. You can use the Automatic Private IP Addressing (APIPA) scheme to assign the IP address. The APIPA address CIDR is 169.254.0.0/16.</td>
</tr>
<tr>
<td>Last Updated</td>
<td>It is blank when creating the Controller for the first time. For an existing Controller, it displays the date, time, and user who last updated the Controller settings.</td>
</tr>
<tr>
<td>Comment</td>
<td>Enter any comments if any.</td>
</tr>
<tr>
<td>Cloud Environment</td>
<td>Select the cloud type as Amazon.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the name of the region in which your vNSP Controller resides.</td>
</tr>
<tr>
<td>Region</td>
<td>Enter the Access Key for API access of your AWS account. This key should allow minimum AmazonEC2ReadOnlyAccess.</td>
</tr>
</tbody>
</table>

Securing your Amazon Web Services (AWS) datacenter

Workflow for deploying Network Security Platform in AWS
### Table 4-6 Option definitions (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secret Key</td>
<td>Enter the Secret Key associated with the Access Key.</td>
</tr>
<tr>
<td>Save</td>
<td>Click to save the settings.</td>
</tr>
</tbody>
</table>

### Figure 4-14 vNSP Controller details panel

4 To view the details for a Controller, double-click the Controller. The Controller Details panel opens. It displays the Controller and Probe version installed along with the date, time and the user who last modified it.

5 To edit a vNSP Controller, double-click the vNSP Controller and edit the required details in the vNSP Controller panel and click Save.

   - You can edit only the Shared Secret, Confirm Shared Secret, Comment, Access Key and Shared Key fields. To change the Hostname (local IP address) and Tunnel Network, you must recreate the vNSP Controller.
   - If you edit the Shared Secret for the Controller, you have to stop the Controller instance in the AWS environment and update the User data to reflect the updated Shared Secret key.

6 To delete a vNSP Controller, select the vNSP Controller and click .

7 To create a .csv list of the list of Controllers, click Save as CSV.
8 (Optional) You can perform the following actions from the Other Actions option at the bottom of the page:

a After configuring the Controller, you can check the connection between the Manager and the AWS environment. Select the Controller and click Other Actions | Test Connection | Cloud Environment to verify your AWS account credentials and the connectivity of the Manager with the AWS environment.

On successful verification, a pop-up displays the message The Manager has successfully connected to the cloud environment.

b (Optional) You can also check the connection between the Manager and the vNSP Controller. Select the Controller, click Other Actions | Test Connection | vNSP Controller to test the connectivity of the Manager with the vNSP Controller.

On successful verification, a pop-up displays the message The Manager has successfully connected to the vNSP Controller.

c To download the logs for the Controller, click Other Actions | Download Controller Logs. The Controller logs are downloaded in the form of a zip file.

d For a Controller HA pair, you can swap the Controller HA Role between Active and Standby. To swap the Controller HA Role, click Other Actions | Swap HA Role (Active/Standby).

e To upgrade the Controller software, click Other Actions | Upgrade Controller Software. For a Controller HA pair, both the Controllers are upgraded together. The Virtual Probe is bundled with the Controller software. Hence, when you upgrade the Controller, the Virtual Probe software is also upgraded. The Virtual Probe automatically restarts after an upgrade and a reboot of the protected machine is not required.
Launch the vNSP Controller AMI instance

Before you begin
You will need an Amazon S3 Bucket to store the shared secret key. To conceal the S3 Bucket URL you can generate a signed URL using the following steps:

1. Limit the access to the Amazon S3 bucket to the user who will be using the shared secret key.
2. Using an example Python script (such as the one provided in the link below) and the user's Access Key and Secret Key create a signed URL.

This link takes you to a sample script to generate the signed URL for the S3 bucket.
3. Execute the following command in the command prompt to run the script:

   ```bash
   ./<Script_Name>.py -b S3BucketName -p Sharedkey.txt --expiry=<Duration> -a <AccessKey> -s <SharedKey>
   ```

Table 4-7  Option definitions

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Script_Name</td>
<td>The name of the Python script as you have saved in your system.</td>
</tr>
<tr>
<td>S3BucketName</td>
<td>The name of your S3 bucket.</td>
</tr>
<tr>
<td>Sharedkey.txt</td>
<td>The text file which contains the shared secret key in json format.</td>
</tr>
<tr>
<td>Duration</td>
<td>The duration till which the URL will be valid.</td>
</tr>
<tr>
<td>AccessKey</td>
<td>The Access Key of the user who will use the shared secret key.</td>
</tr>
<tr>
<td>SharedKey</td>
<td>The Shared Key of the user who will use the shared secret key.</td>
</tr>
</tbody>
</table>

As part of Network Security Platform deployment, you have to launch an instance of the vNSP Controller in the AWS environment. The Controller image is provided to you in the form an AMI. You need the following before launching a Controller instance.

- Security group with the ports opened as specified in Requirements to deploy Network Security Platform in AWS environment on page 192.
- Shared Secret configured in the Manager for this vNSP Controller.

To launch an instance using the Controller AMI provided through AWS console, follow the steps below. The instance can be launched through AWS API or CLI using similar steps.

**Task**

1. Log in to the AWS console, and navigate to Services | EC2.
2. In the left panel, under IMAGES, click AMIs.
3. Search for the AMI ID of the Controller and click Launch.
4. Under the Choose the Instance type tab, select the instance type as c4.xlarge (vCPUs: 4, Memory 7.5GB), and click Next: Configure Instance Details.
5 In the **Configure Instance** page, from the drop-down lists for **Network** and **Subnet**, choose the Management network and the corresponding subnet.

6 Make sure EBS-optimized setting is selected.

7 (Optional) If you are using the **User Data** to launch the Controller instance, in the **Advanced area** enter the following information in the **User data** to register the Controller with the Manager:

   If you are using the customized AMI method to launch the Controller image, skip this step and proceed to step 8.

   ```json
   {"Primary NSM IP": "10.x.x.x", "Controller Name": "Controller_Name", "Cloud Data URL": "URL_for_S3_bucket"}
   ```

   If you have an MDR pair, use the following user data to establish trust between the Manager pair and the Sensor:

   ```json
   {"Primary NSM IP": "10.x.x.x", "Secondary NSM IP": "10.x.x.x", "Controller Name": "Controller_Name", "Cloud Data URL": "URL_for_S3_bucket"}
   ```

   The user data is represented in JSON and represents the following information.

   **Table 4-8 Option definitions**

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary NSM IP</td>
<td>IP address of the Primary Manager.</td>
</tr>
<tr>
<td>Secondary NSM IP</td>
<td>IP address of the Secondary Manager.</td>
</tr>
<tr>
<td>Controller Name</td>
<td>Name of the Controller to which this Sensor belongs to.</td>
</tr>
<tr>
<td>Cloud Data URL</td>
<td>Signed URL for the Shared Secret Key file in Amazon S3 bucket.</td>
</tr>
</tbody>
</table>

8 Under the **Add Storage** tab, use the default Size (64 GiB), and click **Next: Add Tags**.
9 Define a tag for your Sensor instance, and click **Next: Configure Security Group**.

10 In the **Configure Security Group** page, you can create a new Security Group to define the firewall rules to control traffic to the Sensor or choose an existing Security group.

For a Controller HA, you have to enable ports 22, 3306, and 443.

Once you have configured the Security Group, click on **Review and Launch**.

11 Under the **Review Instance Launch** page, review the details provided for the creation of the instance. You can either edit specific details or click on **Launch** to assign a key pair to your Sensor instance.
12 In the **Select an existing key pair or create a new key pair** window, you can either choose an existing key pair or create a new key pair, and click **Launch instances**. The instance is now launched.

![Select an existing key pair or create a new key pair](image)

You cannot login to Controller instance even though you provide a key pair.

13 Perform the following steps once the Controller starts and the Manager will show that it is online:

   a. Stop the Controller instance.

   b. Delete the **Controller Shared Key** from the user data of the instance.

   c. Restart the instance.

   Once the Controller starts, it pairs with the Manager.

14 (Optional) If you are using the customized AMI method to launch the Controller image, complete the steps in **Create a customized AMI for Controller or Sensor** on page 233.

**Create a vNSP Cluster**

A vNSP Cluster is a collection of Virtual IPS Sensors that protect a group of virtual machines. The **vNSP Clusters** page allows you to configure vNSP Clusters and the corresponding protected groups.
Task

1. In the Manager, select Devices | <Admin Domain Name> | Global | vNSP Clusters.

The vNSP Clusters page displays the currently available vNSP Clusters. Selecting any of the vNSP Clusters displays the specific VM groups protected by them.

<table>
<thead>
<tr>
<th>Column</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Name</td>
<td>Name of the vNSP Cluster.</td>
</tr>
<tr>
<td>Description</td>
<td>Description for the vNSP Cluster.</td>
</tr>
<tr>
<td>vNSP Controller</td>
<td>Controller to which the cluster belongs.</td>
</tr>
<tr>
<td>Member Sensors</td>
<td>Number of Member Sensors in the selected vNSP Cluster.</td>
</tr>
<tr>
<td>Last Updated</td>
<td>Time - Date in &lt;mmm-yy&gt; format, and time when the vNSP Cluster was last updated. By - User who modified the vNSP Cluster.</td>
</tr>
</tbody>
</table>
2 To add a new vNSP Cluster, click +.

When you create a vNSP cluster for the first time, a pop-up window displays a confirmation message. Clicking OK takes you to the Add vNSP Cluster window. Click Cancel to stay on the vNSP Clusters page.

It is mandatory to acquire and add at least one license file provided to you by McAfee. In the absence of a license file, creation of a vNSP Cluster will be prevented, and you will be redirected to the Manager | Setup | Licenses page to add a license.

3 The Add vNSP Cluster window allows you to update the vNSP Controller configuration, and enter the shared secret key for the vNSP Cluster to establish communication with your Network Security Manager.

4 In the Name field, enter a unique name that enables you to easily identify the vNSP Cluster.

   ![Warning]
   The name can contain up to 50 alphanumeric (upper or lower case letters and numbers) characters, including hyphens and underscores. The name must begin with a letter.

5 In the Description field, enter a description for the vNSP Cluster.

6 If you have not yet created a vNSP Controller, click + to create one.

   After creating the vNSP Controller, click Other Actions | Test Connection the connectivity of the Manager with the AWS environment and the vNSP Controller.

   If you have already created one, select it from the drop-down list.

   The vNSP Controllers field allows you to specify vNSP Controller information.

   For information about creating a vNSP Controller, refer section Configure a vNSP Controller on page 213.
7 Enter the **Shared Secret** key that will be used by the Sensor to establish communication with the Manager.

   ![Enter the Shared Secret key](image)

   You must enter the same shared secret key while creating the Sensor template AMI.

For information about launching the Sensor instance, refer section **Launch the Virtual IPS Sensor AMI instance** on page 229.

8 Click **Save** to save the details to the Manager database.

9 After you click save, a confirmation window displays the successful creation of the vNSP Cluster, and it prompts you to create a Protected group.

   ![Confirmation window](image)

   Click **OK** to create a Protected group.

   For information about creating a Protected group, see section **Create a protected group** on page 226.

10 To download Virtual Probe for a selected vNSP cluster, select **Endpoint Actions | Download Virtual Probe Installer for: <vNSP Cluster>**.

   For more information, see section **Download the Virtual Probe** on page 234.
11 To view the managed endpoints per cluster, select **Endpoint Actions** | **View Managed Endpoints**. A window with the list of managed endpoints is displayed.

Figure 4-15 List of managed endpoints

12 To delete a vNSP Cluster, select it and click **Cancel** to return to the vNSP Clusters page.

13 Click **Save as CSV** to save the information in the form of a .csv file. The default CSV file name is ManagedEndpoints.csv.

**Create a protected group**

A protected group is a group of virtual machines in AWS environment. Virtual machines can be added to protected VM group by adding the AWS subnets that they belong to. All virtual machines in a protected VM group redirect their traffic to the selected vNSP Cluster for inspection. Security policies can be applied to protected groups.

A virtual machine can have more than one network interface, each belonging to a different subnet. As a result, a virtual machine can belong to multiple protected groups.
Task

1. In the Manager, select Devices | <Admin Domain Name> | Global | vNSP Clusters.

2. The vNSP Clusters page displays the available vNSP Clusters currently. Selecting any of the vNSP Clusters displays these specific details of the VM groups protected by it.

<table>
<thead>
<tr>
<th>Column</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Name of the protected group.</td>
</tr>
<tr>
<td>Description</td>
<td>Description for the protected group.</td>
</tr>
<tr>
<td>VPC</td>
<td>Name of the VPC from which virtual machines are assigned to this group.</td>
</tr>
<tr>
<td>Protected Objects</td>
<td>Subnets belonging to the chosen VPC.</td>
</tr>
<tr>
<td>Advanced Probe Settings</td>
<td>Traffic Processing — Direction of the traffic that is considered for inspection. Inspection Mode — Mode of traffic inspection used by the Virtual IPS Sensor.</td>
</tr>
<tr>
<td>Last Updated</td>
<td>Time — Time when the protected group was last updated. By — User who modified the protected group.</td>
</tr>
</tbody>
</table>

3. To create a new protected group, select the vNSP Cluster for which a protected group has to be created, and click the icon in the Protected Groups for: <vNSP Cluster name> section.

The Add Protected Group window opens.
Enter the required details:

**Table 4-9 Option definitions**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Enter the unique group name to identify the protected group. The name can contain up to 50 alphanumeric (upper or lower case letters and numbers) characters, including hyphens, underscores and periods. The name must begin with a letter.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for your protected group.</td>
</tr>
<tr>
<td>vNSP Cluster</td>
<td>Displays the name of the vNSP Cluster for which the VM group is created.</td>
</tr>
<tr>
<td>vNSP Controller</td>
<td>Displays the environment in which the vNSP Cluster resides.</td>
</tr>
<tr>
<td>VPC</td>
<td>Select the VPC from which the VMs have to be assigned to this protected group.</td>
</tr>
<tr>
<td>Available</td>
<td>Displays the list of subnets available under the selected VPC. Click the icon to move the subnet from the Available list to the Selected list.</td>
</tr>
<tr>
<td>Selected</td>
<td>Displays the list of subnets under the selected VPC to be protected. A VM group can span Availability Zones but it is recommended to have separate vNSP Cluster for each Availability Zone and as a result VM groups are separated by Availability Zones.</td>
</tr>
</tbody>
</table>

**Advanced Probe Settings**

| Traffic Processing | Traffic direction that is inspected. Both ingress and egress are inspected by default.                                                                                                          |
| Inspect Mode       | Select the mode of inspection by the Virtual IPS Sensor.IPS — Deploys the Sensor in prevention mode where attacks can be blocked. IDS — Deploys the Sensor in detection mode where attacks are detected and a TCP channel is reset. |
| Save               | Click to save the settings that creates a protected group.                                                                                                                                     |
To edit the settings for the protected group, double-click the protected group for which you want to edit the settings. The **Add Protected Group** window opens. Make the required changes and click **Save** to save the changes.

You can edit the group name, description, direction of traffic which is inspected, inspection mode, VPC, and the subnets selected for the VPC.

To delete a protected group, select the group that you want to delete and click ![Delete](image). In the **Confirmation** window, click **OK** to delete the selected protected group, or click **Cancel** to return to the **vNSP Clusters** page.

Click **Save as CSV** to save the information to the Manager database in the form of a .csv file.

### Launch the Virtual IPS Sensor AMI instance

**Before you begin**

You will need an Amazon S3 Bucket to store the shared secret key. To conceal the S3 Bucket URL you can generate a signed URL using the following steps:

1. Limit the access to the Amazon S3 bucket to the user who will be using the shared secret key.
2. Using an example Python script (such as the one provided in the link below) and the user’s Access Key and Secret Key create a signed URL.
   
   This [link](#) takes you to a sample script to generate the signed URL for the S3 bucket.

3. Execute the following command in the command prompt to run the script:

   ```bash
   ./<Script_Name>.py -b S3BucketName -p Sharedkey.txt --expiry=<Duration> -a <AccessKey> -s <SharedKey>
   ```

<table>
<thead>
<tr>
<th><strong>Table 4-10 Option definitions</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key</strong></td>
</tr>
<tr>
<td>Script_Name</td>
</tr>
<tr>
<td>S3BucketName</td>
</tr>
<tr>
<td>Sharedkey.txt</td>
</tr>
<tr>
<td>Duration</td>
</tr>
<tr>
<td>AccessKey</td>
</tr>
<tr>
<td>SharedKey</td>
</tr>
</tbody>
</table>
As part of Network Security Platform deployment, you have to launch an instance of the Virtual IPS Sensor in the AWS environment. The Sensor image provided to you in the form an AMI is the template AMI. To launch an instance using the template AMI, follow the steps below.

Sensors can be launched as part of an AWS Auto Scaling group. You should create a Launch Configuration similar to the settings provided below. See Create an auto scaling group for Virtual IPS Sensors in AWS on page 243 for more information on how to use sensor auto scaling.

**Task**

1. Log in to the AWS console, and navigate to Services | EC2.
2. In the left panel, under IMAGES, click AMIs.
3. Search for the AMI ID of the Virtual IPS Sensor and click Launch.
4. Under the Choose the Instance type tab, select the instance type as c4.xlarge (vCPUs: 4, Memory 7.5GB), and click Next: Configure Instance Details.
5. In the Configure Instance page, from the drop-down lists for Network and Subnet, choose the Management network and the corresponding subnet.
6. (Optional) If you are using the User Data to launch the Sensor instance, in the Advanced area enter the following information in the User data to register the Sensor with the Manager:

   If you are using the customized AMI method to launch the Sensor image, skip this step and proceed to step 7.

   ```json
   {"Primary NSM IP": "10.x.x.x", "Cluster Name": "Cluster_Name", "Cloud Data URL": "URL_for_S3_bucket"}
   ```

   If you have an MDR pair, use the following user data to establish trust between the Manager pair and the Sensor:

   ```json
   {"Primary NSM IP": "10.x.x.x", "Secondary NSM IP": "10.x.x.x", "Cluster Name": "Cluster_Name", "Cloud Data URL": "URL_for_S3_bucket"}
   ```

   The user data is represented in JSON and represents the following information.

   **Table 4-11 Option definitions**

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary NSM IP</td>
<td>IP address of the Primary Manager.</td>
</tr>
<tr>
<td>Secondary NSM IP</td>
<td>IP address of the Secondary Manager.</td>
</tr>
<tr>
<td>Cluster Name</td>
<td>Name of the vNSP Cluster to which this Sensor belongs to.</td>
</tr>
<tr>
<td>Cloud Data URL</td>
<td>Signed URL for the Shared Secret Key file in Amazon S3 bucket.</td>
</tr>
</tbody>
</table>

7. Scroll down and expand the Network interfaces menu option. Click Add Device to add a second interface.

   The first interface, eth0, is the management port of the Sensor. If you have defined a second interface for the Manager, enter the IP address of that interface for Sensor-Manager communication. The second interface, eth1, is for the monitoring and response ports in IDS configuration. For eth1, select the subnet in which the VMs to be protected reside.

8. Under the Add Storage tab, use the default Size (64 GiB), and click Next: Add Tags.

10 In the **Configure Security Group** page, you can create a new Security Group to define the firewall rules to control traffic to the Sensor or choose an existing Security group.

Once you have configured the Security Group, click on **Review and Launch**.

11 Under the **Review Instance Launch** page, review the details provided for the creation of the instance. You can either edit specific details or click on **Launch** to assign a key pair to your Sensor instance.
12 In the Select an existing key pair or create a new key pair window, you can either choose an existing key pair or create a new key pair, and click Launch instances. The instance is now launched.

13 (Optional) If you are using the customized AMI method to launch the Sensor image, complete the steps in Create a customized AMI for Controller or Sensor on page 233.

Tasks

- Create a customized AMI for Controller or Sensor on page 233
- Register the vNSP Controller or Virtual IPS Sensor with the Manager on page 234

Create a customized AMI for Controller or Sensor

A customized AMI is a snapshot of the template AMI. Follow the steps below to create a customized AMI. You are creating a customized AMI that contains the shared secret key used to register the Controller or Sensor with the Manager. Later, this AMI can be used to instantiate other instances without needing to configure the secret.

Task

1 After launching the instance of the Controller or Sensor using the template AMI, set the shared secret key for the instance.

While configuring the Controller instance details, scroll down to Advanced Details, and provide the User data in the format shown below.

```
"Controller Shared Key"="Controller_Sharet_Key"
```

The shared secret key for the Sensor can be set using two methods:

- Log in to the Sensor and set the Shared secret key using the CLI command `set cloud-cluster sharedsecretkey`.
- While configuring the instance details, scroll down to Advanced Details, and provide the User data in the format shown below.

```
{"Sensor Shared Key":"Sensor_Sharet_Key"}
```

The user data is represented in JSON and represents the following information.
### Table 4-12  Option definitions

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller Shared Key</td>
<td>Shared Secret Key for the Controller.</td>
</tr>
<tr>
<td>Sensor Shared Key</td>
<td>Shared Secret Key for the Sensor.</td>
</tr>
</tbody>
</table>

2. Take a snapshot of the Sensor AMI. This is the customized AMI. It may take up to 15 minutes to initialize the Sensor and push the signature set and initialize the Virtual Probe.

   For more information on launching an instance, refer section *Create a customized AMI for Controller or Sensor* on page 233.

3. Terminate the instance of the Controller or Sensor.

### Register the vNSP Controller or Virtual IPS Sensor with the Manager

To register the for Controller or Virtual IPS Sensor with the Manager, follow the steps below.

**Task**

1. Create the customized AMI.
   
   For information on the procedure to create a customized AMI, refer section *Create a customized AMI for Controller or Sensor* on page 233.

2. Launch an instance using this customized AMI.
   
   For information on the procedure to launch a Controller instance, refer section *Launch the vNSP Controller AMI instance* on page 219.
   
   For information on the procedure to launch a Sensor instance, refer section *Create a customized AMI for Controller or Sensor* on page 233.

### Stop a Virtual IPS Sensor instance

You can stop a Virtual IPS Sensor instance from the AWS console. However, it is recommended to stop a Sensor instance by executing the `shutdown` command from the Sensor CLI.

### Limiting SSH connections to Virtual IPS Sensor

The Virtual IPS Sensor can have many concurrent connections at any given time. It is recommended to restrict SSH access to Virtual IPS Sensor to provide security to the Sensor. You can restrict the access by allowing only certain network range or IP address to login to the Sensor. You can add the network range and IP address (IPv4 and IPv6 addresses) in the *Advanced Device Settings* page of the Manager which restricts the number of SSH connections. The IP address of the client trying to connect to the Sensor should be added to the list so that only those valid IP addresses are allowed to access the Sensor. You can add it at the global level for an admin domain or at the device level.

To add the network range or IP address for SSH access to the Sensor, see the section *Configure advanced device settings* in the *McAfee Network Security Platform IPS Administration Guide*.

### Download the Virtual Probe

A Virtual Probe has to be installed on every instance that has to be protected by Network Security Platform. In order to install a Virtual Probe, you will have to first download the Probe Installation Package from the Manager.

> Just installing the Virtual Probe does not ensure security.

Follow the steps given below to download the Probe Installation Package.
Task
1 In the Manager, select Devices | Global | vNSP Clusters.
2 From the vNSP Clusters section, select a cluster, and select Endpoint Actions | Virtual Probe Actions | Download Probe Installer for: <vNSP Cluster Name> | <OS> Virtual Probe.

![Probe packages are specific to vNSP Clusters. They cannot be interchanged across clusters.]

3 The Probe Installation Package with the file name NSPVirtualProbe.tar.gz will be downloaded onto your machine.

Install the Virtual Probe
The procedure to install a Virtual Probe on your virtual machine is specific to the Operating System running on it. This section provides the installation steps for Linux and Windows virtual machines.

For Linux virtual machines
To install the Virtual Probe on your Linux machines, as a root user, follow the steps below.

Task
1 Move the downloaded Probe Installation Package NSPVirtualProbe.tar.gz into an appropriate folder.
2 To unzip the package, execute the command:
   ```
   $ tar xzf NSPVirtualProbe.tar.gz
   ```
3 To install the package, run the command:
   ```
   ./install-zlink.sh
   ```
   The Virtual Probe is now installed on your Linux machine.

For Windows virtual machines
To install the Virtual Probe on your Windows Virtual Machines, as an administrator, follow the steps below.

Task
1 Move the downloaded Probe Installation Package NSPVirtualProbe.tar.gz into an appropriate folder.
2 Navigate to the folder where your Probe Installation Package is installed and unzip it.
3 At the command prompt, navigate to the location of your batch file and run it using the command:
   ```
   install.bat
   ```
4 The command window will hang for a few seconds and disappear. This indicates the completion of the installation process.

Deploy Virtual Probes through orchestration methods
Tools like Chef, Puppet, and Ansible can be used to deploy the probes in virtual machines. It can also be installed through Cloud-Init mechanism that runs scripts during instance launch. To use install the probe programmatically through a Linux Shell, perform the following steps:

1 Download the Probe from Network Security Manager using an HTTPS link.
   ```
   https://<NSM host>/sdkapi/cloud/cluster/downloadprobeagent?name=<vNSP Cluster Name>&ostype=<OS type>
   ```
   For example:
   ```
   ```

Where,

- NSM host is the Manager's IP address or domain name
- vNSP Cluster Name is the name of the vNSP Cluster that should secure the virtual machine
- OS type is linux or windows

Ensure that the URL is given within double quotation marks. This is to prevent the shell from interpreting characters in the URL.

2 Install the Probe using the steps described earlier in this section.

To allow virtual machines to download the probe, you have to open the security group on the Manager to allow inbound connections from your virtual machines.

The Manager has a limitation on the number of simultaneous downloads of the probe. If the download does not succeed, try again later.

**View summary details of a selected vNSP Cluster**

You might want to view the details of vNSP Cluster instances in the Manager.
Task

1. In the Manager, select Devices | <Admin Domain Name> | Devices | <vNSP Cluster> | Summary. The device Summary page displays.

Figure 4-16  Summary details of a virtual security system

Table 4-13  Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Displays whether there are pending changes to be deployed to the virtual security system or if it is up to date. Green indicates that the system is up to date and blue indicates that there are pending changes to be deployed.</td>
</tr>
<tr>
<td>Device Type</td>
<td>The type of device. For example, vNSP Cluster.</td>
</tr>
<tr>
<td>vNSP Controller</td>
<td>Displays the name of the vNSP Controller.</td>
</tr>
<tr>
<td>Controller Software</td>
<td>Displays the vNSP Controller image version that is currently installed.</td>
</tr>
<tr>
<td>Virtual Probe Software</td>
<td>Displays the Virtual Probe image version that is currently installed.</td>
</tr>
<tr>
<td>Member Sensor Software</td>
<td>Displays the Sensor software version that is currently installed.</td>
</tr>
<tr>
<td>Name</td>
<td>Display the status and name of the Sensor instance.</td>
</tr>
<tr>
<td>Protections</td>
<td>Displays the Software, Signature set, and Callback Detector versions of the Sensor.</td>
</tr>
<tr>
<td>Last Deployment</td>
<td>The time stamp of when pending changes were deployed last.</td>
</tr>
<tr>
<td>Software</td>
<td>Displays the version of the Sensor and status and version of the Virtual Probe.</td>
</tr>
<tr>
<td>Monitoring Port IP</td>
<td>The Monitoring Port IP address configured for the Sensor.</td>
</tr>
<tr>
<td>Management Port</td>
<td>The network settings of Virtual IPS Sensor.</td>
</tr>
<tr>
<td>Last Reboot</td>
<td>The time stamp of when a Virtual IPS Sensor instance was last restarted.</td>
</tr>
</tbody>
</table>

2. To update the vNSP Cluster details, click Edit Cluster. You can edit the Description and the Sensor the vNSP Cluster is associated with.

3. To view details of a managed endpoint:
   a. Select Endpoint Actions | View Managed Endpoints.

4. To download Virtual Probe, select Virtual Probe Actions | Download Probe Installer for: <vNSP Cluster Name> | <OS> Virtual Probe.
5. To restart the Sensor, click **Member Sensor Actions | Reboot**.

6. To run a diagnostic trace for the Sensor, click **Member Sensor Actions | Run diagnostics**.

7. To export the Sensor software information in the form of a .csv file, click **Save as CSV**.

### Uninstall the Virtual Probe

The procedure to uninstall a Virtual Probe from your virtual machines is Operating System specific. Uninstalling probes from virtual machines in a Protected VM group stops the redirection of traffic to the Virtual IPS Sensor.

**For Linux machines**

#### Before you begin

Before you attempt to uninstall a Virtual Probe from your Linux machine, ensure that you have RPM Package Manager installed.

To uninstall a Virtual Probe from your Linux machine, run the following commands.

**Task**

1. `rpm -e zasa`
2. `rpm -e zasa-dep`

**For Windows machines**

To uninstall a Virtual Probe from your windows machine, follow the steps below.

**Task**

1. From the Task Manager, stop the zasa service.
2. Navigate to **Control Panel | Programs | Programs and features**. Right click *z-link* and select **Uninstall**.

### Jumbo frame parsing

Jumbo frames are Ethernet frames, which carry larger payloads per packet than the standard Ethernet frame. They are designed to enhance network throughput and improve CPU utilization for large file transfers, by enabling more efficient payloads per packet. For example, a jumbo frame size packet can carry more than 1500 bytes of payload in an Ethernet frame.

Network Security Platform parses jumbo frames in attack detections. The Virtual IPS Sensors in the public cloud environment support jumbo frame parsing in the inline, tap, and SPAN modes.

- Jumbo frame parsing is supported for a maximum IP payload of 9KB (9216 bytes).

**Tasks**

- *Enable jumbo frame parsing from the Manager* on page 238
- *Enable jumbo frame parsing for auto-scaled Sensors* on page 240

### Enable jumbo frame parsing from the Manager

For the Virtual IPS Sensors in a vNSP Cluster to inspect jumbo frames for attacks and other supported IPS features, you must enable jumbo frame parsing at the vNSP Cluster level.
**Task**

1. In the Manager, select Devices | <Admin Domain Name> | Devices | <vNSP Cluster> | Setup | Advanced | IP Settings tab.

2. In the **Common IP Parameters** section of the IP Settings page, select **Enabled** from the **Jumbo Frame Parsing** drop-down list and click **Update** to update the Sensor of the configuration change.

![Common IP Parameters dialog](image-url)

If your Virtual IPS Sensors are running pre-9.1 software, you will need to reboot them for the changes to be effective.

**Enable jumbo frame parsing from the Sensor**

For the Sensor to inspect jumbo frames for attacks and other supported IPS features, you must enable jumbo frame parsing at the Sensor level. To enable jumbo frame parsing, use the following CLI command from the Virtual IPS Sensors.

**Syntax:**

```
set jumboframeparsing <enable|disable>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;enable&gt;</td>
<td>Enables the jumbo frame parsing feature.</td>
</tr>
<tr>
<td>&lt;disable&gt;</td>
<td>Disables the jumbo frame parsing feature.</td>
</tr>
</tbody>
</table>

If your Virtual IPS Sensors are running pre-9.1 software, you will need to reboot them for the changes to be effective.

**Default Value:**

The jumbo frame parsing feature is disabled by default.

**View the status of jumbo frame parsing feature**

The `show jumboframeparsing status` CLI command shows whether the status of the jumbo frame parsing feature is enabled or disabled. This command has no parameter.

**Syntax:**

```
show jumboframeparsing status
```

**Sample Output:**

```
intruShell@john> show jumboframeparsing status
Jumbo Parsing Status : Enabled
```

You can create a customized AMI with jumbo frame parsing enabled that will allow you to create many instances from it.
Enable jumbo frame parsing for auto-scaled Sensors

In auto scaling of Virtual IPS Sensors where you need to scale a number of instances, follow the steps below to enable jumbo frame parsing.

The following steps are applicable if your Virtual IPS Sensors are running pre-9.1 software. You will need to reboot the Virtual IPS Sensors for the changes to be effective. If your Virtual IPS Sensors are running 9.1 software, jumbo frame parsing can be enabled from the Manager.

Task

1. Log in to the AWS console, and navigate to Services | EC2.

2. Launch a new Sensor instance from an AMI. This instance should only be a template and not contain any user data. For more information on launching an instance, see the section Launch the Virtual IPS Sensor AMI instance on page 229.

3. Log in to the Sensor.

4. Enable jumbo frame parsing using the command `set jumboframeparsing enable`.

5. Reboot the Sensor.

6. Log in to the Sensor to check if jumbo frame parsing is enabled by executing the command `show jumboframeparsing status`.

7. In the AWS console, create a Sensor image by selecting Create image under Actions.

   ![Actions](image)

   After creating Sensor image ensure that the image is seen under AMIs.

8. Go to Services | Compute | EC2 and click Launch Configurations under AUTO SCALING located in the left panel.

9. Click Create launch configuration.

10. Select the newly created jumbo frame parsing enabled AMI.

    For more information on auto scaling, see the section Auto scaling of Sensors to improve traffic throughput on page 241.
Auto scaling of Sensors to improve traffic throughput

An AWS auto scaling group contains a collection of EC2 instances that share similar characteristics and are treated as a logical grouping for the purposes of instance scaling and management. The auto scaling group is an AWS service that provides a method to increase or decrease the Virtual IPS Sensors based on the traffic load in the network. For more information on AWS auto scaling groups, see AWS auto scaling groups.

Virtual IPS Sensors auto scaling in AWS

Load balancing among the Virtual IPS Sensors provides the capability to handle higher network throughput. This is achieved due to the Virtual IPS Sensor scale out capability in auto scaling groups. As the traffic in the network increases, the Virtual IPS Sensors are launched through the auto scaling feature in AWS. In case of excessive traffic flows, a single Virtual IPS Sensor may be overloaded due to which the traffic may not be inspected. In such a scenario, auto scaling of Virtual IPS Sensors is capable of handling excessive flows by launching new instances of the Sensor. This way the traffic load is evenly distributed among the Virtual IPS Sensors.

Virtual Probes are able to load balance traffic to all of the Virtual IPS Sensors in the vNSP Cluster. The distribution is done on a flow by flow basis. Probes are able to send traffic to a newly launched Sensor as well as redirect traffic from a Sensor that is removed due to a scale-in event.

TCP Flow Violation feature must be set to Permit out-of-order for vNSP Clusters that are enabled for auto scaling.

You can configure the limit to launch a new Virtual IPS Sensor in auto scaling groups. When the traffic load in the network reaches the configured limit, a new Virtual IPS Sensor instance is launched and a part of the traffic is redirected to the new Sensor instance. The auto scaling group launches new instances of the Virtual IPS Sensor based on the alarm configured for “CPU Utilization” and “Network In” parameters through AWS cloudwatch. The AWS cloudwatch maintains the alarms and monitors the traffic throughput. When the traffic exceeds the configured limit, it notifies the auto scaling group to launch a new instance of the Virtual IPS Sensor.

The Virtual IPS Sensors are either in active state or inactive state which depends on whether the Probe in each virtual machine is able to forward traffic to a Sensor. The list of active and inactive Sensors are maintained by the Probes to forward traffic.
The vNSP cluster uses the AWS auto scaling group to provide a method to increase the bandwidth of traffic to be inspected. Auto scaling groups use the scale out and scale in concept for launching the Virtual IPS Sensor. Instead of using a single Sensor to handle traffic, multiple Sensors with the same configurations are used. This provides failover for Sensors, that is, even if one Sensor becomes inactive or is terminated, the traffic load is distributed between the other active Sensors in the cluster.

While designing your network for auto scaling, it is recommended to have a VPC dedicated for vNSP cloud solution which includes the Virtual IPS Sensor, vNSP Controller, and the Network Security Manager. VPC peering makes sure that the traffic from the VPC to be protected is directed to the security VPC.

It is also recommended to have separate vNSP Clusters for each Availability Zone. This provides Availability Zone level redundancy as well as avoids the cost of forwarding traffic from one zone to another for inspection.

Following are some scenarios under which the Virtual IPS Sensors are auto-scaled:

- You can configure to launch new Virtual IPS Sensors when the traffic exceeds the CPU utilization of Sensors or bandwidth to the Sensors exceed the threshold in AWS. You can also launch new Sensors based on custom monitoring configured for virtual machines.
- A Virtual IPS Sensor instance is terminated when the condition used to launch an instance no longer exists.
- To maintain the minimum number of Sensors configured in auto scale, a new Virtual IPS Sensor instance is launched when a Sensor instance is terminated.
- New Virtual IPS Sensor instances are not launched when a Sensor reboots or is down due to network failure. The Sensor is moved to the inactive list till the time it is active again.

**Configuration of Sensors to protect Web Servers with an Elastic Load Balancer (ELB)**

Web Servers are launched behind Elastic Load Balancers in AWS. In such a case the true client IP of the web server is not displayed when alerts are generated for an attack. To view the true client IP of the web server, you have to enable the XFF header feature in the Network Security Manager. For more information on XFF header feature, see *McAfee Network Security Platform IPS Administration Guide*.

**vNSP cluster configuration**

The Network Security Manager manages the Virtual IPS Sensor instances launched in AWS. The vNSP cluster is a group of Virtual IPS Sensors. The virtual machines in a VPC are protected by the Virtual IPS Sensors assigned to that VPC. You can add multiple VPC groups to be protected within a vNSP cluster. All the Virtual IPS Sensors in a cluster have the same policies, attack detection methods, rules, signature sets and software versions.
Before creating a launch configuration for auto scaling group, you have to first create a vNSP cluster for auto scale in the Network Security Manager. For more information on creating a cluster, see the section Create a vNSP Cluster on page 222.

Create an auto scaling group for Virtual IPS Sensors in AWS

The AWS deployment to auto scale Virtual IPS Sensors is created under the Auto Scaling Groups option in the AWS interface. A new Virtual IPS Sensor instance is launched in AWS based on the alarms configured under the auto scaling policy. You have to first define the launch configuration before creating an auto scaling groups. All Sensor instances launched in an auto scaling group will have the same configuration since it is based on the launch configuration defined for the group. You can launch an auto scaling group for Sensors with or without an AWS Elastic Load Balancer. You can also configure an auto scaling group by defining the required parameters through scripts. For more information on auto scaling groups, see AWS auto scaling groups.

In the Network Security Manager, it is recommended to create a new vNSP Cluster for auto scaling Sensors. You cannot convert an existing cluster to auto scaling Sensors.

High level steps to configure an auto scale group

Before you begin

- Only permit out-of-order flows can be inspected by the Virtual IPS Sensor for auto scaling groups. To use the auto scaling feature, do not change the settings for TCP Flow Violation in the Network Security Manager under Devices | <Admin Domain Name> | Devices | <Device Name> | Setup | Advanced | Protocol Settings.
- Network Security Manager has to be installed with the required settings.
Configure the vNSP Controller in Network Security Manager.
• Install the Virtual Probe in the virtual machine to be protected.
• Define the customized AMI from AWS Marketplace with the shared secret key.
• Create an IAM role with the required rights to add and modify an interface enabled.
• Create a launch configuration for the auto scaling group along with user data that defines the Network Security Manager IP address and the vNSP Cluster name.
• AWS cloudwatch services enabled to create new alarms that triggers launching of new instances.

To create an auto scaling group for Sensors without an AWS elastic load balancer, follow the steps below:

**Task**
1. Create a vNSP Cluster in Network Security Manager. See the section, Create a vNSP Cluster on page 222.

2. Create a launch configuration for auto scaling groups in AWS with the following recommended settings:
   • Select only the IAM role you created with the necessary rights enabled. To create the required IAM role, see the topic Create IAM roles and policies on page 196
   • Virtual IPS Sensor AMI that has the Network Security Manager shared secret key enabled. To create the customized Sensor AMI, see the topic Create a customized AMI for Controller or Sensor on page 233
   • User data containing Network Security Manager IP address and the vNSP Cluster name. It is recommended to use the same Cluster name defined in the Network Security Manager. To establish the trust with Network Security Manager, see the topic Create IAM roles and policies on page 196

3. Create an auto scaling group in AWS. Create alarms that contains the thresholds for increasing or decreasing the number of instances.

4. Create scheduled actions for launching the Virtual IPS Sensor instances one after the other.

5. Define cloudwatch events in the cloudwatch console.

**Create a launch configuration with the Virtual IPS Sensor AMI**

The Virtual IPS Sensor image is available under My AMIs tab in AWS. You have to create a launch configuration using the Virtual IPS Sensor AMI. For auto scaling groups feature, a launch configuration has to be defined first before creating an auto scaling group. While creating an auto scaling group, this launch configuration has to be selected to launch new Virtual IPS Sensor instances. The Network Security Manager IP address and Cluster name are defined in the launch configuration.

**Task**
To create a launch configuration for auto scaling groups, follow the steps below:

1. In AWS, go to Services | Compute | EC2.

2. In the left panel, under AUTO SCALING, click Launch Configurations.

3. Click Create launch configuration.
4 Under **Create Launch Configuration**, go to the **My AMIs** tab, search the required AMI and click **Select**.

5 Under the **Choose Instance Type** tab, select the instance type as **c4.xlarge** (vCPUs: 4, Memory 7.5GB), and click **Next: Configure details**.
6 In the **Configure details** page, enter the name for the launch configuration and define the Network Security Manager IP address and the vNSP Cluster name.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name of the launch configuration.</td>
</tr>
<tr>
<td>Purchasing option</td>
<td>Request Spot Instances to name your own price for the instance types and lower your overall computing cost for time-flexible interruption-tolerant tasks.</td>
</tr>
<tr>
<td>IAM role</td>
<td>IAM roles allow you to manage permissions of IAM users and AWS services to your EC2 resources. Select the IAM role you created with the &quot;Network Administrator&quot; rights enabled. For the script to create an IAM role, see the topic <strong>High level steps to configure an auto scale group</strong> on page 243.</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Enables you to monitor, collect, and analyze metrics about your instances through Amazon CloudWatch.</td>
</tr>
<tr>
<td>EBS-optimized instance</td>
<td>Enables additional, dedicated throughput between Amazon EC2 and Amazon EBS, and therefore improved performance for your Amazon EBS volumes.</td>
</tr>
<tr>
<td>Advanced details</td>
<td></td>
</tr>
<tr>
<td>Kernel ID</td>
<td>Available kernels that you can use for your instance.</td>
</tr>
<tr>
<td>RAM Disk ID</td>
<td>A RAM disk that contains the necessary drivers (such as Xen drivers or video drivers) to make the chosen kernel work.</td>
</tr>
<tr>
<td>User data</td>
<td>You can specify user data to configure an instance or run a configuration script during launch. If you launch more than one instance at a time, the user data is available to all the instances in that reservation. You have to provide the Network Security Manager IP address, vNSP Cluster name, subnet, and the security group name in the script. For the script to define the parameters, see the topic <strong>High level steps to configure an auto scale group</strong> on page 243.</td>
</tr>
<tr>
<td>IP Address Type</td>
<td>When you launch an instance into your Amazon Virtual Private Cloud (VPC), you can optionally assign a public IP address to it.</td>
</tr>
</tbody>
</table>
7 Click **Next: Add Storage**.
Under the Add Storage page, define the database server details.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume Type</td>
<td>Amazon EBS is a block-level storage volume that persists independently from the lifetime of an EC2 instance, so you can stop and restart your instance at a later time.</td>
</tr>
<tr>
<td>Device</td>
<td>The available device names for the volume. Depending on the block device driver of the selected AMI's kernel, the device may be attached with a different name than what you specify.</td>
</tr>
<tr>
<td>Snapshot</td>
<td>A snapshot is a backup of an EC2 volume that’s stored in S3.</td>
</tr>
<tr>
<td>Size (GiB)</td>
<td>Volume size must be greater than zero or the size of the snapshot used.</td>
</tr>
<tr>
<td></td>
<td>Use the default size as 64 GiB.</td>
</tr>
<tr>
<td>Volume Type</td>
<td>General Purpose (SSD) volumes can burst to 3000 IOPS, and deliver a consistent baseline of 3 IOPS/GiB.</td>
</tr>
<tr>
<td>IOPS</td>
<td>The requested number of I/O operations per second that the volume can support.</td>
</tr>
<tr>
<td>Throughput</td>
<td>Throughput that the volume can support is specified for Streaming Optimized volumes: ST1 and SC1.</td>
</tr>
<tr>
<td>Delete on Termination</td>
<td>EBS volumes persist independently from the running life of an EC2 instance.</td>
</tr>
<tr>
<td></td>
<td>Ensure that Delete on Termination checkbox is selected.</td>
</tr>
<tr>
<td>Encrypted</td>
<td>Volumes that are created from encrypted snapshots are automatically encrypted, and volumes that are created from unencrypted snapshots are automatically unencrypted. If no snapshot is selected, you can choose to encrypt the volume.</td>
</tr>
</tbody>
</table>

The management and data subnets should be configured in the same availability zone as the instance for the deployment to be successful.

Click Next: Configure Security Group.
10 In the Configure Security Group page, you can create a new Security Group to define the firewall rules to control traffic to the Sensor or choose an existing Security group.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign a security group</td>
<td>Create a security group or assign an existing security group.</td>
</tr>
<tr>
<td>Security group name</td>
<td>Name for the security group.</td>
</tr>
<tr>
<td>Description</td>
<td>Description for the security group.</td>
</tr>
<tr>
<td>Type</td>
<td>The protocol to open to network traffic. You can choose a common protocol, such as SSH (for a Linux instance), RDP (for a Windows instance), and HTTP and HTTPS to allow Internet traffic to reach your instance. You can also manually enter a custom port or port ranges.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The type of protocol, for example TCP or UDP. Provides an additional selection for ICMP.</td>
</tr>
<tr>
<td>Port Range</td>
<td>For custom rules and protocols, you can manually enter a port number or a port range.</td>
</tr>
<tr>
<td>Source</td>
<td>Determines the traffic that can reach your instance. Specify a single IP address, or an IP address range in CIDR notation (for example, 203.0.113.5/32).</td>
</tr>
</tbody>
</table>

11 Click **Review** to review the details for the AMI instance, and click **Create launch configuration**. The launch configuration is created and is available in the list of launch configurations.

12 To delete a launch configuration, select the launch configuration, click **Actions**, and then click **Delete launch configuration**.

**Create an auto scaling group**

An auto scaling group provides the capability to handle higher traffic throughput by launching new Virtual IPS Sensor instances.

**Task**

1. In the AWS under **Services | EC2 | Compute**.
2. In the left panel, under **AUTO SCALING**, click **Auto Scaling Groups**.
3 Click Create Auto Scaling Group. The Create Auto Scaling Group page opens.

4 Select Create an Auto Scaling group from an existing launch configuration, select the required AMI, and click Next Step.

   The Create Auto Scaling Group page opens.
5 Define the network, subnet and name for the group.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Launch Configuration</td>
<td>The name of the launch configuration associated with this auto scaling group.</td>
</tr>
<tr>
<td>Group name</td>
<td>Name of the auto scaling group.</td>
</tr>
<tr>
<td>Group size</td>
<td>Number of instances the group should have at any time.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>When creating the auto scaling group for the first time, you have to launch only one Sensor instance and then create scheduled actions to launch the other Sensor instances.</td>
</tr>
<tr>
<td>Network</td>
<td>Launch your instance into an Amazon VPC to get complete control over your virtual networking environment.</td>
</tr>
<tr>
<td>Subnet</td>
<td>Subnet where the virtual machines exist.</td>
</tr>
<tr>
<td>Load Balancing</td>
<td>Classic load balancers attached to the auto scaling group.</td>
</tr>
<tr>
<td>Health Check Grace Period</td>
<td>The length of time that auto scaling waits before checking an instance's health status.</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Enables you to monitor, collect, and analyze metrics about your instances through Amazon cloudwatch.</td>
</tr>
<tr>
<td>Instance Protection</td>
<td>If protect from scale in is set, newly launched instances will be protected from scale in by default. auto scaling will not select protected instances for termination during scale in.</td>
</tr>
</tbody>
</table>

6 Click **Next: Configure scaling policies**.
7 Define policies to increase or decrease the group size that is to launch a new instance or terminate an existing instance.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Increase Group Size</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Name for the alarm when a new instance is launched.</td>
</tr>
<tr>
<td><strong>Execute policy when</strong></td>
<td>Policy for which a new instance has to be launched.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Add new alarm</strong> directs you to cloudwatch where you can define new alarms. To add an alarm you have to have the cloudwatch services enabled.</td>
</tr>
<tr>
<td><strong>Take the action</strong></td>
<td>Action to be taken when the parameter reaches the configured limit.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Important note: You have to launch one Sensor instance per alarm. To launch multiple Sensor instances, you have to create multiple alarms with varying parameters for CPU utilization." /></td>
</tr>
<tr>
<td><strong>Instanced need</strong></td>
<td>Time interval between each launch instance.</td>
</tr>
<tr>
<td><strong>Decrease Group Size</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Name for the alarm when an instance has to be terminated.</td>
</tr>
<tr>
<td><strong>Execute policy when</strong></td>
<td>Policy for which the instance has to be terminated.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Add new alarm</strong> directs you to cloudwatch where you can define new alarms. To add an alarm you have to have the cloudwatch services enabled.</td>
</tr>
<tr>
<td><strong>Take the action</strong></td>
<td>Action to be taken when the parameter reaches the configured limit.</td>
</tr>
</tbody>
</table>

8 Click **Next: Configure Notifications**. Configure notifications to be sent to mail ID during an event of scale out or scale in.
<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send a notification to</td>
<td>Email ID to which the notification has to be sent.</td>
</tr>
<tr>
<td>Whenever instances</td>
<td>Parameter for which the notification has to be sent. The parameters are as follows:</td>
</tr>
<tr>
<td></td>
<td>• launch</td>
</tr>
<tr>
<td></td>
<td>• terminate</td>
</tr>
<tr>
<td></td>
<td>• fail to launch</td>
</tr>
<tr>
<td></td>
<td>• fail to terminate</td>
</tr>
</tbody>
</table>

9 Click Next: Configure Tags.
10 Define tags to the auto scale group which helps identify the group.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>Key name for the auto scaling group.</td>
</tr>
<tr>
<td>Value</td>
<td>Tag New Instances When this flag is set, the tag will also be applied to any newly launched instances in this Auto Scaling group.</td>
</tr>
</tbody>
</table>

11 Click Review to review the configuration defined for the group.

12 Click Create Auto Scaling Group. The auto scaling group is created and is available in the Auto Scaling Groups page.

13 To delete an auto scaling group, select the auto scaling group, click Actions, and then Delete.

Manage alarms using AWS cloudwatch

The alarms created for an auto scaling group are available in AWS cloudwatch. The alarms are created for an auto scaling group to increase or decrease the instances to be launched when the traffic reaches the configured limit. To access cloudwatch, you have to have the cloudwatch services enabled. To view the alarms configured for auto scaling groups in AWS, go to Services, and under the Management Tools section, click CloudWatch.
You can create new alarms and assign it to an auto scaling group from cloudwatch. You can also edit and view
the alarms configured. The trigger timing for an instance can be defined in cloudwatch.

Figure 4-20  CloudWatch alarms

You can view specific metrics in cloudwatch with regard to traffic load in the network. These are graphical
representation of the metrics that helps maintain traffic load in the network.

Figure 4-21  CloudWatch metrics
View the Virtual IPS Sensors launched in a vNSP cluster

You can view the health of the vNSP Sensor cluster in the **Health Check** in the Network Security Manager. The list of active and inactive Sensors is available in the **Summary** page of the Network Security Manager as either **Connected** or **Disconnected**. You can view the Virtual IPS Sensors launched in a vNSP Cluster under Devices | Admin Domain Name > Devices > Summary. The Sensor details are displayed in the Member Instances section. Hovering over the colored icon displays the status of the Sensor.

<table>
<thead>
<tr>
<th>Color</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Connected</td>
</tr>
<tr>
<td></td>
<td>Disconnected</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status</th>
<th>Connected</th>
</tr>
</thead>
</table>
| Connected |_ping

Use this page to view essential information about this vNSP cluster to manage its member sensors and discover virtual probe software for installation on endpoints.

![vNSP Cluster summary](image)

**Figure 4-22  vNSP Cluster summary**

Viewing alerts detected by vNSP cluster

You can view the alerts generated for an attack in the **Attack Log** page. The alerts generated are displayed for the cluster. Alert details for a vNSP Cluster does not display the Sensor name that detected the attack. It displays the cluster name followed by the IP address of the Sensor that detected the attack. To view the alerts generated, go to Analysis | Admin Domain Name > Attack Log.

![Viewing alerts in Attack Log](image)

**Figure 4-23  Viewing alerts in Attack Log**

Securing your Amazon Web Services (AWS) datacenter

Auto scaling of Sensors to improve traffic throughput

<table>
<thead>
<tr>
<th>No.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>256</td>
<td>McAfee Network Security Platform 9.1</td>
</tr>
</tbody>
</table>
Features not supported

The following features are not supported:

<table>
<thead>
<tr>
<th>Feature name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware detection of files downloaded using HTTP range request (Split file download)</td>
</tr>
<tr>
<td>Rate Limiting</td>
</tr>
<tr>
<td>Remediation</td>
</tr>
<tr>
<td>IPv6 traffic on Monitoring port (IPv6 traffic inspection)</td>
</tr>
<tr>
<td>IPv6 traffic support on the Management port</td>
</tr>
<tr>
<td>Monitoring Sensor Performance</td>
</tr>
<tr>
<td>Netflow export to NTBA</td>
</tr>
<tr>
<td>Passive Device Profiling</td>
</tr>
<tr>
<td>Traffic Prioritization with Application Content (Rate Limiting with App ID)</td>
</tr>
</tbody>
</table>

Best Practices

It is recommended to follow these practices while deploying Network Security Platform in AWS environment.

- Deploying Virtual IPS Sensors in the same availability zone as the virtual machines to be protected minimizes latency and costs.
- It is recommended to not share a vNSP Controller across different regions in the AWS environment.
- The vNSP Controller should be assigned a static IP address. Ensure that the security group allows intended communication only to the assigned static IP address.

Virtual IPS Sensor capacity by model number

The following table describes the supported Virtual IPS Sensor capacity.

Table 4-14 Virtual IPS Sensor capacity by model number

<table>
<thead>
<tr>
<th>Maximum Type</th>
<th>IPS-VM100</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregate Performance</td>
<td>550 Mbps</td>
</tr>
<tr>
<td>Maximum throughput with test equipment sending UDP packet size of 1518 bytes</td>
<td>Up to 700 Mbps</td>
</tr>
<tr>
<td>Concurrent connections</td>
<td>1,000</td>
</tr>
<tr>
<td>Connections established per second</td>
<td>600</td>
</tr>
<tr>
<td>Latency (Average UDP per packet Latency)</td>
<td>&lt; 25 micro seconds</td>
</tr>
<tr>
<td>Quarantine rules per Sensor - IPv4</td>
<td>1,000</td>
</tr>
<tr>
<td>Quarantine rules per Sensor - IPv6</td>
<td>500</td>
</tr>
<tr>
<td>Quarantine Zones per Sensor</td>
<td>50</td>
</tr>
<tr>
<td>Quarantine Zone ACLs per Sensor</td>
<td>1,000</td>
</tr>
<tr>
<td>Customized attacks</td>
<td>20,000</td>
</tr>
<tr>
<td>Ignore rules</td>
<td>32,768</td>
</tr>
<tr>
<td>Number of attacks with ignore rules</td>
<td>20,000</td>
</tr>
</tbody>
</table>

See the note below on how the number of customized attacks is affected.
Table 4-14 Virtual IPS Sensor capacity by model number (continued)

<table>
<thead>
<tr>
<th>Maximum Type</th>
<th>IPS-VM100</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoS Profiles</td>
<td>100</td>
</tr>
<tr>
<td>SYN cookie rate (64-byte packets per second)</td>
<td>200,000</td>
</tr>
<tr>
<td>Effective (Firewall) access rules</td>
<td>1,000</td>
</tr>
<tr>
<td>Firewall rule objects</td>
<td>7,000</td>
</tr>
<tr>
<td>Firewall DNS rule objects</td>
<td>500</td>
</tr>
<tr>
<td>Firewall rule object groups</td>
<td>100</td>
</tr>
<tr>
<td>Application on Custom Port rule objects</td>
<td>150</td>
</tr>
<tr>
<td>Firewall user-based rule objects</td>
<td>500</td>
</tr>
<tr>
<td>Firewall user groups in access rules</td>
<td>2,000</td>
</tr>
<tr>
<td>Number of whitelist entries permitted for IP Reputation</td>
<td>32</td>
</tr>
<tr>
<td>Maximum host entries permitted for Connection Limiting policies</td>
<td>55,000</td>
</tr>
<tr>
<td>Passive device profile limits</td>
<td>10,000</td>
</tr>
<tr>
<td>Advanced Malware - Maximum simultaneous file scan capacity when the file is saved in the Sensor</td>
<td>16</td>
</tr>
<tr>
<td>See the note below for more information.</td>
<td></td>
</tr>
<tr>
<td>Advanced Malware - Maximum simultaneous file scan capacity without saving files in the Sensor</td>
<td>255</td>
</tr>
<tr>
<td>See the note below for more information.</td>
<td></td>
</tr>
</tbody>
</table>

Note for Advanced Malware - Maximum simultaneous file scan

This feature is not the same as the file saving feature that is enabled through the Save File checkbox in the Advanced Malware Policies page of the Manager. It mentions the aspect of file saving that occurs temporarily within the Sensor during analysis. If the analysis result matches the severity configured in the Manager then the file is sent to the Manager to save.

Different outcomes based on your file saving configuration in the Advanced Malware Policies page are below:

- If you have set the Save File to Disable in the Advanced Malware Policies page then the scanned files are not sent to the Manager.

- If you have set the Save File to Always, then all the scanned files are sent to the Manager to be archived. Before using this option ensure that you have adequate disk space.

- If you have set a severity for Save File, then the scanned files are saved in the Sensor so that they can be analyzed by internal scanning engines like the PDF-JavaScript Engine. Once the analysis is complete and if the result is same or higher than the severity set then the file is sent to the Manager. When the Manager receives the file then it is saved in the Manager for future analysis by a security administrator.

Note for customized attacks

Customized attacks are not to be confused with custom attacks. A custom attack is a user-defined attack definition either in the McAfee's format or the Snort rules language. Whereas a customized attack is an attack definition (as part of the signature set), for which you modified its default settings. For example, if the default severity of an attack is 5 and you change it to 7, it is a customized attack.

The signature set push from the Manager to a Sensor fails if the number of customized attacks on the Sensor exceeds the customized attack limit.
The number of customized attacks can increase due to:

- Modifications done to attacks on a policy by users.
- Recommended for blocking (RFB) attacks.
- User created asymmetric policies.

**Example:** How numerous customized attacks are created in asymmetric policies.

1. Create a policy.
2. Set the Inbound rule set to "File Server rule set".
3. Set the Outbound rule set to "Default Testing rule set".

You see that:

- The File Server rule set has 166 exploit attacks.
- The Default Testing rule set has 2204 exploit attacks.

The total number of customized attacks for this policy is 2204 - 116 = 2038 customized attacks.

---

**Usage guidelines**

- VPCs with overlapping IP addresses should use different vNSP clusters.
- Though same policy group can be applied to all the VM groups, VM groups cannot span across multiple VPCs.
- Probe installation packages are cluster specific and they cannot be interchanged across clusters.
- The name of the attacker VM will be derived by querying your AWS account for the attacker IP address. If the attacker is external, and has an IP address that matches with any of the virtual machines in the AWS account, then the virtual machine with the matching IP address will be identified as the attacker.
- Based on the virtual machine instance type, AWS has limitations on the traffic. Redirection of traffic to the Sensor is within this limit. For example, in a web server type of application, 50% of the bandwidth is consumed for redirection of traffic to the Sensors.

McAfee recommends you to deploy the Virtual IPS Sensor and the protected groups in the same Availability Zones with private IP addresses.
Securing your Amazon Web Services (AWS) datacenter
Usage guidelines
Upgrade AWS components

This chapter provides information for upgrade of AWS components and the versions supported for upgrade.

The AWS components must be upgraded in the following sequence to avoid communication breakdown between the components. Note that there is no packet drop during the upgrade of any AWS component. McAfee recommends you to follow the sequence mentioned during the upgrade for AWS components:

1. Network Security Manager
2. vNSP Controller (Virtual Probe is upgraded along with the Controller)
3. Virtual IPS Sensor (procedure mentioned in Upgrade of Virtual IPS Sensors)

Following are few points for consideration before upgrade:

- All the AWS components have to be upgraded to the correct, supported release version for the solution to work seamlessly.
- During upgrade of any of the component, you cannot do a configuration update but the attack detection takes place without any interruption.
- The 9.1 Network Security Manager supports a heterogeneous environment for Virtual IPS Sensors. This implies that a 9.1 Manager can manage both, a 9.1 Virtual IPS Sensor and an 8.3 Virtual IPS Sensor.
- Only the following combination of Network Security Manager, vNSP Controller, and the Virtual Probe are supported for their respective releases:

<table>
<thead>
<tr>
<th>Network Security Manager</th>
<th>vNSP Controller</th>
<th>Virtual Probe</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4</td>
<td>3.5.3</td>
<td>3.5.3</td>
</tr>
<tr>
<td>9.1</td>
<td>3.6.1</td>
<td>3.6.1</td>
</tr>
</tbody>
</table>

Contents
- Review the upgrade considerations for an AWS environment
- Upgrade a vNSP Controller
- Upgrade Virtual IPS Sensors

Review the upgrade considerations for an AWS environment

Controller High-Availability (HA)

In release 8.4, you could deploy only a standalone Controller in AWS. Release 9.1 supports Controller High-Availability (HA) where two instances of the Controller are deployed. This provides a failover feature where one Controller is in active mode and the other in standby mode. When one Controller fails the other Controller becomes active so that there is no disruption in traffic flow.
As a part of the support for Controller HA feature, the vNSP Controllers page is updated in the Manager. Following are the changes in the vNSP Controllers page:

<table>
<thead>
<tr>
<th>Feature</th>
<th>8.4</th>
<th>9.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh</td>
<td>Refresh was available both at the page level and per Controller. Can refresh only at the page level, refresh per Controller is removed.</td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>Controller status was displayed along with the Controller name. Controller status is displayed along the Controller software version.</td>
<td></td>
</tr>
<tr>
<td>Hostname or IP Address</td>
<td>Displayed the name or the IP address of the Controller Server. Replaced with Hostname (local IP address).</td>
<td></td>
</tr>
<tr>
<td>Controller Software/Virtual Probe Software</td>
<td>Separate columns to display the Controller and Virtual Probe software versions. Single column that displays the Controller software and Virtual probe software version as Controller/Probe Software</td>
<td></td>
</tr>
<tr>
<td>Subnet used for communication with Sensor and Probe</td>
<td>Private Communication Subnet</td>
<td>Renamed to Tunnel Network</td>
</tr>
</tbody>
</table>

Following are the new options added in the vNSP Controllers page:

- **Mode** — Displays the mode in which the Controller is deployed. It can be a standalone Controller or a Controller HA.
- **Service IP address** — The Service IP address column displays the elastic IP address assigned to the Controller or it displays the private IP address of the Controller in case of a standalone Controller. Previously you had to configure the elastic IP address in the user data while launching the Controller instance in AWS. You can now configure the elastic IP address in the Manager. For a standalone Controller this is an optional field, but for a Controller HA, this is a mandatory field.
- **HA Role** — Displays the mode of the Controller as active or standby. For a standalone Controller it is displayed as active.
- **HA Timeout** — Time period for which the standby Controller waits before switching to active mode.
- Under **Other Actions**, the following options are added:
  - **Download Controller Logs** — Downloads logs for the Controller in zip format.
  - **Swap HA Role (Active/Standby)** — You can swap the Controller mode between Active and Standby.

**Sensor deployment in IDS mode**

With release 9.1, the Virtual IPS Sensor can be deployed in IDS mode. In IDS mode the Sensor is deployed in SPAN mode where a copy of the packet is sent to the Sensor. When an attack is detected, the Sensor resets the TCP channel.

To configure an existing Sensor in IDS mode, perform the following steps:

1. Go to Devices | <Admin Domain Name> | Global | vNSP Clusters.
2. Double-click on the protected group for which you want to change the Sensor deployment.
3. Select IDS from the Inspection Mode drop-down.
4. Click Save.

**Enable jumbo frame parsing in the Manager**

In release 8.4, you had to enable jumbo frame parsing through the `set jumobeframeparsing <enable|disable>` CLI command.
In release 9.1, you can enable jumbo frame parsing for the Virtual IPS Sensor in the Manager. To enable jumbo frame parsing, perform the following steps:

1. Select Devices | <Admin Domain Name> | Devices | <Cluster Name> | Setup | Advanced | IP Settings.

2. In the Common IP Parameters section, select Enabled from the Jumbo Frame Parsing drop-down list and click Update to update the Sensor of the configuration change.

   - If the Virtual IPS Sensors are pre-9.1 software, reboot the Sensors to update the changes.

   - Jumbo frame parsing is not supported for Virtual IPS Sensors deployed on KVM even though the option is available in the Manager.

### On-premise Network Security Manager

With release 9.1, Virtual IPS Sensor deployed in AWS can be managed by an on-premise Network Security Manager. To establish connection with the Sensor, you have to connect to the Sensor through a VPN connection.

### View endpoint details

The managed endpoint details in release 8.4 was available under Endpoint Actions as Check Endpoint Status in the vNSP Clusters and Cluster Summary pages.

In release 9.1, the user interface is enhanced to provide detailed information about the endpoint. The Check Endpoint Status is renamed as View Managed Endpoints. Endpoint information for all the Probes are displayed in the window.

To view the endpoints details, go to Devices | <Admin Domain Name> | Global | vNSP Clusters | Endpoint Actions | View Managed Endpoints or Devices | <Admin Domain Name> | Devices | <Cluster Name> | Summary | Endpoint Actions | View Managed Endpoints.

### Upgrade a vNSP Controller

To upgrade the vNSP Controller from version 8.4 to 9.1, you should launch a new instance of the 9.1 Controller AMI. For the latest Controller image, contact McAfee Support. For information about creating a vNSP Controller, refer section Configure a vNSP Controller on page 213.

### Upgrade Virtual IPS Sensors

You can upgrade the standalone Virtual IPS Sensors with the new AMI for the Sensor. To upgrade the Virtual IPS Sensors, you should launch new instances of the Sensor with the new AMI. The environment after an upgrade of the Virtual IPS Sensors can be as follows:

- You launch new instances of the Virtual IPS Sensor and add it to an existing vNSP Cluster. This is a hetero environment which will contain the old version of the Sensor as well as the new version of the Sensor. The Network Security Manager can manage both versions of the Sensor in case you want to retain the old Sensors.

- If you do not want the old version of the Sensor, you have to first launch new instances of the Virtual IPS Sensor with the new AMI. Once the new Sensors are up and in good health, you should manually terminate the old instances of the Virtual IPS Sensors.

- You can create a new vNSP Cluster with the new Virtual IPS Sensor AMI.
For more information on how to launch a Virtual IPS Sensor instance, see Launch the vNSP Controller AMI instance on page 219.

**Upgrade Virtual IPS Sensors in auto scaling group**

The Virtual IPS Sensor software has to be upgraded through new launch configuration in AWS. When an upgraded version of the Sensor software is available, an AMI with a new launch configuration has to be created. This new launch configuration has to be linked to the existing auto scaling group. So when a new Virtual IPS Sensor instance is launched, the Sensor is launched with the new configuration which will have the latest software version.

In case of an upgrade, when you link the new launch configuration with the latest Virtual IPS Sensor AMI to the auto scaling group, the old launch configuration is automatically disassociated from the auto scaling group. The old instances of the Virtual IPS Sensors are automatically terminated once the new launch configuration starts deploying the new AMI of the Virtual IPS Sensors.

When new instances of the Virtual IPS Sensors are being deployed, there will be downtime where no traffic inspection takes place.

To update the new launch configuration for an auto scaling group, perform the following steps in the AWS console:

1. In the **Auto Scaling Groups** page, select the auto scaling group for which you want to update the launch configuration.
2. In the **Details** tab, click **Edit**.
3. Select the new launch configuration from the **Launch Configuration** drop-down.
4. Click **Save**. The new launch configuration is linked to the auto scaling group.

For more information on auto scaling groups, see the section **Auto scaling of Sensors to improve traffic throughput** on page 241.
Use case scenarios

Network Security Platform for AWS is a probe-based solution that is capable of inspecting traffic flowing into and out of protected AWS instances. The solution has been designed to adapt to a public cloud environment and to scale with the requirements of your organization's network.

Deployment of Network Security Platform can be fulfilled to suit your requirements based on the direction of traffic and inspection mode. In this section, we provide you with some scenarios which can serve as basic guidelines in your deployment.

Consider a scenario where Network Security Platform is deployed to protect an organization's assets in the AWS environment. We assume that some of these assets to be protected are web servers with public IP addresses, and that you have performed the following steps as part of the deployment:

• The Network Security Manager:
  • Is installed in the AWS environment
  • Is able to reach required vNSP Clusters in the AWS environment which will be setup
• The vNSP Controller is installed by McAfee Technical Support and is able to reach the Network Security Manager.
• The vNSP Connector is configured and the communication between the Network Security Manager and the vNSP Controller is successful.
• A vNSP Cluster and the associated VM groups are configured in the Manager.
• The Virtual Probes are installed on every machine that has to be secured by Network Security Platform.
Scenario 1: Deployment of Virtual IPS Sensors in IDS mode

Virtual IPS Sensors deployed in IDS mode detects the attacks in traffic. When the traffic first enters the network it is directed to the required destination for example, a web server. This traffic reaches the web server which is deployed in IDS mode. A copy of the packet is sent to the Virtual IPS Sensor for inspection. If the Sensor detects malicious content in the traffic, it resets the TCP channels which evades the attack. An alert is generated in the Attack Log with the attack details.

![Diagram of Deployment of Sensors in IDS mode](img)
Scenario 2: On-premises Network Security Manager managing Sensors in AWS environment

McAfee Network Security Manager that is installed on-premises can be used to manage Virtual IPS Sensors in the AWS environment if the Manager is connected to AWS using VPN. This Manager can also be used to manage physical Sensors.

![On-premises Manager managing Virtual and physical IPS Sensors](image)

Figure 6-2  On-premises Manager managing Virtual and physical IPS Sensors

Scenario 3: Virtual IPS Sensor with AWS load balancer deployment

The AWS elastic load balancer directs traffic to the web servers to ensure that traffic load is distributed evenly. An AWS environment with the elastic load balancer can be protected by the Virtual IPS Sensor. The load balancer usually resides before the web servers.

Traffic from outside enters the AWS environment and is directed to the elastic load balancer first. The load balancer then distributes the traffic to the web servers. When traffic appears on the endpoint, the Virtual Probe installed on the web server, intercepts the traffic and directs it to the Virtual IPS Sensor. The Virtual IPS Sensor
inspects the traffic after which a pre-configured response action is taken in case of malicious traffic. An alert is generated in the Network Security Manager with the attack details based on the policies configured for malicious traffic. If the traffic is not malicious, it is allowed to proceed to the web servers.

Figure 6-3  Virtual IPS Sensor with AWS load balancer deployment

Scenario 4: Single Sensor per protected VPC deployment

In an environment with a Virtual IPS Sensor Cluster deployed per VPC, traffic load on the individual Virtual IPS Sensor is reduced. The Virtual IPS Sensor is deployed within a VPC where virtual machines must be protected. In such a scenario, the Virtual IPS Sensor inspects traffic from web servers that are present within that VPC. The Network Security Manager and the vNSP Controller are installed in a separate VPC. This way, traffic only exchanged with the protected VPC.
Traffic entering the AWS environment is directed to the web server. The Virtual Probe installed on the protected web servers, intercepts the traffic and routes it to the Virtual IPS Sensors. In case of malicious traffic, an alert is generated in the Network Security Manager, and the configured response action is taken. If traffic is found not to be malicious, it is directed back to the web servers. VPC peering must be enabled between the protected VPC and the VPC that contains the Network Security Manager and the vNSP Controller.

**Scenario 5: Multi-zone deployment with auto scaling of Virtual IPS Sensors**

With the Manager Disaster Recovery and Controller high availability features, failover functionality is supported in the network. Failover functionality is possible between two availability zones. You can create two availability zones which are managed by separate Network Security Managers which are an MDR pair. This is in turn are
connected to two Controllers deployed in high availability mode. In such a setup, there is a Manager and Controller always in Active mode. When one availability zone fails, the traffic is directed through the other availability zone which has both the Manager and Controller. Due to this the traffic flow is not disrupted.

Figure 6-5  Multi-zone deployment with auto scaling of Virtual IPS Sensors

Scenario 6: Securing multiple AWS accounts

When you want to secure your resources distributed across multiple AWS accounts, you must install each of these components separately for every AWS account:

- vNSP Controller
- vNSP Cluster
- Protected groups
Failure of components

Contents
- Network Security Manager failure
- Sensor failure
- Controller failure
- Virtual Probe failure

Network Security Manager failure

When the Network Security Manager is not reachable, there are no changes to the policies previously configured. You can view the policies after the Manager is back online.

The protected groups created in the Manager remain intact. The traffic from the virtual machines are directed to the Sensor for inspection. Also, you can add or delete new virtual machine instances within the protected subnet but cannot create new protected groups. The Manager database is populated with the virtual machine information once it is back online.

Sensor failure

In a situation where the Virtual IPS Sensor is not working, the traffic is load balanced between the other active Sensors. The AWS auto scaling group option also provides for Sensor failover, where when a Sensor fails, a new Sensor instance is launched to load balance the traffic.

The Virtual Probe pings the Sensor multiple times within a second to check the status of the Sensor. In a scenario when the Sensor is not reachable, the Probe immediately directs the packet to another Sensor. This allows for rapid failure detection and rerouting of traffic to the next available Sensor. When there is no Sensor available, due to the fail-open functionality in the Probe, there is no inspection of packets.

Controller failure

Controller failure does not have any impact on the traffic flow in the network. It is recommended not to create new virtual machines in the protected group when there is a Controller failure. If a new virtual machine is created when there is a Controller failure, it cannot be protected unless the Controller comes online.

In case of existing virtual machines, they continue to redirect the traffic with the configurations before the Controller failure.
Virtual Probe failure

The Virtual Probe are built to fail open in case of a Probe failure. In such situations, the traffic flow forwarded without inspection.
Troubleshooting scenarios

Contents

- System faults
- Licensing error in Network Security Manager
- vNSP Controller troubleshooting
- Virtual Probe troubleshooting
- Virtual IPS Sensor troubleshooting

System faults

These are the critical faults for a Manager.

This section lists the system fault messages visible in the Manager Operational Status viewer, organized by severity, with Critical messages first, then Errors, then Warnings, then Informational messages.

The Manager faults can be classified into critical, error, warning, and informational. The Action column provides you with troubleshooting tips.

Manager Critical Faults

These are the critical faults for a Manager.

<table>
<thead>
<tr>
<th>Fault</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insufficient licenses detected</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description/Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Manager does not have enough licenses to support the number of virtual sensors it is currently managing. Additional licenses are required to become compliant.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import the additional number of licenses to the Manager after installation, or contact McAfee Technical Support.</td>
</tr>
</tbody>
</table>

Manager Warning Faults

These are the warning faults for a Manager.
### Fault \( \rightarrow \) Severity \( \rightarrow \) Description/Cause \( \rightarrow \) Action

| Fault \( \rightarrow \) Severity \( \rightarrow \) Description/Cause \( \rightarrow \) Action |
|---|---|---|---|
| License Required for vNSP Cluster \( \rightarrow \) Warning \( \rightarrow \) A valid license is required to manage vNSP clusters, however, no license currently exists on the Manager. Without at least one license, deployment of pending changes to vNSP clusters will be prevented. A license is required to correct the problem. \( \rightarrow \) Import at least one license to your Manager after installation, or contact McAfee Technical Support. |
| Internet Connectivity Required for vNSP Cluster Usage \( \rightarrow \) Warning \( \rightarrow \) vNSP cluster usage data must be sent to McAfee for proper vNSP cluster function, however, this Manager is currently unable to send the usage data to McAfee. Deployment of pending changes to vNSP clusters will be prevented until connectivity has been restored. \( \rightarrow \) Check your internet connectivity. |
| Telemetry Enabled for vNSP Cluster Usage \( \rightarrow \) Informational \( \rightarrow \) Telemetry for vNSP cluster usage data has been automatically enabled because one or more vNSP cluster is defined on this Manager. You can view the details of what is being sent to McAfee on the GTI page. (The Telemetry data will be sent as long as one or more vNSP clusters is defined) \( \rightarrow \) This message is for user information. No action is required. |

### Manager Informational Faults

These are the informational faults for a Manager.

| Fault \( \rightarrow \) Severity \( \rightarrow \) Description/Cause \( \rightarrow \) Action |
|---|---|---|---|
| Telemetry Enabled for vNSP Cluster Usage \( \rightarrow \) Informational \( \rightarrow \) Telemetry for vNSP cluster usage data has been automatically enabled because one or more vNSP cluster is defined on this Manager. You can view the details of what is being sent to McAfee on the GTI page. (The Telemetry data will be sent as long as one or more vNSP clusters is defined) \( \rightarrow \) This message is for user information. No action is required. |

### Licensing error in Network Security Manager

Network Security Manager requires internet connectivity to validate licenses. If the license is not validated, you cannot create vNSP Clusters even if the license is available. When you try to create a vNSP Cluster, the error is displayed and you cannot create the Cluster. Configuration update to the Virtual IPS Sensors is also not possible if the license cannot be validated.

Once the internet connectivity is restored in the Manager, perform the following steps:

1. Go to Devices | <Admin Domain Name> | Global | Deploy Pending Changes page.
2. Refresh the configuration and retry for internet connectivity.

### vNSP Controller troubleshooting

#### Controller status

After the deployment of the Controller, if the Controller status is still displayed as disconnected due to registration error/failure with the Network Security Manager, click the refresh button in the Network Security Manager to refresh the Controller status.
Controller registration failure

If the controller is not online after the deployment, perform the following steps:

Go to `<Manager installation directory>\App\cim_web log` file and validate if the following request is displayed:

```
    {'controller_name': 'nsat_controller',
     'controller_instance_id': 'i-0dfd9ed658a78f770',
     'controller_ip': '10.10.90.226'},
    'hmac': 'E3QSogxONLpt6ModX54ZHoIDTa4='}
```

1. If there are no registration requests, check the following:
   - Network Security Manager IP address is correct in the user data.
   - Controller is able to connect to the Network Security Manager on port 443.
   - Controller has access to the internet.

2. If there is a HMAC validation error in the registration as follows:
   ```
   ControllerRegistrationWeb: HMAC validation failed! Request Payload ->
   {'register':
    {'controller_name': 'SOC-IPS-POC-Mcafee-IPSController',
     'controller_instance_id': 'i-079b45aa34a25c178',
     'controller_ip': '10.30.10.114'},
    'hmac': 'nrbxSjhlS1qZNZj8LxRSttU0hXQ="'}
   ```

   In such a scenario perform the following steps:
   a. Ensure that the shared secret key in the user data used to establish trust between the Controller and Network Security Manager is identical.
   b. If it is incorrect, then stop the Controller, edit the user data to set the correct shared secret key and restart the Controller to establish the trust.

Controller port reachability

Ensure that port 22 is reachable from the Network Security Manager to activate the Controller.

Ensure that port 443 of the Controller is reachable from the Network Security Manager, Virtual IPS Sensor and all the protected VMs.

Virtual Probe troubleshooting

Virtual Probe installation failure

The following sections describe how to troubleshoot in case of Virtual Probe installation failure both in Linux and Windows.

Installation failure in Linux

Ensure that the endpoint is connected to the internet while installing the Virtual Probe as the installer downloads files from the internet during installation. Install the Probe using `wget` or `curl` URLs, or download the files manually.

Install the Virtual Probe
If you are using private endpoints use NAT Gateways to access the internet. You can download the Virtual probes from the following locations:

- **curl** "https://<nsm_ip>/sdkapi/cloud/cluster/downloadprobeagent?name=<cluster>&ostype=linux" -o <Desiredfilename>.tar.gz
- **wget** "https://<nsmip>/sdkapi/cloud/cluster/downloadprobeagent?name=<Clustername>&ostype=<linux>" --no-check-certificate -O <Desiredfilename>.tar.gz

To uninstall the Virtual Probe, see Uninstall the Virtual Probe on page 238.

**Troubleshoot the Virtual Probe**

1. The installation of the Virtual Probe requires root privileges.

2. Run the `/etc/init.d/zasad status` command and validate that the process is running which is as follows:

   ```
   [root@ip-10-10-90-9 ~]# /etc/init.d/zasad status
   Checking zasa ... Service is running - [OK][0]
   ```

   a. **If the status is displayed as endpoint ID is not valid**, then delete the .epid file from `/usr/local/zasa` folder and restart the process using the command `/etc/init.d/zasad restart`.

   b. **If the status is displayed as Customer ID or pool tag is invalid**, then validate if you have downloaded the probe for the correct Cluster.

   c. **If the error is displayed as Failure to read/open certificate**, then download the correct Probe version and reinstall.

   d. **If the error is displayed as Failure to establish channel with Controller**, then check the network settings by running the `netstat -natp|grep 443` command to check if the Virtual Probe has established connection with the vNSP Controller. If not check the firewall rules to ensure that the Controller port is accessible in port 443.

   ```
   [root@ip-10-10-90-9 ~]# netstat -anp|grep 443
   tcp 0 0 10.10.90.9:42422 10.10.90.226:443 ESTABLISHED 16037/zasa
   ```

   where 10.10.90.9 is the protected machine and 10.10.90.226 is the Controller.

   - **Port 443 is the default port used by the probe to communicate with the vNSP Controller.**

**Points for consideration**

- Ensure that you do not create a copy of the AMI, which has the Virtual Probe installed in it, and launch another endpoint with the same AMI. This will cause duplication of the .epid file and the service will not function properly.

- If you want to launch another endpoint with the same AMI, ensure that you delete the .epid file. When the Virtual Probe in the new AMI registers with the vNSP Controller it will be assigned a new .epid.

- Incorrect Probe installed also can result in traffic being forwarded to a different Cluster, which results in data charges by AWS in case the Sensor is across Availability Zones.

**Installation failure in Windows**

Complete the following step to troubleshoot installation failure in Windows.

- **While installing the Virtual Probe in a Windows endpoint, there may be a brief interruption in traffic flow.**

Ensure that you are installing the Virtual Probe using Administrator privileges.
Virtual probe fails to inspect traffic

The following sections describe how to troubleshoot in case of Virtual Probe failure to redirect traffic.
**Failure to inspect traffic in Linux**

Complete the following steps to troubleshoot failure to inspect traffic in Linux.

1. Make sure that your virtual machines are within the protected group in the Network Security Manager. If you do not have a Protected Group which contains the subnet attached with the protected machine in Network Security Manager, then create a Protected Group before proceeding.

2. The Virtual Probes use iptables for traffic redirection. Make sure the iptables are enabled. To check if the iptable is enabled, verify the ip_tables module in the kernel modules list.

```
AcmeEnt > lsmod
Module Size Used by
fuse 79932 0
ipt_LOG 7854 2
nfnetlink_queue 6111 0
nfnetlink_log 8710 0
nfnetlink 4200 2 nfnetlink_queue,nfnetlink_log
blueooth 97893 0
rfkill 19255 1 bluetooth
tun 17094 2
8021q 20362 0
garp 7132 1 8021q
tcp 2218 1 garp
11c 5418 2 garp,stp
xenfs 5705 1
ipt_REJECT 2351 0
iptables_filter 2793 1
nf_conntrack_ipv4 9186 99
nf_defrag_ipv4 1483 1 nf_conntrack_ipv4
xt_state 1492 99
xt_CONNMARK 1507 0
iptable_mangle 3249 0
ip_tables 17831 2 iptable_filter,iptable_mangle
iptable_filter 4340 2
nf_contrack_ipv6 7985 2
nf_defrag_ipv6 26468 1 nf_contrack_ipv6
xt_contrack 2776 2
nf_contrack 79377 5 nf_contrack_ipv4,xt_state,xt_CONNMARK,nf_contrack_ipv6,xt_contrack_ipv6
iptable_mangle 2689 1
ip_tables 18732 1 iptable_filter
ipv6 336282 15 ip6t_REJECT,nf_contrack_ipv6,nf_defrag_ipv6
xen_netfront 18930 0
ext3 240420 1
jbd 80652 1 ext3
mbcache 8193 1 ext3
xen_bpfkm 21998 2
dm_mirror 14964 0
dm_region_hash 12085 1 dm_mirror
dm_log 9930 2 dm_mirror,dm_region_hash
dm_mod 102467 2 dm_mirror,dm_log
AcmeEnt >
```

Alternately, you can verify the default iptable in the console session.

```
AcmeEnt (Root) > iptables -L
Chain INPUT (policy ACCEPT)
 target prot opt source             destination
     ACCEPT                        0 0 0 0
     ACCEPT                        0 0 0 0

Chain FORWARD (policy ACCEPT)
 target prot opt source             destination
     ACCEPT                        0 0 0 0

Chain OUTPUT (policy ACCEPT)
 target prot opt source             destination
     ACCEPT                        0 0 0 0
AcmeEnt (Root) >
```

The output for the `iptables -L` command varies depending on the rules enabled.
3 Run the `netstat grep 9797` command and verify that the channel is established with the Sensors and the vNSP Cluster. If not check the firewall rule to make sure that the Sensor is reachable from the Virtual Probe.

```
[root@ip-10-10-90-9 ~]# netstat -an|grep 9797
 tcp 0 0 10.10.90.9:49176 10.10.91.137:9797 ESTABLISHED
```

Where 10.10.91.137 is the Virtual IPS Sensor

The Protected Group takes around 5 minutes to build the tunnel. If the tunnel is not formed in 5 minutes, make sure that the subnet of the virtual machine is part of a Protected Group.

4 Run the `show ingress-egress stat` command in the Sensor to view the statistics for the number of packets received, sent or dropped.

5 If there are any issues with the Sensor:
   a In the Manager, select `Devices` | `<Admin Domain Name>` | `Devices` | `<Device Name>` | `Troubleshooting` | `Diagnostic Trace`.
   b Select the `Upload?` checkbox if it is not already selected.
   c Click `Upload`.
   d Export a diagnostics file to a client machine by selecting the file from the `Uploaded Diagnostics Files` listed and clicking `Export`.
   e Once exported from your Manager, this file can be sent through email to McAfee Technical Support for analysis and troubleshooting advice.

6 To debug on the protected VM:
   a Open the `zasa.config` file using the `vi zasa.config` command.
   b Add a line `enable-inline-cnt` and save the file.
   c Reload the `zasa.config` file by running `/etc/init.d/zasad reload` command.
   d Run `/usr/local/zasa/inline_counters` command to view the statistics of the Sensor in the file. The command also displays the number of packets sent and the number of packets failed to reach the Sensor.

**Virtual Probe reboot due to vNSP Controller restart**

**Scenario**

Virtual Probe reboot due to vNSP Controller restart

**Applicable to Sensor models:** Virtual IPS Sensors.

**Sensor software version:** 9.1, 9.2

**Problem type to be solved**

In AWS environment, after restarting the virtual probe, firewall settings in the windows machine are restored to configurations available at the time of probe installation.

Note: The Virtual Probe restart can be triggered manually or due to vNSP Controller restart.
Troubleshooting steps
1. In the windows machine, go to C:\Program\Files\McAfee\zasa\firewall.
2. Delete firewall.bk.

Virtual IPS Sensor troubleshooting

This section lists the troubleshooting steps for Sensor.

Second interface not attached to Virtual IPS Sensor in autoscaling group

To attach the second interface to Virtual IPS Sensor in autoscaling group using an IAM role, see Create IAM roles and policies on page 196.

If the second interface fails to initialize, please ensure the following conditions are met:

- IAM role is attached to the launch configuration
- Launched Sensors have internet access
- User data in Sensor for the second interface has the correct datasubnet and security group information
This chapter contains CLI commands for preparing or configuring the Virtual IPS Sensor for the AWS Environment.

Contents
- set cloud-cluster sharedsecretkey
- resetcloudclusterkey

**set cloud-cluster sharedsecretkey**

Sets the shared secret key value that the Manager and the Sensor will use to establish a trust relationship.

Type the command in the CLI as shown in the Syntax below. The Sensor prompts you for a secret key value. The value you enter is not shown. You will be prompted to type the value again to verify that the two entries match.

```
set cloud-cluster sharedsecretkey
```

The shared secret key value specified here must match with value used in the Manager interface, or, the Sensor and Manager will be unable to communicate. If you want to change the value, you must change the value in the Sensor CLI, as well as, the Manager interface.

**Syntax:**

```
set cloud-cluster sharedsecretkey
```

At the Sensor’s prompt for a secret key value, enter a case-sensitive character string between 8 and 25 characters of any ASCII text.

**Applicable to:** Virtual IPS Sensors on AWS.

**resetcloudclusterkey**

Resets the shared secret key value configured in the Sensor.

**Syntax:**

```
resetcloudclusterkey
```

**Applicable to:** Virtual IPS Sensors for AWS.
CLI commands for AWS
resetcloudclusterkey
Index

A
about this guide 7

C
conventions and icons used in this guide 7

D
documentation
  audience for this guide 7
  product-specific, finding 8
  typographical conventions and icons 7

J
jumbo frame parsing 238

M
McAfee ServicePortal, accessing 8

S
Sensor capacity by model number
  Virtual IPS 257
  ServicePortal, finding product documentation 8

T
technical support, finding product information 8