

# Juniper Advanced Threat Prevention Appliance

## Traffic Collector Quick Start Guide

Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, California 94089  
USA

408-745-2000

[www.juniper.net](http://www.juniper.net)

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Juniper Advanced Threat Prevention Traffic Collector Quick Start Guide  
Copyright© 2018 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

#### YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

#### END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical document consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# About the Documentation

## Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes. Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

## Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>.
- Search for known bugs: <https://prsearch.juniper.net/>.
- Find product documentation: <http://www.juniper.net/documentation/>.
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>.
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>.
- Search technical bulletins for relevant hardware and software notifications: <http://kb.juniper.net/InfoCenter/>.
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>.
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>.

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>.

### Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).
- For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>

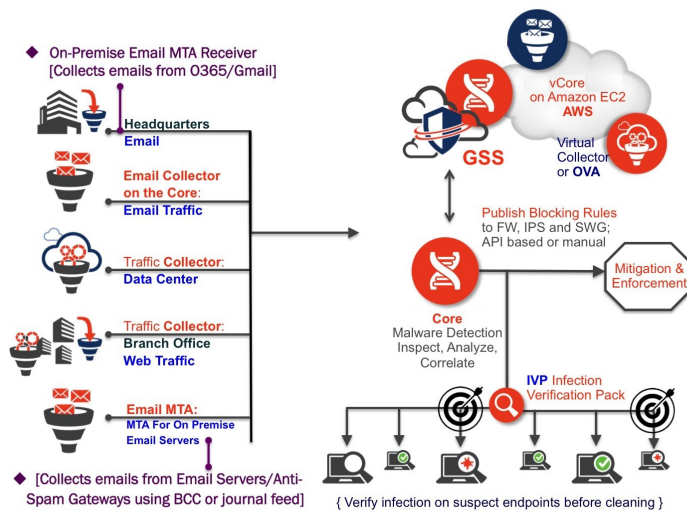
## Inside This Guide

- FIREWALL & MANAGEMENT NETWORK INTERFACE CONNECTIVITY
- INSTALLING THE JUNIPER ATP APPLIANCE COLLECTOR OPEN VIRTUAL APPLIANCE (OVA)
- CONFIGURING JUNIPER ATP APPLIANCE WEB TRAFFIC COLLECTION
- SETTING THE SAME DEVICE KEY PASSPHRASE ON ALL JUNIPER ATP APPLIANCE DEVICES
- VERIFYING CONFIGURATIONS AND TRAFFIC FROM THE CLI
- ACCESSING THE JUNIPER ATP APPLIANCE CENTRAL MANAGER WEB UI
- SETTING SSH HONEYPOT DETECTION
- VERIFYING TRAFFIC COLLECTION FROM THE WEB UI
- WHAT TO DO NEXT?

Welcome to the Juniper ATP Appliance Traffic Collectors Quick Start Guide.

When linked logically to the Core, the Juniper ATP Appliance Traffic Collectors continuously monitor and inspect all network traffic for malware objects; extracting and sending objects to the Core for Windows or Mac OS X object analysis and detection. Juniper ATP Appliance Web/Email Collectors efficiently separate traffic monitoring and inspection from behavioral analysis, multi-platform detonation and context reasoning.

Figure 1 DISTRIBUTED TRAFFIC COLLECTOR(S) EXTEND THREAT VISIBILITY



All detected threats and breaches are analyzed by the detonation and intelligence engines within the Juniper ATP Appliance Core, then aggregated and reported in real-time to the Juniper ATP Appliance Central Manager Web UI. In the Web UI, all threats are detailed with corresponding context-specific mitigation options.

Use this guide to install a Juniper ATP Appliance Traffic Collector and to

configure its logical connection to a network switch TAP port and a Juniper ATP Appliance Core/CM or All-in-One Server.

- For hardware specifications and set up instructions, refer to the **JATP700 Appliance Hardware Guide**.
- To configure an inside outside data path SPAN-traffic proxy, or management network proxy, refer to the Juniper ATP Appliance CLI Command Reference.

**NOTE** This document assumes you have already installed and configured the Juniper ATP Appliance Core/Central Manager or All-in-One Server. Refer to the respective Quick Start Guides for combined and separate Core/Central Manager Server(s), All-in-One, and/or Mac OS X installations.

## Firewall & Management Network Interface Connectivity

Connectivity requirements for the Juniper ATP Appliance management interface (eth0) allow for transfer of inspected network objects, live malware behavior analysis, intelligence reporting, and product updates. If the enterprise network firewall uses an outgoing “default allow” rule, this is sufficient. Otherwise, create the following firewall rules:

- SSH port 443 should be open from the Collector to the Core/CM or All-in-One (for traffic inspection and malware behavior analysis).

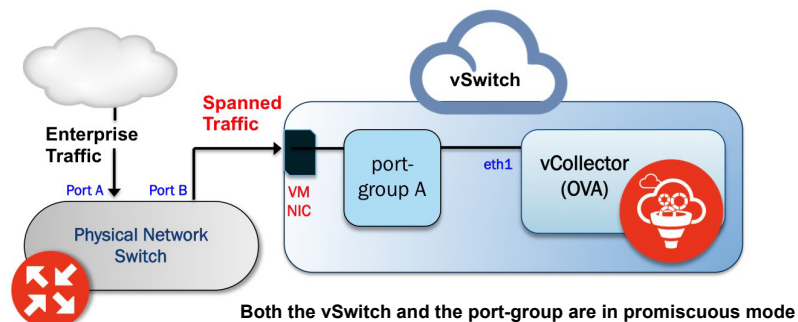
**IMPORTANT:** Primary Core/CM and Secondary Cores/Mac Cores must be on the same network, and allow all ports, with no Port Address (PAT) or Network Address Translation (NAT).

**NOTE** All GSS communications for security and content auto-updates are handled by the Core/CM or All-in-One system.

## Installing the Juniper ATP Appliance Collector Open Virtual Appliance (OVA)

Juniper ATP Appliance’s extensible deployment options include a Virtual Collector (vCollector) product, as an Open Virtual Appliance, or OVA, that runs in virtual machines. Specifically, a Juniper ATP Appliance OVA-packaged image is available for VMware Hypervisor for vSphere 5.1, 5.5 and 6.0. Virtual Collector models supporting 25 Mbps, 100 Mbps, 500 Mbps and a 1.0 Gbps are available.

An OVF package consists of several files contained in a single directory with an OVF descriptor file that describes the Juniper ATP Appliance virtual machine template and package: metadata for the OVF package, and a Juniper ATP Appliance software image. The directory is distributed as an OVA package (a tar archive file with the OVF directory inside).



**RECOMMENDATION:** Juniper advises use of a dedicated physical NIC assigned to the vCollector for best collection results.

## Virtual Collector Deployment Options

Two types of vCollector deployments are supported for a network switch SPAN/TAP:

1. Traffic that is spanned to a vCollector from a physical switch. In this case, traffic is spanned from portA to portB. ESXi containing the Juniper ATP Appliance vCollector OVA is connected to portB. This deployment scenario is shown in the figure above.
2. Traffic from a virtual machine that is on the same vSwitch as the vCollector. In this deployment scenario, because the vSwitch containing the vCollector is in promiscuous mode, by default all port-groups created will also be in promiscuous mode. Therefore, 2 port groups are recommended wherein port-groupA (vCollector) in promiscuous mode is associated with the vCollector, and port-groupB (vTraffic) represents traffic that is not in promiscuous mode.

**NOTE** Traffic from a virtual machine that is not on the same vSwitch as the vCollector is not supported. Also, a dedicated NIC adapter is required for the vCollector deployment; attach the NIC to a virtual switch in promiscuous mode (to collect all traffic). If a vSwitch is in promiscuous mode, by default all port-groups are put in promiscuous mode and that means other regular VMs are also receiving unnecessary traffic. A workaround for that is to create a different port-group for the other VMs and configure without promiscuous mode.

## Provisioning Requirements

VM vCenter Version Support	Recommended vCollector ESXi Hardware	vCollector CPUs	vCollector Memory
VM vCenter Server Version: 5.5.0 vSphere Client Version: 5.5.0 ESXi version: 5.5.0 and 5.5.1	Processor speed 2.3-3.3 GHz As many physical CORES as virtual CPUs Hyperthreading: either enable or disable	CPU Reservation: Default CPU Limit: Unlimited Hyperthreaded Core Sharing Mode: None (if Hyperthreading is enabled on the ESXi)	Memory Reservation: Default Memory Limit: Unlimited

Model	Performance	Number of vCPUs	Memory	Disk Storage
vC-v50M	50 Mbps	1	1.5GB	16 GB
vC-v100M	100 Mbps	2	4 GB	16 GB
vC--v500M	500 Mbps	4	16 GB	512 GB
vC--v1G	1 Gbps	8	32 GB	512 GB
vC-v2.5G	2.5 Gbps	24	64 GB	512 GB

## OVA vCollector Sizing Options

1. Identify the physical network adapter from which the spanned traffic is received, then create a new VMware Virtual Switch and associate it with the physical network adapter.
2. Click on Virtual Switch Properties. On the Ports tab, select vSwitch and click on the Edit button.

3. Select the Security tab and change Promiscuous Mode to accept, then click OK. Click OK again to exit.
4. Create a new port-group “vtraffic” in the Virtual Switch. This new port-group will be assigned to your vCollector later. See [vSwitch Tip](#) below for information about troubleshooting this setup.

### OVA Deployment vSwitch Setup

1. Download the Juniper ATP Appliance OVA file from the location specified.
2. Connect to vCenter and click on File>Deploy OVF Template.
3. Browse the Downloads directory and select the OVA file, then click Next to view the OVF Template Details page.
4. Click Next to display and review the End User License Agreement page.
5. Accept the EULA and click Next to view the Name and Location page.
6. The default name for the Virtual Collector is Juniper ATP Appliance Virtual Collector Appliance. If desired, enter a new name for the Virtual Collector.
7. Choose the Data Center on which the vCollector will be deployed, then click Next to view the Host/Cluster page.
8. Choose the host/cluster on which the vCollector will reside, then click Next to view the Storage page.
9. Choose the destination file storage for the vCollector virtual machine files, then click Next to view the Disk Format page. The default is THIN PROVISION LAZY ZEROED which requires 512GB of free space on the storage device. Using Thin disk provisioning to initially save on disk space is also supported. Click Next to view the Network Mapping page.
10. Set up the two vCollector interfaces:
  - › Management (Administrative): This interface is used to communicate with the Juniper ATP Appliance Central Manager (CM). Assign the destination network to the port-group that has connectivity to the CM Management Network IP Address.
  - › Monitoring: This interface is used to inspect and collect network traffic. Assign the destination network to a port-group that is receiving mirrored traffic; this is the port-group “vtraffic” configured in the requirements section above. Click Next to view the Juniper ATP Appliance Properties page.
11. IP Allocation Policy can be configured for DHCP or Static addressing-- Juniper recommends using STATIC addressing. For DHCP instructions, skip to Step 12. For IP Allocation Policy as Static, perform the following assignments:
  - › IP Address: Assign the Management Network IP Address for the Virtual Collector; it should be in the same subnet as the management IP address for the Juniper ATP Appliance Central Manager.
  - › Netmask: Assign the netmask for the Virtual Collector.
  - › Gateway: Assign the gateway for the Virtual Collector.
  - › DNS Address 1: Assign the primary DNS address for the Virtual Collector.
  - › DNS Address 2: Assign the secondary DNS address for the Virtual Collector.
12. Enter the Search Domain and Hostname for the Virtual Collector.



13. Complete the Juniper ATP Appliance vCollector Settings:
  - › New Juniper ATP Appliance CLI Admin Password: this is the password for accessing the Virtual Collector from the CLI.
  - › Juniper ATP Appliance Central Manager IP Address: Enter the management network IP Address configured for the Central Manager. This IP Address should be reachable by the Virtual Collector Management IP Address.
  - › Juniper ATP Appliance Device Name: Enter a unique device name for the Virtual Collector.
  - › Juniper ATP Appliance Device Description: Enter a description for the Virtual Collector.
  - › Juniper ATP Appliance Device Key Passphrase: Enter the passphrase for the Virtual Collector; it should be identical to the passphrase configured in the Central Manager for the Core/CM. Click Next to view the Ready to Complete page.
14. Do not check the Power-On After Deployment option because you must first (next) modify the CPU and Memory requirements (depending on the Virtual Collector model--either 100Mbps, 500Mbps, or 1Gbps; refer to [OVA vCollector Sizing Options on page 3](#) for sizing information. It is important to reserve CPU and memory for any virtual deployment.
15. To configure the number of vCPUs and memory:
  - A. Power off the virtual collector.
  - B. Right click on the virtual collector -> Edit Settings
  - C. Select Memory in the hardware tab. Enter the required memory in the Memory Size combination box on the right.
  - D. Select CPU in the hardware tab. Enter the required number of virtual CPUs combination box on the right. Click OK to set.
16. To configure CPU and memory reservation:
  - A. For CPU reservation: Right click on vCollector-> Edit settings:
  - B. Select Resources tab, then select CPU.
  - C. Under Reservation, specify the guaranteed CPU allocation for the VM. It can be calculated based on Number of vCPUs \*processor speed.
  - D. For Memory Reservation: Right click on vCollector -> Edit settings.
  - E. In the Resources tab, select Memory.
  - F. Under Reservation, specify the amount of Memory to reserve for the VM. It should be the same as the memory specified by the Sizing guide.
17. If Hyperthreading is enabled, perform the following selections:
  - A. Right click on the virtual collector -> Edit settings.
  - B. In the Resources tab, select HT Sharing: None for Advanced CPU.
18. Power on the Virtual Collector.

### To install the Juniper ATP Appliance OVA to a VM

1. Obtain requisite login information from your sales representative, then download the Juniper ATP Appliance ISO file [JATP.iso] and the Juniper ATP Appliance Collector image file [img.zip] to your Linux system's local directory.
2. Start a terminal session then plug in the first USB drive (Kingston USB flash drives are recommended) to the Linux system and identify its drive ID (ls /dev/sd\*).

3. Use the Linux “dd” utility to write the local ISO content to the first USB flash drive; we refer to drive “sdb” in our example below but your drive ID will likely be different:

```
dd if=JATP.iso of=/dev/sdb
```

---

**NOTE** It is very important that you take note of the drive ID and install the ISO only to that correct USB drive or the dd utility will overwrite all data on the drive selected.

---

4. OPTIONAL: To view status, use the pv utility [you may need to install the pv utility first]; for example:  
dd if=JATP.iso | pv | dd of=/dev/sdb
5. When the ISO is fully copied to the bootable USB drive, remove USB drive1 and insert USB drive2.
6. Copy the zipped Collector image file img.zip to the 2nd USB drive:
7. You are now ready to install the Collector ISO to the Mac Mini from the bootable USB drive. The ISO will unzip and install the Collector image file.

---

**NOTE** There are Windows and Mac Utilities that are also available for creating bootable USB drives from the ISO image.

---

**REQUIRED:** Before beginning the Mac Mini installation, be sure you have obtained an Apple USB Ethernet Adapter (Model No. MC704ZM/A) and a DVI monitor cable.

Plug in all connectors and cables to the Mac Mini:

- A DVI Monitor connection
- USB keyboard
- Mac Mini Power cable
- Ethernet cable for the eth1 interface SPAN/TAP port connection.  
Note: the onboard NIC is the Juniper ATP Appliance eth1 interface; the ethernet cable from the SPAN/TAP port on the network switch connects to the Mac Mini onboard built-in NIC which the system recognizes as eth1.
- Ethernet cable connected to a USB Ethernet Adapter connected to a USB port for the eth0 management interface (the USB NIC is the eth0 interface).

### To Create a Bootable USB Drive

---

**NOTE** It is important to not disconnect the USB NIC from the USB port on the Mac Mini (or move the USB NIC to another the port) during or after the installation.

---

1. Insert the USB drive containing the Juniper ATP Appliance ISO image to the Mac Mini then depress and hold down the ALT key while powering ON the Mac Mini device.
2. Two icons are displayed on the monitor display: Windows HDD and Windows USB; select the Windows USB icon and Enter.
3. The installation begins with the message: INSTALLING JUNIPER ATP APPLIANCE SOFTWARE. This step takes ~30 minutes.
4. Follow the prompt to remove the USB drive; the system will reboot itself. This reboot may take up to 20 minutes.
5. After reboot, the Juniper ATP Appliance CLI prompt appears. At the CLI, log in to the Juniper ATP Appliance CLI with the username `admin` and the password `1JATP234`.
6. The End User License Agreement (EULA) displays; review and press `q` to continue. When prompted to accept the Juniper ATP Appliance End User License Agreement (EULA), enter `yes`. Configuration will not continue until the EULA is accepted.
7. At the prompt, enter a new CLI administrator password. Weak passwords are not accepted. Note that the CLI admin password is maintained separately from the Juniper ATP Appliance Central Manager Web UI interface

8. Prompts for the Configuration Wizard will be displayed.

To Install the Juniper ATP Appliance Collector ISO to the Mac Mini from the USB Drive

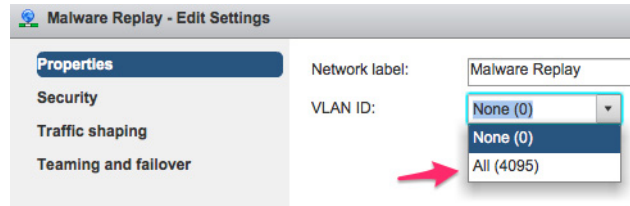
1. At the login prompt, enter the default username `admin` and the password `1JATP234`. Review the displayed EULA and press `q` to continue.
2. When prompted to accept the Juniper ATP Appliance End User License Agreement (EULA), enter `yes`. Configuration cannot continue until the EULA is accepted.
3. At the prompt, enter a new CLI administrator password. Weak passwords are not accepted. Note that the CLI admin password is maintained separately from the Juniper ATP Appliance Central Manager Web UI interface.
4. When prompted with the query “Do you want to configure the system using the Configuration Wizard (Yes/No)?”, enter `yes`.
5. Next, respond to the Configuration Wizard questions as follows in the Configuration Wizard section below.

Configuration Wizard Prompts	Customer Responses/Actions
Use DHCP to obtain the IP address and DNS server address for the management interface (Yes/No)?	We strongly discourage the use of DHCP addressing because it changes dynamically. A static IP address is preferred.  Recommended: Respond with <b>no</b> :
Note: Only if your DHCP response is <b>no</b> , enter the following information when prompted:  a. IP address b. Netmask c. Enter a gateway IP address for this management (administrative) interface:	Enter a gateway IP X.X.X.X and quad-tuple netmask using the form 255.255.255.0 (no CIDR format).  a. Enter an IP address b. Enter a netmask c. Enter a gateway IP address.
d. Enter primary DNS server IP address. e. Do you have a secondary DNS Server (Yes/No). f. Do you want to enter the search domains? g. Enter the search domain (separate multiple search domains by space):	d. Enter the DNS Server IP address  e. If <b>yes</b> , enter the IP address of the secondary DNS server. f. Enter <b>yes</b> if you want DNS lookups to use a specific domain. g. Enter search domain(s) separated by spaces; for example: example.com lan.com dom2.com
Restart the eth0 interface (Yes/No)?	Enter <b>yes</b> to restart with the new configuration settings applied.
Enter a valid hostname.	Type a unique hostname when prompted; do not include the domain; for example: <b>juniperatp1</b>

<p>[OPTIONAL] If the system detects a Secondary Core with an eth2 port, then the alternate CnC exhaust option is displayed:</p> <p>Use alternate-exhaust for the analysis engine exhaust traffic (Yes/No)?</p> <p>Enter IP address for the alternate-exhaust (eth2) interface:</p> <p>Enter netmask for the alternate-exhaust (eth2) interface: (example: 255.255.0.0)</p> <p>Enter gateway IP Address for the alternate-exhaust (eth2) interface: (example:10.6.0.1)</p> <p>Enter primary DNS server IP Address for the alternate-exhaust (eth2) interface: (example: 8.8.8.8)</p> <p>Do you have a secondary DNS server for the alternate-exhaust (eth2) interface?</p> <p>Do you want to enter the search domains for the alternate-exhaust (eth2) interface?</p> <p>Note: A complete network interface restart can take more than 60 seconds</p>	<p>Enter yes to configure an alternate eth2 interface.</p> <p>Enter the IP address for the eth2 interface.</p> <p>Enter the eth2 netmask.</p> <p>Enter the gateway IP address.</p> <p>Enter the primary DNS server IP Address for the alternate-exhaust (eth2) interface.</p> <p>Enter yes or no to confirm or deny an eth2 secondary DNS server.</p> <p>Enter yes or no to indicate whether you want to enter search domain.</p>
<p>Enter the following server attributes:</p> <p>Central Manager (CM) IP Address:</p> <p>Device Name: (must be unique)</p> <p>Device Description</p> <p>Device Key PassPhrase</p> <p>NOTE: Remember this passphrase and use for all distributed devices!</p>	<p>Enter the CM external IP address, not the loopback. in order to register with and view the Collector in the CM Web UI.</p> <p>Enter the Juniper ATP Appliance Collector device name; this identifies the Collector in the Web UI.</p> <p>Enter a device Description</p> <p>Enter the same PassPhrase used to authenticate the Core to the Central Manager.</p>

**TIP** **vSwitch Setup Troubleshooting:** If your Virtual Collector is not seeing traffic, (1) confirm your environment setup [ESXi installation with OVA installation of a Juniper ATP Appliance vCollector; your vNIC for traffic collection is connected to a tap-aggregation switch]. (2) Verify symptoms [ESXi host-level interface monitoring shows expected tap traffic levels; TCPdump packet capture shows only spanning-tree traffic and no data; basic system configuration conforms to documentation. Probable Solution: If the switch port preserves VLAN tags (trunking), set the VMkernel adapter to just look at ALL (4095) VLANs and not only at default VLAN (0) as shown in Settings below:

vSwitch VLAN  
Troubleshooting  
Config in port-groups



**TIP** Although Juniper still provides an .ova for customers who use vCenter, in addition, Juniper also generates an .ovf and a .vmdk file for every build. The .ovf and .vmdk are bundled into a .tar file that you download and expand.

For customers who do not want to use vCenter for the virtual collector deployment: download the .tar file and expand both the OVF and the VMDK into the same directory. Then, from the vSphere client, click on File -> Deploy OVF Template. Choose the .ovf file and then complete the deployment of the ovf wizard. The configuration wizard prompts for collector/core properties such as IP address, hostname, device key. Log in to the CLI and configure each setting.

## Configuring Juniper ATP Appliance Web Traffic Collection

When powered up, the Juniper ATP Appliance Collector performs its boot process and then displays a CLI login prompt. Use the following procedure to configure the Juniper ATP Appliance Server using the CLI command line and Configuration Wizard.

**NOTE** FOR OVA DEPLOYMENTS: this configuration process is optional and can be skipped because these settings are addressed during OVA deployment to the VM vSwitch.

**TIP** Integration requirements for the Email Collector: Microsoft Exchange 2010+

To Configure the Collector

1. In the Login window, enter the default username `admin` and the password `juniper`.

**NOTE** The Juniper ATP Appliance Web UI login username and password are separate from the CLI admin username and password.

2. When prompted to reset the password, re-enter the password `juniper` as the "old" password, and enter a new password (twice).

The CM Web UI supports passwords up to 32 characters, and at least 8 characters. Letters (uppercase/lowercase), numbers, and special characters can be used with the exception of double-quotes (") , spaces, or backslash characters (\) in passwords.

3. At login, the Juniper ATP Appliance Central Manager Dashboard is displayed, as shown below. The Dashboard tab includes aggregated malware detection information and provides system status and health information. Additional configurations are made from the Config tab. The main Juniper ATP Appliance CM Web UI tabs are described below.

The Traffic Collector will now automatically “call home” to the Central Manager to announce it is online and active.

Wait ~5 minutes and confirm Collector connectivity from the Juniper ATP Appliance Web UI, as described further below.

When the Configuration Wizard exits to display the CLI, you may use the commands listed in [Verifying Configurations and Traffic from the CLI on page 10](#) to view interface configurations and to whitelist an Email Collector (in distributed systems) if one is already installed and configured. Special characters used in CLI parameters must be enclosed in double quotation marks.

- To exit the CLI, type **exit**. Be sure to confirm Collector activity from the Juniper ATP Appliance Central Manager Web UI (below).

```
JATP (collector) # exit
```

## Setting the same Device Key Passphrase on all Juniper ATP Appliance Devices

The same device key must be set on all Juniper ATP Appliances in your network, no matter how remote the distributed devices may be. To set a device key passphrase, SSH into the device, login, and use the following CLI commands:

```
JATP (server) # set passphrase <strongPassphraseHash>
JATP (server) # show device key
```

Most characters are valid for the passphrase, except for the following cases:

- Passphrases including white spaces must be put inside quotations “”.
- Passphrases including the character \ must be put inside quotations “”.
- If the passphrase includes the “ character, the “ character itself needs to be escaped.

**NOTE** Always use the latest version of Putty for SSH operations, if using Putty as an SSH client.

## Verifying Configurations and Traffic from the CLI

To verify interface configurations, use the following CLI commands. Refer also to the Juniper ATP Appliance CLI Command Reference for more information and to set traffic-filter and x-forwarded-for configurations:

Table 1 Verify CLI Commands

CLI Mode & Command	Purpose
JATP (diagnosis) # setupcheck all	Run a check of all system components
JATP (server) # show interface	Verify interface connectivity and status
JATP (server) # show ip <interface>	Verify traffic [example: show ip eth1]
JATP (server) # ping x.x.x.x	Ping connected devices.
JATP (diagnosis) # capture-start <IP address> <interface>	Starts packet capture as a means for diagnosing and debugging network traffic and obtaining stats (not part of the Collector traffic capture engine).

**NOTE:** Be sure to refer to the Juniper ATP Appliance CLI Command Reference for more information. Special characters used in CLI parameters must be enclosed in double quotation marks.

## Accessing the Juniper ATP Appliance Central Manager Web UI

To access the Juniper ATP Appliance Central Manager (CM) Web UI, use HTTP/HTTPS and enter the configured Juniper ATP Appliance CM IP address or hostname in a web browser address field, then accept the SSL certificate when prompted. Login is required.

### To Log in to the Central Manager Web UI

- The Juniper ATP Appliance CM Dashboard views (Operations | Research | System | Collectors [Web | Email]) provide in-context and aggregated malware detection information as well as system status and health statistics.

Use the Config>Web Collectors and Config>Email Collectors tab to verify that a new Collector is calling the Central Manager (CM) Web UI, and is online and actively inspecting and collecting traffic. Instructions are provided in the next section and the Operator's Guide.

### Setting SSH Honeypot Detection

A honeypot deployed within a customer enterprise network can be used to detect network activity generated by malware attempting to infect or attack other machines in a local area network. Attempted SSH login honeypots are used to supplement detection of lateral spread events. A honeypot can be deployed on a customer Traffic Collector from which event information is sent to the Juniper ATP Appliance Core for processing. Customers can place a honeypot on any local network they desire.

A malicious actor attempting to perform brute force SSH entry, or execute targeted SSH access to a "root" account, will also be detected by the Juniper ATP Appliance SSH Honeypot feature.

Results of SSH Honeypot detections are displayed on the Central Manager Web UI Incidents page, and included in generated Reports.

Data sent to the Juniper ATP Appliance GSS for honeypot detection events include "Threat Target" and a detailing of all attempted "SSH sessions" (including username and password) with timestamps.

---

**NOTE** NOTE: A Juniper ATP Appliance Enterprise License is required for SSH Honeypot lateral Detection configurations.

---

A honeypots can operate on a Juniper ATP Appliance All-in-One system or on a Traffic Collector-only device, as long as the host has enough physical interfaces. Each honeypot uses two interfaces, one externally-facing interface for internet/intranet traffic and one for internal host-to-guest communication. This means that each honeypot will use the eth3 interface for all outbound traffic.

---

**TIP** Note that eth3 is not necessarily the fourth interface on a device. On a Collector-only device with three interfaces, the interfaces are named eth0, eth1, and eth3. A collector with four interfaces uses eth0, eth1, eth2, and eth3 naming. If a Collector has less than three interfaces, then the honeypot feature cannot be enabled. An All-in-One device requires at least four interfaces for the honeypot feature, because the 3rd interface is already reserved as the analysis exhaust interface.

---

SSH Honeypot is configured from the Juniper ATP Appliance device CLI. There are two parameters that can be set for a honeypot:

- Enable/disable the honeypot
- Provide a Static IP (IP, mask, and gateway) or DHCP of the publicly addressable interface

---

**NOTE** The static IP configuration does not require configuring DNS; at this time, honeypots do not require a DNS server.

---

For more information:

- Refer to the CLI Command Reference for usage of the SSH Honeypot commands.
- Refer to the Operator's Guide for information about honeypots and lateral detections.

## Verifying Traffic Collection from the Web UI

Verify that configured Collectors are calling the Central Manager (CM) Web UI and are online and actively collecting traffic. Use the CLI to show interface and packet statistics; see [Verifying Configurations and Traffic from the CLI](#).

### Verifying Collector Activity from the Central Manager Web UI

- Select Config>System Settings> Web Collectors or Config>System Settings> Email Collectors from the Central Manager Web UI to confirm Collector(s) connectivity.

Figure 2 Central Manager Web and Email Traffic Collector(s) Configurations

#### Configuration Tab

The screenshot shows the 'Config' tab of the Juniper ATP Appliance web interface. The left sidebar contains a navigation menu with 'Web Collectors' and 'Email Collectors' highlighted. The main content area displays a table of configured collectors.

Collector	Hardware	IP address	Description	Zone	Software	Threat Protection	Enabled
PartnerDemo-File-w-Coll...	8 CPUs	192.168.1.131	PartnerDemo-File-w-Coll...	Default Zone	4.1.1.13	4.1.1.8	✓
PartnerDemo-File-w-Coll...	8 CPUs	192.168.1.170	PartnerDemo-File-w-Coll...	Default Zone	5.0.1.5	5.0.1.3	✓
vcoll149	8 CPUs	10.2.10.149	vcoll149	Default Zone	4.0.1.19	4.0.1.3	✓
demo-next2-core	16 CPUs	192.168.1.122	webcollector	Default Zone	4.1.0.780	4.1.0.156	✓
demo-next2-colle-ctor	8 CPUs	192.168.1.164	demo next x colle-ctor	Default Zone	4.1.1.13	4.1.1.8	✓
Partner-Collector-De...	8 CPUs	192.168.1.131	Partner-Collector-Demo-Next	Default Zone	4.0.1.31	4.0.1.8	✓
PartnerDemo-File-w-Coll...	8 CPUs	192.168.1.143	PartnerDemo-File-w-Coll...	Default Zone	4.1.1.13	4.1.1.8	✓

- Once the Collectors have called home to the CM, further configuration options and modifications are available from the Configuration Web UI pages.

**NOTE** The Central Manager updates Collector activity and intelligence every 5 minutes.

To verify traffic collection from the CLI, refer to Verifying Configurations and Traffic from the CLI in this guide.

Be sure to refer to the CLI Command Reference for all command details syntax and usage.

**TIP** A Web Collector or Secondary Core will be shown as down if it has not reported to the Juniper ATP Appliance Central Manager for longer than 25 minutes (in other words, 5 reporting cycles).

**RECOMMENDATION:** Juniper recommends you clear the system database after becoming familiar with incidents and kill chain flows. If you are running a trial version, clear the database and remove sample incidents and events before putting the system into full production.



---

**NOTE** Refer to the Operator's Guide for information about using the Incidents page and the interactive Dashboard views.

---

## Traffic Collector Performance

The following tables show the objects processed per hour for each Traffic Collector hardware-based model option. Note that the All-in-One product includes an embedded Traffic Collector.

The second table provides performance information for Virtual Collectors.

## What to Do Next?

- Navigate to the Config tab and select System Profiles > Licensing from the left panel; upload your license key (obtained from your sales representative).

---

**NOTE:** SMB Lateral Detection and SSH Honeypot Detection require an Enterprise License.

---

- Use the Central Manager (CM) Web UI Dashboard and Config pages to confirm traffic monitoring and detection activity. The CM updates security intelligence every 5 minutes, so you may need to wait 5 minutes to see activity at the Web UI. Refer to the Operator's Guide for more detailed information.
- For Email Traffic Collector deployments, refer to the Operator's Guide for information about deploying Collectors in MSSP Tenant Zones, configuring Email Detection Enhancements, Email Threat Quarantine options, and Email Journaling.
- Refer to the Core/CM Quick Start Guide or All-in-One Quick Start Guide for more information about installing and managing distributed Collectors.
- Refer to the Mac Mini OS X Quick Start Guide for information about installing a Mac Mini Detection Engine.
- Refer to the CLI Command Reference for information about Collector CLI commands.
- Refer to the Operator's Guide for information about all products and usage.
- Refer to the API Guide for information about accessing and managing advanced threat detection using APIs, including processing data, device and software configuration.
- Refer to the CEF Logging Support for SIEM Integration Guide for information about CEF logging.

