



Corero Network Security

SmartWall Threat Defense Director Getting Started Guide (ESXi)

Software 10.3.2

05 November 2021

Part Number: 9503-1032-00

Legal and Copyright Information

Corero Network Security, Inc. (Corero) reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of Corero to provide notification of such revision or change. Corero provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. Corero may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If you are a United States government agency, this documentation and the software described herein are provided to you subject to the following:

This paragraph applies to all acquisitions of the software by or for the United States Government, or by any prime contractor or subcontractor (at any tier) under any contract, grant, cooperative agreement or other activity with the United States Government (collectively, the "Government"). All technical data and computer software are commercial in nature and developed solely at private expense. The software and documentation respectively are "commercial computer software" and "commercial computer software documentation" as defined in DFARS 252.227-7014 (June 1995) and "commercial items" as defined in FAR 2.101(a) and, to the maximum extent permitted by law, are provided with only such rights as are provided in Corero's standard commercial license for the software and documentation and this notice. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (November 1995) or FAR 52.227-14 (June 1987), whichever is applicable. Corero's standard commercial license for the software and documentation and this notice shall govern the Government's use of the software, documentation, and technical data, and shall supersede any conflicting contractual terms or conditions. If these terms and conditions fail to meet the Government's needs or is inconsistent in any respect with Federal law, the Government must return the software and the documentation unused to Corero. The following additional statement applies only to acquisitions governed by DFARS Subpart 227.4 (October 1988): "Restricted Rights – Use, duplication and disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 (OCT. 1988)." The Contractor is Corero Network Security, Inc.

You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this document.

No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from Corero.

The products described in this document are protected by US Patent No. 9,442,782, US Patent No. 10,341,364, and European Patent No. 1319296.

Any software on removable media described in this documentation, is furnished under a license agreement which is located on the Corero web site.

Corero®, First Line of Defense®, SecureWatch®, and SmartWall® are registered trademarks of Corero Network Security, Inc. All other trademarks and registered trademarks are the property of their respective holders.

For warranty, licensing and maintenance agreement information, visit http://www.corero.com/support/End_User_Agreements.html.

Copyright © 2014- 2021, Corero Network Security, Inc.

CONTENTS

Legal and Copyright Information	2
Contents	3
TDD Documentation	8
SmartWall Threat Defense Director	9
Working with the SmartWall TDD applications and documentation	9
Juniper Networks MX Series router Requirements	11
Core Concepts	12
Provisioning Command Line Interface (pCLI)	12
Policy	12
Protection Profiles	12
Clusters	12
Devices	12
Segments	12
Defense Mode	13
Licenses	13
Analytics	13
Sampled Traffic	13
Telemetry	14
NETCONF	14
SmartWall Service Portal	14
Deployment Checklist	16
Network Configuration for TDD Deployment	18
Sending traffic samples to the vNTD	18

CONTENTS

Securing your SmartWall applications	18
Firewall Considerations	19
SmartWall TDD Deployment	20
Separately hosted TDD applications managing one Juniper Networks MX Series router	20
TDD applications, on one host, managing one Juniper Networks MX Series router	22
Deploying vNTDs for Different Sampled Traffic Rates	23
Using this document to deploy a vNTD	23
Deploying the TDD Virtual Components	24
Juniper Networks MX Series router Requirements	24
Virtual Editions components	24
Required information	25
System requirements	25
Host requirements	25
Virtual appliance requirements	26
Additional Requirements	28
Clustering and vMotion Requirements	29
Deploying a virtual edition on an ESXi server	30
To deploy a Corero Virtual Appliance using ovftool	30
To deploy a Corero Virtual Appliance using vSphere WebClient	32
Resizing a vSWA application	38
Verify TDD Component Installation	38
Configuring the TDD Components	40
Accessing the pCLI on a virtual appliance	40

CONTENTS

Configuring SmartWall Components Using the pCLI	40
Using the pCLI Setup Wizard to Configure a SmartWall Component	40
(Optional) SmartWall SecureWatch Analytics Considerations	45
Installing the TDD license file	47
To upload a license file to the SWA	47
Use with an HTTP Proxy	47
Uploading a vNTD license to the CMS	49
Setting the Inbound Sample Rate between the vNTD and the CMS	50
Adding a vNTD to the CMS	50
Prerequisites	50
To edit the default Cluster to expect sampled traffic	50
To add a vNTD to the CMS	51
Configuring the vNTD Segment for TDD	53
To configure a Segment for TDD	53
To disable the second Segment	53
Connecting CMS with SWA	55
(Optional) Add a signed certificate to the CMS - SWA connection	56
To add CMS credentials to the SWA	57
(Optional) Uploading a custom SSL certificate to the CMS	57
Configuring the Juniper Networks MX Series router	58
Prerequisites	58
To configure a Juniper Networks MX Series router for use with the SmartWall TDD system	59
Prerequisite: Accessing and editing router configuration	60
Step 1: Transport sampled packets from the router to the vNTD	60

CONTENTS

Step 2: Configure the router to accept filters from TDD	65
Step 3: Configure the router to accept filters from TDD	65
(Optional) Step 4: Set up role-based access	67
Adding a Juniper Networks MX Series router as a Remote Device ...	68
To add a router to the SWA	68
To configure the Mitigation Alerts to send mitigations to those devices ..	69
Verifying the TDD System is Connected	70
To verify the TDD system is connected	70
To force a Remote Device Info system check	70
Configuring the TDD Policy for your Network	72
Troubleshooting	73
Cannot access the Web UI (CMS or SWA)	73
Getting help for using the CMS or SWA	73
CMS configuration change does not take effect	73
Defense device not reachable from CMS	73
The Defense device shows out-of-sync in the CMS	74
vNTD device showing as not-licensed	74
Remote Device added to the CMS Devices table instead of the SWA	75
Cannot add a new vNTD to a CMS Cluster	75
SWA doesn't show any data from the CMS	75
Remote Device Info table (System > Health) is showing warning against new router	76
SWA doesn't show any telemetry data from a router	76
Telemetry traffic is only showing for one of my connected routers	77

CONTENTS

Traffic is entering the network, but the Defense device does not seem to do anything with it	77
Mitigations are not performing the actions I expect	78
To change the Operating Mode to Mitigate	78
CMS shows uncleared alarms	78
Lost administrative user credentials	78
Downloading diagnostic packages	79
After restarting my server, the Corero applications haven't come back up	79
To configure the host to auto-start VMs after a restart	79
Requesting Technical Support	81
Self-Help Online Tools and Resources	81
Creating a Service Request with JTAC	81
Requesting Licenses	82
Appendix A – Deploying a vNTD for High Inspection Rates	83
To deploy a vNTD using vSphere WebClient	83
Isolate the sampled traffic NICs for PCI Passthrough and optimize host ..	83
Deploy a vNTD for high sampled traffic rates	84
Allocate sampled traffic NICs to complete PCI Passthrough and optimize the vNTD	89

TDD Documentation

There are three main documents which you can use to learn more about the SmartWall TDD:

Document	Location	Use
SmartWall TDD Getting Started Guide	The appropriate guide (KVM or ESXi) is provided by your Support representative or available on the Juniper support portal	Deploy a SmartWall TDD on your own servers. After completing the tasks in this guide, your TDD will be ready for use.
SmartWall TDD User Guide	PDF help from the top menu of the SWA Web UI or available on the Juniper support portal	Manage your SmartWall TDD. Contains TDD specific tasks and reference information for the SWA Web UI.
SmartWall TDD CMS User Guide	Context sensitive help site built into the CMS Web UI or available on the Juniper support portal	Understand general system tasks, enabling you manage your Defense devices and troubleshoot any issues. Contains reference information for the CMS Web UI, CLI, pCLI and REST API.

Note: The SmartWall TDD User Guide available from inside the SWA and CMS User Guide available from inside the CMS contain additional information compared to the versions of the guides available on the Juniper Support Portal. This information is only available to customers and is not publicly accessible.

SmartWall Threat Defense Director


The SmartWall Threat Defense Director (SmartWall TDD) works together with Juniper Networks® MX Series routers to filter out DDoS attack traffic at the edge of your network.

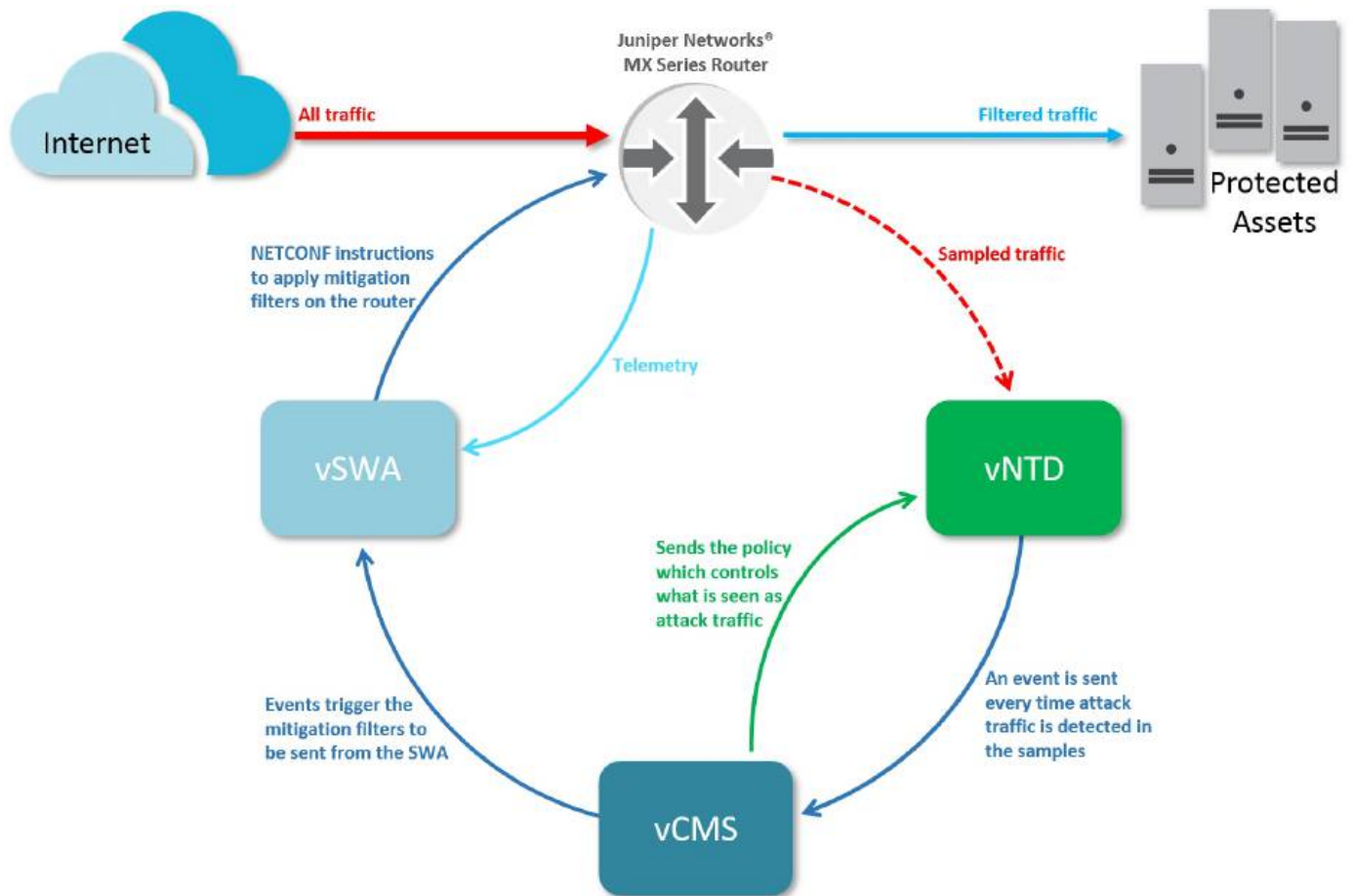
A SmartWall TDD system requires the following components:

- **Remote Devices** – The Juniper Networks MX Series router at the edge of the network being protected. They send sampled traffic to the vNTD and are directed by vSWA to apply firewall filters to block DDoS attack traffic.
- **Defense Director** – A bundle of three virtual applications:
 - **vSWA** – The SmartWall SecureWatch Analytics Virtual Edition (vSWA) receives information from the Detection Engine (via the vCMS) to identify the DDoS attacks currently active against your network. The vSWA application then sends firewall filter commands to the router to filter the attack traffic as it arrives at the router. The vSWA application also displays real-time and historical statistics that enable you to analyze attacks on your network.
 - **vCMS** – The SmartWall Central Management Server Virtual Edition (vCMS) controls the Detection Engine and enables you to configure the attack mitigation policy used to distinguish attack traffic from normal network traffic.
 - **Detection Engine (vNTD)** – The SmartWall Network Threat Defense Virtual Edition (vNTD) is the Detection Engine for the SmartWall TDD. It detects DDoS attack traffic in mirrored samples sent from the edge routers.
- **Additional Detection Engines** – The Defense Director bundle includes a single Detection Engine (vNTD). You may need to purchase additional Detection Engines for your deployment.

Working with the SmartWall TDD applications and documentation

The same three applications which power the SmartWall TDD are also used in the Corero SmartWall Threat Defense System (SmartWall TDS). The SmartWall TDS is primarily used inline or in a scrubbing configuration, where the Defense devices block traffic directly. As the system shares common components, you may see the following types of information relating to the SmartWall TDS:

- Some features in the CMS are designed for NTD inline mitigation and will not be available in a SmartWall TDD deployment. When working in the CMS, if you are unsure if a feature applies to the SmartWall TDD, click  the help icon in the top left and look for a note labeled **TDD deployments**.
- In the CMS interface, events, and documentation you will see references to "blocking traffic". In a SmartWall TDD deployment, this should be interpreted as "identifying DDoS attacks".



Juniper Networks MX Series router Requirements

Your Juniper Networks MX Series routers must meet the following criteria:

- It must support Sampled Mirror, Flexible Filtering, Ephemeral Configuration, and Remote Telemetry.
- Your router should be running one of the following JunOS versions:
 - For production deployments:
 - 17.2R3
 - 17.3R3
 - **17.3R3-S8 recommended**
 - 17.4R2
 - 18.1R3
 - 18.2R2
 - 18.3R1
 - **18.3R3-S2 recommended**
 - **19.2R3 recommended**
 - **20.1R2 recommended**

Note: Recommended versions have had a broad and successful use with Corero SmartWall TDD.

- For lab tests or proof of concept deployments:
 - Any of the above
 - 16.2R3

Caution: For JunOS versions not listed, please refer to your support representative for compatibility.

Core Concepts

Provisioning Command Line Interface (pCLI)

When you install a SmartWall device or application, you need to execute essential configuration tasks using the Corero Provisioning Command Line Interface (pCLI). The pCLI is a set of commands you can use to define the initial configuration of each SmartWall® component. For initial configuration of any component, type `setup` in the pCLI to launch a wizard which will guide you through the initial configuration options.

Policy

A Policy is a configuration of the attack mitigation features which tells the Defense devices how to handle incoming traffic. Each policy is contained in a Protection Profile.

Protection Profiles

A Protection Profile is a container for a configuration of the attack mitigation features (Policy) in the CMS. When you associate a Protection Profile with a Cluster, it provides all the Defense devices in that Cluster with the same Policy for handling incoming traffic. You can create one Protection Profile for your network or multiple Protection Profiles each containing a different Policy.

Clusters

A Cluster is a set of identically configured Defense devices. When you create a new Cluster you must associate it with a Protection Profile containing the Policy which controls how the devices in that Cluster respond to traffic.

Devices

There are two types of devices in the SmartWall TDD system:

- **Defense devices** – This is broader term for the vNTDs (SmartWall Network Threat Defense Virtual Edition devices) which are used purely as Detection Engines in a SmartWall TDD deployment
- **Remote Devices** – This is a broader term for the Juniper Networks MX Series router used to mitigate DDoS attack traffic

While the SmartWall TDD only uses the above device types, in the user interface and documentation you should be aware that device can refer to any of the Defense devices compatible with the SmartWall TDS system (vNTD, NTD1100, NTD280, NTD120 and Bypass Devices).

Segments

A Segment is a set of 1 or 2 interfaces to which DDoS protection is applied. The first time you connect a Defense device to the CMS, it identifies the available interfaces and records them as Segments. A vNTD has two available interface

ports which act as 2 single interface Detector Segments. If you don't require the second Segment, you can disable it after deployment.

Defense Mode

The Defense Mode is the default traffic handling mode which tells the system whether it should use the rest of the Policy features to block attack traffic, just inspect the traffic, or send the traffic to the internal network without any inspection.

For a TDD deployment, when you select a defense mode you have the following options:

- **Mitigate** mode – The TDD system instructs the router to discard attack traffic.
- **Monitor** mode – The router will complete all steps as if it was mitigating traffic (i.e. sending telemetry to SWA) but will accept the attack traffic.

Note: In the CMS documentation and user interface, the Defense Mode is described for an inline SmartWall TDS deployment where the Defense device is able to directly block traffic. In the TDD system the blocking is only ever performed by the routers. Pass-through mode only applies to the TDS system.

Licenses

The SmartWall TDD system requires two types of license:

- **TDD License** – The main license for your TDD system
- **vNTD License(s)** – The correct number of licenses to cover all of your vNTD detection devices

Due to the different security measures protecting each license type, they must be requested and installed in different ways.

Analytics

Analytics is the process of collecting and analyzing the event and system information generated by the Defense devices. The Defense devices send analytics syslog messages to the CMS where that information is aggregated and sent to SWA.

Sampled Traffic

This is a feed of a proportion of the traffic received by the Juniper Networks MX Series router ahead of any mitigation. The vNTD uses this traffic to detect DDoS attacks, and enables the TDD system to generate the filter instructions it sends to the Remote Device to block that attack traffic and permit non-attack traffic. For example, if you have 1Tbps of traffic coming into a Remote Device, and a sample rate of 1:1000, the vNTD will see 1Gbps of sampled traffic.

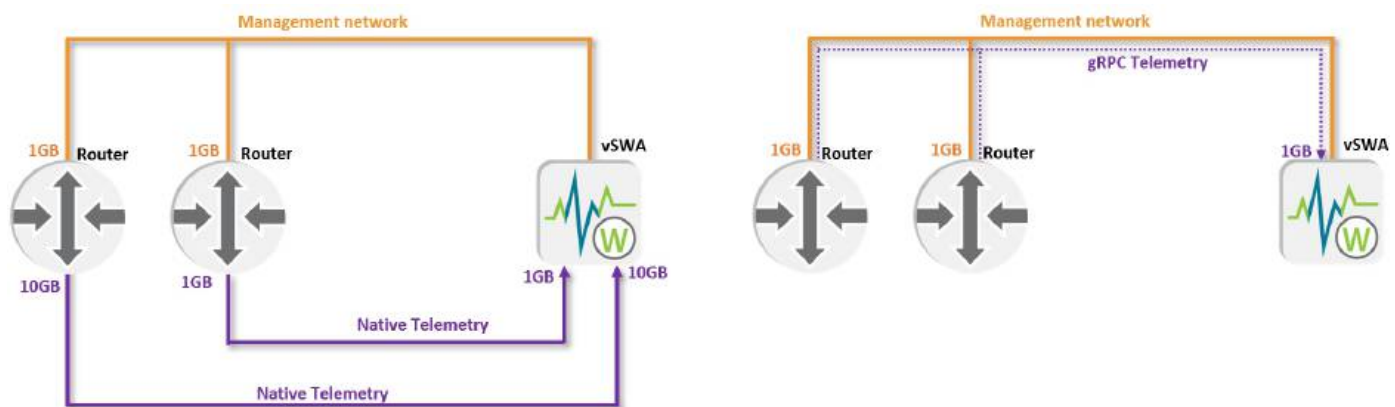
Telemetry

Telemetry is sent from the Juniper Networks MX Series router to the vSWA. It shows the network traffic processed by the router including what was permitted or blocked by the TDD system.

The TDD requires a telemetry feed from every monitored router to the SWA application. There are two main telemetry delivery methods:

- **Native telemetry** (UDP) – Telemetry is sent over your traffic network between the router and SWA. This requires a non-management interface on the router and on the SWA host unit.
- **gRPC telemetry** – Telemetry is sent over the 1GB Management network. With gRPC telemetry you have the option to encrypt the telemetry traffic using SSL certificates.

You decide which telemetry type is used when you [configure the Juniper Networks MX Series router](#). If you choose gRPC telemetry, you must download 2 additional software files to the router during set up and then provide additional configuration information when [adding the router to the SWA as a remote device](#).



NETCONF

The TDD system uses NETCONF to configure the ephemeral firewall rules in the Juniper Networks MX Series router to block or permit network traffic.

SmartWall Service Portal

The SmartWall Service Portal enables you to offer Corero SmartWall DDoS Protection, as a managed service, to your customers. The Service Portal is a customer-facing DDoS protection portal which uses traffic data from your SmartWall TDD and displays the information in easy to read dashboards and reports. Your customers can log in to the portal and view the attacks you have protected them against. For information on Service Portal versions which are compatible with your SmartWall TDD, see the SmartWall TDD release notes.

Note: If you do not have a Service Portal and would like to add one to your existing TDD system, contact your support representative for more information.

Deployment Checklist

The following checklist provides an overview of the deployment process. Verify each step is complete before moving on:

Location	Action	Done?
On your PC	Save the TDD license file you received when you purchased the TDD.	
On the host server	Setup host server(s) and make any network changes.	
On the host server	Download the following install files from https://corero.force.com : corero-ntd-virtual-edition_10.3.2.xxxx-vmware.ova, corero-cms_10.3.2.xxxx-vmware.ova, corero-swa_10.3.2.xxxx-vmware.ova	
On the host server	Deploy vSWA and use the pCLI to setup management and secondary network interfaces.	
On the host server	Deploy vCMS and use the pCLI to setup management interface.	
On the host server	Deploy vNTDs (or high sampled traffic rate vNTDs) and use the pCLI to setup management interfaces.	
On your PC: SWA web UI	Upload TDD license file to SWA.	
On your PC	Request your vNTD Licenses and save files.	
On your PC: CMS web UI	Upload the vNTD license to the CMS.	
On your PC: CMS web UI	Add vNTD to CMS.	
On your PC: CMS web UI	Disable 2nd interface and disable LSP for each vNTD.	
On your PC: CMS web UI	Setup the connection between CMS and SWA.	
On router CLI	Configure routers to send traffic samples to the vNTDs and receive filters from SWA.	
On your PC: CMS web UI and SWA web UI	Add router authentication credentials to CMS and SWA.	
On your PC: CMS CLI	Configure default defense policy for TDD system.	

Location	Action	Done?
On your PC: CMS web UI and SWA web UI	Tune Policy for your network and, optionally, setup multiple Clusters and Protection Profiles.	

Caution: When the TDD system is installed, it is recommended to set it to Monitor Mode (the CMS Defense Mode which shows how the system will affect traffic when mitigating but does not block any traffic). When you have evaluated and tuned the CMS Policy for your network traffic, you can then switch the system into Mitigate Mode and begin blocking DDoS attack traffic.

Network Configuration for TDD Deployment

To operate correctly, a SmartWall TDD installation will require network configuration settings and certain ports to be available between components.

- You may want to have the IP addresses ready for any other syslog clients you intend to use.
- You must allow outbound TCP port 443 traffic to enable the TDD to connect to the Corero License server. To establish licensing, you must [install a SecureWatch package](#) on the vSWA.
- **Port-Mirroring Traffic samples only:** When hosting a SmartWall TDD, truncated samples should not be used on the Juniper Networks MX Series router. The JunOS command `set forwarding-options port-mirroring maximum-packet-length` should have a value of 0 (disabled).
- **Port-Mirroring Traffic samples only:** The MTU path from routers to the SmartWall TDD should account for encapsulations (e.g GRE). An MTU of 2000 is usually adequate.
- **Port-Mirroring Traffic samples only:** Port-mirroring samples should not be received on the same physical port as telemetry or management traffic.

Sending traffic samples to the vNTD

Note: The traffic sampling method is configured during [router configuration](#) and when you [add the vNTD to the CMS](#).

When you're using a detector segment, the vNTD can accept traffic samples in the following ways. Using the CMS, you need to configure the Segment differently, depending how your traffic samples arrived at the vNTD:

- **Mirrored traffic samples direct from the router** – The vNTD must be directly connected to the router with no truncated samples. No additional configuration required on the CMS.
- **Mirrored traffic samples over a GRE tunnel** – The vNTD only needs to be accessible from the router. Edit the Segment to add an **IPv4 Address**, a **Peer IPv4 Address**, and enable **GRE Ingestion**.

Caution: If you have multiple routers sending traffic samples in different formats, you **must** ensure all sample rates are the same. Otherwise, the mitigation thresholds and traffic charts in the SWA will not work correctly.

Securing your SmartWall applications

Corero recommends following best practice industry standards to secure your SmartWall deployment:

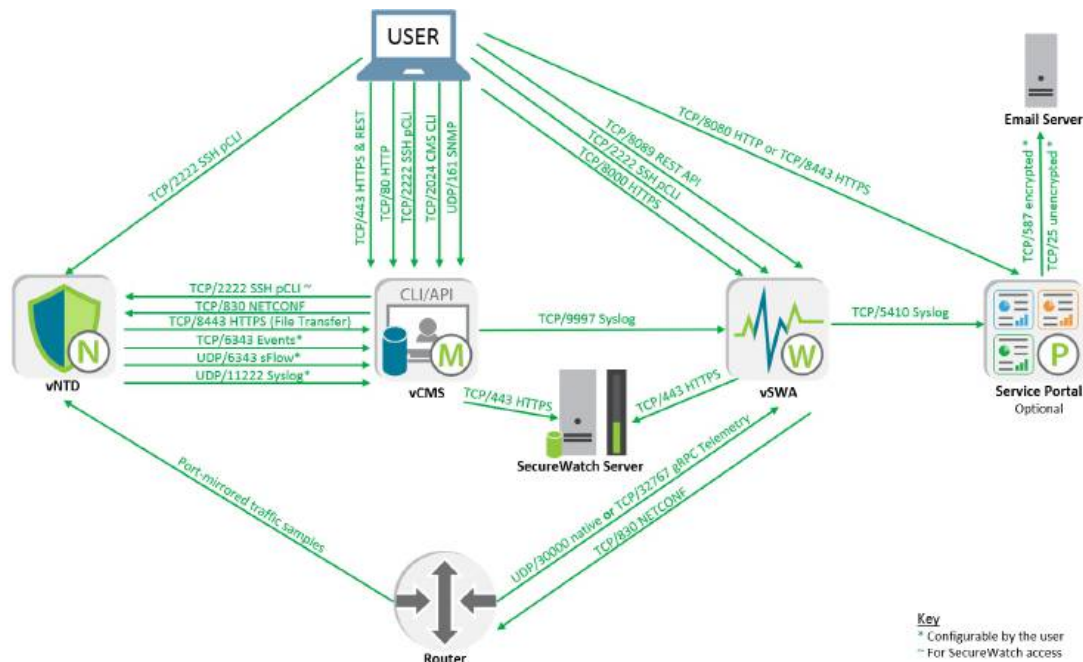
- Connect management interfaces to secure networks, isolated from the Internet, to prevent unauthorized access to the SWA, CMS, or NTD.

- If practical, run Corero CMS and SWA virtual machines on a dedicated server to physically isolate them from other guest virtual machines.
- If running CMS and SWA on shared virtual infrastructure, ensure you apply latest security fixes as they emerge. This may require:
 - Patching the server BIOS for new CPU firmware.
 - Patching the hypervisor.
 - Patching other guest virtual machines operating systems
 - Patching other guest VMs and applications that may be running on the same server as Corero management components.
- Limit access to the CMS and SWA to authorized personnel. Ensure adequate access controls are in place.
- Ensure authorized personnel are associated with the correct access roles on the CMS and NTD.
- Use strong access credentials, regularly changed, through authentication service such as LDAP or RADIUS to authenticate access to your users.
- Limit knowledge of privileged account credentials.
- After deployment, change default NTD credentials and manage using Authentication Groups in the CMS. **Note:** The same NTD credentials are used for managing NTDs from the CMS and for accessing the NTD pCLI.
- Apply the latest software updates from Corero which contain the latest available security patches.

Firewall Considerations

Your SmartWall deployment should be protected by your network infrastructure's firewall. You will need to modify your firewall policy to allow access on certain ports.

The following diagram shows the default network ports required for a full SmartWall TDD deployment:



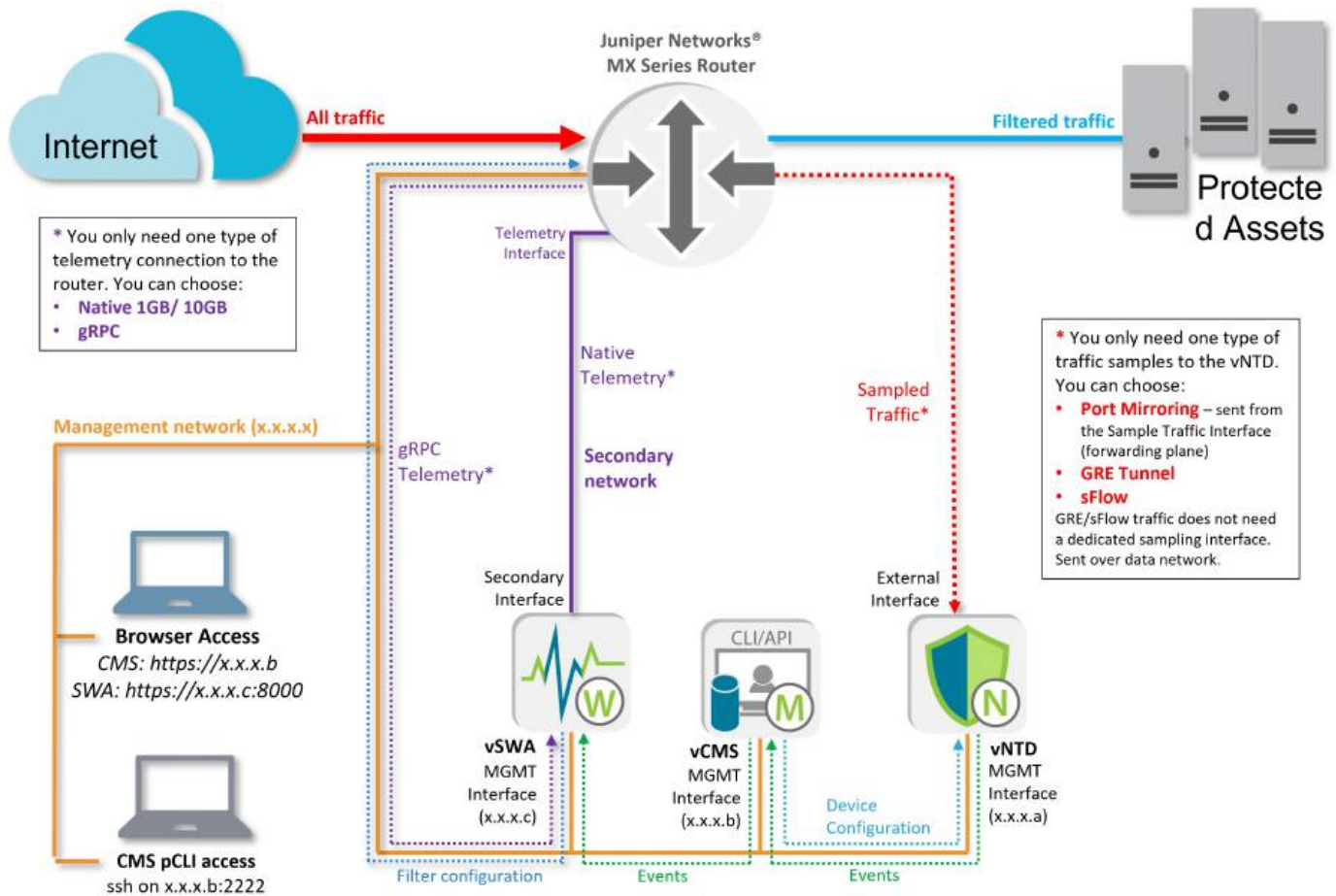
Note: If your SmartWall TDD comes with Corero's SecureWatch Service, this also requires a change to your firewall policy. Contact your support representative for the required information.

SmartWall TDD Deployment

The following diagram shows a common deployment scenario for the SmartWall TDD. If you require further assistance configuring the best deployment for your network, contact your support representative.

Separately hosted TDD applications managing one Juniper Networks MX Series router

In this scenario, the three SmartWall TDD applications are all installed separately, on the same management network as the router they are receiving sampled traffic from. The diagram shows the three possible routes for telemetry to be passed from the router to the SWA.



Deploying vNTDs for Different Sampled Traffic Rates

There are multiple ways to deploy a vNTD on your own server. If you expect a high sampled traffic rate, you must dedicate hardware resources on the host for the vNTD. If you expect a lower sampled traffic level, you can speed up your installation by skipping those steps.

Sampled Traffic Rate (sampled mirror traffic of mixed packet sizes)	ESXi
<p>Sampled traffic rates up to 250 Kpps or 1.2Gbps per core .</p> <p>Note: With a sample rate of 1:1000, this equates to up to 1.2 Tbps of protected traffic (or up to 250 million pps).</p>	<p>NICs: VMXNET3</p> <p>2 core vNTD</p> <p>No PCI Passthrough</p>
Sampled traffic rates between 1.2Gbps and 10Gbps	<p>NICs: X710/X520</p> <p>7 core vNTD</p> <p>PCI Passthrough required (see Appendix A)</p>

Caution: For the vNTD External Interface, e1000 NICs are not supported. You will experience issues viewing some statistics like packet drops and bad CRC packets. Contact your support representative for more information on choosing a NIC.

Using this document to deploy a vNTD

The main deployment method focuses on vNTDs expecting sampled traffic rates of less than 1.2Gbps per core, which do not need dedicated hardware resources to achieve necessary performance. Follow the [standard vNTD deployment instructions](#).

If you need to handle up to 10Gbps sampled traffic rates, you should use the alternative high sampled traffic rate vNTD deployment guides in [Appendix A using PCI Passthrough](#).

Deploying the TDD Virtual Components

The virtual components of the SmartWall Threat Defense Director (TDD) can be installed on a your own ESXi server. Your Corero representative will have provided you with the files you need for ESXi installation.

Juniper Networks MX Series router Requirements

Your Juniper Networks MX Series routers must meet the following criteria:

- It must support Sampled Mirror, Flexible Filtering, Ephemeral Configuration, and Remote Telemetry.
- Your router should be running one of the following JunOS versions:
 - For production deployments:
 - 17.2R3
 - 17.3R3
 - **17.3R3-S8 recommended**
 - 17.4R2
 - 18.1R3
 - 18.2R2
 - 18.3R1
 - **18.3R3-S2 recommended**
 - **19.2R3 recommended**
 - **20.1R2 recommended**

Note: Recommended versions have had a broad and successful use with Corero SmartWall TDD.

- For lab tests or proof of concept deployments:
 - Any of the above
 - 16.2R3

Caution: For JunOS versions not listed, please refer to your support representative for compatibility.

Virtual Editions components

You should have the following files saved locally (where xxxx represents the variable section of the file name):

- corero-ntd-virtual-edition_10.3.2.xxxx-vmware.ova – The vNTD OVA package
- corero-cms_10.3.2.xxxx-vmware.ova – The vCMS OVA package

- corero-swa_10.3.2.xxxx-vmware.ova – The vSWA OVA package

Required information

You need to have the following network information available for each virtual edition before you begin to install:

- **IP address and subnet mask** – The IP address you will use to access the application from your core network.
- **DNS IP address** – The address of the DNS server you will use for the site. You may have more than one of these.
- **Default gateway IP address** – The address of the default gateway for your site.
- **NTP IP address** – The address of the NTP server you wish to use for the site. You may have more than one of these. Corero can provide you with an NTP server address if you do not have one of your own.

For vCMS and vSWA, you also need **A SecureWatch® package file and unlock code**. To connect your CMS and SWA applications to the SecureWatch® Service, you will need to upload a SecureWatch® package file to both applications after deployment.

System requirements

Host requirements

Before you begin, make sure the server you plan to deploy an application on meets the following requirements:

	Defense Director (vCMS)	Defense Director (vSWA)	Detection Engine (vNTD)
Supported OS	vCenter Server 6.5 or later with ESX/ESXi 6.5 or later	vCenter Server 6.5 or later with ESX/ESXi 6.5 or later	vCenter Server 6.5 or later with ESX/ESXi 6.5 or later
Memory	ECC memory is required.	ECC memory is required.	ECC memory is required.
CPU	The CPU must support VT-x.	The CPU must support VT-x.	The CPU must support VT-x (and VT-d for high sample traffic rates). They must be enabled.

	Defense Director (vCMS)	Defense Director (vSWA)	Detection Engine (vNTD)
Datastore	Datastore provided by redundant RAID storage: <ul style="list-style-type: none"> • Minimum SAN or NAS datastore • Recommended VirtIO 	Datastore provided by redundant RAID storage: <ul style="list-style-type: none"> • Minimum SAN or NAS datastore • Recommended VirtIO 	Datastore provided by redundant RAID storage: <ul style="list-style-type: none"> • Minimum SAN or NAS datastore • Recommended VirtIO
NICs	Management NIC: E1000 or virtIO	Management NIC: E1000 or virtIO	Management NIC: e1000 or virtIO External Interfaces: <div> Caution: vNTDs MUST have an even number of external interfaces. </div> <ul style="list-style-type: none"> • For low sampled traffic rates – VMXNET3 • For high sampled traffic rates – X710 (recommended to use firmware 6.8 or higher) or equivalent NICs utilizing VT-d directed I/O technology (PCI Passthrough).

Virtual appliance requirements

The table below lists the minimum requirements for each virtual appliance that you install.

Note: When listing the number of cores, this refers to the physical cores not the hyper-thread cores. These are set to enable optimum performance of the SmartWall system.

	Defense Director (vCMS)	Defense Director (vSWA)	Detection Engine (vNTD)
Memory	<ul style="list-style-type: none"> Standard – Minimum 16 GB of memory. Large – Minimum 24 GB of memory. 	Minimum 12 GB of memory.	Minimum 12GB per socket (with seven 1GB -or equivalent- huge pages available for high sample traffic rates).
CPU	<p>Intel® Xeon® 64-Bit CPU (x86_64) Processor minimum 2GHz</p> <p>vCMS must have:</p> <ul style="list-style-type: none"> Standard – 6 physical cores Large – 8 physical cores 	<p>Intel® Xeon® 64-Bit CPU (x86_64) Processor minimum 2GHz</p> <p>vSWA is recommended to have 12 physical cores</p>	<p>Note: It is normal for vNTD to show high CPU utilization. Sometimes up to 100%.</p> <p>Intel® Xeon® 64-Bit CPU (x86_64) Processor from E3 family or later with minimum 2GHz</p> <p>vNTD must have the correct core number for its external NIC type:</p> <ul style="list-style-type: none"> VMXNET3 NIC – 2 physical cores X710 (recommended to use firmware 6.8 or higher) or equivalent NIC – 7 or more physical cores

	Defense Director (vCMS)	Defense Director (vSWA)	Detection Engine (vNTD)
Datastore	Required 120 GB datastore.	<p>Required 70 GB datastore for disk 1 and minimum 240 GB datastore for disk 2. However disk 2 can be expanded to your required size after deployment (ESXi method).</p> <p>The space required by the SWA depends on your frequency of attack and how long you need the data to be available. A good rule of thumb for most installations is 1.5 TB for 13 months of data.</p> <p>Caution: After extending the disk size, indexes must be resized.</p>	Required 20 GB datastore.
Networking	1 management interface and 1 optional secondary interface	1 management interface and 1 optional secondary interface	1 management interface and 2 or 4 data interfaces (for traffic sample inspection)

Additional Requirements

Observe the following additional requirements when deploying virtual appliances:

- **vNTDs MUST have an even number of external interfaces.**
- Changing of virtual hardware components or updating the virtual hardware version is not supported.
- Virtual Disk Storage – There are three disk formats available for virtual disk storage:
 - **Thin Provision** – Allocates only as much disk space as the VM needs on install. If there isn't adequate space when the storage needs expand, you could experience failures. **Caution:** If you use Thin provisioning, you must make sure there is ample room for the disks to reach their full size in the future.
 - **Thick Provision Lazy Zeroed** (Recommended) – Allocates all required disk space to the VM, but only prepares space as it is required.
 - **Thick Provision Eager Zeroed** – Allocates all required disk space to the VM, and immediately prepares it for the VM. This can take some time to complete.

- You need at least one management network connection with connectivity to SmartWall devices, CMS and SWA. The SWA requires a secondary network connection on the same subnet as the router's telemetry port, to receive native telemetry from the routers.
- All TDD applications must use NTP servers for system time. Any time difference between applications can cause unexpected behavior.
- NUMA Memory/CPU Affinity is recommended but not required on a NUMA system.

Clustering and vMotion Requirements

- You need multiple 1-gigabit+ links with vMotion enabled.
- You need redundant and multi-pathed SAN or NFS datastore for storage of VMs.
- If a cluster has non-identical CPUs, then EVC Mode must be enabled:
 - “Sandybridge” EVC mode or later for Intel CPUs

Deploying a virtual edition on an ESXi server

The following instructions cover how to deploy a virtual edition on an ESXi server which meets the necessary system requirements. See the [Appendix](#) for deployment instructions for vNTDs expecting high inspection rates.

To deploy a Corero Virtual Appliance using ovftool

Run the required command (below), replacing the following information:

- `<vmName>` – A name for this VM.
- `<datastoreName>` – The name of your datastore location for this VM (e.g. my-esx-server-HDD1).
- `<managementInterface>` – The name of the VMWare network label for your management network (e.g. management_subnet).
- `<secondaryNetwork>` – (Optional) The name of your secondary interface (e.g. smartwall_subnet). If you're not using a secondary network, remove `--net:Secondary=<secondarySwitch>` from the command.
- `<External_1_NetworkName>` – **(vNTD only)** The name of the first external network you need to connect the device to.
- `<External_2_NetworkName>` – **(vNTD only)** The name of the second external network you need to connect the device to. A vNTD must be deployed with an even number of interfaces. If you don't plan to use the second external interface, you can [disable it in the CMS](#) after deployment.
- `<CoreroFileName>` – The file name (including extension) of the OVA file for this VM (e.g. vcms_10.3.2.ova).
- `<hostName>` – The name of the ESXi server you're deploying the VM on (e.g. my-esx-server).

Note: The following commands include the `--powerOn` command to start the VM. If you don't want to start the VM at this point, you can use VMWare client at a later time.

vSWA or vCMS:

```
ovftool --name="<vmName>" --datastore=<datastoreName> --diskMode=lazyZeroedThick
--net:Management="<managementNetworkName>" --net:Secondary="<secondaryNetwork>"
--acceptAllEulas --powerOn <CoreroFileName> vi://root@<hostName>
```

vNTD:

Caution: Never deploy multiple vNTDs with the same network labels (`<External_1_NetworkName>` and `<External_2_NetworkName>`) as that can cause a network loop. If you do not specify network labels, the vNTD is given the default External and Internal labels. For a single VM, ensure the `<External_1_NetworkName>` and `<External_2_NetworkName>` are not the same. **vNTDs MUST have an even number of external interfaces.**

```
ovftool --name="<vmName>" --datastore=<datastoreName> --diskMode=lazyZeroedThick
--net:Management="<managementNetworkName>" --net:External="<External_1_NetworkName>"
```

```
--net:Internal="<External_2_NetworkName>" --acceptAllEulas --powerOn
<CoreroFileName> vi://root@<hostName>
```

Note: Do not specify `diskMode` when using NAS/NFS volumes.

Next Steps (vNTD only)

After install, the vNTD network adapters are not automatically connected, in case the selected ports will cause a network loop once enabled. Check the allocated ports will not create a network loop, then enable ports using vSphere WebClient.

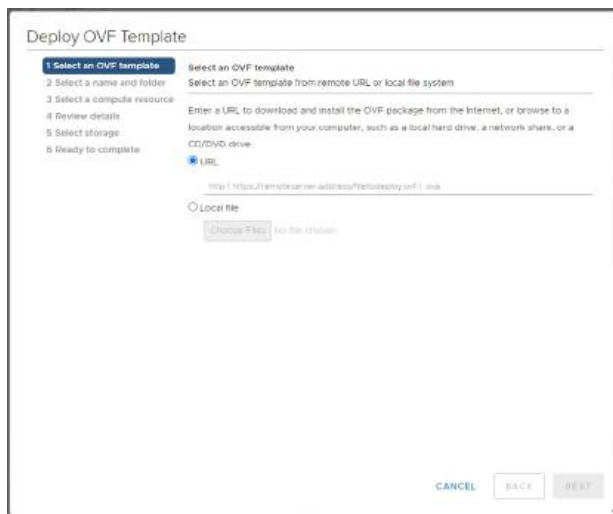
1. In vSphere WebClient, right click on your new VM and select **Edit Settings**.
2. Scroll down to **Network adapter 2**. Check the network label is correct and then under Device Status, select the **Connect** check box.
3. Repeat for **Network adapter 3**.
4. Click **OK**.

To deploy a Corero Virtual Appliance using vSphere WebClient

Caution: You must use ESXi version 6.5 or later.

To deploy the Virtual Appliance

1. In vSphere WebClient, right-click the **Host** you want to create this Virtual Appliance on, and select **Deploy OVF template**.
2. Select an OVF template:
 - Select **URL** and type the full URL to the OVA file stored on an HTTP/HTTPS server.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select an OVF template
Select an OVF template from remote URL, or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

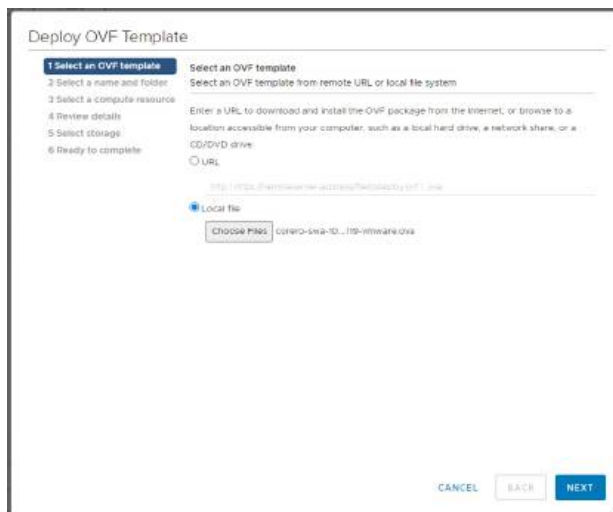
☒ URL
☐ Local file

http://https://remoteuser-access/vf/tdesploy/ovf1.ova

Choose Files No file chosen

CANCEL BACK NEXT

- Select **Local file**, click **Choose Files** and select the OVA file for your required VM.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select an OVF template
Select an OVF template from remote URL, or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

☒ URL
☐ Local file

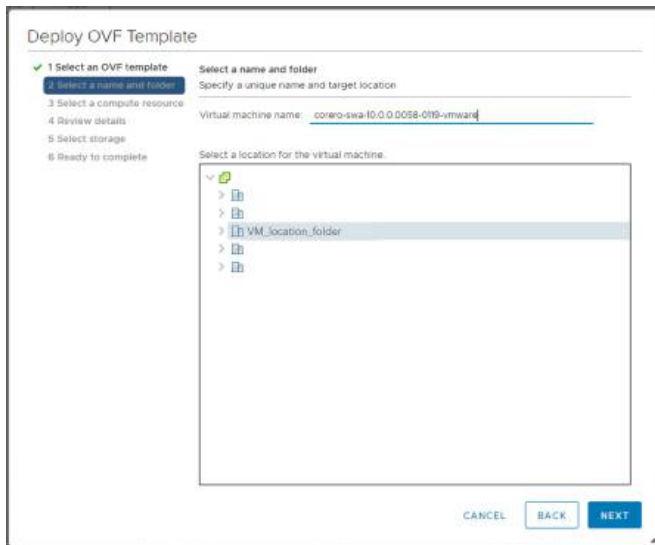
http://https://remoteuser-access/vf/tdesploy/ovf1.ova

Choose Files corero-swa-td...1hp-vmware.ova

CANCEL BACK NEXT

3. Click **Next**.
4. Type a **Virtual Machine name**.

5. Select where you want to deploy the VM.



Deploy OVF Template

✓ 1 Select an OVF template
 2 Select a name and folder
 3 Select a compute resource
 4 Review details
 5 Select storage
 6 Ready to complete

Select a name and folder
 Specify a unique name and target location

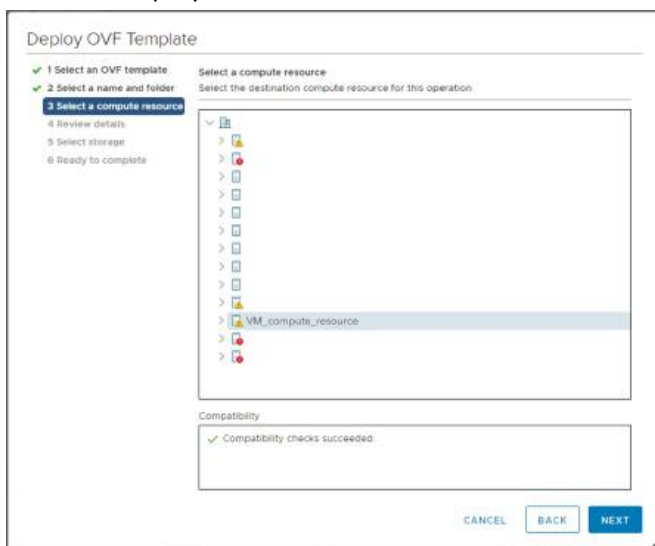
Virtual machine name:

Select a location for the virtual machine.

- > [icon]
- > [icon]
- > VM_location_folder
- > [icon]
- > [icon]

CANCEL BACK NEXT

6. Click **Next**.
7. Select the destination compute resource you want to use for this VM. This will be the host where you want the VM to be deployed.



Deploy OVF Template

✓ 1 Select an OVF template
 ✓ 2 Select a name and folder
 3 Select a compute resource
 4 Review details
 5 Select storage
 6 Ready to complete

Select a compute resource
 Select the destination compute resource for this operation.

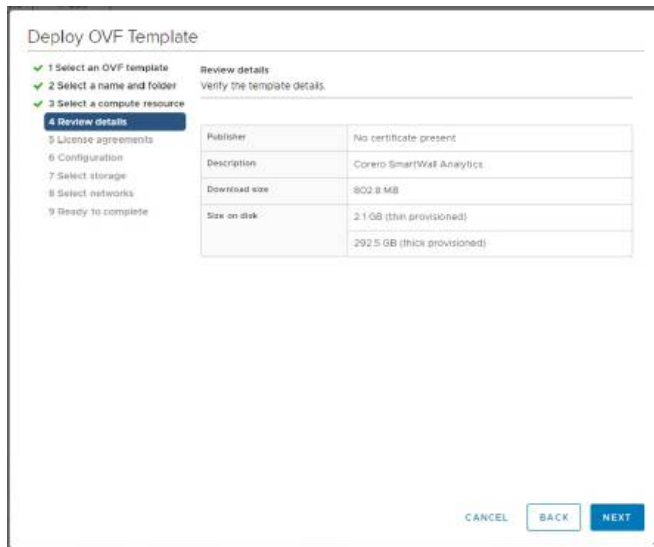
- > [icon]
- > [icon]
- > [icon]
- > [icon]
- > [icon]
- > [icon]
- > [icon]
- > [icon]
- > VM_compute_resource
- > [icon]
- > [icon]

Compatibility
 ✓ Compatibility checks succeeded.

CANCEL BACK NEXT

8. Click **Next**. The VM will be validated.

9. Review the template details.



Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details**
- 5 License agreements
- 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Ready to complete

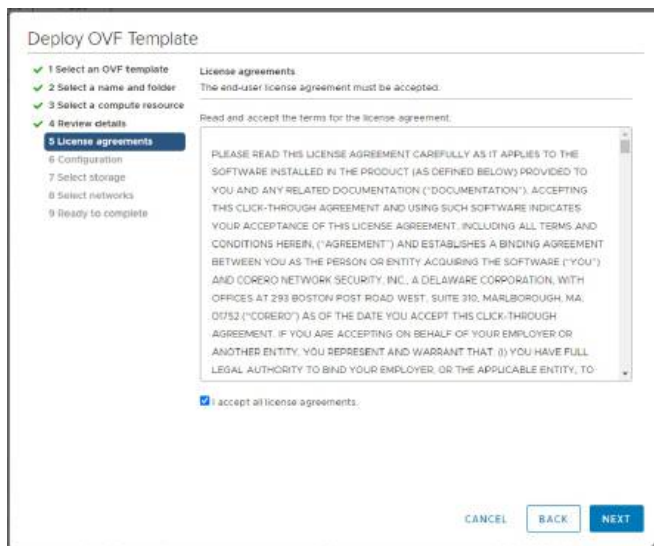
Review details
Verify the template details.

Publisher	No certificate present
Description	Corero SmartWall Analytics
Download size	802.8 MB
Size on disk	2.1 GB (thin provisioned) 292.5 GB (thick provisioned)

CANCEL BACK NEXT

10. Click **Next**.

11. Read the end user agreement and check the box next to **I accept all license agreements**.



Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements**
- 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Ready to complete

License agreements
The end-user license agreement must be accepted.

Read and accept the terms for the license agreement:

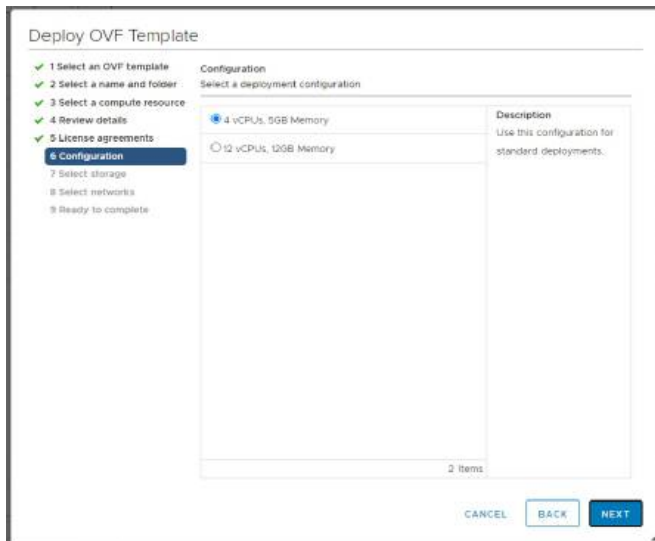
PLEASE READ THIS LICENSE AGREEMENT CAREFULLY AS IT APPLIES TO THE SOFTWARE INSTALLED IN THE PRODUCT (AS DEFINED BELOW) PROVIDED TO YOU AND ANY RELATED DOCUMENTATION ("DOCUMENTATION"). ACCEPTING THIS CLICK-THROUGH AGREEMENT AND USING SUCH SOFTWARE INDICATES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT, INCLUDING ALL TERMS AND CONDITIONS HEREIN, ("AGREEMENT") AND ESTABLISHES A BINDING AGREEMENT BETWEEN YOU AS THE PERSON OR ENTITY ACQUIRING THE SOFTWARE ("YOU") AND CORERO NETWORK SECURITY, INC., A DELAWARE CORPORATION, WITH OFFICES AT 293 BOSTON POST ROAD WEST, SUITE 310, MARLBOROUGH, MA, 01752 ("CORERO") AS OF THE DATE YOU ACCEPT THIS CLICK-THROUGH AGREEMENT. IF YOU ARE ACCEPTING ON BEHALF OF YOUR EMPLOYER OR ANOTHER ENTITY, YOU REPRESENT AND WARRANT THAT: (i) YOU HAVE FULL LEGAL AUTHORITY TO BIND YOUR EMPLOYER, OR THE APPLICABLE ENTITY, TO:

☒ I accept all license agreements.

CANCEL BACK NEXT

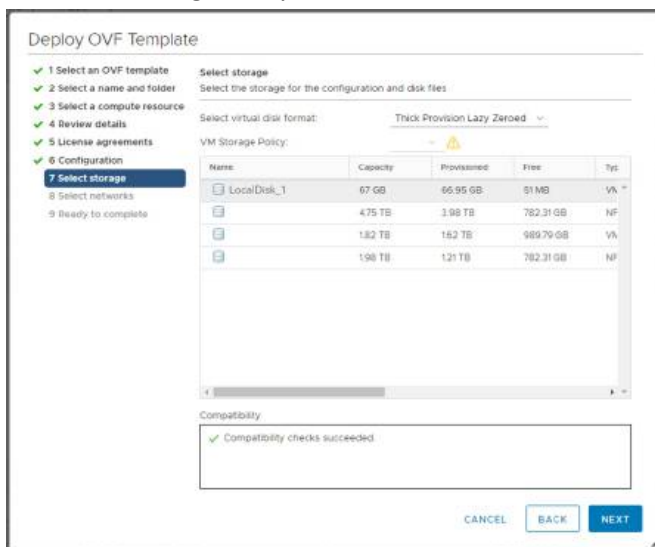
12. Click **Next**.

13. **CMS and SWA only:** Make sure the standard deployment configuration is selected:



14. From Select virtual disk format, select **Thick Provision Lazy Zeroed**.

15. Select the storage disk you want to use.



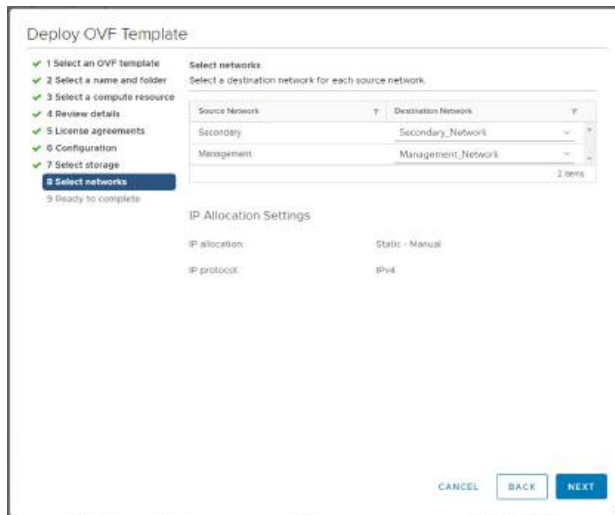
Name	Capacity	Provisioned	Free	Type
LocalDisk_1	67 GB	66.95 GB	81 MB	VN
	4.75 TB	3.98 TB	782.31 GB	NP
	1.82 TB	1.82 TB	989.79 GB	VN
	1.98 TB	1.21 TB	782.31 GB	NP

Compatibility
 ✓ Compatibility checks succeeded

16. Click **Next**.

17. Under Select networks, select the networks you require:

- For the CMS and SWA you need the **Management** network and, optionally, the **Secondary** network.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Configuration
7 Select storage
8 **Select networks**
9 Ready to complete

Select networks
Select a destination network for each source network.

Source Network	Destination Network
Secondary	Secondary_Network
Management	Management_Network

2 items

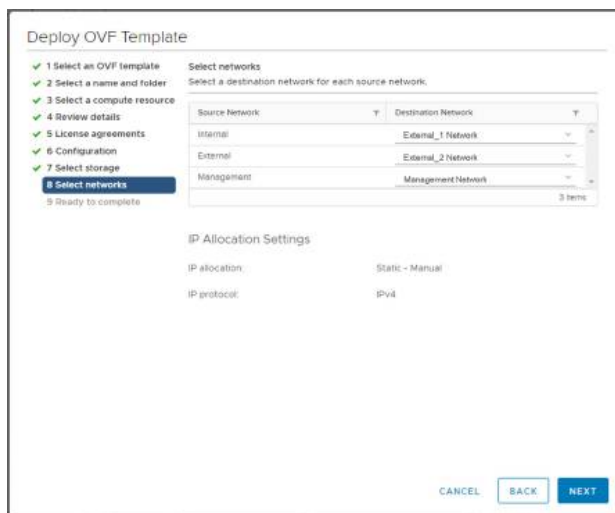
IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL BACK NEXT

- For the vNTD you need the **Management** network and an **External_1** and **External_2** network. **Caution:** The two External networks cannot be the same.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Configuration
7 Select storage
8 **Select networks**
9 Ready to complete

Select networks
Select a destination network for each source network.

Source Network	Destination Network
Internal	External_1 Network
External	External_2 Network
Management	Management Network

3 items

IP Allocation Settings

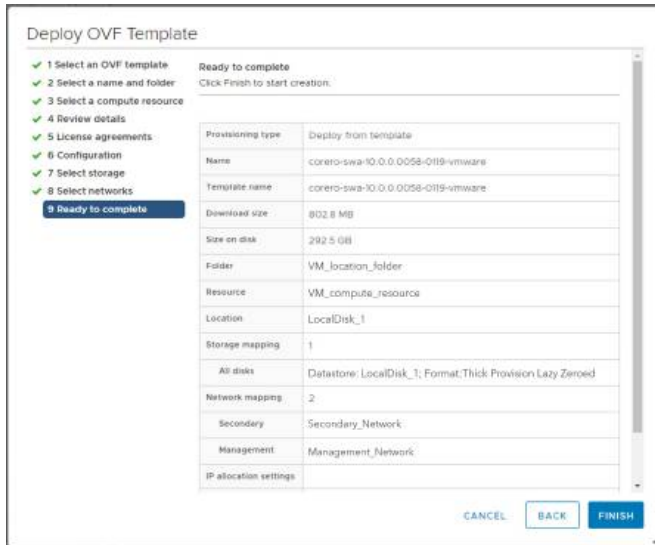
IP allocation: Static - Manual

IP protocol: IPv4

CANCEL BACK NEXT

18. Click **Next**.

19. Review your selections.



Deploy OVF Template

Ready to complete
Click Finish to start creation.

Provisioning type	Deploy from template
Name	corero-swa-10.0.0.0058-0119-vmware
Template name	corero-swa-10.0.0.0058-0119-vmware
Download size	802.8 MB
Size on disk	292.5 GB
Folder	VM_location_folder
Resource	VM_compute_resource
Location	LocalDisk_1
Storage mapping	1
All disks	Datastore: LocalDisk_1; Format: Thick Provision Lazy Zeroed
Network mapping	2
Secondary	Secondary_Network
Management	Management_Network
IP allocation settings	

CANCEL BACK FINISH

20. Click **Finish**. The VM is created powered off. Do not power it on yet.

21. **vNTD only:** Check the allocated ports will not create a network loop when enabled, then enable ports:

- In vSphere WebClient, right click on your new VM and select **Edit Settings**.
- Scroll down to **Network adapter 2**. Check the network label is correct and then under Device Status, select the **Connect** check box.
- Repeat for **Network adapter 3**.
- Click **OK**.

Resizing a vSWA application

The amount of space required by the SWA depends on your frequency of attack and how long you need the data to be available. A good rule of thumb for most installations is 1.5 TB for 13 months of data. The default disk image for a vSWA deployment is 240GB. You can choose to resize disk 2 after deployment.

Note: If your SWA was installed prior to 9.5.0, you will need to resize disk 3 rather than disk 2.

1. Check the current disk size:
 - a. After deployment, make sure the vSWA VM is running, and [access the pCLI](#).
 - b. Enter the following command to check the current disk size: `show data-disk`.
 - c. Make a note of the current disk size and exit the pCLI.
2. Resize the data disk:
 - a. Access the vSphere WebClient.
 - b. Right click on your vSWA VM and select **Edit Settings**.
 - c. Scroll down to **Hard Disk** and change the number to the required size in GB. For example, 2000.
 - d. Click **OK**.
 - e. Restart the vSWA VM Guest OS. This is necessary so the VM detects the new storage space.
 - f. Exit the vSphere WebClient
3. Repartition the disk to make use of the additional space:
 - a. Access the pCLI. If you enter the `show data-disk` command at this stage you will still see the previous disk size; that is expected.
 - b. Enter the following command to re-partition the disk to match the new size: `setup data-disk`
 - c. You should see something similar to this message: Found 500 GB of unallocated space. Do you want to continue? <Y, [N]>:
 - d. Enter `y` to re-partition the disk.
 - e. You should then see the option to autosize your indexes. Enter `y` to continue.
 - f. If you are happy with your changes, when prompted enter `A` to accept and apply the changes.
4. You can check this was successful by using the command `show data-disk`, it should now display the updated size.

Verify TDD Component Installation

Once you have installed the SWA, CMS, and vNTD applications on a KVM host, you can use the Corero Virtual Edition Installation Checker to verify that the three applications are correctly installed. The script checks the following areas:

- **Memory** – 8GB for CMS, 12GB for SWA or vNTD.
- **CPU count** – 4 for CMS, 12 for SWA, 2 for a vNTD expecting up to 1.2Gbps sample traffic, and 7 for a vNTD expecting over 1.2Gbps.

- **CPU allocation** – Checks to see if there are any overlaps in the cpusets allocated to each VM. Also checks that, if there are any pinned CPUs, they are in a VM's cpuset.
- **Disks** – 1 disk expected for CMS or vNTD and 2 for a SWA. Disks are expected to be set with `preallocation=falloc` disk provisioning (equivalent of thick)
- **Interfaces** – 1 management interface expected for a vNTD and 1-2 for a CMS or SWA. The vNTD also requires 2 or 4 data ports (the data ports for vNTDs expecting sample traffic over 1.2Gbps must be PCI devices).
- For vNTD's expecting sample traffic rates over 1.2Gbps the following additional checks take place:
 - **VT-d** – Must be enabled
 - **Huge Pages** – Checks 1GB Huge Pages is enabled and there are 12 allocated per socket
 - **CPU Pinning** – Required for high traffic rates. Checks to make sure all vNTD CPUs are pinned, that all pinned CPUs are isolated, and that no isolated CPUs on the host are unpinned.

Your documentation package should include the **Corero Virtual Edition Installation Checker script** and accompanying **PDF guide** which explains how to run the checker and how to resolve any issues shown.

Configuring the TDD Components

After deploying the three SmartWall TDD components (vNTD, vCMS, and vSWA), there are some immediate configuration actions you need to complete to get them fully functional. Each component needs to be setup using the pCLI, then you must connect the CMS to the SWA and add the vNTD to the CMS.

Accessing the pCLI on a virtual appliance

After deployment, you need to configure the virtual appliance. To do this you need to access the pCLI and run the setup wizard:

1. Open a console session to the virtual appliance:
 - **ESXi server** – In VMware client, select the VM and click **Open Console**
2. Log in to the virtual appliance using the default user account (`admin`) and password (`smartwall`).

Tip: Once you have an IP address associated with the appliance, you can use SSH on port 2222 using the default admin user account (e.g. `ssh -p 2222 admin@<ipAddress>`) and type the default password `smartwall` when prompted.

Configuring SmartWall Components Using the pCLI

This section describes how to use the provisioning CLI (pCLI) to set each component's basic configuration. To access the pCLI for each SmartWall® component see the application specific instructions earlier in this guide.

The pCLI provides the initial interface for configuring SmartWall™ components. Once you use the setup wizard to configure the application, you should perform all other tasks in the corresponding web interfaces. You can return to the pCLI if you need to edit these basic configuration settings later.

Tip: You can type `help` at the pCLI console command prompt to see a list of all the other available pCLI commands and Tab-completion is supported, enabling you to type a portion of the command that identifies it uniquely and press **Tab** to finish it.

Using the pCLI Setup Wizard to Configure a SmartWall Component

Note: This example shows the use of the pCLI to run the setup wizard on the vCMS. Other setup wizard sessions may vary slightly, depending on the component.

To use the setup wizard:

1. Open the pCLI for the component. When you log in to the pCLI, you will see something similar to the following example:

```
Corero SmartWall Central Management Server
Copyright (C) 2016-2017 Corero Network Security, Inc. All rights reserved.
```

```
cms login: admin
Password:
Last login: Thu Apr 28 10:42:38 on tty1
```

```
Welcome to the Corero Network Security initial setup CLI.
Please type 'setup' to start the initial configuration wizard.
For details of further options, please type 'help'.
cms>
```

2. Type **setup** to start the initial setup wizard, which will prompt you to change a number of basic configuration settings. For each group of settings, type **A** to accept changes you've made, type **C** to go back and change a setting, or type **E** to leave the current settings unchanged.

```
cms>setup
You will be asked a number of questions, along with the current values
in brackets. Please type in the desired configuration or you may press
Enter to keep the current value. After each section, you will be given
a chance to confirm and apply your configuration.
```

3. Change the username and password from their defaults. This is strongly recommended. If you are configuring SWA, you will be asked if you want to enable LDAP, as well.

```
Please configure the authentication settings:
```

```
Warning: Applying changes here will overwrite any users created in the
application
```

```
Enter user-name for the administrative account [admin]:
Enter password (press Enter to leave unchanged):
```

```
Enter [C]hange or [E]xit without changing [C]: E
```

4. Configure the management port settings: MTU and DHCP. If you choose not to use DHCP, specify the management IPv4 address, management IPv4 subnet mask, and management IPv4 default gateway (Note: All SmartWall applications require IPv4 addresses for management. IPv6 is not supported).

Please configure the Management Interface:

Enter MTU [1500]:

Enable DHCP? Y, [N]: N

Enter IPv4 Address [10.20.27.100]:

Enter IPv4 Subnet Mask [255.255.255.0]:

Enter IPv4 Default Gateway [10.20.27.254]:

5. vSWA only: You must set up your secondary interface to receive native telemetry from the Juniper Networks MX Series router. The IP address for the secondary interface must be on the same subnet as the Telemetry port on the router. The Default Gateway should be left blank for most TDD deployments.

Please configure the optional Secondary Interface:

Enable interface? Y, [N]:

Management Interface:

MTU : 1500

IPv4 Address : 192.168.54.13

IPv4 Subnet Mask : 255.255.255.0

IPv4 Default Gateway :

Secondary Interface:

State : Disabled

6. Configure the DNS settings: hostname, and the option for manual DNS configuration (DNS servers, DNS domain, DNS search domains).

Please configure the Domain Name System (DNS) settings:

Enter hostname [cms]:

Enter primary DNS server [None]:

Enter DNS domain [None]: corero.com

Enter DNS search domains (separated by space) [None]:

Configuration:

Hostname : cms

DNS Servers : None

DNS Domain : corero.com

DNS Search Domains :

Enter [A]ccept, [C]hange, or [E]xit without saving [C]: A

7. Configure the time settings: NTP server (primary, secondary, and tertiary) and time zone.

Caution: You must use NTP servers for all TDD applications. Time differences between applications can cause unexpected behavior.

Please configure the time settings:

Would you like to enable NTP? Y, [N]:

Enter time zone or '?' for complete list [America/New_York]:

Configuration:

Time source : Hypervisor

Time zone : America/New_York

Enter [C]hange or [E]xit without changing [C]: E

cms>

8. After you complete the basic configuration using the pCLI, you can review your changes by typing the command `show`.

```
cms>show
```

```
Management:
```

```
State : Enabled
```

```
Link State : Up
```

```
MAC Address : 00:50:56:88:62:82
```

```
MTU : 1500
```

```
DHCP Enabled : No
```

```
IPv4 Address : 10.20.27.100
```

```
Subnet Mask : 255.255.255.0
```

```
Default Gateway : 10.20.27.254
```

```
Secondary:
```

```
State : Disabled
```

```
Link State : Down
```

```
MAC Address : 00:50:56:88:20:ad
```

```
MTU : 1500
```

```
IPv4 Address : None
```

```
Subnet Mask : None
```

```
SecureWatch Status:
```

```
State : Disabled
```

```
SecureWatch ID : No package loaded
```

```
cms>
```

(Optional) SmartWall SecureWatch Analytics Considerations

The following pCLI options are specific to configuring the SWA:

SSL Certificates

The pCLI can be used to load a signed SSL certificate for use with the web UI, to avoid the browser security warnings which appear when you use the default unsigned certificate. The certificate must be in PKCS#12 format, and include the key, certificate, and CA certificate change to be used for SSL. The common name should match the hostname assigned to the SWA appliance.

To load a certificate, type `ssl-certificates https` followed by the URI to the certificate file. The supported protocols are FTP, SFTP, HTTP, and HTTPS. For example:

```
ssl-certificates https sftp://admin@10.20.30.40/certs/my_cert.p12
```

Installing the TDD license file

You must install a TDD license file in the SWA application as it enables the SWA to check you are licensed to use the TDD system. The license file is provided in a SecureWatch Package format which is compatible with the SWA application upload process.

Corero offers three forms of licensing for SmartWall TDD depending on your environment and service level choice:

- Corero SecureWatch Service customers – The license is delivered via the SecureWatch package file that is delivered to connect to the SecureWatch Service via a secure VPN. Install the SecureWatch package file and the licensing process does not require any further steps.
- Customers who are not connecting to Corero SecureWatch Service and have internet access available to the SWA – With this option, the license is delivered through a SecureWatch package file that points to an internet based license server. Install the SecureWatch package file and the SWA licensing process will contact the internet based license server.

Note: The SecureWatch License File does not create a persistent connection to the license server. It only requires a daily check. No data is ever sent over that connection.

- Customers who are not connecting to the SecureWatch Service and the SWA does not have access to the internet – Please contact your Corero customer support representative for more information on disconnected licensing.

To upload a license file to the SWA

1. You will receive the SecureWatch package and unlock code from Customer Support.
2. Save this file in a location that you can easily access from the computer you're using to access the SWA web UI.
3. Open the SWA Web UI in a browser.
4. Navigate to **System > SecureWatch Packages**.
5. Click **Choose File** and select the saved package file.
6. If required, type in the **Unlock Code**.
7. Click **Install Package**. This will cause the SWA to restart and may take several minutes. When it's complete you can log back in.

Use with an HTTP Proxy

If your internet connectivity is through an HTTP Proxy then you will need to setup the SWA to enable the external connection. This will differ depending on your chosen licensing method.

- **SecureWatch Service VPN** – The HTTP Proxy is setup and enabled in SecureWatch Packages:
 1. Navigate to **System > Settings > SecureWatch Packages**
 2. Check the box to **Enable SecureWatch HTTP Proxy**.
 3. Type the IP **Address** of the HTTP Proxy Server.
 4. Type the **Port** number for the HTTP Proxy port on your server. The default port on most servers is 3128.
 5. (Optional) Configure authentication:
 - a. Select an **Authentication Type** : **Basic** or **NTLM**
 - b. Type the authentication **Username** and **Password** for the HTTP Server.
 6. Click **Save**.
- **SecureWatch License File** – The HTTP Proxy is setup and enabled in General Settings:
 1. Navigate to **System > Settings > General Settings**
 2. Check the box to **Enable HTTP Proxy**.
 3. Type the IP **Address** of the HTTP Proxy Server.
 4. Type the **Port** number for the HTTP Proxy port on your server. The default port on most servers is 3128.
 5. Click **Save**. This may cause the SWA to restart.

Uploading a vNTD license to the CMS

For each vNTD you want to add to your CMS, you need a 10G license. After your vCMS is deployed and configured, you can contact support for a license file unique to your system.

1. In the CMS Web UI, you can see your CMS's UUID at the top of the **Home** screen.
2. Contact your support representative to request a vNTD license file . You must quote your CMS UUID and your Juniper SSRN (the SSRN will be on your sales agreement information).

Caution: License files are created to be specific to your CMS and cannot be transferred.

3. Save the license file somewhere you can easily access, from the computer you're using to access the CMS web UI.
4. Open the CMS application in a browser and log in. (If you have not yet changed them, the default user-name/password is *admin/smartwall*).
5. Navigate to **System > Licensing**.
6. Click **Add**.
7. You can either:
 - Copy and paste the contents of the license file into the text box. You must include the license header and footer: `----BEGIN-CORERO-LICENSE----` and `----END-CORERO-LICENSE----`
 - Select **Upload License File** and click **Choose file** and browse for the license file on your computer. Click **Open**.
8. Once you have a license file by one of those methods, click **Save**.

Setting the Inbound Sample Rate between the vNTD and the CMS

The Port-Mirror Sample Rate you will configure on the router (and the Ingress Sample rate you configure when adding a vNTD to the CMS) controls how many samples are sent from the router to the vNTD. In addition to this, you need to control the rate of samples sent from the vNTD to the CMS. The default setting in a CMS (1 in 1999) is not suitable for a TDD deployment and must be adjusted.

1. In a browser, open the CMS Web UI and log in.
2. Use the left-hand menu to navigate to **Network > Devices**.
3. Click the **ADVANCED SETTINGS** tab.
4. Edit the **Inbound Sample Rate** for **sFlow** and **aFlow**. This is the rate of samples sent from the Defense devices to the CMS. The following sample rates should be used for your deployment type:
 - SmartWall TDD production system – Change the value to **16**. This samples 1 in every 16 packets.
 - SmartWall TDD lab test system using smaller traffic volumes and attacks (from a traffic generator) – Change the value to **1**. This samples every packet received by the Defense device.
5. If you want to save the new configuration, and push your changes to any affected Defense devices, click **Commit**. Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Note: The default sample rates given above are correct for the majority of deployments and you should make sure the Port-Mirror Sample Rate on your router is correct before adjusting the Inbound Sample Rate.

Adding a vNTD to the CMS

You must add a SmartWall Defense device to the CMS before you can manage the attack mitigation Policy on that device. The Defense devices are managed in a Cluster. You must edit this Cluster to expect devices which are using sampled traffic.



Prerequisites

- Deploy and configure (using the pCLI) a CMS
- Deploy and configure (using the pCLI) a vNTD
- (Optional) Contact Corero for a vNTD license and upload the license to the CMS. If you haven't uploaded the license before you add the vNTDs, you can upload the license and apply it to the vNTDs after deployment.



To edit the default Cluster to expect sampled traffic

Note: The Port-Mirror Sample Rate (configured on the router) and Ingress Sample rate should be identical. Both must be the rate factor which reduces the amount of traffic seen by the router to a manageable size for the vNTD. A default value of **1000** would normally scale to approx 1Tbit/sec.

Values less than 1000 will give better fidelity on attack detection and traffic visualization but will add load to the vNTD. A single vNTD has a peak capacity of 10Gbit/sec of sampled traffic when optimized. (Note: the sample rate assumes a run-length of 0)

1. Open the CMS application in a browser and log in.
2. Navigate to **Network > Clusters**.
3. From the table, locate the Cluster you want to add the device to, and click  the edit button. You can type a text string into the Search field to narrow down the list.
4. In the **Ingress Sample Rate** field, type the sample rate: **1000**
5. Click **Save**.
6. Click . Then, on the pop-up dialog, click **Commit** to push the changes.

To add a vNTD to the CMS



1. Open the CMS application in a browser and log in.
2. Navigate to **Network > Devices**.
3. At the Devices table, click **Add**.
4. Type a **Name** for the device.
5. (Optional) Type a **Description** of this device.
6. Type the device's IP **Address** (you will have configured this in the vNTD pCLI).
7. Select the **Cluster** you want to add this device to. The CMS has a **default** Cluster you can add all your devices to. This Cluster uses the policy stored in the default Protection Profile.
8. Select the **Authentication Group** which matches the authentication credentials on this device. The CMS has a **default** Authentication Group which uses the admin/smartwall credentials. If you have changed the device credentials during pCLI set up, you may need to create/edit an Authentication Group.
9. Click **Save**.
10. Repeat this method to add all the devices you require.
11. Click . Then, on the pop-up dialog, click **Commit** to push the changes.
12. If you have already uploaded your vNTD license, your devices will have been automatically licensed when they deployed. If you haven't uploaded the vNTD license, you should do so now following the [method above](#) and then manually apply the license to each vNTD:
 - a. In the CMS, use the left-hand menu to navigate to **Network > Devices**.
 - b. On the Devices table, locate the vNTD you want to license.
 - c. In the Actions column, click  and select **License**.

Note: Adding a device to the CMS does not cause any existing Policy to be pushed to it. You must first add the device to a Cluster. To learn more about creating Clusters and managing Policy, see the SmartWall Central Management Server User Guide.


Configuring the vNTD Segment for TDD



After you've connected your vNTD to the vCMS, you can view information on the available interfaces on the device. By default the vNTD comes with two available Segments. If you only require one Segment, you can disable the additional segment.

To configure a Segment for TDD

1. Open the CMS in a browser.
2. Use the left-hand menu to navigate to **Network > Segments**.
3. From the Segments table, locate the Segment you want to edit and click  the edit button. You can type a text string into the Search field to narrow down the list.
4. (Optional) Edit the **Name**. This must be unique among Segments. You must only use alphanumeric, spaces, or .-&()/_@:= symbols.
5. (Optional) Type a **Description** of up to 265 characters.
6. Check that the **External** Interface on the vNTD is selected and the **Internal** Interface drop-down shows **none - detector**.
7. How you configure the Segment depends on the traffic sampling method you chose when configuring your routers during set up:
 - For samples sent by **Port-Mirroring**:
 - a. No additional changes
 - For samples sent by **GRE tunnel**:
 - a. Set the External **IPv4 Address** to the IP address of the external interface on the vNTD (for termination this is the tunnel endpoint)
 - b. Set the External **Peer IPv4 Address** to the IP address of the interface which is the last hop before the traffic arrives at the vNTD (e.g the interface on the router which has received the sampled traffic and is connected to the vNTD)
 - c. Set the **GRE Ingestion** drop-down to **enabled**.
8. Click **Save**.
9. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).


To disable the second Segment

1. Open the CMS in a browser.
2. Use the left-hand menu to navigate to **Network > Segments**.
3. From the Segments table, locate the Segment you want to delete and click  the delete button.
4. Use the left-hand menu to navigate to **Network > Devices**.

5. Click the **INTERFACES** tab.
6. From the **Device(s)** drop-down, choose the device where this interface is located.
7. From the **View** drop-down, make sure **Summary** is selected.
8. From the table, locate the interface you want to edit, click  the edit button. You can type a text string into the Search field to narrow down the list.
9. From the **Admin State** drop-down, select **disabled**.
10. Click **Save**.
11. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).


Connecting CMS with SWA

By default, SWA listens for syslog messages on port 9997. You will need to configure CMS to send syslog messages to SWA on this port.

1. Open the CMS application in a browser and log in. (If you have not yet changed them, the default user-name/password is *admin/smartwall*).
2. Use the left-hand menu to navigate to **System > Analytics & Syslog**. Make sure the SERVERS tab is selected.
3. At the **Analytics Servers** table, click **Add Server**.
4. Type a **Name** for this server. You must only use alphanumeric, spaces, or `.-&()/_@:=` symbols.
5. Type the IP **Address** of the server (or its DNS name).
6. Enable or Disable **Encryption** for this server. The CMS and SWA come with self-signed SSL certificates. You can choose to upload signed certificates to the CMS and SWA- see optional steps below.
7. Leave the default **Port: 9997** for unencrypted or **9998** for encrypted connections.
8. Click **Save**.
9. Click . Then, on the pop-up dialog, click **Commit** to push the changes.

(Optional) Add a signed certificate to the CMS - SWA connection

If you enable encryption, the connection between the CMS and SWA uses, by default, an in-built self-signed certificate. If you want to use a signed certificate, you need to upload a PKCS#12 certificate to both sides of the connection.

1. Add a signed SSL certificate in the CMS side of the connection:
 - a. Open the CMS application in a browser and log in. (If you have not yet changed them, the default username/password is *admin/smartwall*).
 - b. Use the left-hand menu to navigate to **System > Analytics & Syslog**.
 - c. Open the **SSL CERTIFICATE** tab.
 - d. Click **Upload Certificate**.
 - e. Select a pkcs12 certificate file on your computer, and click **Open**.
 - f. (Optional) Type in the **Password** for the certificate file.
 - g. Click **OK**.
 - h. If necessary, refresh the browser to ensure the new certificate has been loaded.
 - i. Click . Then, on the pop-up dialog, click **Commit** to push the changes.
2. Add a signed certificate to the part of the SWA that receives information from CMS:
 - a. Access the SWA pCLI:
 - Open a console session. On an ESXi server, you can use VMware (select the VM and click **Open Console**) or on a KVM server you can use virsh (command: `virsh console <vmName>`).
 - SSH to the pCLI: `ssh -p 2222 admin@<ipAddress>`
 - b. Log in. If you haven't yet changed them, the default username and password is *admin/smartwall*.
 - c. To load a certificate, type `ssl-certificates forwarder` followed by the URI to the PKCS#12 format certificate file. The supported protocols are FTP, SFTP, HTTP, and HTTPS. For example: `ssl-certificates forwarder sftp://admin@10.20.30.40/certs/my_cert.p12`
 - d. You will be prompted for a password to access the file location. If you password protected the PKCS#12 file, you will also be prompted for that password.

To add CMS credentials to the SWA

You must add a set of CMS admin credentials to enable the SWA to communicate mitigation changes back to the CMS.

1. Open the SWA application in a browser and log in.
2. Use the top menu to navigate to **Mitigation > Remote Devices**.
3. At the table, click **Add Device**.
4. Type a **Name** for your CMS. You must only use alphanumeric, spaces, or `.-&()/_/@:=` symbols.
5. Type the IP **Address** (IPv4) of your CMS.
6. In the **Type** field, type: **CMS**. **Caution:** You must use uppercase for all letters or it will not be recognized.
7. (Optional) Type a **Description** of your CMS.
8. Enter a **Username** for an admin account on your CMS.
9. Enter a **Password** for an admin account on your CMS.
10. Click **Save**.

(Optional) Uploading a custom SSL certificate to the CMS

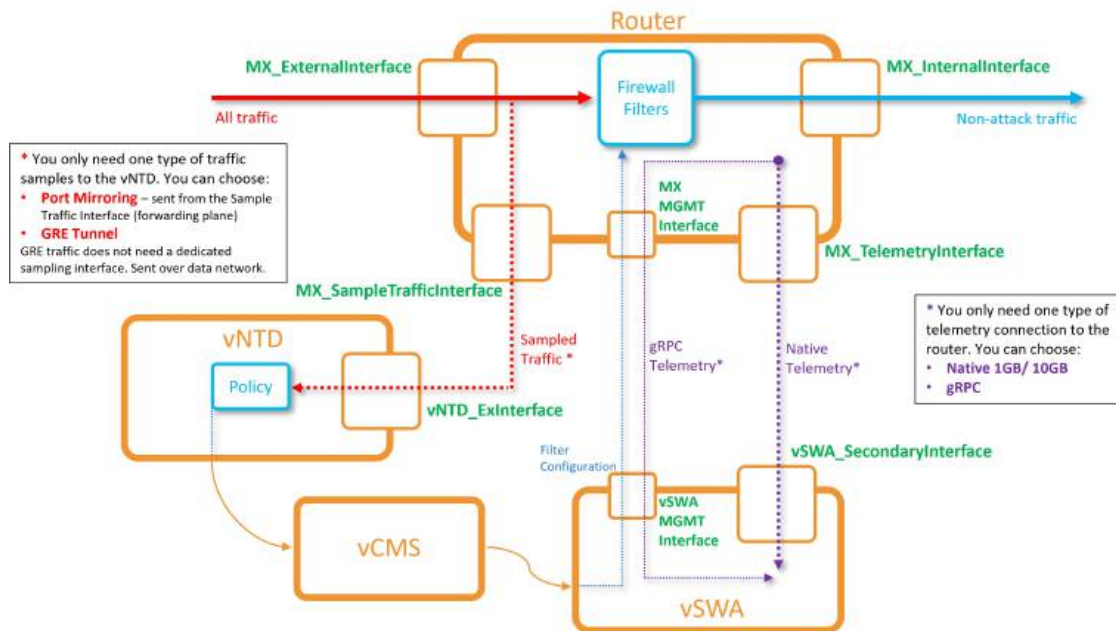
The CMS comes with a default self-signed Corero SSL certificate which your browser will list as "not secure". As soon as possible, you should replace this with a signed certificate. This must be packaged in pkcs12 format and can optionally be password protected.

1. Open the CMS application in a browser and log in. (If you have not yet changed them, the default username/password is *admin/smartwall*).
2. Navigate to **System > HTTPS**.
3. Click **Upload Certificate**.
4. Select the pkcs12 certificate file on your computer, and click **Open**.
5. (Optional) Type in the **Password** for the certificate file.
6. Click **OK**.
7. Refresh the browser to view the new security rating.

Note: The certificate must be in PKCS#12 format, and include the private key, signed certificate, and CA certificate change to be used for SSL. The common name should match the hostname assigned to the SWA appliance.

Configuring the Juniper Networks MX Series router

To enable a router to accept DDoS mitigation filters from the SmartWall TDD, you must configure the following settings. The configuration provided assumes you have a new system, so you may need to modify some commands if you're using an existing router.



Prerequisites

The configuration provided below assumes you have a new system with initial configuration already setup for your network. At a minimum, the system must be licensed, have SSH enabled, be connected to your management network and have a host name (`set system host-name <name>`).

Note: The hostname must be enabled on the forwarding plane of the Juniper Networks MX Series router.

For gRPC telemetry only: You must download two additional software files. Contact your support representative for assistance.

- network-agent-x86-32-17.4R1.16-C1.tgz
- junos-openconfig-x86-32-0.0.0.9.tgz

Before you begin, you also need to know the following information which you will use to replace the placeholders in the commands below:

- `<MX_ExternalInterface_Name>` – The names of the external interfaces on your router which you want to protect with the TDD system (e.g. `xe-0/0/0`).
- `<MX_SampleTrafficInterface_Name>` – The name of the interface on your router which you have allocated for sending sample traffic to the vNTD (e.g. `xe-0/0/2`).
- `<MX_SampleTrafficInterface_IPv4_Subnet>` – The IPv4 address of the interface on your router which you have allocated for sample traffic, formatted as a CIDR (e.g. `192.168.66.201/24`).
- `<MX_SampleTrafficInterface_IPv6_Subnet>` – The IPv6 address of the interface on your router which you have allocated for sample traffic, formatted as a CIDR (e.g. `2000:2000:cccc:cccc::1/64`).
- `<MX_TelemetryInterface_Name>` – **(Native telemetry only)** The name of the interface on your router which you have allocated for sending telemetry to the vSWA (e.g. `xe-0/0/3`).
- `<MX_TelemetryInterface_IP>` – **(Native telemetry only)** The IPv4 address of the interface on your router which you have allocated for telemetry (e.g. `192.168.99.201`).
- `<vNTD_ExInterface_MAC>` – The MAC address of the external interface on your vNTD (e.g. `00:0c:29:36:94:5a`). To find this, log into the vNTD pCLI and type the command `show nic` and look for the MAC address under `External`.
- `<vNTD_ExInterface_IPv4>` and `<vNTD_ExInterface_IPv6>` – The IPv4 and IPv6 address you want to allocate to the external interface on the vNTD (e.g. `192.168.66.105` and `2000:2000:cccc:cccc::2`).
 - For sampled traffic sent via port-mirroring and port mirror instances, this must be in the same subnet as the interface on the router which you allocated for mirroring (`<MX_SampleTrafficInterface_Name>`).
 - For sampled traffic sent via a GRE tunnel, this must be the IP address you configured on the external interface on the vNTD when you [configured the Segment](#).
- `<vSWA_SecondaryInterface_IP>` – **(Native telemetry only)** The IP address of the secondary interface on the vSWA (e.g. `192.168.99.113`). You can configure this IP address by logging into the vSWA pCLI and using the setup network wizard. The IP must be on the same network as the interface on the router which you allocated for telemetry (`MX_TelemetryInterface`).

To configure a Juniper Networks MX Series router for use with the SmartWall TDD system

Caution: If copying and pasting from the PDF, you can experience some loss of characters. If possible, use the online help version of the documentation. Alternately, first copy this set of commands into a plain text word processor (e.g. notepad) and check none of the hyphens or spaces have been removed and that no additional returns have been added.

The following steps are required to configure a Juniper Networks MX Series router:

1. Transport sampled packets from the router to the vNTD. Select one of the four methods provided:
 - [Using port mirror sampling over a layer 2 direct connection](#)
 - [Using port mirror instances over a layer 2 direct connection](#)
 - [Using port mirror sampling with a GRE logical tunnel type](#)
2. [Configure the router to accept filters from TDD.](#)
3. Configure the router to accept filters from TDD. Select one of the two methods provided:
 - [Using native telemetry](#)
 - [Using gRPC telemetry](#)
4. (Optional) [Set up role-based access.](#)

Prerequisite: Accessing and editing router configuration

1. All methods below, unless stated, are performed in the configuration area of the router. To access the router configuration area:
 - a. Open the Juniper Networks MX Series router CLI using an SSH client: `ssh <username>@<ipaddress>`
 - b. Enter your password to log in.
 - c. Enter configuration mode: `configure`
 - d. Use the example commands in each section to input your required configuration changes. Each line is an individual command- paste a single line and press **Enter** before moving on to the next line.
2. Once you have performed all the commands in a section, you must commit the changes and exit configuration mode:
 - a. To save your changes: `commit`
 - b. Exit configuration mode: `exit`

Step 1: Transport sampled packets from the router to the vNTD

Caution: If you have multiple routers sending traffic samples in different formats, you **must** ensure all sample rates are the same. Otherwise, the mitigation thresholds and traffic charts in the SWA will not work correctly.

There are multiple methods for sending traffic samples to your vNTD. Select one of the following methods:

Using port mirror sampling over a layer 2 direct connection

Note: The 1000 value you enter, in the first command in step 1, is the rate factor which reduces the amount of traffic seen by the router to a manageable size for the vNTD (10Gbps or less). 1 in every 1000 packets is sampled and sent to the vNTD. This enables you to sample from up to 10Tbit/sec of traffic for each vNTD. (Note: the sample rate assumes a run-length of 0). This is the rate required by the vNTD.

1. Identify an interface on the router which can be used for sending mirrored traffic to the vNTD. Set and label this interface (using the description field):

```
set interfaces <MX_SampleTrafficInterface_Name> description Sample_Port_to_vNTD
```

2. Configure Port-Mirroring to forward a sample rate of traffic from the router to the vNTD. When you configured the vNTD to accept Port-Mirroring samples, you did not have to set an IP address on the external interface. In the commands below, the vNTD_ExInterface variables can be dummy IP addresses (in the same subnet as the allocated sample forwarding interface on the router), as you are creating a static arp to the vNTD MAC address.

```
set forwarding-options port-mirroring input rate 1000
```

```
set forwarding-options port-mirroring input run-length 0
```

```
set forwarding-options port-mirroring family inet output interface <MX_SampleTrafficInterface_Name> next-hop <vNTD_ExInterface_IPv4>
```

```
set forwarding-options port-mirroring family inet6 output interface <MX_SampleTrafficInterface_Name> next-hop <vNTD_ExInterface_IPv6>
```

```
set interfaces <MX_SampleTrafficInterface_Name> unit 0 family inet address <MX_SampleTrafficInterface_IPv4_Subnet> arp <vNTD_ExInterface_IPv4> mac <vNTD_ExInterface_MAC>
```

```
set interfaces <MX_SampleTrafficInterface_Name> unit 0 family inet6 address <MX_SampleTrafficInterface_IPv6_Subnet> ndp <vNTD_ExInterface_IPv6> mac <vNTD_ExInterface_MAC>
```

3. Add new filters to the firewall (IPv4 and IPv6) . The default terms configured here count the traffic for telemetry, use the port-mirroring configuration to mirror the traffic samples to the vNTD, and accept the actual traffic. When the TDD sends configuration to the router to block attack traffic, that configuration is added as an ephemeral term.

```
set firewall family inet filter CORERO-MITIGATE term default-term then count
Corero-Allowed
```

```
set firewall family inet filter CORERO-MITIGATE term default-term then port-mirror
```

```
set firewall family inet filter CORERO-MITIGATE term default-term then accept
```

```
set firewall family inet6 filter CORERO-MITIGATE6 term default-term then count
Corero-Allowed6
```

```
set firewall family inet6 filter CORERO-MITIGATE6 term default-term then port-mirror
```

```
set firewall family inet6 filter CORERO-MITIGATE6 term default-term then accept
```

4. For every external interface whose traffic you want to protect with the TDD system, you must add the CORERO filters (IPv4 and IPv6).

```
set interfaces <MX_ExternalInterface_Name> unit 0 family inet filter input CORERO-MITIGATE
set interfaces <MX_ExternalInterface_Name> unit 0 family inet6 filter input CORERO-MITIGATE6
```

Using port mirror instances over a layer 2 direct connection

The deployment instructions above use port-mirroring, set up as part of the CORERO-MITIGATE filter. If you need the flexibility of using a port mirror instance outside of the CORERO-MITIGATE filter, you can use the following alternative commands. The <MirrorFilter> and <MirrorFilter_IPv6> values must be replaced with the name of the IPv4 and IPv6 filters you want to use to mirror traffic samples to the vNTD. The <instanceName> must be replaced with the port mirror instance you want to use.

1. Identify an interface on the router which can be used for sending mirrored traffic to the vNTD. Set and label this interface (using the description field):
2. Configure Port-Mirroring to forward a sample rate of traffic from the router to the vNTD. When you configured the vNTD to accept Port-Mirroring samples, you did not have to set an IP address on the external interface. In the commands below, the vNTD_ExInterface variables can be dummy IP addresses (in the same subnet as the allocated sample forwarding interface on the router), as you are creating a static arp to the vNTD MAC address.

```
set forwarding-options port-mirroring input rate 1000
set forwarding-options port-mirroring input run-length 0
set forwarding-options port-mirroring family inet output interface <MX_SampleTrafficInterface_Name> next-hop <vNTD_ExInterface_IPv4>
set forwarding-options port-mirroring family inet6 output interface <MX_SampleTrafficInterface_Name> next-hop <vNTD_ExInterface_IPv6>
set interfaces <MX_SampleTrafficInterface_Name> unit 0 family inet address <MX_SampleTrafficInterface_IPv4_Subnet> arp <vNTD_ExInterface_IPv4> mac <vNTD_ExInterface_MAC>
set interfaces <MX_SampleTrafficInterface_Name> unit 0 family inet6 address <MX_SampleTrafficInterface_IPv6_Subnet> ndp <vNTD_ExInterface_IPv6> mac <vNTD_ExInterface_MAC>
```

3. Add new filters to the firewall (IPv4 and IPv6) . The default terms configured here count the traffic for telemetry, use the port-mirroring configuration to mirror the traffic samples to the vNTD, and accept the actual traffic. When the TDD sends configuration to the router to block attack traffic, that configuration is added as an ephemeral term.

```
set firewall family inet filter COREERO-MITIGATE term default-term then count
Corero-Allowed
set firewall family inet filter COREERO-MITIGATE term default-term then accept
set firewall family inet filter <MirrorFilter> term default-term then port-mirror-
instance <instanceName>
set firewall family inet filter <MirrorFilter> term default-term then next term
set firewall family inet6 filter COREERO-MITIGATE6 term default-term then count
Corero-Allowed6
set firewall family inet6 filter COREERO-MITIGATE6 term default-term then accept
set firewall family inet6 filter <MirrorFilter_IPv6> term default-term then port-
mirror-instance <instanceName>
set firewall family inet6 filter <MirrorFilter_IPv6> term default-term then next
term
```

4. For every external interface whose traffic you want to protect with the TDD system, you must add the CORERO filters (IPv4 and IPv6).

```
set interfaces <MX_ExternalInterface_Name> unit 0 family inet filter input-list
<MirrorFilter>
set interfaces <MX_ExternalInterface_Name> unit 0 family inet filter input-list
COREERO-MITIGATE
set interfaces <MX_ExternalInterface_Name> unit 0 family inet6 filter input-list
<MirrorFilter_IPv6>
set interfaces <MX_ExternalInterface_Name> unit 0 family inet6 filter input-list
COREERO-MITIGATE6
```

Note: The <MirrorFilter> must be in front of the COREERO-MITIGATE filter.

5. When you [add this router to the SWA as a Remote Device](#), you must give it the device type **ST_MX** (rather than the standard device type MX).

Using port mirror sampling with a GRE logical tunnel type

Note: If you require an alternative logical tunnel type, contact your support representative.

On the router a GRE tunnel needs to be configured from the router to the vNTD. Then you need to setup Port-Mirroring to send the samples over this tunnel. The following placeholders are specific to this GRE tunnel method:

- `<MX_GRETunnel_Name>` – The GRE Tunnel (`<MX_GRETunnel_Name>`) must be named using the following format where `n` is replaced with unique values for this GRE tunnel: `gr-n/n/n` (e.g. `gr-0/0/0` if you have no other tunnels by that name).
- `<MX_IPv4>` – One of the IP addresses associated with your router.

Note: The tunnel needs to be given any IP address in order for it to come up, a dummy one (`10.99.100.0/31`) is given in the commands below and can be left or modified if required.

1. Enable tunnel services and create the GRE logical tunnel:

```
set chassis fpc 0 pic 0 tunnel-services bandwidth 10g
set interfaces <MX_GRETunnel_Name> description "GRE tunnel to NTD"
set interfaces <MX_GRETunnel_Name> unit 0 tunnel source <MX_IPv4>
set interfaces <MX_GRETunnel_Name> unit 0 tunnel destination <vNTD_ExInterface_IPv4>
set interfaces <MX_GRETunnel_Name> unit 0 family inet address 10.99.100.0/31
```

2. Configure port-mirroring to send samples over the GRE Tunnel:

```
set forwarding-options port-mirroring input rate 1000
set forwarding-options port-mirroring input run-length 0
set forwarding-options port-mirroring family inet output interface <MX_GRETunnel_Name>
```

3. Add new filters to the firewall (IPv4 and IPv6) . The default terms configured here count the traffic for telemetry, use the port-mirroring configuration to mirror the traffic samples to the vNTD, and accept the actual traffic. When the TDD sends configuration to the router to block attack traffic, that configuration is added as an ephemeral term.

```
set firewall family inet filter COREERO-MITIGATE term default-term then count Corero-Allowed
set firewall family inet filter COREERO-MITIGATE term default-term then port-mirror
set firewall family inet filter COREERO-MITIGATE term default-term then accept
set firewall family inet6 filter COREERO-MITIGATE6 term default-term then count Corero-Allowed6
set firewall family inet6 filter COREERO-MITIGATE6 term default-term then port-mirror
set firewall family inet6 filter COREERO-MITIGATE6 term default-term then accept
```


4. For every external interface whose traffic you want to protect with the TDD system, you must add the CORERO filters (IPv4 and IPv6).

```
set interfaces <MX_ExternalInterface_Name> unit 0 family inet filter input CORERO-MITIGATE
set interfaces <MX_ExternalInterface_Name> unit 0 family inet6 filter input CORERO-MITIGATE6
```

Step 2: Configure the router to accept filters from TDD

1. Unless already enabled, you must enable the router to accept NetConf. This enables the TDD to push configuration to the router:

```
set system services netconf ssh port 830
```

Note: If you want to use a custom NetConf port, you can replace 830 with your required port number. You must also add the custom port number to the [Remote Devices table entry](#) for this router.

2. Create an ephemeral instance of the configuration database named Corero and limit it to only store the last 500 commits in memory. This is where configuration from the TDD is sent.

```
set system configuration-database ephemeral instance Corero
set system configuration-database ephemeral purge-on-version 500
```

Step 3: Configure the router to accept filters from TDD

There are two options for configuring telemetry. Choose the method below which works for your network:

Using native telemetry

1. Identify an interface on the router (different from the sample traffic interface) which can be used for sending telemetry to the vSWA. Set and label this interface (using the description field):

```
set interfaces <MX_TelemetryInterface_Name> description Interface_for_telemetry
```

2. Configure the telemetry sent to the SWA:

```
set services analytics streaming-server Corero remote-address <vSWA_SecondaryInterface_IP>
set services analytics streaming-server Corero remote-port 30000
```

Tip: If you need to add a new certificate to this router, you can use the following command:

```
set security certificates local <certificateName> load-key-file <URL>
```

3. Configure the telemetry sent to the SWA.

```
set services analytics export-profile Corero-FF-mitigate local-address <MX_Tele-
metryInterface_IP>
set services analytics export-profile Corero-FF-mitigate local-port 22222
set services analytics export-profile Corero-FF-mitigate reporting-rate 1
set services analytics export-profile Corero-FF-mitigate payload-size 9000
set services analytics export-profile Corero-FF-mitigate format gpb
set services analytics export-profile Corero-FF-mitigate transport udp
set services analytics sensor Corero-FF-mitigate server-name Corero
set services analytics sensor Corero-FF-mitigate export-name Corero-FF-mitigate
set services analytics sensor Corero-FF-mitigate resource /jun-
os/system/linecard/firewall/
set services analytics sensor Corero-FF-mitigate resource-filter CORERO.*
```

Note: If your router is using Input Lists, you should replace the last command with the following:

```
set services analytics sensor Corero-FF-mitigate resource-filter "^
[^_].*"
```

Using gRPC telemetry

1. If required, download additional packages:

a. Commit any changes and exit from configuration mode:

```
commit
exit
```

b. Enter the following commands to enable the router to send telemetry over the management interface:

```
request system software add network-agent-x86-32-17.4R1.16-C1.tgz
request system software add junos-openconfig-x86-32-0.0.0.9.tgz
```

c. Return to configuration mode for the remaining steps:

```
configure
```

2. Configure the type of telemetry sent to the SWA:

- For unencrypted gRPC telemetry use the following command. Note: `clear-text` is a hidden option and must be typed in full:

```
set system services extension-service request-response grpc clear-text port
32767
```

- For SSL encrypted gRPC telemetry, you must already have an SSL certificate on this router. If you already have a certificate on the router, use the following command:

```
set system services extension-service request-response grpc ssl local-cer-
tificate <certificateName> port 32767
```

Tip: If you need to add a new certificate to this router, you can use the following command:

```
set security certificates local <certificateName> load-key-file <URL>
```

(Optional) Step 4: Set up role-based access

1. Configure role-based access to routers by creating a new login class called TDD and a user within that class called corero.

```
set system login user corero class TDD
set system login user corero authentication plain-text-password
set system login class TDD permissions configure
set system login class TDD permissions view
set system login class TDD permissions firewall-control
```

Note: When you [add your routers to the Remote Devices table](#) in SWA, you must enter the username `corero` and the same password you configured here.

Adding a Juniper Networks MX Series router as a Remote Device

To enable the SmartWall TDD system to send instructions to a Juniper Networks MX Series router, that router must be added to the SWA as a Remote Mitigation Device. Once you add all the Remote Devices to the SWA, you must complete the configuration by editing the Mitigation Alerts (Mitigation Activation and Mitigation Removal) to send mitigations to those devices.

To add a router to the SWA

1. Open the SWA application in a browser and log in.
2. Use the top menu to navigate to **Mitigation > Remote Devices**.
3. At the table, click **Add Device**.
4. In the **Name** field type the host name for this router. The host name is configured on your router and must match what you enter here exactly. You must only use alphanumeric, spaces, or .-&()/@:= symbols.
5. In the **Address** field, type the IPv4 address of the router or the router hostname (must be DNS resolvable).
6. (Optional) If you're using the standard NetConf port 830, leave this field blank. Otherwise, you can specify the custom NetConf port you want to use to communicate with the router. **Caution:** You must also use the custom port when [configuring the router](#).
7. In the **Type** field, type: **MX** (If your router is configured to use port mirror instances you need to use **ST_MX** in this field, see more information on using [port mirror instances](#)). **Caution:** You must use uppercase for both letters or it will not be recognized.
8. (Optional) Type a **Description** of the router.
9. Enter a **Username** for a user account with permission to configure the router.

Note: If you configured [role-based access](#) when you set up the router, you must enter the username `corero` and the same password you configured there.

10. Enter an authentication method for this device. Either:
 - Enter a **Password** for the user credentials to allow the SmartWall TDD system access to edit configuration on the router.
 - **(Native Telemetry only)** Paste in an **SSH Key** and **SSH Key Passphrase**. The SSH Key must be valid ASCII data for the private key, in PEM format (text starting with '-----BEGIN DSA PRIVATE KEY-----' or '-----BEGIN RSA PRIVATE KEY-----').

11. **(gRPC Telemetry only)** Set up gRPC Telemetry (if you don't want to use gRPC, leave the telemetry drop-down as **Native**).
 - a. From the Telemetry drop-down, select **gRPC**.
 - b. If required, edit the **gRPC Port**. The default port is 32767.
 - c. (Optional) If you're using SSL encryption on your gRPC telemetry connection:
 - i. Upload a **gRPC SSL Certificate Authority** using the **Choose File** button to select a certificate from your computer.
 - ii. In the **gRPC SSL Expected Server** field, type the CN name from the router's certificate. The CN name must be formatted as a DNS name. **Tip:** If the CN name is the same as the router hostname you entered in the Address field, you can leave this field blank.
12. Click **Save**.

Tip: On the table, you can use the following action options to **Edit** or **Delete** a remote device.

To configure the Mitigation Alerts to send mitigations to those devices

1. Open the SWA application in a browser and log in.
2. Use the top menu to navigate to **Alerts**.
3. At the table, locate the **Mitigation Application** alert template.
 - a. In the Action column click **Edit**.
 - b. Select **Enable**.
 - c. In the Action column click **Edit** again, then select **Edit Alert**.
 - d. Under Trigger Actions, expand **Corero Autonomic Response**.
 - e. In the **Devices Name** field you must type the hostnames of all your Remote Devices separated by commas (e.g. `router1,router2,router3`). This must exactly match the hostname on the router, and the name you provided in the Remote Mitigation table.
 - f. Click **Save**.
4. Repeat **steps a-f** for the **Mitigation Removal** alert template.

Verifying the TDD System is Connected

After completing all the tasks in this guide. Your TDD system should be in the following state:

Juniper Networks MX Series router:

- Configured to accept instructions from the vSWA
- Configured to send telemetry to the vSWA
- Configured to send port-mirrored traffic samples to the vNTD

vNTD:

- Accessible on your Management Network (pCLI only)
- Connected to the vCMS
- Licensed with your unique vNTD license (uploaded to the vCMS)

vCMS:

- Accessible on your Management Network (pCLI, CLI and Web UI)
- Connected to the vNTD and vSWA
- Operational Mode left in Monitor, ready to switch to Mitigate once you're happy with your defense Policy

vSWA:

- Accessible on your Management Network (pCLI and Web UI)
- Connected to vCMS
- Upload a SecureWatch Package File to manage your TDD license
- Remote Mitigation table contains all routers
- Add the names of the routers to the Corero Autonomics Alert

To verify the TDD system is connected

You can check your system is now fully connected in the SWA web UI.

1. Open the SWA web UI in a browser.
2. Open the **System > Health** screen.
3. You should now see green checks against every item, except:
 - Remote Device Info – This should be amber (warning) until a filter has been active on the system.
 - Slack Notifications – Will show blue (information). This is normal.

To force a Remote Device Info system check

On the **System > Health** screen, the **Remote Device Info** table won't show green ticks against a router until a filter has been sent and successfully received by the router. If you want to verify the connection before sending an active filter,

you can use the method below to send a dummy filter to your connected routers:

1. Open the SWA web UI in a browser.
2. Navigate to the **Dashboards** screen.
3. Click on **Flexible Configuration Tool** to open the dashboard.
4. From the **Action** drop-down, select **Detect**.
5. In the **Destination Host or CIDR** field, type **1.1.1.1/32** and press enter.
6. From the **Protocol** drop-down, select **IP** or **UDP**.
7. At the bottom right of the green area, click **Add**.
8. Click **Add** to send the filter to your routers.
9. Navigate to **System > Health** screen. The **Remote Device Info** table should now show green ticks against the routers.

Configuring the TDD Policy for your Network

You should now have a fully connected SmartWall TDD system communicating with your Remote Devices. By default, the SmartWall TDD system is in Monitor mode. In this mode, when it identifies DDoS attack traffic, it sends filters to the routers that will detect DDoS attacks but not block any traffic. You can see in the SWA analytics application which traffic the system would be blocking if it was in Mitigate mode.

You should leave the system in this mode for a few days, until you have analytics on enough traffic to determine what is normal for you. You can then adjust the Policy settings for your network.

Only once you have evaluated the defense Policy for your network traffic, should you then switch the system into **Mitigate** Mode and begin blocking DDoS attack traffic.

Troubleshooting

This section describes methods for addressing some problems that can occur when installing the system and making it operational.

Cannot access the Web UI (CMS or SWA)


Access to the CMS web UI and the SWA web UI is provided via the management IP address configured for each at setup time; make sure to use HTTPS for both, and specify port 8000 when accessing SWA:

- **CMS:** `https://x.x.x.x [management IP address]`
- **SWA:** `https://x.x.x.x:8000 [management IP address]`

To log in to CMS and SWA, make sure to use the administrator credentials that were specified at setup time. The default username is *admin* and the default password is *smartwall*. If a different username/password combination was specified during setup, you need to use those credentials instead.

Getting help for using the CMS or SWA

CMS and SWA each provides a link to help documentation in the top menu bar.

In the CMS, click  the help icon to access the CMS Knowledgebase. From the home page of the Knowledgebase you can download additional help PDFs, browse for information using the expandable left-hand menu, or type a search term in the search bar.

In SWA, clicking **Help > User Guide** displays a PDF file that describes the controls shown in each SWA screen.

CMS configuration change does not take effect

Configuration changes in the CMS do not take effect until they are committed and any uncommitted changes can be lost when you logout. Always remember to commit your changes (**Commit > Commit**), before you log out.

Defense device not reachable from CMS

Adding a Defense device to the CMS doesn't automatically mean the device is reachable from the CMS, you are just telling the CMS what device to look for. A variety of different problems could prevent the CMS from communicating with the device.

In the CMS, click **Network > Devices** to display the Devices table. The **Deployment State** column shows connectivity information for each managed device. The following states indicate the device is not connected:



- **Connection refused** – The CMS successfully sent a request to the device but the device refused to send a response.
- **Connection timed out** – The CMS attempted a connection but the attempt timed out.
- **Authentication failed** – The CMS attempted a connection but the authentication credentials on the CMS did not match the credentials on the device.

Most issues can be remedied by performing the following checks:

- Does the device have power?
- Is the device management port connected to the network?
- Does the CMS have connectivity to the network on which the devices management interface is connected?
- Does your firewall allow the connection?
- Does the CMS have the correct IP address for that device?
- Is the device in the correct Authentication Group in the CMS? Do those credentials need to be updated?

The Defense device shows out-of-sync in the CMS

If a device is "out of sync" it means that the Policy on the device does not match the corresponding Policy in the CMS. You may occasionally see a device become out of sync after the device has been restarted, or after you perform a software upgrade. In the CMS, click **Network > Devices** display the Devices table and look in the **Deployment State** column to see which device is out of sync, and what action is required:

- **Sync required** – The device is connected but its Policy configuration does not match the current Policy committed to the CMS. The device could have become out of sync if it was unavailable when a change was committed in the CMS or if you have replaced a connected device with a new version (with the same IP address). In the Devices table, click  the action button and select **Sync Device** to push the Policy changes to the device.
- **Force sync required** – The device is connected but there has been an unexpected error in the Policy configuration. In the Devices table, click  the action button and select **Force Sync Device** to wipe the old Policy from the device and replace it with the current version stored in the CMS.
- **Not in cluster** – The device is not in a Cluster. Go to **Network > Clusters**, add the device to an existing Cluster or create a new Cluster for it.
- **Initial sync pending** – The device is new and the CMS has not yet sent its Policy configuration. Wait a few minutes and check again.

vNTD device showing as not-licensed

You must have at least 10Gbps available license capacity for the Defense device to automatically license and connect to the CMS. If you don't, you will have to create some space by delicensing an old vNTD or buying additional license capacity from your Corero representative. You can then license the device manually:

1. In the CMS, use the left-hand menu to navigate to **Network > Devices**.
2. On the Devices table, locate the vNTD you want to license.
3. In the Actions column, click **...** and select **License**.

Tip: If you need to delicense a vNTD, in the Actions column, click **...** and select **Delicense**. The delicense option is only available for currently licensed vNTDs. When you delicense a vNTD (or add it to the CMS when there isn't enough license capacity available), it enters the not-licensed state. In the not-licensed state, the devices do not send any information via syslog message (except the device status), and cannot function as Detection Engines for the TDD.


Remote Device added to the CMS Devices table instead of the SWA

If you accidentally add a Remote Device (e.g. a router) to the Devices table in the CMS (**Network > Devices**), it will appear with a status message of `unexpected device type`. Remote Devices cannot be stored in this table, it is only for vNTDs. Delete the Remote Device from the table and instead add it to the Remote Devices screen in the SWA Web UI (**Mitigation > Remote Devices**).

Cannot add a new vNTD to a CMS Cluster

To use SmartWall Network Threat Defense virtual editions (vNTDs) you need to have a license for them. If you do not have a vNTD license, or you have already allocated your full license capacity, when you add a new vNTD to the CMS you will be unable to add it to a Cluster. In the CMS, click **Network > Devices** to display the Devices table and check the **Deployment State** column to see if the vNTD is listed as **not-licensed**. To license this vNTD you need to contact your Corero representative for additional license capacity and upload the new license file. Alternately, you can choose to delicense another vNTD. Once you have the available license capacity, at the Devices table click **...** the action button next to the unlicensed vNTD, and select **License**.

SWA doesn't show any data from the CMS

SWA receives data from the managed Defense and Bypass devices via the CMS. If SWA is not receiving data, it will not show any information on the Overview screen. Open the CMS in a browser and navigate to **System > Analytics & Syslog**. On the Servers table, check the details of your SWA application to make sure you have the correct IP address and the right port number (the default should be 9997). If you need to make a change click  the edit button and remember to commit your changes (**Commit > Commit**).

If the CMS is configured correctly to send data to SWA, but you still don't see all the expected data in SWA, it may be that your devices are not reachable from the CMS. In the CMS, click **Network > Devices** to display the Devices table and check the **Deployment State** column to see if the devices are connected. If they aren't connected, follow the checks in the above method: [Defense device not reachable from CMS](#).

Remote Device Info table (System > Health) is showing warning against new router

On the **System > Health** screen, the **Remote Device Info** table won't show green ticks against a router until a filter has been sent and successfully received by the router. If you want to verify the connection before sending an active filter, you can use the method below to send a dummy filter to your connected routers:

1. Open the SWA web UI in a browser.
2. Navigate to the **Dashboards** screen.
3. Click on **Flexible Configuration Tool** to open the dashboard.
4. From the **Action** drop-down, select **Detect**.
5. In the **Destination Host or CIDR** field, type **1.1.1.1/32** and press enter.
6. From the **Protocol** drop-down, select **IP** or **UDP**.
7. At the bottom right of the green area, click **Add**.
8. Click **Add** to send the filter to your routers.
9. Navigate to **System > Health** screen. The **Remote Device Info** table should now show green ticks against the routers.

SWA doesn't show any telemetry data from a router

If you are expecting to see telemetry from a router but none is appearing in the SWA, you must check the router has been successfully added to the SWA and CMS application.

First, check the SWA. On the Health screen (**System>Health**), if you cannot see the router in the Remote Devices Info table, there has most likely been a mistake made when adding the routers.

Check the mitigation alerts have the correct hostnames for the routers: **Alerts > Mitigation Application and Mitigation Removal >Edit > Edit Alert > Corero Autonomic Response**. Then under Device Names, make sure the router hostnames are spelled identically to how they appear in the router and in the SWA Remote Devices table. Also check that they are all separated by a single comma (no spaces).

Check the SWA to make sure the correct IP addresses and access credentials are stored for each router. Open the SWA Web UI > **Mitigation > Remote Devices** and click **Edit** next to each router to check the stored information. The name shown must be the hostname for the device, check it is identical to how it is displayed on the router. The password is obfuscated so you may need to re-enter it.

Finally, check the configuration on the forwarding plane of the Juniper Networks MX Series router. A good place to start is to check the router is reachable and receiving traffic as expected. The following three troubleshooting commands can help you begin to diagnose an issue, for more information see the Juniper documentation for your router.

- `show chassis fpc` – Display status information
- `ping 128.0.0.16 routing-instance __juniper_private1__` – Check the connection between the forwarding plane and control plane
- `monitor interface traffic` – Display real-time statistics about interfaces

Caution: Be careful to get the order of words correct in `monitor interface traffic`. Typing `monitor traffic interface` may start a TCP dump.

Telemetry traffic is only showing for one of my connected routers

If you have some of your routers in a remote subnet from the SWA, the telemetry traffic may not be recognized on the secondary interface. To fix this, you need to add a static route from the SWA to each router on the remote subnet. You can do this in the SWA pCLI, for each router:

1. Open the SWA pCLI and log in as the admin user.
2. Type the command: `setup routes`
3. Type `I` to insert a new route.
4. Enter the following information:
 - Destination IPv4 Address – The IP address of the telemetry interface on the router.
 - Network Mask – 255.255.255.255
 - Gateway – The IP of the next hop router from your SWA
5. Type `A` to accept the change.

Traffic is entering the network, but the Defense device does not seem to do anything with it

If the tables and charts in SWA show inbound traffic entering the network, but there's no evidence that rules are being triggered on the SWA, there may be no DDoS attacks occurring. However, if the traffic appears abnormal but the system is not responding to it as expected, you should first check the system is healthy:

1. Open the SWA Web UI and log in.
2. Navigate to **System > Health**.
3. Check all table rows are showing as expected with **green ticks** to indicate good health. If there are any errors, warning, or information messages, you can investigate to see if these are the route of the issue.

If your system is in good health, another possibility is that you may have accidentally changed the necessary defense policy settings required to trigger mitigations. Check the CMS defense policy defaults are still in place. You can contact your support representative for more information.


Note: If the TDD Flex-Rules show a revision number higher than 1, you may have accidentally edited the filter definition . This can disrupt the TDD system's ability to mitigate attack traffic. Contact your support representative for a copy of the original filter definition if you're concerned.

Mitigations are not performing the actions I expect

For the TDD mitigations to work as described, your CMS Operating Mode must be set to Mitigate. If the Operating Mode is in Monitor you will see the following behavior:


- Block mitigations > accept action on router
- Detect mitigations > accept action on router
- Redirect mitigations > act as disabled mitigations
- Policer mitigations > act as disabled mitigations
- Ignore and disabled work as expected

To change the Operating Mode to Mitigate

1. Open the CMS web UI in a browser and log in.
2. Use the left-hand menu to navigate to **Network > Operating Modes**.
3. Use the **Global Defense Mode** drop-down to change the default mode to **mitigate**.
4. If you want to save the new configuration, and push your changes to any affected Defense devices, click  . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Note: The Monitor mode can be used for testing new mitigations and is the default mode for new installations.

CMS shows uncleared alarms

In the CMS application, click on  the Alarm icon in the Status bar and open the Alarm Center. Uncleared alarms are listed, describing issues that require your attention.

Lost administrative user credentials

If you have lost the admin user credentials for a vNTD, vCMS or vSWA virtual machine, you can reset the username/password to their default values (admin/smartwall) without redeploying the VM.

Note: Resetting the administrative username and password will not affect any other user credentials.

1. Create a password reset ISO file. You can use the following command to create a password reset ISO file in Linux. These commands assume you already have the package containing the mkisofs command installed; if you don't, you should download this first using the Linux package manager.

```
>reset_pw
mkisofs -input-charset utf-8 -quiet -o reset.iso reset_pw
```
2. Transfer the ISO file to a datastore which can be accessed by the virtual machine.
3. On the host where the virtual machine is deployed, set the CD-ROM drive for the virtual machine to the datastore ISO file. Ensure that the device status is connected.
4. Restart the guest virtual machine. When the virtual machine reboots, it should display the following message:

```
Username/password reset to default
```
5. Login with the username: `admin` and the password: `smartwall`. After logging in, you can change the user-name and/or password using the `setup aaa` command in the pCLI.
6. Disconnect the CD-ROM from the virtual machine (e.g. in VMware you can do this by clicking **Edit virtual machine settings**, opening the **CD/DVD drive 1** settings, and deselecting **Connected**). If you don't, the user-name and password will be reset to default every time you restart the VM.

Downloading diagnostic packages

During troubleshooting, customer support may ask you for diagnostic packages from the affected systems. You can download them through your browser in the following locations:

- **For SWA** – Open the SWA in a browser. **System > Settings > Diagnostic Package > Download**
- **For CMS** – Open the CMS in a browser. **System > Diagnostics**. Under **Download file from CMS appliance**, select a **source** package type and click **Download File**.
- **For a vNTD** – Open the CMS in a browser. **System > Diagnostics**. Under **Download file from a device**, select a **source package** type and the specific **device**. Click **Download File**.

After restarting my server, the Corero applications haven't come back up

By default, Corero VMs are not configured to automatically start on ESXi server boot. Corero recommends you set the VMs to automatically start by editing the ESXi servers host settings:

To configure the host to auto-start VMs after a restart

1. Open vSphere Web Client.
2. Select the host.
3. Open the **Configure** tab.
4. From the menu, under **Virtual Machines**, select **VM Startup/Shutdown**.
5. Click **EDIT**.

6. Check the box next to **Automatically start and stop the virtual machines with the system**.
7. Click **OK**.

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 <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://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: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://corero.force.com/support>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <https://apex.juniper.net/>

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

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://apex.juniper.net/>
- 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 <https://support.juniper.net/support/requesting-support/>.

Requesting Licenses

The system requires a TDD license key, plus keys for each vNTD, to become fully operational. Juniper devices do not require license keys to support the solution. To obtain the keys, please contact the Corero Customer Services team by one of the following methods:

- Email: Support.Portal@corero.com
- Web: <https://corero.force.com/support>
- Telephone: Dial +1.978.212.1500 -> Select Option 2

Appendix A – Deploying a vNTD for High Inspection Rates

The following instructions cover how to deploy a vNTD for deployments expecting traffic rates of 1.2Gbps or higher per core. For high performance rates the vNTD requires dedicated hardware resources to achieve performance and some host optimization.

To deploy a vNTD for high sampled traffic rates, you must complete the following steps:

1. Use an X710 or equivalent NIC (VMXNET3 is not compatible with this method).
2. Deploy using vSphere WebClient
3. Isolate sampled traffic NICs to prepare for PCI Passthrough, and optimize the host
4. Deploy the vNTD
5. Allocate sampled traffic NICs to the vNTD to complete PCI Passthrough

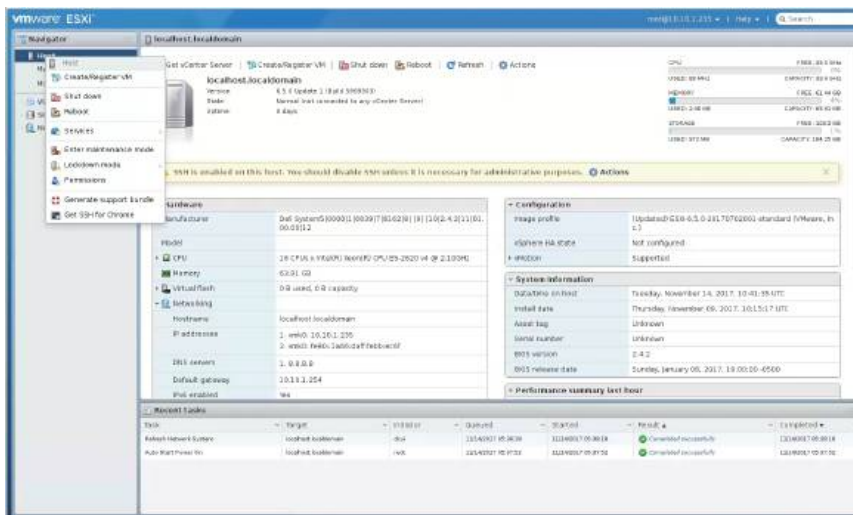
To deploy a vNTD using vSphere WebClient

Caution: You must use ESXi version 6.5 or later.

Isolate the sampled traffic NICs for PCI Passthrough and optimize host

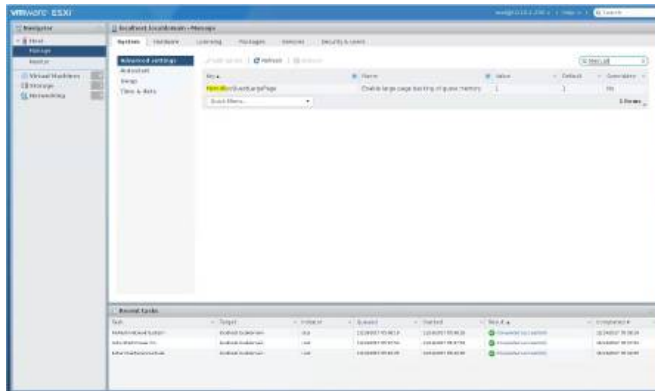
Caution: When you deploy a vNTD using vSphere Client, you cannot enable 1G HugePages to improve performance. For line rate performance at small packet sizes, use a KVM deployment.

1. In the vSphere WebClient, put the Host into maintenance mode:
 - a. Right click on **Host** and select **Enter maintenance mode**.

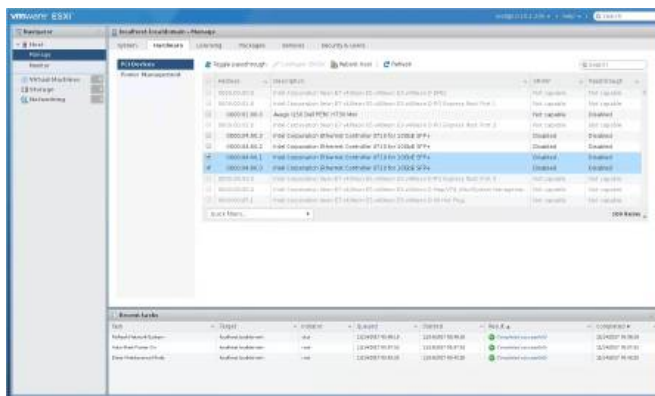


- b. Click **Yes** to confirm
2. In the Navigator, under Host, click **Manage**.

3. Check large pages is enabled. In the System tab, locate **Mem.AllocGuestLargePage** in the Advanced Settings table, and check it has the value **1**.



4. Isolate the NICs. In the Hardware tab, select the two NICs you want to use for the vNTD then click **Toggle passthrough**.



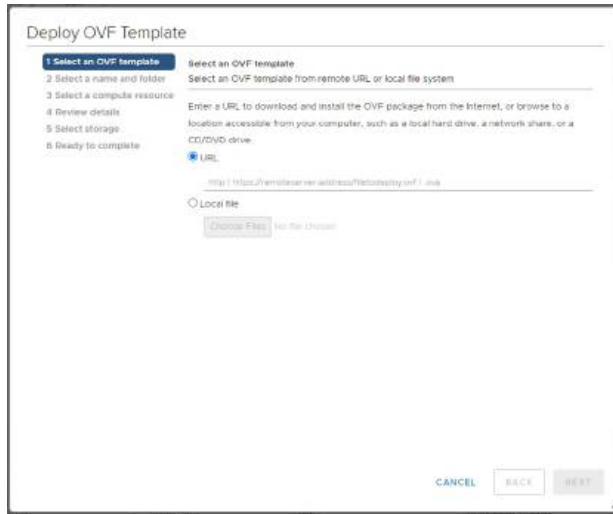
5. Click **Reboot host**. Click **Reboot** to confirm.
6. When reboot complete, log back in.
7. Right click on **Host** and select **Exit maintenance mode**.

Deploy a vNTD for high sampled traffic rates

1. In vSphere WebClient, right-click the **Host** you want to create this Virtual Appliance on, and select **Deploy OVF template**.

2. Select an OVF template:

- Select **URL** and type the full URL to the OVA file stored on an HTTP/HTTPS server.



Deploy OVF Template

1 Select an OVF template

Select an OVF template

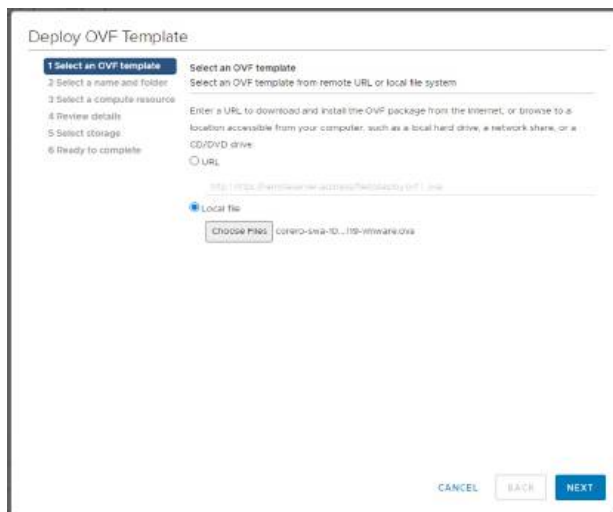
Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

☒ URL

☐ Local file

- Select **Local file**, click **Choose Files** and select the OVA file for your required VM.



Deploy OVF Template

1 Select an OVF template

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

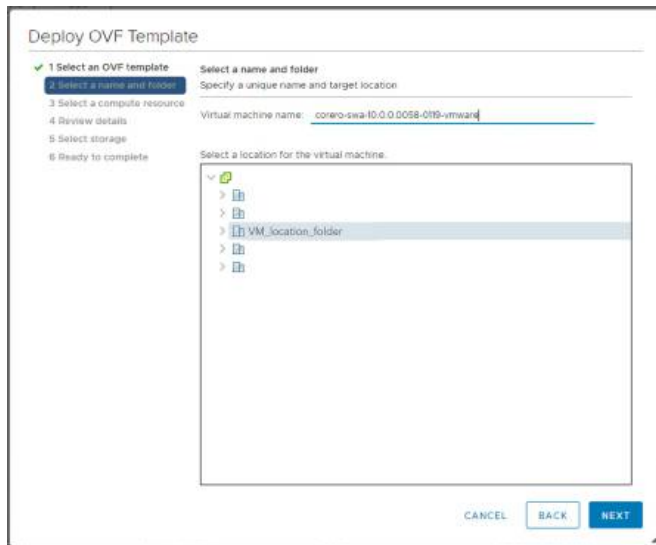
☐ URL

☒ Local file

3. Click **Next**.

4. Type a **Virtual Machine name**.

5. Select where you want to deploy the VM.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select a name and folder
Specify a unique name and target location

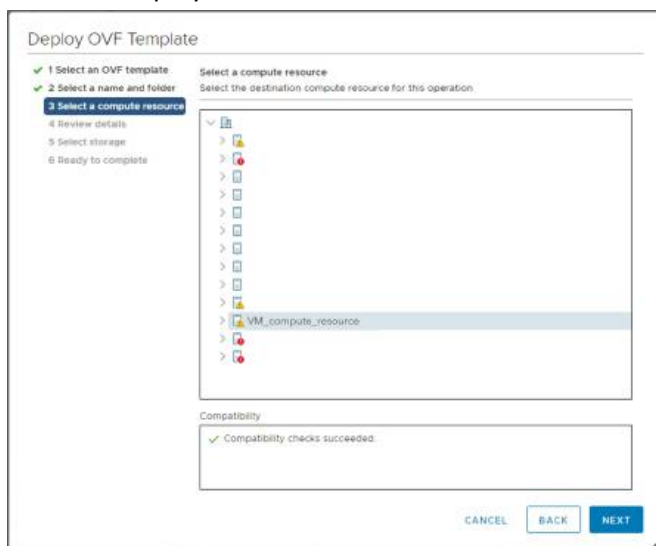
Virtual machine name:

Select a location for the virtual machine.

☒ >
☐ >
☐ >
☒ > VM_location_folder
☐ >
☐ >

CANCEL BACK NEXT

6. Click **Next**.
7. Select the destination compute resource you want to use for this VM. This will be the host where you want the VM to be deployed.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select a compute resource
Select the destination compute resource for this operation.

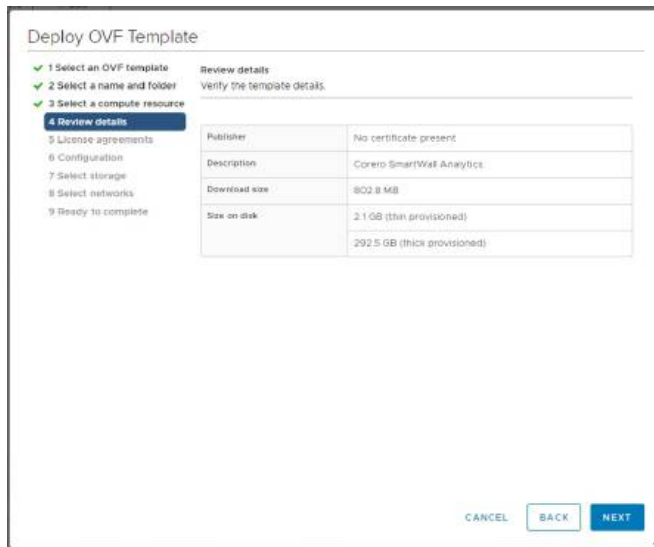
☒ >
☐ >
☐ >
☐ >
☐ >
☐ >
☐ >
☐ >
☐ >
☒ > VM_compute_resource
☐ >
☐ >

Compatibility
☒ Compatibility checks succeeded.

CANCEL BACK NEXT

8. Click **Next**. The VM will be validated.

9. Review the template details.



Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details**
- 5 License agreements
- 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Ready to complete

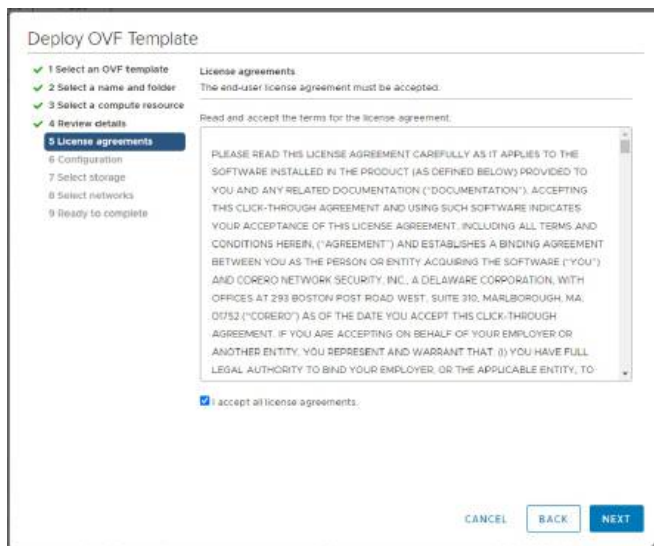
Review details
Verify the template details.

Publisher	No certificate present
Description	Corero SmartWall Analytics
Download size	802.8 MB
Size on disk	2.1 GB (thin provisioned) 292.5 GB (thick provisioned)

CANCEL BACK NEXT

10. Click **Next**.

11. Read the end user agreement and check the box next to **I accept all license agreements**.



Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements**
- 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Ready to complete

License agreements
The end-user license agreement must be accepted.

Read and accept the terms for the license agreement:

PLEASE READ THIS LICENSE AGREEMENT CAREFULLY AS IT APPLIES TO THE SOFTWARE INSTALLED IN THE PRODUCT (AS DEFINED BELOW) PROVIDED TO YOU AND ANY RELATED DOCUMENTATION ("DOCUMENTATION"). ACCEPTING THIS CLICK-THROUGH AGREEMENT AND USING SUCH SOFTWARE INDICATES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT, INCLUDING ALL TERMS AND CONDITIONS HEREIN, ("AGREEMENT") AND ESTABLISHES A BINDING AGREEMENT BETWEEN YOU AS THE PERSON OR ENTITY ACQUIRING THE SOFTWARE ("YOU") AND CORERO NETWORK SECURITY, INC., A DELAWARE CORPORATION, WITH OFFICES AT 293 BOSTON POST ROAD WEST, SUITE 310, MARLBOROUGH, MA, 01752 ("CORERO") AS OF THE DATE YOU ACCEPT THIS CLICK-THROUGH AGREEMENT. IF YOU ARE ACCEPTING ON BEHALF OF YOUR EMPLOYER OR ANOTHER ENTITY, YOU REPRESENT AND WARRANT THAT: (i) YOU HAVE FULL LEGAL AUTHORITY TO BIND YOUR EMPLOYER, OR THE APPLICABLE ENTITY, TO:

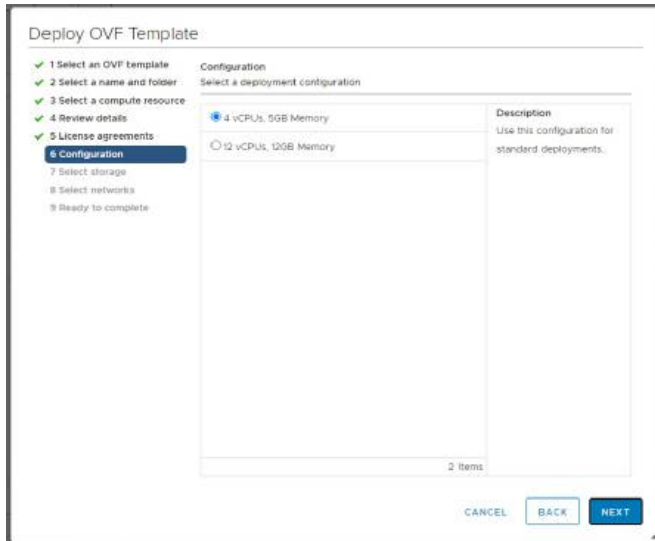
☒ I accept all license agreements.

CANCEL BACK NEXT

12. Click **Next**.

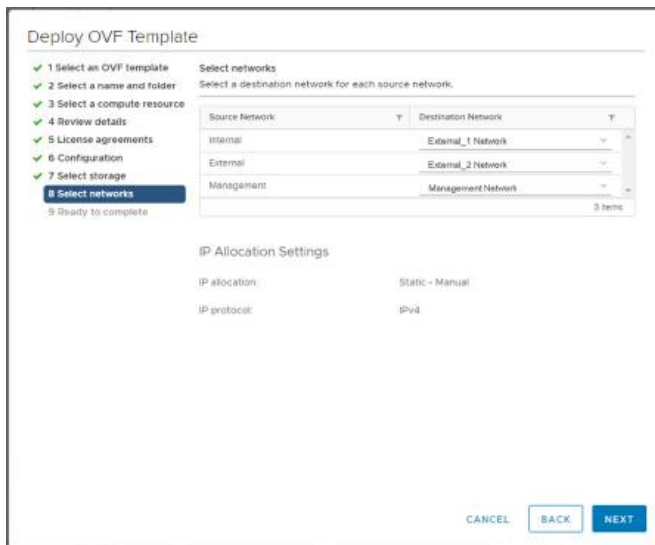
13. From Select virtual disk format, select **Thick Provision Eager Zeroed**.

14. Select the storage disk you want to use.



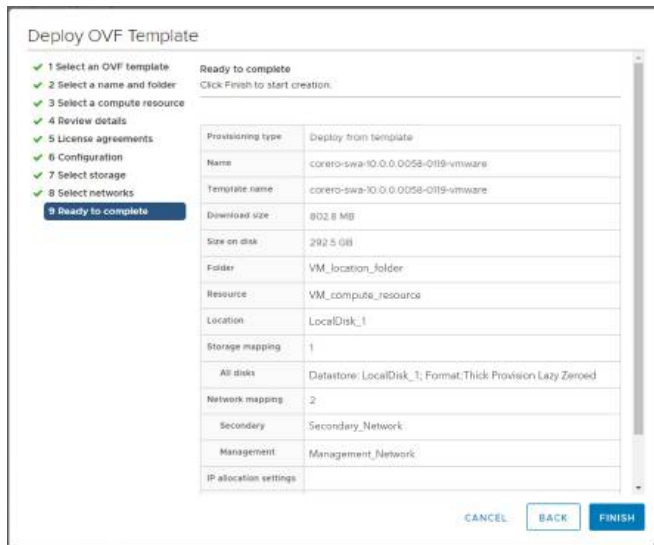
15. Click **Next**.

16. Under Select networks, select the networks you require. For the vNTD you need the **Management** network and an **External_1** and **External_2** network. **Caution:** The External_1 and External_2 networks cannot be the same.



17. Click **Next**.

18. Review your selections.



Deploy OVF Template

Ready to complete
Click Finish to start creation.

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Configuration
7 Select storage
8 Select networks
9 Ready to complete

Provisioning type	Deploy from template
Name	corero-swa-10.0.0.0058-0119-vmware
Template name	corero-swa-10.0.0.0058-0119-vmware
Download size	802.8 MB
Size on disk	292.5 GB
Folder	VM_location_folder
Resource	VM_compute_resource
Location	LocalDisk_1
Storage mapping	1
All disks	Datastore: LocalDisk_1; Format: Thick Provision Lazy Zeroed
Network mapping	2
Secondary	Secondary_Network
Management	Management_Network
IP allocation settings	

CANCEL BACK FINISH

19. Click **Finish**. The VM is created powered off. Do not power it on yet.

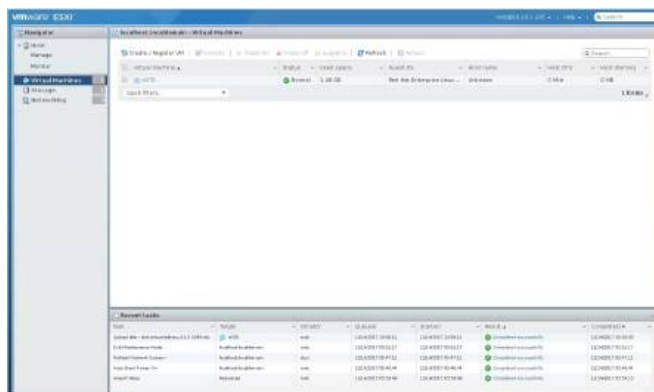
20. Check the allocated ports will not create a network loop when enabled, then enable ports:

- In vSphere WebClient, right click on your new VM and select **Edit Settings**.
- Scroll down to **Network adapter 2**. Check the network label is correct and then under Device Status, select the **Connect** check box.
- Repeat for **Network adapter 3**.
- Click **OK**.

Allocate sampled traffic NICs to complete PCI Passthrough and optimize the vNTD

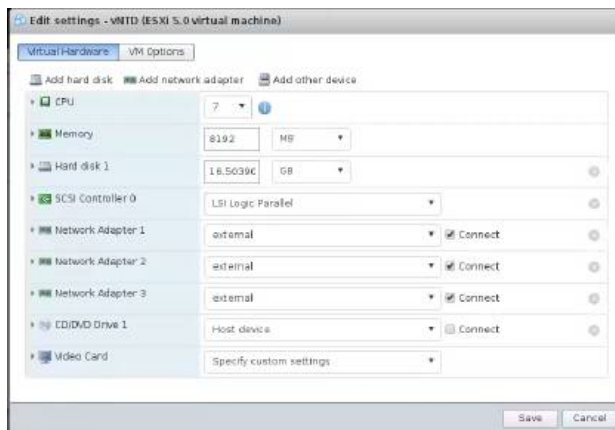
Caution: The VM must be powered off before completing the following steps.

- In vSphere WebClient, wait for the vNTD Virtual Appliance to finish building. **Make sure it is powered off.**
- In the Navigator, click on **Virtual Machines** and click on the name of the new vNTD Virtual Appliance.

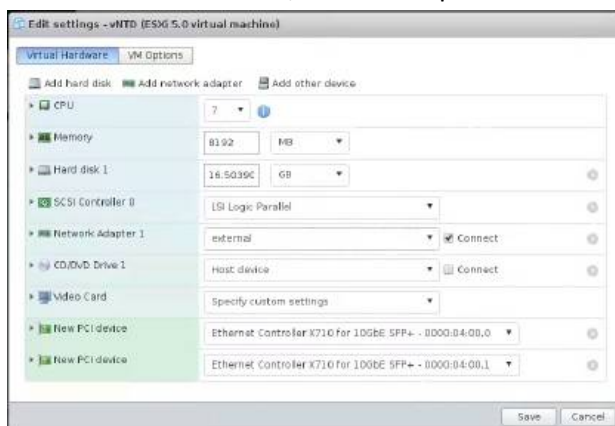


3. Allocate the NICs:

- In the toolbar, click **Edit**.
- Use the **X** buttons to remove **Network Adapter 2** and **Network Adapter 3**.



- Add two PCI devices using **Add other device > PCI device**.
- On each new PCI device, use the drop-down list to select the correct isolated NIC.



- For the PCI device allocated to each NIC, click on the expand arrow next to New PCI device to display more options and click **Reserve all memory**.



4. Optimize the VM settings for performance:

- Still in the edit dialog, at the top of the hardware list, click the expand arrow next to CPU.
- For **Scheduling Affinity**, in the **Available CPUs** field, type the range of processors available (e.g. **1-7**).
- For **CPU/MMU Virtualization**, use the drop-down to select **Hardware CPU and MMU**.



- Click **Save**.

5. In the VM toolbar, click **Power on**.