Corero Network Security

SmartWall Threat Defense Director User Guide

Software 9.7.5

09 December 2020

Part Number: 9501-0975-00-J

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.

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

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.

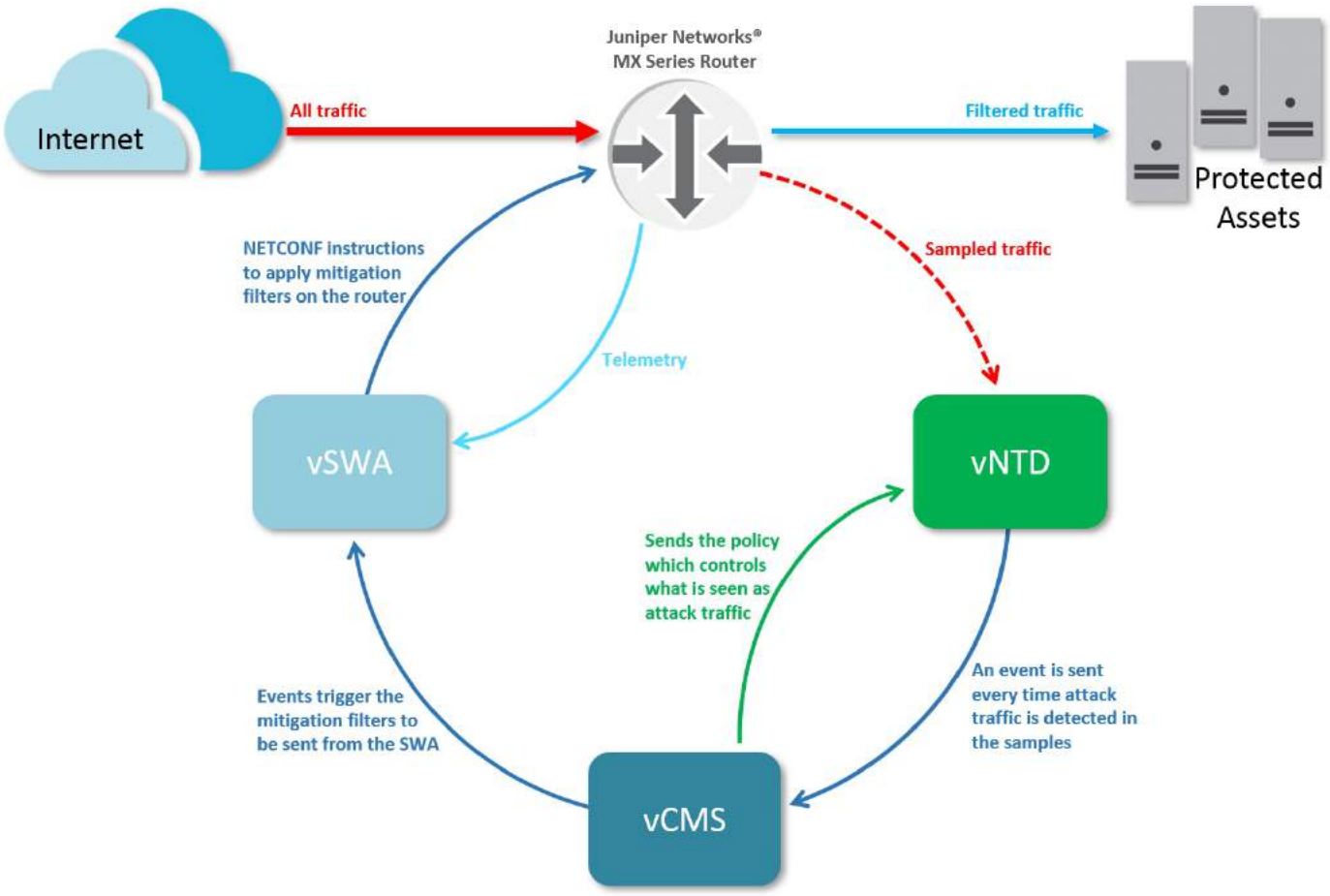
Note: The SmartWall TDD User Guide available from inside the SWA and CMS User Guide available from inside the CMS contain additional information compared to the versions of the guides available on the Juniper Support Portal. This information is only available to customers and is not publicly accessible.

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".

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, and NTD120) or a Bypass Device.

Segments

A Segment is an interface pair to which DDoS protection is applied. The segment is associated with a port pair on a Defense device. The first time you connect a Defense device to the CMS, it identifies the available interfaces and records them as Segments.

> **Note:** A vNTD has two available interface ports which act as one Segment. For SmartWall TDD deployments only the 1st interface will be used. The 2nd interface should be disabled in the CMS.

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-though mode only applies to the TDS system.

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.

> **Caution**: Do not use truncated samples on the Juniper Networks MX Series router.

Telemetry

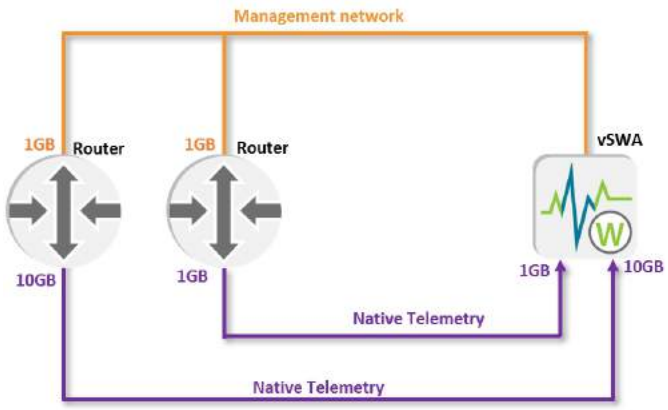
Telemetry is sent from the Juniper Networks MX Series router to the vSWA. It shows the network traffic processed by the router including what was permitted or blocked by the TDD system.

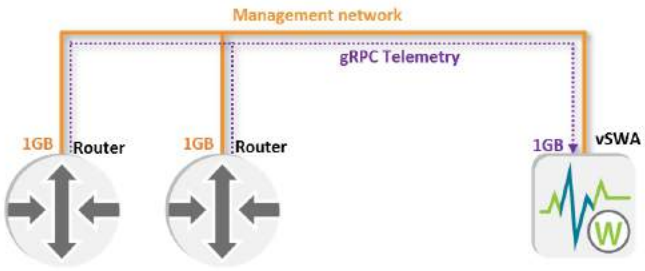
The TDD requires a telemetry feed from every monitored router to the SWA application. There are two main telemetry delivery methods:

- **Native telemetry** (UDP) – Telemetry is sent over your traffic network between the router and SWA. This requires a dedicated 10GB port on the router and a 10GB, or 1GB, port on the SWA host.
- **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.

You decided which telemetry type is used when you configure the Juniper Networks MX Series router (See SmartWall TDD Getting Started Guide for instructions). 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.

Accessing the TDD Components

After you deploy the SmartWall TDD, you will have 4 configured component types working together to protect your network:

- Juniper Networks MX Series router
- SmartWall Network Threat Defense devices (vNTD devices working as Detection Engines)
- SmartWall Central Management Server (CMS)
- SmartWall SecureWatch Analytics(SWA)

For regular operation, you will mostly use the SWA application, but you will also need to maintain some configuration settings in the CMS application, including managing your Defense devices.

SWA

You can access the SWA Web UI through a browser by typing the IP address of your SWA application followed by :8000 (e.g. *https://10.10.100.200:8000*) or by the DNS address, if you set one up during installation. You can access all analytics and TDD functions through the Web UI.

After initial configuration, if you need to perform a higher level operation, like changing the application IP address or NTP server, you can access the pCLI by opening the console connection or using an SSH client: `ssh -p 2222 <username>@<SWAipAddress>`

Monitor users also have read-only access to the **REST API** on port 8089.

> **Caution:** If you plan to allow monitor access to the REST API, you should configure IP filtering to limit access to only trusted accessors and ensure you have changed the default passwords.

CMS

There are 3 ways to access the CMS:

- **Web UI** – You can access the CMS Web UI through a browser by typing the IP address of your CMS application (e.g. *https://10.10.100.100*) or DNS address, if you set one up during installation. You can access all main CMS functions through the Web UI.
- **CLI** – You can access the CMS CLI using an SSH client to connect to the IP Address of your CMS, on the default port 2024 . You can access all CMS functions through the CLI.
- **REST API** – You can access the REST API using any tool that sends HTTP requests to a URL, but it is most easily available using Swagger: In a browser type the IP address of your CMS followed by /api(e.g. *https://10.10.100.100/api*) and log in with your CMS credentials. You can affect Protection Policy changes through the REST API and view device status information.

After initial configuration, if you need to perform a higher level operation, like changing the application IP address or NTP server, you can access the pCLI by opening the console connection or using an SSH client: `ssh -p 2222 <username>@<CMSipAddress>`

vNTD

After initial configuration, you can manage the vast majority of the Defense device configuration from within the CMS (Network>Devices). If you need to perform a higher level operation, like changing the device's IP address or NTP server, you can access the device's pCLI by opening the console connection or using an SSH client: `ssh -p 2222 <username>@<vNTDipAddress>`

Supported web browsers for the Web UI

- **Chrome:** 71 or newer
- **Edge:** 44 or newer
- **Firefox:** 64 or newer
- **Safari:** 12 or newer
- **Internet Explorer:** not supported

Juniper Networks MX Series router

After initial configuration, you should be able to manage the connection to the router in the SWA (Mitigation > Remote Devices). If you need to access the router, you can use an SSH client: : `ssh -p 22 <username>@<MXipaddress>`

Juniper Networks MX Series router requirements

Your Juniper Networks MX Series router 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 minimum

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

Working in the TDD Applications

After configuration, the majority of TDD tasks are performed in the SWA Web UI, but there are occasions where you may still need to use the CMS to complete a task. The following lists can give you an general idea of the roles performed by each application:

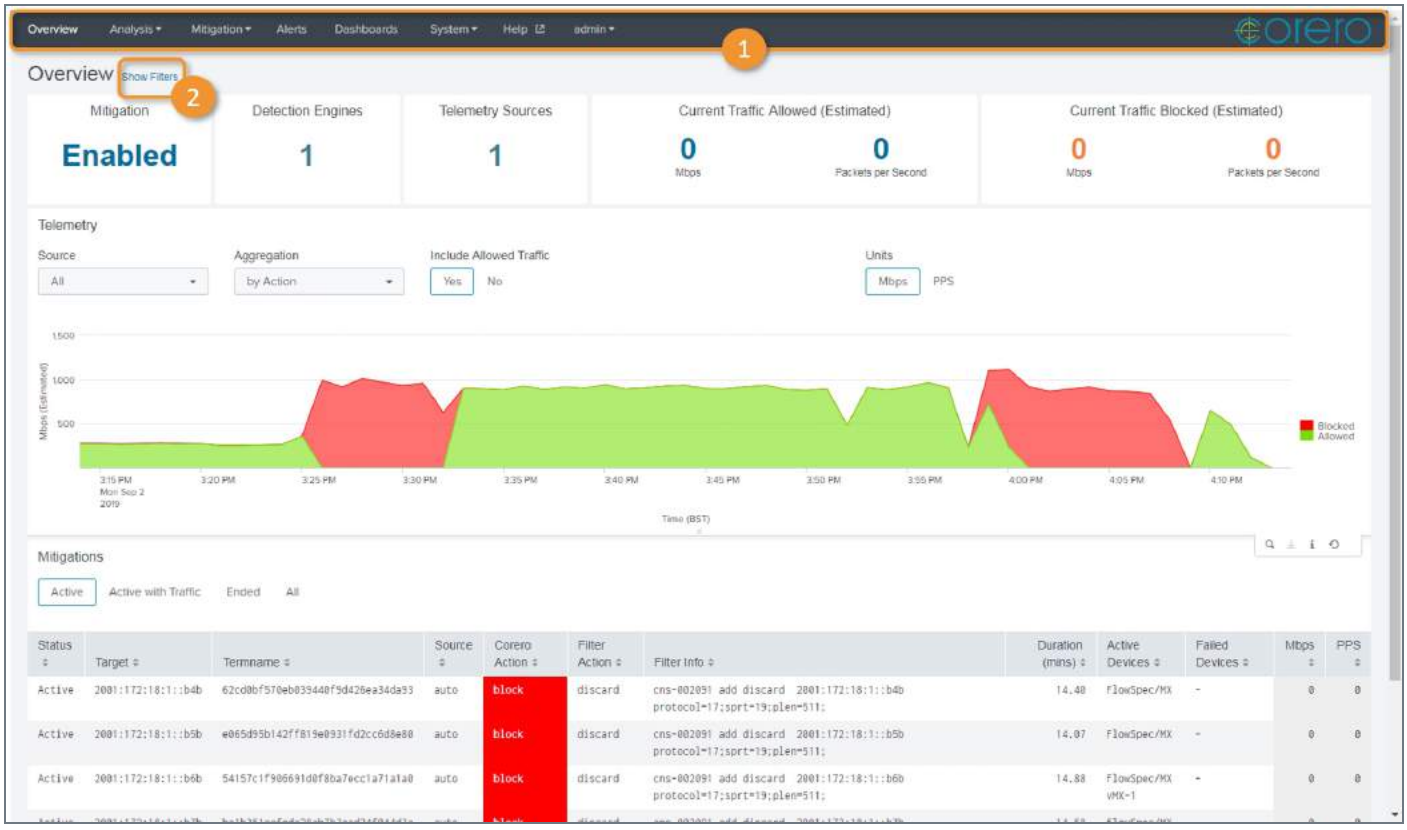
When to use SWA:

- Viewing telemetry from the routers and system status
- Analyzing traffic
- Managing alerts
- Managing router access credentials

When to use CMS:

- Managing connection to the vNTDs and SWA application
- Making minor modifications to the defense Policy
- Managing your licenses

The SWA Web UI



1. Top Menu

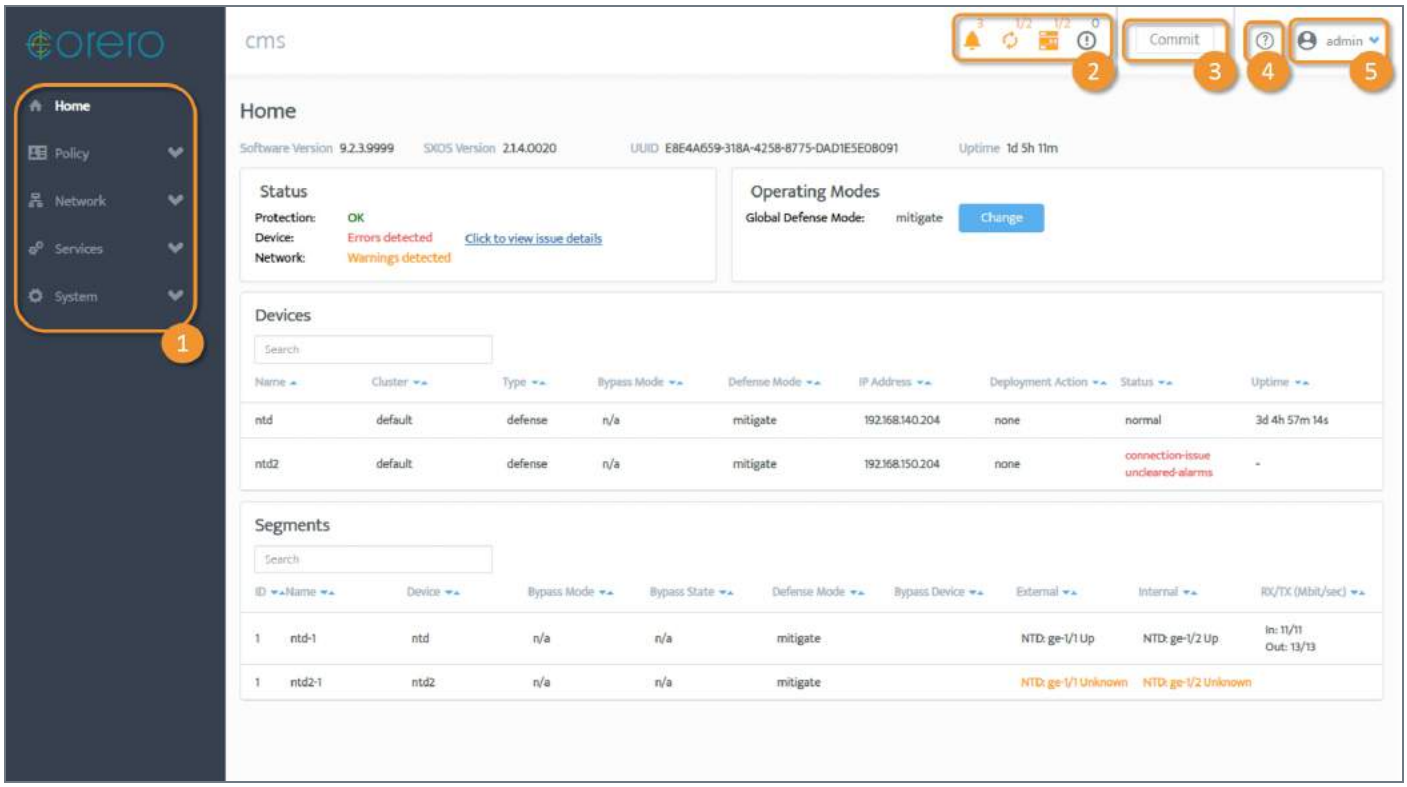
This is the main navigation toolbar for the SWA application. You can access the following screens:

- **Overview** – Opens the Overview screen where you can see high level charts showing data from the managed routers. You can also click the Corero logo to reach this page
- **Analysis** – Opens the Analysis sub-menu, where you can access screens which enable you to analyze the data coming from the vNTD rather than the routers (**Charts** and **Events**), and **Search** syslog messages
- **Mitigation** – Opens the Mitigation sub-menu, where you can access screens which enable you to modify mitigations (**Actions**), manage your **Remote Devices**, and modify defense policy for specific destination IP addresses (**CIDR Policy**).
- **Alerts** – Opens the Alerts screen where you can create and edit system alerts
- **Dashboards** – Opens the Dashboard Manager where you can create your own variations of the existing screens
- **System** – Opens the System sub-menu, where you can perform the following tasks:
    - View TDD system **Health**
    - Manage your connected **Email Server**
    - **User Management**
    - Configure **LDAP**
    - Configure **RADIUS**
    - **SecureWatch Packages**
    - Manage **Snapshots**
    - Download a **Diagnostic Package**
    - View the **Lookup Editor**
    - **Restart Server**
- **Help** – Opens this User Guide as a PDF in a new tab
- ***<userName>*** – Your username is displayed here in the top menu. Click to open a sub-menu which enables you to **Logout** or **Change Password**.

2. Show filters (Overview, Charts, Events, and Actions screens only)

On some screens in the SWA, you can use the screen filters to change what the screen shows. The settings are specific to each screen but generally they can control the timeframe shown, display additional charts, and change the units charts are shown in.

The CMS Web UI



> **Note:** The screenshots in this guide show the interface as a **cns-admin** user. Some features or screens may not be visible to other user roles.

Surrounding the main interface area there are the following navigation and information aids:

1. Menu

The expandable menu on the left of the screen contains a link back to the **Home** screen and then four expandable sections:

- **Policy** – Options related to creating Protection Profiles and tuning the Policies they contain
- **Network** – Options related to managing Clusters, Devices, and Segments
- **Services** – Options related to using external mitigation capabilities
- **System** – Options related to managing the CMS, and its connection to SmartWall SecureWatch Analytics

2. Status bar

At the top right of the screen, there are 4 icons that summarize the status of the CMS and your devices. If the icon is green, this indicates there are no problems. If the icon turns orange, then something needs your attention.

The icons represent:

- **Alarms** – When this icon is orange, there is an uncleared alarm. Click this icon to open the Alarm Center and view the list of cleared and uncleared alarms.
- **Devices in sync** – When this icon is orange, there is a device which is not in-sync. Click this icon to open the Devices screen to sync the device.
- **Devices reachable** – When this icon is orange, there is a device which is not reachable by the CMS. Click this icon to open the Devices screen to see what device cannot be reached.
- **Notifications** – Click this icon to view or clear previous notifications from this session.

3. Commit button

In the top right of the screen, you can see the Commit button. This remains inactive until you make a change that needs to be saved and sent to a Defense device. When it is active, you can click the button to view a list of your pending changes. On that dialog, click **Commit** to send those changes to the appropriate devices, or **Discard** to delete those pending changes.

> **Caution:** If you log out, or the CMS logs you out after a period of inactivity, you will lose any changes which you have not committed.

4. Help button

On the top right of the screen, you can click the help button to open the CMS knowledge base in a new tab. You can search for the information you need or browse the help guide using the left hand menu. In addition to the CMS support information, you can download further SmartWall® documentation PDFs.

5. Account settings

On the top far right of the screen, you can see your account name. Click this to display a drop-down with two options:

- **Change Password** – Enables you to change your user account password
- **Log Out** – Logs you out of the CMS

Managing the TDD System

This section provides the following information:

Viewing System Status

You can see an overview of your system in the SWA application. If you identify any issues, you may need to use a combination of the SWA analytics engine and CMS configuration management application to resolve them.

To view system status

1. Open the SWA application in a browser where x.x.x.x is the management IP address of the SWA: *https://x.x.x.x:8000*
2. Navigate to the **Overview** screen.
3. Use the following charts to check the status of you system:
    - **Mitigation** – This chart, on the top left of the screen, should display "Enabled". If it is showing anything else there is a problem with your TDD system. Hover over the text to see more information then see Troubleshooting for steps to correct the issue.
    - **Telemetry** – View a chart of the Blocked and Allowed traffic from the selected timeframe (default 60 minutes). Indications that you may have a mitigation issue:
        - A spike of blocked traffic (red) represents a successfully blocked attack. If you see a spike of allowed traffic (green), your defense Policy may be missing a specific type of attack.
        - If you see an unexpected drop in the allowed traffic (green), your defense Policy may be too aggressive.

Investigating mitigation issues

1. You first need to identify the type of traffic which isn't being handled correctly. You can use the Analytics information in the SWA application to identify a type of traffic.
2. Once you know the type of traffic you need to block/allow, open the CMS in a browser.
3. Using the CMS, from the left-hand menu open the **Policy** section. This contains all the configuration settings for your defense Policy. Refer to the built in CMS help (using the help icon in the top right) to find the correct configuration area for your traffic type.
4. **Commit** the change.
5. If the attack is still on going, you should see the change reflected in the SWA Overview screen.

Viewing the Filters Sent to the Router

Once configured, the TDD system sends instructions to your routers to block DDoS attack traffic. This is done by creating temporary firewall filters on the router.

To view filters sent to the router from the TDD

1. Open the SWA Web UI in a browser.
2. On the **Overview** screen, and optionally change the timeframe to the one required.
3. View the **Mitigations** chart:
    - The table shows all mitigations sent in the timeframe
    - The **Termname** column shows the unique termname for this attack. On the router, you can use the command `show firewall` to see a list of the filters currently applied. You will see matching termnames to the ones shown in this table for the current period.
    - The **Filter Info** column shows what traffic that filter will block. If it contains a Corero rule number (e.g. cns-002053), you can use this to view the defense Policy settings (in the CMS) which caused the filter to be applied.

Adjusting the Traffic Sample Rate

When you configured the Juniper Networks MX Series router (see **SmartWall TDD Getting Started Guide**), you set up Port Mirroring to send a copy of some of your traffic to the vNTD. If you need to adjust this sample rate, now the system has been running a while, you can follow the instructions below.

> **Note:** The Port-Mirror Sample Rate 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)

Prerequisites

- The vNTD device which monitors traffic for the TDD system must be in a Cluster.

To configure the Port-Mirroring Sample Rate on the Juniper Networks MX Series router

1. Open the MX router CLI using an SSH client: `ssh <username>@<ipaddress>`
2. Enter your password to log in.
3. Enter configuration mode: `configure`
4. Enter the command: `set forwarding-options port-mirroring input rate <sampleRate>`
5. You must commit the change, enter the following command: `commit`
6. Exit configuration mode: `exit`

To configure the Ingress Sample Rate for a Cluster

1. Open the CMS Web UI in a browser.
2. Use the left-hand menu to navigate to **Network** > **Clusters**.
3. From the table, locate the Cluster containing your TDD vNTD and click  the edit button.
4. In the **Ingress Sample Rate** field, type the same value which is configured as the Port-Mirroring Sample Rate on your router.
5. Click **Save**.
6. If you want to save the new configuration, and push your changes to any affected Defense devices now, click 

. Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

To adjust the Inbound Sample Rate between the vNTD and the CMS

The Port-Mirror Sample Rate you configured on the router (and the Ingress Sample rate you configure on the Cluster) controls how many samples are sent from the router to the vNTD. In addition to this, you may need to adjust the rate of samples sent from the vNTD to the CMS. When you installed the TDD system, you modified the Inbound Sample Rate to use one of the TDD default rates. If you find you're not seeing enough samples in the SWA, you may need to adjust these rates.

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 

. 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.

Corresponding CLI commands

```
configure
edit clusters cluster <clusterName>
set clusters cluster default ingress-sample-rate <rateFactor>
set devices advanced-settings sflow inbound sample-rate <sampleRate>
commit
exit
```

Manually Modify or Remove Mitigations

The TDD is able to automatically detect and mitigate attacks. If you need to apply mitigations manually or remove mitigations quickly, you can use the Actions and CIDR Policy screens in the Mitigation sub-menu.

To manage active mitigations

You can use the Actions screen to remove or modify mitigations currently active on your remote devices.

> **Note:** The actions table enables you to see all active and ended mitigations for the selected timeframe. The default timeframe is 60 minutes. You can modify this by clicking **Show Filters** and selecting a different timeframe. Mitigations which were active during that timeframe will show as ended and cannot be modified now.

1. Open the SWA in a browser and log in.
2. Use the top menu to navigate to **Mitigation** > **Actions**.
3. At the table, you can see the mitigations currently active on your TDD system.
4. (Optional) You can use the options at the top of the table to view only mitigations currently **Active with Traffic**.
5. Click on the row showing the mitigation you want to modify. Possible actions for this mitigation will appear below the table.
6. You can complete the following actions:
    - **Remove** – Click this button to remove the active mitigation from all devices it is currently active on.
    - **Change Action** – (Not available for FlowSpec mitigations) Click this button to change the current action of this mitigation. Select **Block** to discard the specified traffic, or select **Detect** to report on the specified traffic but allow it through the router.

> **Caution:** The Operating Mode of your CMS affects how actions operate. If the CMS is in Mitigate, the actions work as described above. However, if the CMS has been put into Monitor, the block action will not mitigate the traffic.

To modify mitigations for specific customers

You can use the CIDR Policy screen to modify how traffic is handled for specified Destination CIDRs in your protected network. You can modify how all traffic going to that CIDR is handled, or choose specific rules which should be handled differently to the default defense policy.

1. Open the SWA in a browser and log in.
2. Use the top menu to navigate to **Mitigation** > **CIDR Policy**.
3. Click **New entry**.
4. Type the destination **CIDR** you want to modify traffic for (e.g. 192.168.1.0/24)

5. In the **Rule** field, select **all** to modify how all traffic going to that CIDR is handled or select a specific rule you want to modify for this CIDR.

   Note: You can create multiple entries for each CIDR if you want to modify more than one rule. If you use an entry to set **all** rules for a CIDR, you can use additional entries to override that action for specific rules.

6. Select the **Action** you want the TDD to now use for your selected rule. For some actions, you must also add an **Action Parameter**.
   - **block** – The router blocks matching traffic. No Action Parameter required.
   - **detect** – The router reports on matching traffic but puts an accept entry on. No Action Parameter required.
   - **policer** – For matching traffic, the router performs the rate limiting action defined by the specified policer configured on the router. The Action Parameter must be the name of the policer you want to use for this rule, e.g. *smartRulePolicer*.
   - **redirect** – For matching traffic, the router redirects the traffic according to the specified redirect configured on the router. The Action Parameter must be the IP address of the next hop you want to use for traffic matching this rule.
   - **disabled** – The router does not act on matching traffic and does not report it. No Action Parameter required.
   - **ignore** – The router reports on matching traffic but does not put any tags on the traffic. No Action Parameter required.
7. Click **Save**.

Configuring Policers and Redirects on a Juniper Networks MX Series router

Before you can use the policer or redirect Actions, you need corresponding configuration on the associated routers. First you need to log into the Juniper Networks MX Series router CLI using an SSH client: `ssh <username>@<ipaddress>`

Then use the following commands to create a new policer using packets per second:

```
set firewall policer <policer-name> if-exceeding-pps pps-limit <packets-per-second>
set firewall policer <policer-name> if-exceeding-pps packet-burst <packets>
set firewall policer <policer-name> then discard
commit
```

Or use the following commands to create a new policer using bits per second:

```
set firewall policer <policer-name> if-exceeding bandwidth-limit <bits-per-second>
set firewall policer <policer-name> if-exceeding burst-size-limit <bytes>
```

```
set firewall policer <policer-name> then discard
commit
```

> **Tip:** To delete a policer, use the following commands:
> ```
> delete firewall policer <policer-name>
> commit
> ```

To create a new redirect, use the following commands:

```
set firewall filter <filter name> term <term name> then next-ip <ip-address>
commit
```

Example: Configure a customer who only has mitigations applied manually by an operator

If you have a customer who has requested manual mitigations only, you can use the TDD to only detect (and not block) traffic going to their protected IPs. You can then change the mitigation action from detect to block when requested by the customer.

Configure the TDD to not block attack traffic heading to a customer's DIPs:

1. Open the SWA in a browser and log in.
2. Use the top menu to navigate to **Mitigation** > **CIDR Policy**.
3. Click **New entry**.
4. Type the destination **CIDR** you want to modify traffic for (e.g. 192.168.1.0/24)
5. In the **Rule** field, select **all**.
6. In the **Action** action field, select detect. Leave Action Parameter empty.
7. Click **Save**.

When the customer contacts you to manage an attack:

1. Open the SWA in a browser and log in.
2. Use the top menu to navigate to **Mitigation** > **Actions**.
3. At the table, find that customer's current attacks. The Corero Action column will show Detect.
4. Click on the row showing the mitigation you want to modify. Possible actions for this mitigation will appear below the table.
5. Click **Change Action** and select **Block** to begin blocking that attack traffic.

Mitigating New Attack Types with the Flexible Configuration Tool

The TDD Flexible Configuration Dashboard allows the user to add, review or remove filter terms to the TDD system, inclusive of the end routers. This provides a highly granular method of traffic filtering and monitoring. The dashboard can be used to whitelist, block or detect traffic.

The tool is targeted to emergency situations where a user wishes to perform an action to a very specific traffic flow.

> **Caution:** Compiled filter terms are applied regardless of the Operational Mode of the TDD solution. If the TDD solution is set to Monitor, and the compiled filter term has an action of block, then the filter term will be added in a block disposition, NOT in Monitor.

Usage Guidelines

> **Caution:** Filter Terms can impact legitimate traffic.

- Only trained operators should use this feature.
- You must be sure of the potential impact of any Filter Term, before it is applied.
- This tool cannot determine if a compiled Filter Term will block legitimate traffic when applied.
- Configuration of Flexible Filter Terms must be configured and removed only via the TDD Flexible Configuration Tool and NOT directly in the CMS. If you try to configure the same rule using the CMS controls, it will result in no configuration being applied to the router.

If in doubt, or for further details, please contact your Support representative.

Prerequisites

For the TDD Flexible Configuration tool to operate, the following requirements must be met:

- TDD Version 9.7.0 and SWA OS Version 7.2.1
- The TDD system must be fully operational, either in Monitor or Mitigate mode.
- Remote Devices – On the SWA, on the Remote Devices screen (**Mitigation** > **Remote** Devices), the CMS and all protected routers must be added to the remote devices table. Confirm that the type field for the CMS is set to **CMS** and for the routers the type is set to **MX**. You must make sure all table entries have device credentials stored and that the Name of each entry is the device's hostname.
- Real-Time Juniper 3 – On the SWA, on the **Alerts** screen, select **Edit Alert** on the Real-Time Juniper 3 alert. Confirm the alert is enabled, and under **Trigger Actions** > **Corero Autonomic Response**, you can see the names of all your protected routers.

- CMS Configuration – Confirm that the CMS has the necessary Flex-Rule configuration. Navigate to **Policy** >**Flex-Rules** and identify the following rules:
  - **cns-002611** set to **egress**
  - **cns-002612** set to **block**
  - **cns-002613** set to **detect**

> **Caution:** The Flex-Rules must not be adjusted in the CMS at any time, or the tool will no longer function correctly.

To create a new filter term

> **Note:** When typing a value into fields on this screen, you must click enter after the value for it to be accepted.

1. Open the SWA Web UI and log in.
2. Navigate to **Dashboards** > **Flexible Configuration Tool**.
3. Select the **Action** for this filter term:
   - **Whitelist** – Matching traffic is allowed through by the routers
   - **Block** – Matching traffic is blocked by the routers
   - **Detect** – Matching traffic is reported but allowed through by the routers
4. Enter a **Destination Host or CIDR**. Only one Destination can be specified per filter term. The Destination can be entered as an IPv4 host IP or an IPv4 CIDR such as 1.1.1.0/24, 1.0.0.0/8, 1.0.0.0/28 etc.

   > **Note:** Network address validation is not performed until the filter term is added to the routers. Invalid network address specification is rejected by the CMS on application, resulting in an error, and the filter term will not be applied to the router.

5. Select a **Protocol** from the drop-down options **IP** (default), **TCP**, **UDP** or **ICMP**, alternatively type in an IP protocol number. The protocol you select will change what filter options are displayed.
6. To specify the type of traffic you want to affect, add any of the optional filter terms you require. Once a term is selected, the green Term Display Bar will update, adding or adjusting the filter terms to reflect the new selection.

Area	Term	Description
IP Selectors (Available for IP, TCP, UDP, ICMP, or custom protocol numbers)	**Source Host or CIDR**	Multiple source hosts or CIDRs can be specified per filter term. In the current release only IPv4 is supported. The source can be entered as a host IP or a CIDR such as 1.1.1.0/24, 1.0.0.0/8, 1.0.0.0/28 etc. Add one entry at a time, recommended up to 3 values.
	IP Packet Length	This field corresponds to the value set in the IP Header as IP Packet Length. Multiple IP packet lengths can be specified per filter term. Add one entry at a time, recommended up to 3 values.
	Fragments	Use the drop-down values only. Options available: • **First Fragment** – Only the first fragment • **Fragment** – All fragments
	TTL	Multiple TTL values can be specified per filter term. Values can be single TTL values, or the two options available in the drop-down; <65 or >199, or a combination of both. Add one entry at a time, recommended up to 3 values.
UDP Selectors (Only available for **UDP**)	**Source Port**	Multiple source ports can be specified per filter term. Add one entry at a time, recommended up to 3 values. Valid entries are 0-65535.
	Destination Port	Multiple destination ports can be specified per filter term. Add one entry at a time, recommended up to 3 values. Valid entries are 0-65535.
	Other UDP Selectors	From the **Other UDP Selectors** field, you can set one of the following: • **UDP Length** – One UDP packet length can be specified (as a decimal value), per filter term. This field corresponds to the value set in the UDP Header as UDP Length. • **UDP Check Sum** – One UDP checksum value can be specified (as a hex value), per filter term. This field corresponds to the value set in the UDP Header as UDP Checksum. • **UDP Data 1st/2nd/3rd/4th 4 Bytes** – One UDP Payload Data value can be specified (as a hex value), per filter term. This must be up to the first 20 bytes of the payload and must be specified as 4 bytes. Select the 1st/2nd/3rd or 4th dependent on the position to be specified. For example, if the payload to be added to the filter term starts with "ffffffff", then select "UDP Data 1st 4 Bytes".

Area	Term	Description
TCP Selectors (Only available for **TCP**)	**Source Port**	Multiple source ports can be specified per filter term. Add one entry at a time, recommended up to 3 values. Valid entries are 0-65535.
	Destination Port	Multiple destination ports can be specified per filter term. Add one entry at a time, recommended up to 3 values. Valid entries are 0-65535.
	TCP Flags	Filter term TCP flags values can be specified by selecting the appropriate radio buttons: • **Set** – The packet must have the specified flag set to be caught be the filter term • **Not Set** – The packet must not have the specified flag set to be caught by the filter term • **Undefined** – The filter term is not concerned whether the flag is or is not set **Note:** When Specifying values of "Set" or "Not Set" for the **ECE** or **CWR** TCP Flags, it will not be possible to specify further options normally present in the **Other TCP Selectors** drop-down.

Area	Term	Description
	Other TCP Selectors	From the **Other TCP Selectors** field, you can set one of the following: • **TCP Sequence Number** – One TCP sequence number can be specified (as a decimal value), per filter term. • **TCP ACK Number** – One TCP acknowledgment number can be specified (as a decimal value), per filter term. • **TCP Header Length** – One TCP header length can be specified (as a decimal value in bytes), per filter term. This field corresponds to the value set in the packet's TCP header length field. Valid lengths are from 20 to 60, in multiples of 4. • **TCP Window Size** – One TCP window size can be specified (as a decimal value), per filter term. This field corresponds to the value set in the packet's TCP header window size field. • **TCP Checksum** – One TCP checksum can be specified (as a hex value), per filter term. This field corresponds to the value set in the packet's TCP header checksum field. • **TCP Urgent Pointe**r – One TCP urgent pointer value can be specified (as a decimal value), per filter term. This field corresponds to the value set in the packet's TCP header urgent pointer field. • **TCP Options/Data** – One TCP data/option value can be specified (hex value), per filter term. This must be specified as 4bytes, after a 20byte TCP header and could therefore be either TCP options or TCP data payload, dependent on the TCP header length.

Note: If any term entries are not formatted correctly (such as use of alphanumeric characters, or "1.0" for example), then "Invalid Entry" will be displayed and you must re-enter the term.

7. Once you're happy with the new filter term, click **Add**.
8. In the confirmation panel, click **Add**. The Processing message now appears. Once the configuration has been applied to the routers, a Confirmation message will appear. If the configuration has not been successfully applied to one or more routers, then an Error message will appear, pointing to the issue.
9. Click **Close** to exit the dialog and return to the Flexible Configuration Tool.

To view and remove applied filter terms

1. Open the SWA Web UI and log in.
2. Navigate to **Dashboards** > **Flexible Configuration Tool**.
3. At the bottom of the screen, click **Review/Remove**.
4. You can view all applied filter terms in the table. The following information is available for each term:
    - **Action** – Displays the action this filter performs on matching traffic: whitelist, block, or detect
    - **Name** – Displays the filter term name as it appears in the router
    - **Definition** – Displays the filter definition in BPF format
    - **Admin State** – Displays the current admin state of this filter term: enabled or disabled
5. If you need to remove a filter term:
    a. Click on the row containing the required filter term.
    b. Click **Remove** on the confirmation panel. The Processing message now appears. Once the configuration has been applied to the routers, a Confirmation message will appear. If the configuration has not been successfully applied to one or more routers, then an Error message will appear, pointing to the issue.
    c. Click **Close** to exit the dialog.
6. Click **Close** under the table to return to the Flexible Configuration Tool.

Tuning your Defense Policy

For information on tuning your policy, contact your support representative or access the built in help information available in the SWA and CMS Web UIs:

To open the SWA built in help

1. Open the SWA Web UI in a browser and log in.
2. On the top menu, click **Help**.

To open the CMS built in help

1. Open the CMS Web UI in a browser and log in.
2. On the top menu, click  the help button.

Viewing the SSRN Value for your TDD System

Your SmartWall TDD deployment has a unique Service and Support Reference Number (SSRN). You need this number when contacting Juniper about the TDD.

To view the SSRN

1. Open the SWA application in a browser where x.x.x.x is the management IP address of the SWA: *https://x.x.x.x:8000*
2. Navigate to the **System**>**Health** screen.
3. You can see your SSRN in the **TDD License Info** table.

> **Tip:** The SSRN is associated with the vNTD license you received as part of the TDD system. Once you upload your license, you can also view it in the CMS on the Licensing screen (**System** > **Licensing**) and on the **Home Screen** (at the top next to the CMS application information).

Managing Remote Device Credentials and Telemetry Types

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 Device. You can use the Remote Devices Screen (Mitigation > Remote Devices) in the SWA to manage the Remote Devices, remove a router, or add a new router. You must also store your CMS credentials in this table to enable the SWA to communicate mitigation changes to the CMS.

Stored credentials

The SWA needs credentials to access the CMS and every router in your TDD deployment. The credentials you give the SWA to access your Remote Devices must have the necessary permissions:

- **CMS** – You need the credentials for an admin account on the CMS
- **Router** – You need credentials for an account with permission to add and remove filters. For routers, you can choose to store a password for the account or a private SSH Key associated with that username.

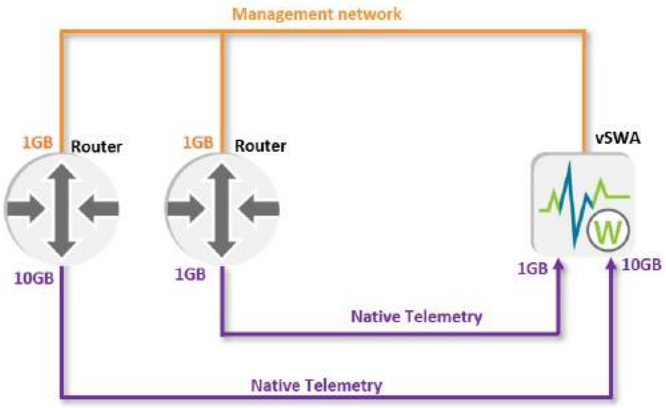
Telemetry types

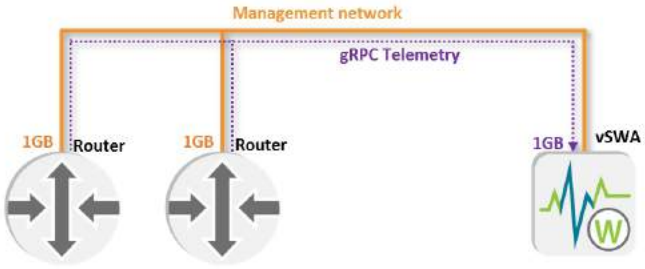
The TDD requires a telemetry feed from every monitored router to the SWA application. There are two main telemetry delivery methods:

- **Native telemetry** (UDP) – Telemetry is sent over your traffic network between the router and SWA. This requires a dedicated 10GB port on the router and a 10GB, or 1GB, port on the SWA host.
- **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.

You decided which telemetry type is used when you configure the Juniper Networks MX Series router (See SmartWall TDD Getting Started Guide for instructions). 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.


Management network
1GB
Router
1GB
Router
vSWA
10GB
1GB
1GB
10GB
Native Telemetry
Native Telemetry


Management network
gRPC Telemetry
1GB
Router
1GB
Router
1GB
vSWA

To add a router to the SWA

1. Open the SWA web UI and log in.
2. Add the router information to the Remote Devices table:
    a. Use the top menu to navigate to **Mitigation** > **Remote Devices**.
    b. At the table, click **Add Device**.
    c. In the **Name** field type the hostname for this router. The host name is configured on your router and must match what you enter here exactly. You must only use alphanumerics, spaces, or .-&()_/@:= symbols.
    d. In the **Address** field, type the IPv4 address of the router or the router hostname.
    e. (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 (See Getting Started Guide for instructions on **Configuring the Juniper Networks MX Series router**).
    f. In the **Type** field, type: **MX**. **Caution:** You must use uppercase for both letters or it will not be recognized.
    g. (Optional) Type a **Description** of the router.
    h. Enter a **Username** for a user account with permission to configure the router.
    i. 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-----').
    j. (Optional) 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:
            a. Upload a **gRPC SSL Certificate Authority** using the **Choose File** button to select a certificate from your computer.
            b. 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.
    k. Click **Save**.

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

3. Enable TDD mitigations to the new router:
    a. Use the top menu to navigate to **Alerts**.
    b. At the table, locate **Real-Time Juniper 3**.
    c. In the Action column click **Edit**.
    d. Select **Edit Alert**.
    e. Under Trigger Actions, expand **Corero Autonomic Response**.
    f. 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 Devices table.
    g. Click **Save**.

To add CMS credentials to the SWA

1. Open the SWA web UI and log in.
2. Use the top menu to navigate to **Mitigation** > **Remote Devices**.
3. At the table, click **Add Device**.
4. Type the **Name** for your CMS. You must only use alphanumerics, 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**.

> **Tip:** On the table, you can use the action options to **Edit** or **Delete** your CMS credentials.

Managing SWA Users

When you install the SWA, you will have one admin user account and one monitor. You can create more user accounts, either locally or by mapping to an external LDAP server.

User roles

There are two standard user roles available for the SWA. The role you have, affects what you can do in the SWA:

- **swa-admin** – The administrative role. An admin user can edit all SWA configurations, including managing users, editing charts, and performing system level actions. The default user credentials are admin/smartwall.
- **swa-monitor** – A primarily read-only role which enables its users to view charts without being able to enact any changes to the main dashboards. A monitor user can interact with existing charts, search syslog messages, create new dashboards, perform GETs on the REST API, and manage their own password. The default user credentials are monitor/smartwall.

Types of user authentication

There are three types of user authentication available on the SWA. If you enable an external authentication feature (LDAP or RADIUS), this becomes the primary authentication system over local authentication:

- **Local Authentication** – Admin users can create and manage local SWA user accounts using the SWA Web UI
- **RADIUS** – Admin users can configure the SWA to enable users to log in using their existing organization credentials by connecting to your organization's authentication server over RADIUS
- **LDAP** – Admin users can configure the SWA to enable users to log in using their existing organization credentials by connecting to your organization's authentication server over LDAP

> **Note:** When you use LDAP or RADIUS authentication, you cannot edit external user details or manage those user passwords from within the SWA. Also, LDAP and RADIUS admin users cannot use their external credentials to access the SWA pCLI.

IP Filters

You can filter which IP addresses are permitted to access the application over the management interface. After you enable IP filtering, you can manage a list of permitted IP addresses. For the SWA, you can manage this list in the pCLI.

Support login

The support account is another type of user account with high level system access. You have one set of support credentials but, if you require assistance from customer support, you can enable access to that account by creating a support token using the pCLI.

pCLI Commands

`support-account status` – View the current Corero support account status.

`support-account enable` *<token>* – Enable the Corero support account. Optionally, you can supply the token used to access the account. To generate a random token, leave blank. No confirmation is shown unless it is already disabled; then you will see an error.

`support-account disable` – Disable the Corero support account. No confirmation is shown unless it is already disabled; then you will see an error.

Managing Local SWA Users

In the SWA application, you can create and delete user accounts and manage passwords. If you need to change your admin user's username, you must use the pCLI.

To create a new local user

1. Open the SWA application in a browser.
2. Navigate to **System** >**User Management**.
3. Click **Create User**.
4. Type a **Username**
5. Select a **Role** from the drop-down:
    - **swa-admin** – The administrative role. An admin user can edit all SWA configurations, including managing users.
    - **swa-monitor** – A primarily read-only role which enables its users to view charts without being able to enact any changes.
6. Type a **Password** and **Confirm password** for this user.
7. Click **Save**.

> **Tip:** You can delete any local user from the table except for your own account. There must always be one user account active.

To change password for local user

1. Open the SWA application in a browser.
2. Navigate to **System** >**User Management**.
3. Find the user in the table and click **Change Password**.
4. Type a new **Password** and **Confirm password** for this user.
5. Click **Save**.

To change your own password

> **Note:** Changing your own password will cause SWA to log you out. Log back in with the new password.

1. Open the SWA application in a browser.
2. On the top menu, click your user name and select **Change Password**.
3. Type a new **Password** and **Confirm password**.
4. Click **Save new password**.

To change the admin user's username

> **Caution:** Changing the Admin user's username or password will delete all local users created in the application. You can change the Admin user's password using the GUI without affecting the other accounts.

1. Access the SWA pCLI:
   - Using a terminal emulator (e.g. Putty) and an SSH connection, use the following command: `ssh -p 2222 <adminUser>@<deviceIP>`
   - For virtual editions, you can also access the pCLI by opening the console window.
2. Log in with the corresponding password for your admin user credentials. The default username/password is admin/smartwall.
3. Enter the command: `setup aaa`
4. Use the wizard to change the admin credentials.
5. Log in to the SWA application in your browser using the new credentials.

Managing LDAP SWA Users

There are three main steps to enable LDAP and connect an LDAP server to the SWA:

- Enable LDAP authentication
- Configure the LDAP bind account details and attributes which the SWA will use to log in to the LDAP server and attempt to look up user details.
- Add the connection details for your LDAP server(s) to the LDAP Servers list.
- Create a mapping of LDAP groups to the user roles on the SWA. This controls what level of access different users on the LDAP server will receive on successful login to the SWA.

To enable and configure LDAP authentication using the Web UI

1. Open the SWA application in a browser.
2. Navigate to **System** >**Settings** >**LDAP**.
3. Select **Enable LDAP authentication**.

4. Add **LDAP Servers**:
    a. Type the IP address of the **Primary LDAP** server.
    b. (Optional) Type the IP address of the **Secondary LDAP** server.
    c. For an LDAPS connection type, choose to **Enable SSL**. To use LDAP connection type, leave the box unchecked.
    d. Enter the **LDAP port** for your configured LDAP servers. The default port for LDAP is **389**, and for LDAPS is **636**.
5. Enter **Bind Credentials** to enable the SWA to log into the LDAP server:
    a. Type in a **Bind DN** (Bind Distinguished Name) for a set of credentials which has read access to the user store.
    b. Type in the **Bind Password** for that Bind DN.
6. Enter **User Settings** to identify users within the user store:
    a. **User Base DN** – The Base DN used to locate user information in the LDAP schema.
    b. **User Search Filter** – Optional filter to restrict user search results to a specific object class.
    c. **User Name Attribute** – The LDAP attribute which contains the user's username (e.g. **sAMAccountName**).
    d. **Real Name Attribute** – The LDAP attribute which contains the user's real name (e.g. **cn**) .
    e. **Email Attribute** – The LDAP attribute which contains the user's email address (e.g. **mail**) .
    f. **Group Mapping Attribute** – The LDAP attribute which references a group member (e.g. **dn**) .
7. Enter **Group Settings** to identify groups within the user store:
    a. **Group Base DN** – The Base DN used to locate group information in the LDAP schema.
    b. **Group Search Filter** – Optional filter to restrict group search results to a specific object class.
    c. **Group Name Attribute** – The LDAP attribute which contains the group's name (e.g. **cn**) .
    d. **Group Member Attribute** – The LDAP attribute which contains a group member (e.g. **member**) .
    e. Choose to **Enable Nested Groups** or not.
8. Add **LDAP Group Mappings**. There are 2 SWA user roles you can map an LDAP group to (**swa-admin** and **swa-monitor**). User's in a mapped group will have the same permissions as their associated role. For each LDAP group you need to map:
    a. Click **Add mapping**.
    b. Type the **Group Common Name** of the LDAP group you want to map.
    c. Use the **Role** drop-down to select the SWA user role you want to map the LDAP group to.
    d. Click **Add**.
9. At the bottom right of the screen, click **Save**.

> **Note:** If a user is assigned to multiple LDAP groups, and those groups are mapped to different CMS user roles, the user is assigned the role with the highest level of access. For example, if a user was in an LDAP group mapped to cns-admin and one mapped to cns-defense, they would receive cns-admin access when they log in to the CMS.

Managing RADIUS SWA Users

There are three main steps to connect an RADIUS server to the SWA:

- Enable RADIUS authentication.
- Select a default role for all users. Use the Filter ID attribute to apply other SWA user roles to specific RADIUS groups.
- Add the connection details for an RADIUS server to the RADIUS Servers list. Optionally add a backup server.

To enable and configure RADIUS authentication using the Web UI

1. Open the SWA application in a browser.
2. Navigate to **System** >**Settings** >**RADIUS**.
3. Select **Enable RADIUS authentication**.
4. Add **RADIUS Servers**:
    a. (Optional) If you need to change the default **Host Identifier** (Splunk), you can edit it.
    b. Type a **RADIUS Server** name. If you're not using port 1812, include the port number (e.g. radius.acme.net:11812).
    c. Type the **RADIUS Server Shard Secret** used to communicate with this RADIUS server.
    d. Type a **Backup RADIUS Server** name. If you're not using port 1812, include the port number (e.g. radius.acme.net:11812).
    e. Type the **Backup RADIUS Server Shard Secret** used to communicate with the backup RADIUS server.
5. Configure the **Role Assignment** to provision a default user role for RADIUS authenticated users, then identify the attribute used to provision a user with a different role:
    a. Select the **Default Role** from the drop-down list. All RADIUS authenticated users will have this role unless they have an attribute ID set.
    b. (Optional) If you want to configure some users to have a different role from the default, type the **Vender Code** and **Attribute ID** for the Vendor Specific Attribute (VSA) containing the role. You'll need to configure which users have this attribute on your RADIUS server.
6. (Optional) Configure Test Settings to test the configuration before saving. If the test fails, you will be able to return and update the settings:
    a. Type a **Test Username** for a RADIUS authenticated user.
    b. Type the **Test Password** for that user account.
7. At the bottom right of the screen, click **Save**.

Managing IP Filters for SWA

To restrict access to the SWA, enable IP Filter management and create a list of permitted IP addresses.

To enable IP filtering and edit the IP filters list

1. Access the SWA pCLI:
    - Using a terminal emulator (e.g. Putty) and an SSH connection, use the following command: `ssh -p 2222 <adminUser>@<deviceIP>`
    - For virtual editions, you can also access the pCLI by opening the console window.
2. Log in with the corresponding password for your admin user credentials. The default username/password is admin/smartwall.
3. Enter the command: `setup ip-filter`
4. Use the wizard to enable IP filtering for this application and manage a list of permitted IP addresses who can access the application over the management interface. You can `[I]nsert` a new IP or `[D]elete` an existing IP.

Managing SWA Snapshots

A snapshot is a package which contains the SWA's configuration from the moment you created it. You can use this to restore the SWA configuration to a previous state. You may want to create snapshots periodically, or before you perform a large configuration change. The SWA can store up to 5 snapshots at a time.

> **Note:** Snapshots can only be restored onto a SWA application running the same SWA version number as the SWA where the snapshot was taken.

To create a snapshot

1. Use the top menu to navigate to **System** > **Snapshots**.
2. Click **Create**.
3. Type a **Name** for your new snapshot.
4. (Optional) Type a **Description** of the snapshot.
5. Click **Create**.

> **Tip:** On the Snapshots table, you can **Delete** snapshots you no longer need.

To restore SWA configuration from a snapshot

If you want to return to a previous SWA configuration, you can restore an earlier snapshot. Restoring a snapshot does not erase your later snapshots, enabling you to move between snapshots to investigate configuration changes.

1. Use the top menu to navigate to **System** > **Snapshots**.
2. From the table, locate the snapshot you want to restore and click **Restore**.

> **Caution:** Restoring a snapshot will cause the SWA to restart.

To export your saved configuration

You can export your snapshots to store externally or use with another SWA application. An exported snapshot is saved as a SecureWatch Snapshot Package file.

1. Use the left-hand menu to navigate to **System** > **Snapshots**.
2. From the table, locate the snapshot you want to export and click **Export**.
3. The snapshot package file is downloaded by your browser.

To import SWA configuration

You can import snapshots you have exported from other SWA applications or which you exported from this SWA to store externally. Once you import a snapshot, you can view it in your snapshot list and use it like any other.

1. Use the left-hand menu to navigate to **System** > **Snapshots**.
2. Click **Choose File** and select the SecureWatch Snapshot Package file on your computer and click **Open**.
3. Click **Import**.

Sending Alerts

> **Note:** The TDD system blocks attacks automatically and does not require you to manually edit configuration to block attacks. Alerts are available to enable you to observe the system and identify any areas for future improvements.

Alerts are essentially search queries which are run periodically. Any results in the query during that time period will trigger an action. There are many actions you could set up; the most common are sending an email and sending a Slack alert.

The SWA comes with a set of Alert Templates, which contain example content but can be cloned, and then edited, to create your own custom alerts.

Alert templates provided:

- Attack Detected
- Bandwidth Alert
- Blocked PPS Alert
- CMS Alert
- Test Alert

To clone and edit an Alert Template for Email or Slack alerts

1. In the SWA application, navigate to **System** > **Alerts**.
2. Next to the Alert Template you want to clone, click **Edit** >**Clone**.
3. Edit the clone alert details:
    a. Type a **New Title** and **New Description** for this alert.
    b. Set **Permissions** to **Clone**.
    c. Click **Clone Alert**.
    d. Click outside the confirmation dialog to return to the alerts table.

4. Edit the search query:
    a. Next to the new cloned alert, click **Open in Search**.
    b. In the search bar, you can see the current search query. For example, a Bandwidth Alert will show: `` `alert_LinkBW(test=50,warning=100,critical=500)` ``
    c. Edit the query as required. For example, the Bandwidth Alert query has bandwidth values in Mbs which trigger different alert emails when they're passed. You may want to adjust those values for your own network.
    d. When you're happy, press the **RETURN** key or click the search button (magnifying glass) to run the new query.
    e. On the top left of the screen, click **Save**. Then in the confirmation message, click **Save**.
    f. Click **View**.

    Note: If you plan to set up a Slack alert, make sure your search query contains a `text` field. Optionally, it can also include a `title` field, `channel` field, and `icon` field.

5. Return to the **Alerts** page, and edit the alert:
    a. Next to your new alert, click **Edit**.
    b. Click **Edit Alert**.
6. Set how often the Alert runs:
    a. **Realtime**
    b. **Scheduled**. Then decide how often the alert is scheduled to run (every hour, day, week, month or on a chron schedule).
7. (Optional) Configure an email alert:
    a. Click **+Add Actions**.
    b. Select **Send Email**.
    c. Under Trigger Actions, click **Send Email** to expand options.
    d. In the **To** field, type one or more email addresses which should receive the alert emails.
    e. Select a **Priority** for the message.
    f. Edit the email **Subject** and **Message** to provide the information you require.

    Note: Click **Learn More** (to the left) to see what replacing-text tokens are available. You can also use the **Include** check boxes to add additional information to your message.

8. (Optional) Configure a Slack alert:
    a. Click **+Add Actions**.
    b. Select **Corero Slack Message**.
    c. Under Trigger Actions, click **Corero Slack Message** to expand options.
    d. Type the URL of your Slack Incoming **Webhook**. **Note:** If you use the standard Incoming Webhook, SWA can overwrite the default channel, title, and icon. However, if you create your own Slack app and use the separate incoming webhooks created for each channel, SWA can only modify the text of the message.
    e. (Optional) Type the name of the Slack **Channel** you want this message to appear on. If you don't it will use the default channel from the webhook.
    f. (Optional) Type a **Title** for the Slack message generated by the alert.
    g. (Optional) Type the emoji code for a Slack **Icon** which will be used by the Slack message.
9. When you're happy, click **Save**. Then click, **Done**.
10. Enable the alert:
    a. Click **Edit**.
    b. Click **Enable**.

Other types of alerts

As well as adding Email and Slack alert triggers, alerts can perform other actions:

- Add a log event
- Run a script
- Send RTBH mitigations (requires a CMS configured as a BGP Client to be added as a Remote Device)
- Swing traffic to a scrubbing center

These actions require additional system changes and should be performed with the help of your support representative.

Importing SecureWatch Package Files

SecureWatch Package Files are the vehicle for importing information into the SWA application. There are 3 categories of SecureWatch Package:

- **Upgrade** – There are two parts of the application you can upgrade, both types of upgrade are performed by importing a SecureWatch package:
  - **Upgrade queries/autonomics** – This is the most common upgrade you'll do. The queries power the charts on all screens and dashboards, and autonomics controls how mitigations are sent to routers. Efficacy improvements and improved reporting are available through these upgrades without needing to upgrade the whole application.
  - **Upgrade application** – When a new version of the product is available, you can upgrade to receive the new features without losing any historic data.
- **SecureWatch License** – Enables the vSWA to check you are licensed to use the TDD system. You will have installed one when you first set up the TDD system.
- **SecureWatch Service** – Connects you to the SecureWatch Service over a secure VPN connection. This is an additional service which enables customer support engineers to monitor your mitigations and tune the system to improve response to attacks.

> **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.

Prerequisites for importing SecureWatch packages

- An upgrade should not be performed during an attack. On the **Overview** screen, check that the **Targets under attack** count shown is zero before starting.
- You should create a snapshot of the system before performing the upgrade.

To install the SecureWatch package using the SWA web UI

1. You will receive the SecureWatch package and unlock code from Customer Support (not all packages require unlock codes).
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 can cause the SWA application to restart and may take several minutes.

8. (Only if restart required) .pkg files always require a restart to complete, however for .tar.gz files, this may not be the case. If the application does need restarted, perform the following steps:
    a. If the restart is not automatic, you will be prompted to click **Restart**.
    b. Once SWA has restarted, log back in and return to **System** > **SecureWatch Packages**.
9. You should see the new packages details in the Packages table.

Setting up the TDD to accept FlowSpec Mitigations

Before you can use FlowSpec with the TDD, you must connect the CMS to your BGP client and add the CMS to the Remote Devices table as a FlowSpec device.

> **Note:** Once you configure the CMS BGP client, you can manage all FlowSpec routes using the CMS REST API. You do not need to use the FlowSpec Routes table in the CMS UI. For more information on the CMS REST API, see the CMS User Guide or the CMS help site (accessed from the help button on the CMS menu).

Prerequisites

You must have a BGP router on your network edge which can send FlowSpec instructions. The router must be accessible from the CMS over a TCP connection.

To configure the CMS BGP client for FlowSpec

1. Open the CMS in a browser and log in.
2. Use the left-hand menu to navigate to **Services** > **BGP Mitigation**.
3. Configure the connection to the BGP router:
    a. Select the **BGP CLIENT** tab.
    b. Change the **Admin State** to **enabled**.
    c. Type the **Router ID** IP address of your local BGP router. This router must be positioned to enable a TCP connection with the CMS.
    d. Type your **Local AS** for this router.

    > **Note:** The CMS only supports a 2-byte AS. It does not support a 4-byte AS.

    e. Add an entry for every neighbor (peer) of your local BGP router which may be contacted:
        i. In the Neighbors table, click **Add**.
        ii. Type the **Address** of the neighbor.
        iii. (Optional) If you don't want to use this neighbor yet, change the **Admin State** to **Disable**. Otherwise, leave as **Enable**.
        iv. Type the **Remote AS** of this neighbor.
        v. Type the **MD5 Password** to access this neighbor.
        vi. Click **Save**.
4. 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).

To add the CMS to the Remote Devices table as a FlowSpec device

> **Note:** You will already see an entry for the CMS in the Remote Devices table. That entry provides the CMS connection for regular TDD mitigations. To also use the CMS as a FlowSpec device, you must create a new entry for it. You will have two entries in the table for the CMS when you complete the method below.

1. Open the SWA 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 alphanumerics, spaces, or .-&()_/@:= symbols.
5. Type the IP **Address** (IPv4) of your CMS.
6. In the **Type** field, type: **FLOWSPEC**. **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**.

> **Tip:** On the table, you can use the action options to **Edit** or **Delete** your CMS FlowSpec entry.

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 scren. 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 Autonomics alert has the correct hostnames for the routers: **Alerts** > **Real-Time Juniper 3** >**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 recieving 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 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 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 data-store 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 then 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 virsh configuration.

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

1. Log into the server hosting your Corero VMs.
2. Use the following command for each VM, replacing `<vmName>` with the name of the VM: `virsh autostart <vmName>`

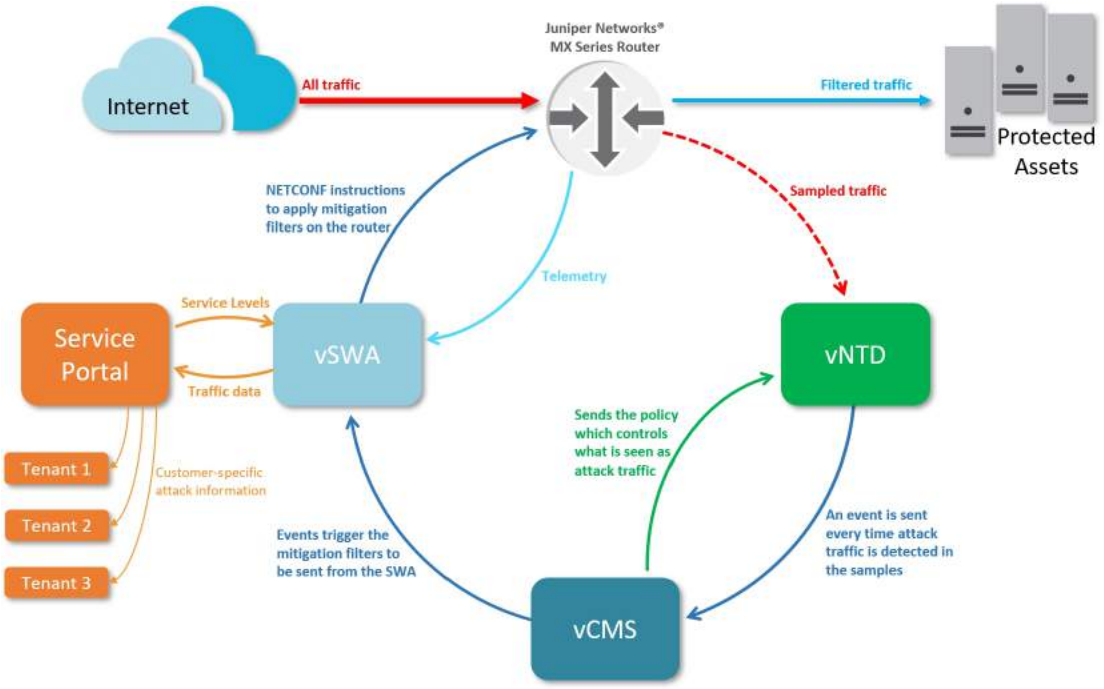
1. Open vSphere Web Client.
2. Select the host.
3. Open the **Configure** tab.
4. From the menu, under **Virtual Machines**, select **VM Startup/Shutdown**.
5. Click **EDIT**.
6. Check the box next to **Automatically start and stop the virtual machines with the system**.
7. Click **OK**.

SmartWall Service Portal

The SmartWall Service Portal is an optional component that enables you to offer Corero SmartWall DDoS Protection, as a managed service, to your customers. There is the option to use your own customer portal.

> **Note:** If you are using a different customer portal, rather than the SmartWall Service Portal, you must first push your own service levels into the SWA using the REST API and never sync the SWA with a Service Portal.

The SmartWall Service Portal uses sampled traffic data from your SmartWall TDD. It displays attack and traffic information in easy to read charts and reports. As the provider, you can view aggregate traffic data and analyze attacks across the whole network, which is protected by the SmartWall System, as well as viewing traffic data on a per-customer basis. Additionally, your customers are able to log into their own view of the Service Portal and see only the attack information that relates to their assets which you protect. This enables them to immediately see the benefit of the DDoS protection service both historically, and in real time.



The Service Portal and SWA have the additional flexibility to help you match how you decide to offer your DDoS protection-as-a-service to your customers. This is accomplished by the application of defined Service Levels that will automatically be applied to ensure the correct DDoS protection service is utilized, for the asset and customer being attacked. The Service Levels are set and controlled by you, at a level that is appropriate to the package you are offering.

Connecting a Service Portal to the TDD

To see your network's traffic information in the SmartWall Service Portal, you need to feed it traffic and attack data from your SWA application. If you're using the SWA to configure the rule actions for Service Levels on the Service Portal, you must also enable syncing between the Service Portal and the SWA.

Forward traffic from a 9.7.5 SWA

Prerequisites

You must have the following:

- A Service Portal running version 1.2 or later

To connect a 9.7.5 SWA application to a Service Portal

1. Open the SWA in a browser and log in.
2. Use the top menu to navigate to **System** > **Service Portal Configuration**.
3. To connect the SWA to a Service Portal and deliver the traffic and attack feed:
    a. Under **Enable Service Portal Feed**, click the grey slider. It will turn green to show the connection is enabled.
    b. Type in the **IP Address** of your Service Portal.
    c. The default **Syslog Port** is **5410**.
4. To enable syncing of Service Levels between the SWA and the Service Portal:
    a. Under **Enable SSP synchronization**, click the grey slider. It will turn green to show syncing is enabled.
    b. Type the **Username** for an MSP Administrator account in the Service Portal.
    c. Type the corresponding **Password** for that account.
    d. The default **REST API Port** is **443**.
    e. Enable the SWA to keep up to date with the Service Portal, by polling for changes every minute. Under **Enable Periodic Sync**, click the grey slider. It will turn green to show syncing is enabled.
5. Click **Save**.
6. (Optional) To immediately sync Service Levels to your SWA from the Service Portal, click **Sync Now**. You will see a message appear above the button to show how many changes were brought over.

Forward traffic and attack information from 9.7.0 and earlier SWA's

Prerequisites

Before you begin, you need an operational vSWA application, to which you have administrative access and an operational Service Portal.

You must know the following information:

- *<swaUsername>* – The username of the SWA administrative user account. You must also know the corresponding password. If you did not change the default SWA credentials after deployment, this will be admin/smartwall.
- *<swaIPaddress>* – The IP address of the SWA application.
- *<ServicePortalIP>* – The IP address of the Service Portal.

To configure a 9.7.0 or earlier vSWA application to forward data to the Service Portal

1. Open a console session to the vSWA and log in with the admin account. If you're using an ssh client, type the following command then when prompted enter your password: `ssh -p 2222 <swaUsername>@<swaIPaddress>`
2. Type the following command:
   `setup service-portal`
3. The setup wizard enables you to configure the connection to the Service Portal.The recommended commands are in italics; where there is no command, press the return key to accept the default value. You must also replace any placeholders with your system information:
   ```
   Please configure the Service Portal connection:
   Enable sending data to the Service Portal? <Y,[N]>: y
   Enter IP Address [None]: <ServicePortalIP>

   Enter Port [5410]:
   ```
4. Once you press the return key to accept the default port, you'll see a summary of the Service Portal configuration:
   ```
   Service Portal:
   State : Enabled
   IP Address : <ServicePortalIP>

   Port : 5410

   Enter [A]ccept, [C]hange, or [E]xit without saving [C]:
   ```
5. If you're happy, press the *A* key, or press the *C* key to change any of those details.
6. To confirm setup was successful, once the changes have been applied type the following command:
   `setup service-portal`

7. You will see the following, note that the **State** is now "Enabled":

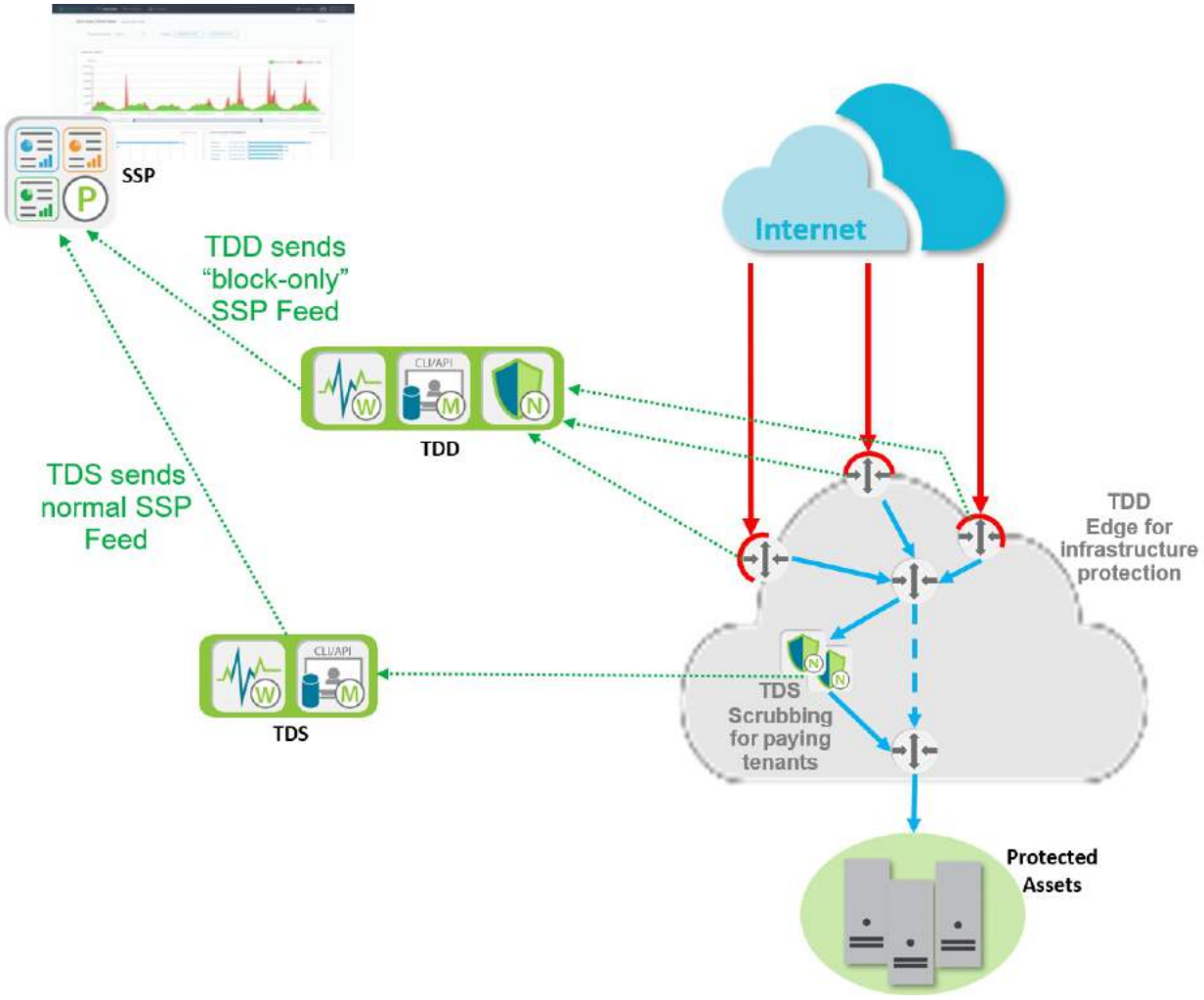
```
Please configure the Service Portal connection:
Enable sending data to the Service Portal? <[Y],N>: y

Service Portal:
State : Enabled

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

8. Press the *E* key to exit setup without changing anything.
9. Open the Service Portal in a browser (https://*<ServicePortalIP>*:8080) and check you can see traffic on the System Overview screen.

Managing your SmartWall TDD system with SmartWall TDS

SmartWall TDD delivers large scale DDoS protection at the edge of your network, and can be combined with SmartWall TDS for more fine-grained and sophisticated DDoS protection. This may be to provide a DDoS service where paying tenants can gain additional protection from SmartWall TDS, enhancing the SmartWall TDD protection provided for all.

When deployed in this way, both the SmartWall TDS and TDD systems may deliver traffic statistics to the SmartWall Service Portal (SSP). This could lead to traffic being counted more than once in the SSP.



To prevent this, disable the SmartWall TDD SecureWatch Analytics *report allowed traffic data* setting. This leaves the SmartWall TDS system enabled to report on the traffic that has been allowed to the protected assets.

The process to Enable or Disable this setting on each SWA is the same:

1. In a browser open the SWA UI.
2. Navigate to **System** > **Settings** > **Service Portal Integration**.
3. Ensure Enable Service Portal Feed is Green to enable the reporting of allowed traffic rates.
4. The **"Report allowed traffic data"** is enabled to report allowed traffic rates to the Service Portal on:
    - TDD only environment.
    - The TDS SWA in a TDD and TDS environment.
5. Click on **Save**.

Managing Service Levels for a Corero SmartWall Service Portal

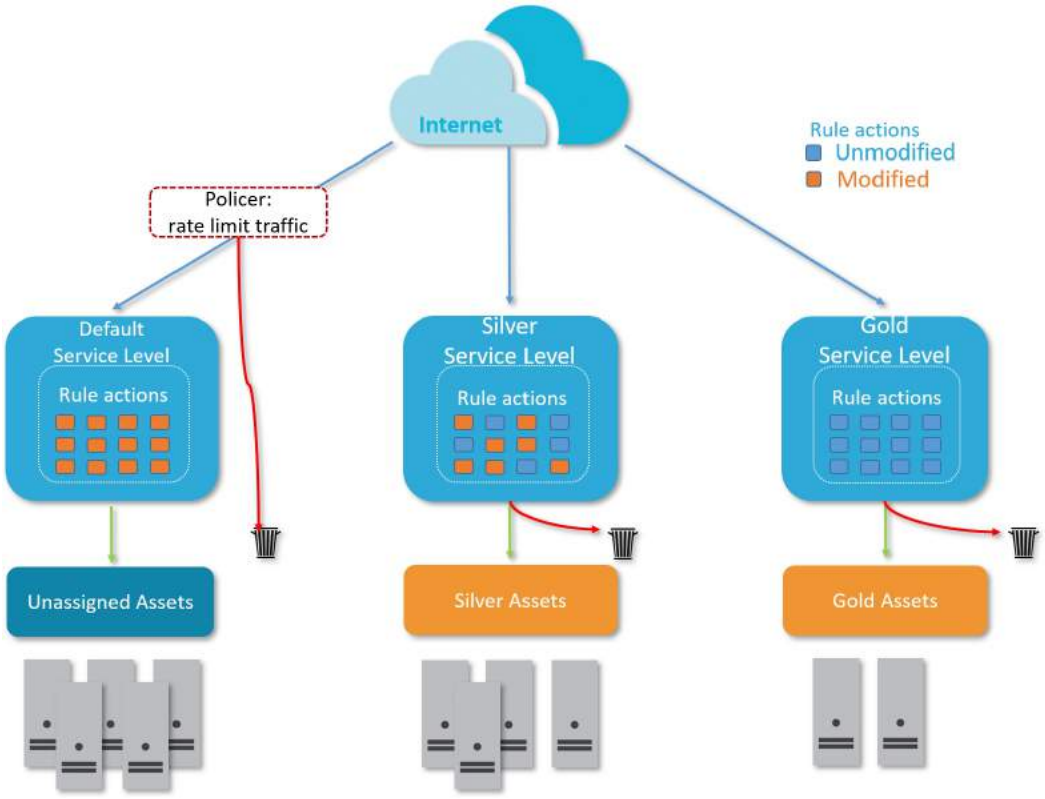
When providing DDoS protection the Service Portal has the flexibility to match how you decide to offer your DDoS protection-as-a-service, with automated blocking, reporting and alerting. This is applied through the use of Service Levels. You can create and configure multiple Service Levels in the Service Portal, each representing a customer of DDoS protection-as-a-service. It is recommended to keep the number of Service Levels and the use of manual mitigation to a minimum.

Each Tenant is assigned a Service Level which corresponds to their protection tier. Each Tenant has a list of assets (IP addresses) assigned to it. Traffic and detected attacks coming to the asset are handled as defined by the Service Level. Attack protection implemented by these Service Levels are managed by the SWA where you make modifications to the Service Level rule actions.

For example, the assets of a Tenant assigned to a higher tier service level may get all of the TDD Smart-Rules set to block attack traffic automatically. Assets of a Tenant on a lower tier may have TDD Smart-Rules set to only detect attack traffic.

Once you connect your Service Portal to the SWA and synchronize the Service Levels, you can import a list of the assigned assets and their Service Levels. The remaining unassigned assets in your network are handled by the Default Service Level.

> **Note:** CIDR Policy overrides are given priority over Service Levels.



Example of Modifying Rule Actions for Service Levels:

The following example setup assumes you have two Service Levels named "Silver and Gold" on your Service Portal. These are defined to offer different attack protection to two different tiers of tenants. Additionally on the SWA the Default Service Level will handle traffic for unassigned assets, not assigned to tenants in your Service Portal. Traffic to assets matching the Default Service Level will not be affected unless it exceeds an acceptable rate. At that point the Default Service Level will invoke a Policer already defined on the MX to prevent the traffic exceeding the rate limit.

- Unassigned – A default level policer named (*defaultLevelPolicer*) has already been set up in the router. The data is blocked when the limit set by the **Policer** has been reached.
- Silver – An asset on Silver gets all DDoS protections set to **block** except Smart-Rules which are set to **Detect**. When traffic crosses a Smart-Rules threshold you will be informed but the traffic will not be blocked. Adjustments need to be made and managed this is completed in the SWA under Mitigation>Service Levels>select the **Edit** option beside Silver. For every Smart-Rule change the action to **detect** and leave the Action Parameter field empty.
- Gold – An asset on Gold gets all DDoS protections, set to automatically **Block**. You do not need to make any adjustments to how the traffic coming to their assets is handled.

Prerequisites

You must have the following:

- A Service Portal running version 1.2 or later
- Your SWA must be connected to the Service Portal
- You must have the SWA configured to sync with the Service Portal. The previous topic, Connecting a Service Portal to the TDD, takes you through how and when to setup the configuration.

> **Note:** For full instructions on managing service levels and tenants in the Service Portal, see the SmartWall Service Portal User Guide.

To view your CIDR Service Level Policy in the SWA

The CIDR Service Level Policy is Read Only, and will show you all of your assets and the Service Level that has been applied to it.

1. Open the SWA in a browser and log in.
2. Use the top menu to navigate to **Mitigation** > **CIDR Service Level Policy**.
3. In the table, you can see the Service Levels pulled from your Service Portal and the Default Service Level. In the table, there is an entry for every CIDR you have configured as an Assigned Asset in the Service Portal. For each CIDR you can see the associated service level, and a description which includes the Tenant Name, the Assigned Asset CIDR, and the Assigned Asset Name (if there is one).

> **Note:** You cannot make modifications to the service level configuration on this screen. If you need to modify your service levels or the CIDRs associated with them, you use the Service Portal. Once you've made your changes, the updated configuration is pulled into the SWA on the next sync. You can use the **Sync Now** button in the SWA (**System** > **Service Portal Configuration**) to force the sync now.

To modify a Service Level's default rule actions

1. Open the SWA in a browser and log in.
2. Use the top menu to navigate to **Mitigation** > **Service Levels**.
3. You should see all of your Service Levels in the table. If you haven't modified a Service Level yet, it will contain the default rule actions for each configurable rule.
4. Click **Edit** next to the Service Level policy you want to modify.

5. For each rule, you can to choose to change the rule action from the **Action** drop-down, and if required add an **Action Parameter**:
    - **block** – The router blocks matching traffic. No Action Parameter required.
    - **detect** – The router reports on matching traffic but puts an accept entry on. No Action Parameter required.
    - **policer** – For matching traffic, the router performs the rate limiting action defined by the specified policer configured on the router. The Action Parameter must be the name of the policer from your router that you want to use for this rule, e.g. *defaultLevelPolicer*.
    - **redirect** – For matching traffic, the router redirects the traffic according to the specified redirect configured on the router. The Action Parameter must be the IP address of the next hop you want to use for traffic matching this rule.
6. When you've completed all the changes you require, click **Save**.

Using a different Customer Portal

If you choose to create your own customer portal, you can use the TDD REST API to populate the SWA UI with your custom service levels.

To push service levels into the SWA via REST API

1. Check the SWA is not connected to a Service Portal
    a. Open the SWA web UI and log in.
    b. Use the top menu to navigate to **System** > **Service Portal Configuration**.
    c. Make sure you do not have Service Portal sync enabled.
2. Use the REST API to push your service levels and associated CIDRs into the SWA using the `cidr-service-level-policy` endpoint. See the **SmartWall TDD REST API Guide** for full details of the request method format required.
3. Manage the rule actions modified for each service level:
    - Using the REST API endpoint `service-levels`. See the **SmartWall TDD REST API Guide** for full details of the request method format required.
    - Using the Web UI (**Mitigation** > **Service Levels**) using the same method required for a Service Portal integration.

Chart Reference

For reference information on the charts available in the SWA Web UI, view the built in help available in your SWA menu.

To open the SWA built in help

1. Open the SWA Web UI in a browser and log in.
2. On the top menu, click **Help**.

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://www.juniper.net/cm/

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://myjuniper.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