© Copyright 2020 Trend Micro.

Trend Micro Incorporated ("Trend Micro") makes no warranty of any kind about this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Trend Micro shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Trend Micro. The information is provided “as is” without warranty of any kind and is subject to change without notice. The only warranties for Trend Micro products and services are outlined in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Trend Micro shall not be liable for technical or editorial errors or omissions contained herein.
# Table Of Contents

1. Introduction ..............................................................................................................................6

2. System Architecture ...................................................................................................................6
   2.1. TSE Connection Table – Blocked Streams ........................................................................... 7
   2.2. TSE Connection Table Timeout ............................................................................................. 7
   2.3. TSE Asymmetric/Symmetric Mode ......................................................................................... 7
   2.4. TSE Adaptive Filtering ............................................................................................................. 8
   2.5. TSE Adaptive Aggregation ...................................................................................................... 9

3. Elements ...................................................................................................................................9
   3.1. Filtering Concepts .................................................................................................................... 9
   3.2. Filter Precedence ..................................................................................................................... 9
   3.3. Flow Inspection Filters ........................................................................................................... 10
   3.4. Trust as an Action Set ................................................................................................................ 10
   3.5. Traffic Management Filters .................................................................................................. 12
   3.6. Flow Management Filters ....................................................................................................... 13
   3.7. VLAN Translation .................................................................................................................... 13

4. Deployment Considerations ..................................................................................................... 14
   4.1. Deployment Guidelines ............................................................................................................. 14
   4.2. TPS Positioning ....................................................................................................................... 14
   4.3. Physical Connections ............................................................................................................. 14
   4.4. Cabling Requirements ............................................................................................................. 15
   4.5. Transparent High Availability (TRHA) .................................................................................... 15
   4.6. Stacking ................................................................................................................................ 16
   4.7. I/O Modules .......................................................................................................................... 19
      4.7.1. Standard Modules .............................................................................................................. 19
      4.7.2. Bypass Modules ................................................................................................................. 20
      4.7.3. General Module Information ............................................................................................... 22
      4.7.4. Module Hot-Swapping Guidelines ........................................................................................ 23
      4.7.5. What happens when modules are swapped? .................................................................... 24
      4.7.6. Fiber-Optic Connection ...................................................................................................... 25
   4.8. Intrusion Detection System (IDS) ............................................................................................. 26
   4.9. SSL Inspection ....................................................................................................................... 27

5. System Administration ............................................................................................................. 30
   5.1. How to turn off SMS Management of the device ................................................................. 30
   5.2. Management port .................................................................................................................. 30
   5.3. Reports available via the Local Security Manager (LSM) ..................................................... 31
5.4. Authentication Levels ............................................................................................................................... 32
5.5. How to Recover the TPS device SuperUser Password? ............................................................................ 33
5.6. How to Reset a TPS device to Factory Settings? ....................................................................................... 35
5.7. What are Inspection Bypass rules? ........................................................................................................... 36
5.8. System Upgrades ...................................................................................................................................... 36
5.9. Traces and Email Notifications ................................................................................................................. 36
5.10. Maximum Frame Sizes ............................................................................................................................ 36
5.11. TPS Storage Devices .................................................................................................................................. 37
5.12. Performance Protection ............................................................................................................................ 37
5.13. Link-Down Synchronization (LDS) ............................................................................................................. 38
5.15. TPS System Backup (Snapshot) ................................................................................................................ 39
5.16. Scan/Sweep Filters ................................................................................................................................... 40
5.17. Common Pitfalls ........................................................................................................................................ 41
5.18. TPS Throughput Licensing ......................................................................................................................... 42

6. Troubleshooting Commands ..................................................................................................... 43
6.1. show np tier-stats ..................................................................................................................................... 43
6.2. show np rule-stats .................................................................................................................................... 48
6.3. debug np congestionx ............................................................................................................................... 49
6.4. debug np regex show average .................................................................................................................. 50
6.5. debug np port show .................................................................................................................................. 51
6.6. debug np port diags <port#> .................................................................................................................... 52

LIST OF TABLES
Table 3-1: VLAN / Virtual Segments .............................................................................................................. 13
Table 4-1: TRHA Information ......................................................................................................................... 15
Table 4-2: Standard Modules .......................................................................................................................... 19
Table 4-3: Bypass Modules ............................................................................................................................. 20
Table 4-4: T/TX-Series TPS Approved Interfaces .............................................................................................. 25
Table 4-5: SSL Deployment Considerations .................................................................................................... 27
Table 5-1: Authentication Levels and Password Requirements ......................................................................... 32
Table 5-2: Do’s and Don’ts .............................................................................................................................. 41
Table 5-3: TPS Throughput Licensing ............................................................................................................ 42
LIST OF FIGURES

Figure 4-1: TX-Series 2-device resilient stack configuration ................................................................. 18
Figure 4-2: TX-Series 5-device resilient stack configuration ................................................................. 18
Figure 5-1: Intrinsic Network HA ........................................................................................................ 39
1. Introduction

This document provides guidance and background information on configuring, managing, and troubleshooting the TippingPoint Threat Protection System (TPS). The information contained in this guide is a compilation of best practices, questions, and scenarios that have been encountered in the field.

The Threat Protection System (TPS) family of devices includes the T-Series (440T, 2200T) TX-Series (1100TX, 5500TX, 8200TX, 8400TX) and vTPS.

The TPS functions as both a network and a security device. It must meet requirements from both disciplines:

- **Inline** - All traffic passes through the TPS making blocking possible and minimizing latency.
- **High availability** – the TPS must be very stable and continue to perform even under increased traffic volumes.
- **Accuracy** – the TPS must accurately detect attacks. It must be able to filter out just the attack traffic and leave innocuous traffic through without issue. Conversely, the TPS cannot have false negatives; otherwise, attacks will get through.
- **Usability** – The TPS must be simple to use and configure while providing the power and flexibility to satisfy a wide range of customer’s security posture needs.

To meet these high-level requirements, TippingPoint has implemented robust architecture consisting of both custom hardware and software elements. This section describes the architecture and essential functions and features implemented.

2. System Architecture

The TippingPoint TPS’s main component is the Threat Suppression Engine (TSE). The TSE deconstructs and inspects flow payloads at the application layer. As each new packet belonging to a flow arrives, the flow is evaluated for malicious content. The instant a flow is deemed malicious, the current packet and all subsequent packets pertaining to the flow are blocked. This ensures that the attack never reaches its destination.

Each flow is tracked in the “connection table” of the TPS. A flow is uniquely identified by the port on which it was received and its packet header information, referred to as the “flow-tuple”:

- IP protocol (ICMP, TCP, UDP, other)
- Source IP address
- Source ports (TCP or UDP)
- Destination IP address
- Destination ports (TCP or UDP)
- VLAN ID
Once classified, each packet is inspected by the appropriate set of protocol and application filters. The TPS filter engine combines pipelined and massively parallel processing hardware to perform simultaneous filter checks on each packet. The parallel filter processing ensures that the packet flow continues to move through the system with a bounded latency (on the order of microseconds) for the most part, independent of the number of filters that are applied. This hardware acceleration is critical in order to support massive amounts of filters without sacrificing performance.

2.1. TSE Connection Table – Blocked Streams

All packets received by the TPS are identified as a member of a flow (packet stream). A flow can consist of one or more packets. All packets received that are classified as a member of a “blocked stream” are discarded. Packets will only be blocked if they match a filter that has an action set of BLOCK.

2.2. TSE Connection Table Timeout

This global timer applies to all “blocked streams” in the TSE connection table, and designates the amount of time that must elapse after a flow is marked as “blocked” before it will be “unblocked.” While blocked, any incoming packets for that stream are discarded. After a flow is unblocked, the next packet for that flow is allowed but may be dropped, and the flow blocked again based on the TPS filters.

For normal operations in production environments, the TSE Connection Table Timer should be left at its default value (1800 seconds). However, for lab testing, this timer can be set to its minimum value (30 seconds) in order to make filter changes become more immediately apparent via seeing repetitive log updates from the same source IP address. Another way to immediately see the effects of filter changes is to “flush” the blocked stream in question from the Connection Table.

Note: Changing a filter status in order to “unblock” a flow, must be done in combination with “flushing” the blocked flow from the TSE Connection Table. Otherwise, the filter changes will not take effect for the “blocked” flow until the TSE Connection Table timer expires for that flow.

2.3. TSE Asymmetric/Symmetric Mode

Asymmetric Network: An asymmetric network has multiple routes for incoming and outgoing network traffic. As such traffic takes a different route when entering or exiting the network.

Symmetric Network: A symmetric network has a single route for incoming and outgoing network traffic. As such traffic takes the same route when entering or exiting the network.
It is very common for traffic to be asymmetrical in both Service Provider and larger Enterprise networks due to the nature of routing within a large, complex environment that has multiple entry and exit points. Since the bulk of the TPS filters are flow-based (meaning state kept per-flow versus per session), attacks are detected in either send or receive directions.

By default, the TPS is shipped with **Asymmetric** mode enabled. This means that the TPS only sees one side of the TCP connection. When using Advanced Distributed Denial of Service (DDoS) protection filters, you must place the TPS device in a **Symmetric** network, and you must disable **Asymmetric** mode. The device must be able to see both sides of the traffic flow. This is configured in the TPS Device Configuration (TSE Settings) tab.

**DDoS filters** - Infrastructure protection filters that detect DDoS attacks which flood a network with requests, including traditional SYN floods, DNS request floods against name servers, and attempts to use protected systems as reflectors or amplifiers in attacks against third parties. These filters detect direct flood attacks and attacks hidden within larger packets and requests.

**Note:** Of the DDoS protection filters, the TPS devices only support **SYN Proxy**. To enable this function, enable and specify the Threshold in the **Profiles** area.

**SYN Proxy** - describes the detection and block of SYN flood attacks. These attacks enact a series of requests with false SYN flags that constantly request a connection. SYN Proxy enables the use of SYN traps to block all new TCP connection requests from a single attacker against a host. Enabling SYN-Proxy will force all spoofed and incomplete TCP connections to be blocked. Only a 3-way handshake TCP connection will proxy to the protected server.

### 2.4. TSE Adaptive Filtering

The TPS Adaptive Filtering feature is designed to protect the TPS from poorly performing filters. When the device detects a poorly performing filter, it automatically disables the offending filter and generates a system log message. A filter is determined to be poorly performing under the following conditions:

- **Filter time out** - Each filter may have one or more specific inspection functions, some of which may be implemented using regular expressions. If a regular expression times out, or exceeds a certain level of recursion, then the TPS will initiate AFC on that filter.

- **When a Filter is creating congestion and not firing** - It is possible that traffic is passing early inspection, but failing the later inspection functions. If the device is experiencing continued congestion, the recommendation is to look for these filters and consider disabling them.
Most filters provide configuration settings for adaptive filtering. If you do not want a filter to be subject to adaptive filtering, you can edit the filter and disable Adaptive Filtering. You can also modify the device-wide adaptive filter configuration for a device using Device Configuration.

2.5. **TSE Adaptive Aggregation**

Because a single packet can trigger an alert, attacks featuring large numbers of packets could potentially flood the alert mechanism causing system congestion. **Adaptive Aggregation** will limit the action set of any selected and defined filters that fire more than x times in the last minute. This is not to be confused with “Alert Aggregation,” which enables you to receive an alert notification at intervals to prevent alert flooding.

“Block & Notify” and “Block & Notify & Trace” action sets are reduced to “Block” when **Adaptive Aggregation** triggers. Identical results will occur for the “Permit” action sets as well. System logs will note entering and leaving this condition. Adaptive Aggregation will stop when the offending filter fires fewer than x/3 times in a minute.

3. **Elements**

3.1. **Filtering Concepts**

The TPS supports different types of filters, each of which provides protection from certain types of attacks or is used to implement the customer’s security policies.

3.2. **Filter Precedence**

The TPS processes filter in the following order of precedence:

- a. Inspection Bypass
- b. Traffic Management Filters
- c. Traffic Capture
- d. SYN- Proxy
- e. Threat DV (IP/DNS Reputation)
- f. Quarantine
- g. Blocked / Trusted Streams
- h. Scan/Sweep Filters
- i. CSW Filters (DV Toolkit)
- j. Mainline DV / Malware DV
3.3. Flow Inspection Filters

The flow inspection filters are the most common type of filter used by the TPS. The filters are used to determine whether a particular flow is malicious or in violation of the established security policy. The defined filters help establish several inspection functions, all of which must succeed for the filter to “fire.”

3.4. Trust as an Action Set

Trust as an Action Set allows trusts to be created and associated with a filter or set of filters. This is useful when you want to trust a certain type of application instead of the entire flow in general.

Actions are configured under shared settings; where you can create a TRUST or TRUST+NOTIFY action set which can then be assigned to any DV filter. If traffic matches a filter with an action set of TRUST, a trusted stream is created, and that flow will pass through the TPS uninspected until the trusted stream times out (default 30 minutes). Trusted streams are also shared with the partner TPS in a TRHA configuration.

3.5. Traffic Management Filters

Traffic Management Filters (TMFs) are similar to firewall rules, although not considered a replacement for them. A TMF is configured with an action and traffic matching criteria. In general terms, the more specific TMF filters should be listed first.

As an example of this concept, is the placement of a more specific IP filter that might block traffic with the fully qualified source and destination IP addresses along with the ports. While more general ones, like those that apply to entire subnets, should follow.

Specific example:

Source IP of 192.168.1.12 to Destination of 10.10.3.8 on TCP Port of 8080

General example:

Source of 192.168.1.0/24 to Destination of 10.10.3.0/24

The configurable actions for a TMF are:

- **Block** – drop all traffic meeting the specified criteria
- **Allow** – allow traffic and continue to inspect the traffic with other filters
- **Trust** – allow the traffic to pass through the TPS uninspected
- **Rate limit** – limit the matching traffic to the throughput specified in the action set (the traffic will still be inspected for other attacks)
  The following traffic matching criteria may be specified:

- **IP fragments** – apply the TMF action only to IP fragments

- **Traffic direction** – apply the TMF to traffic flowing from port A to port B; port B to port A; or both directions on the segment

- **Protocol** – IP, TCP, UDP, or ICMP. For TCP and UDP, specific ports may also be configured. For ICMP, specific Type and Code attributes may be specified

- **Source and Destination IP Addresses and CIDR blocks** – the scope of the TMF may be limited to a specific source and/or destination IP addresses

**Note:** Traffic Management filters do not generate alerts.

Traffic Management Filters, particularly those with a Trust action, should be used carefully. They are commonly used in the following situations:

- **Rate Limit** - Customer wants to rate limit an entire class of traffic, as specified by the TCP port. This may be used to preserve bandwidth for other applications.

  **Note:** Rate Limiting is only a reservation and not a guarantee of bandwidth at all times. It could create latency and other issues when TMFs meet rate limitations for flows being inspected or examined.

- **Block or Allow based on ports or protocols** - The use of trust TMF to improve the performance of certain applications is possible when considered against select Filters or Categories. This is common and recommended with certain applications, in particular, streaming media, where payloads consisting of essentially random data. It is possible that this data will look suspicious to the TPS (i.e., match some filters’ triggers) and cause the flow to be submitted for deeper inspection. The deeper detailed inspection fails; however, this process can possibly create jitter and result in packets being delivered out of order. Streaming media clients are very sensitive to these conditions, and the overall application performance may suffer. In these cases, a TMF using the trust action can alleviate the condition. This should be written “tightly,” meaning it should specify the application port(s) as well as the IP addresses of the media servers.

- **Trust** - When Network File System (NFS) backups running through the TPS. They may generate very large packets, which are fragmented at the IP layer. The TPS will reassemble IP fragments; however, this operation is very costly in performance of the
sensor. If the NFS data is trusted, (i.e., known to be free of attacks) then a TMF trust rule applied to IP fragments will help improve the throughput of this application.

**Note:** As indicated above, a TMF filter set to trust will cause the TPS to forward traffic meeting the matching criteria without inspecting it for attacks. Therefore, the matching criteria should be written in the most restrictive manner possible.

### 3.6. Flow Management Filters

Flow Management Filters are a special set of policy-based DV filters which "trigger" once a certain amount of traffic has passed and matches the defined filter. These filters are to be used in conjunction with TRUST as an "Action Set."

It is commonly assumed that most attacks occur within the first few bytes of a flow; using these filters you can trust a flow after the flow has been determined to be clean for either the first 5, 10, 100 or 500MB of transferred data. When a filter match occurs, the stream is added to the Trusted Streams table and all traffic afterward will follow the TMF recommendations for trust. Only one TCP and/or one UDP filter should be enabled.

<table>
<thead>
<tr>
<th>Flow Management Filters</th>
</tr>
</thead>
<tbody>
<tr>
<td>7620: TCP Flow Management (5MB)</td>
</tr>
<tr>
<td>7621: TCP Flow Management (10MB)</td>
</tr>
<tr>
<td>7622: TCP Flow Management (100MB)</td>
</tr>
<tr>
<td>7623: TCP Flow Management (500MB)</td>
</tr>
</tbody>
</table>

**Implementation and Management**

Best practice calls for the Traffic Management Filter to be set to a TRUST action, however, during the initial configuration and observation period, the filter should be set to an action of TRUST+NOTIFY. After the system has been verified to be working properly, the filter should be set to TRUST.

**Note:** Setting the filter to PERMIT+NOTIFY is not the recommended action for these filters as it will send all flows to deeper inspections.

You may view the TRUSTED streams table at the following locations:

1. **SMS:** Devices ➔ Member Summary ➔ Events ➔ Trusted Streams
2. **LSM:** Monitor ➔ Trusted Streams
3.7. VLAN Translation

TPS devices are capable of translating VLAN IDs per segment (assuming they follow the industry standard of dot1q). The translation occurs after the inspection, so incoming VLANs are used for Virtual Segments.

### Table 3-1: VLAN / Virtual Segments

<table>
<thead>
<tr>
<th>Setting</th>
<th>440T</th>
<th>2200T</th>
<th>vTPS</th>
<th>1100TX</th>
<th>5500TX</th>
<th>8200TX</th>
<th>8400TX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Segments</td>
<td>64</td>
<td>124</td>
<td>64</td>
<td>256</td>
<td>256</td>
<td>256</td>
<td>256</td>
</tr>
<tr>
<td>VLAN per virtual segment</td>
<td>4094</td>
<td>4094</td>
<td>4094</td>
<td>4094</td>
<td>4094</td>
<td>4094</td>
<td>4094</td>
</tr>
<tr>
<td>IP Address per virtual Segment</td>
<td>250</td>
<td>250</td>
<td>250</td>
<td>250</td>
<td>250</td>
<td>250</td>
<td>250</td>
</tr>
<tr>
<td>VLAN Translation Rules</td>
<td>8000</td>
<td>8000</td>
<td>Not supported</td>
<td>8000</td>
<td>8000</td>
<td>8000</td>
<td>8000</td>
</tr>
</tbody>
</table>

- Increase port density options by leveraging switches as a port aggregation point
- Only supports policy by VLAN as received by TPS
- All policy, security, events, etc. happen on ingress VLAN id only
  - VLAN Translation will strip all VLAN tags and inspect the traffic payload, once the inspection is completed, all VLAN tags will be reinserted except the outer most VLAN tag will be changed to VLAN specified by VLAN translation.
  - No concept of “dest VLAN” in virtual ports
- Typical usage involves symmetric translation
- Mappings must be unique - a given ingress VLAN must map to a single egress VLAN
  - Although it is valid to apply a 1: many translation, the TPS won’t be able to translate the return traffic

**Note:** VLAN Translation does not work while Zero Power High Availability (ZPHA) is active.
4. Deployment Considerations

4.1. Deployment Guidelines

The TippingPoint TPS and the Security Management System (SMS) server are very easy to deploy. The initial configuration is performed using the Out-of-Box Experience (OBE) wizard; this script prompts the user for the needed and essential configuration values. Typically, the baseline configuration of an SMS or TPS will require less than 10 minutes.

However, as with any in-line network device, the deployment should be carefully planned. The following section provides guidance on planning and executing the initial deployment of the TippingPoint solution. The following section will summarize key TPS configuration parameters.

4.2. TPS Positioning

The most common TPS deployment is at the customer network perimeter, which is those links connecting the customer network to the Internet. Although the TPS may be deployed in front of the firewall, most customers will deploy it behind the firewall. In this way, the firewall will drop traffic per its Access Control Lists (ACLs), thereby reducing the load on the TPS. With the introduction of the T/TX-Series devices not only can these devices be installed at the perimeter, but they can also be installed at the Core.

In today’s network environments, the “network perimeter” is becoming blurred. This is due to employees entering the network using a Virtual Private Network (VPN) or mobile users - employees and guests connecting to the network while at the customer site, particularly using wireless access points.

This drives the need to consider a “defense-in-depth” strategy. In addition to the network border, the internal network is subdivided into separate “attack domains” (also known as “security broadcast domains”); this not only contains outbreaks within the LAN but also allows continued TPS protection if one unit is bypassed for maintenance. In most cases, user traffic can pass through as many as three TPS’s before any cumulative latency is noticed.

4.3. Physical Connections

The TPS is placed in-line between two network elements (i.e., between 2 routers or switches) or can be placed on a switch where it can translate VLANs.

The TPS doesn’t act as a network element in the sense that it does not route traffic – it simply inspects the traffic. Because the TPS is an in-line device, the physical interfaces must match the segment in which it will be placed. Individual segments and are not shared.
4.4. Cabling Requirements

The TPS ships with the following cables:
- Two (2) AC power cables for the redundant power supplies
- Serial cable (RJ45, DB-9 FM) for (COM) port

4.5. Transparent High Availability (TRHA)

TRHA is a redundancy option for two TPS devices installed on parallel network paths. TRHA requires configuring two TPS devices with the same TRHA settings. Enabling this option configures the TPSs to share information, allowing for asymmetric routing and/or failover. Synchronization works with both IPv4 and IPv6 traffic.

Transparent HA keeps the devices in sync so that if one experiences a system failure, the network flow can be routed to the other with no interruption in intrusion prevention services. The also provides protection in the event that a network failure, outside of the TPS, causes network traffic to be routed to the TPS on the redundant path.

Table 4-1: TRHA Information

<table>
<thead>
<tr>
<th>Information shared between TRHA pairs</th>
<th>Information not shared</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blocked flows</td>
<td>TCP state</td>
</tr>
<tr>
<td>Rate limited flows</td>
<td>TCP reassembly information</td>
</tr>
<tr>
<td>Quarantined flows</td>
<td>Information about flows that are not being blocked or rate limited.</td>
</tr>
<tr>
<td>SYN proxy sequence number</td>
<td></td>
</tr>
</tbody>
</table>

Notes:
- Both TPS devices must be from the same product family and running the same TOS version.
- Function not supported by vTPS
4.6. Stacking

Stacking enables you to increase the overall inspection capacity of your Threat Protection System (TPS) devices by grouping multiple devices and pooling their resources. You can configure up to five devices in a stack. The stack operates as a single device that you manage on the TippingPoint Security Management System (SMS). Devices in a stack can be the same or a mixture of both 8200TX and 8400TX TPS security devices.

All devices in a stack should be licensed for the same inspection throughput. In-line inspection capacity increases with each device that you add to the stack. For example, for each 8200TX or 8400TX added to a stack of devices, the inspection capacity increases according to the licensed inspection capacity of each device, up to a stacking maximum of 120 Gbps.

Stacking requirements

- Any combination (up to five) of 8200TX or 8400TX devices
- One TippingPoint 40G QSFP+ Active Optical Cable (AOC) or discrete QSFP+ Transceivers and cables for each device
- TPS TOS v5.0.3 or later
- SMS v5.0.0 or later

Important Notes

- You must use an SMS SuperUser role to create a stack.

- All stack members must have the same TOS (v5.0.3 or later) version.

- Install the AOC or QSFP+ cables in the SP ports of the devices so that each device connects to its peer in a ring topology.

- Install the I/O modules in the stacking device that you plan to use as the network segment device. A network segment device operates in-line in the network and distributes network traffic to each stack member for inspection. The other stack members do not need network I/O modules.

- If you have a mixed stack configuration with 8400TX and 8200TX devices, maximize the physical network I/O slots that are available to the stack by installing network I/O modules in any of the network I/O slots on the 8400TX security device.

- When you install the AOC cable, you should orient the QSFP+ transceiver with the tab on top. There is only one way to correctly insert the AOC cable. If the cable does not slide in easily and click to latch, it may be upside down.
• If the devices are more than 3 meters apart, you will need to use standard multimode fiber with the two TippingPoint S146 40G QSFP+ SR4 850nm for each 40Gbe port.

• Do not reboot all devices in a stack at the same time. When you have to reboot devices in a stack configuration, reboot each device that you updated sequentially. Allow each device to finish the boot sequence, ensuring that the SMS has successfully managed the device before rebooting the next device.

• Before you distribute a TOS update, enable Intrinsic HA Layer-2 Fallback (L2FB) on the stack. L2FB remains enabled until the stack master confirms that there are enough devices in the stack with the same TOS version that are ready to inspect.

• If a TOS update does not install properly on a stack member, distribute the TOS update to the stack again. If the stacking device has issues, remove it from the stack to make any updates, and then add the device to the stack.

• To reuse a device after it is removed from the stack, either as a standalone device or as part of a different stack, use the `debug factory-reset` command in conjunction with a TippingPoint technical support representative to restore the device to its original settings.

• The same Digital Vaccine must be distributed to all devices in the stack; failure to do this will result in errors from the stack.

• Each time you add or delete a member in a stack, you must update the Digital Vaccine distribution schedule. This is because Digital Vaccines are always distributed according to which members were in the stack at the time the distribution was first scheduled. For example, if you schedule distribution and then remove a device from the stack, the SMS still distributes the package to all the devices that were members of the stack when the distribution was first scheduled, including the device you removed.

• For more information about stacking, refer to the TippingPoint Threat Protection System (TPS) TX-Series Stacking User Guide found at http://docs.trendmicro.com.
Figure 4-1: TX-Series 2-device resilient stack configuration

Figure 4-2: TX-Series 5-device resilient stack configuration
4.7. I/O Modules

The TippingPoint TX-Series devices support both standard I/O modules and bypass I/O modules for fiber and copper components. Only optical transceiver modules (including SFP, SFP+, and QSFP+) available from TippingPoint have been validated to achieve optimal performance with TippingPoint products. Other vendor devices are not supported. Using other vendor devices could be detrimental to the proper operation of the TippingPoint system.

Bypass I/O modules are zero-power high-availability (ZPHA) modules that permit network traffic and services while bypassing the device entirely when the device loses power. The purpose of the bypass modules is to route traffic around the device if and when there is a power failure. If the power is interrupted due to power supply failure, power loss, or unplugging, the module continues to pass traffic (uninspected) through the network while bypassing the device. Depending on the device, the bypass module comes in a different configuration to include copper and fiber.

4.7.1. Standard Modules

The TX-Series devices support up to four I/O modules, which enable the user to customize the device to suit the needs of the network. Each module occupies a slot, and each slot can contain up to 12 physical ports or 6 segments, depending on the module that is installed.

<table>
<thead>
<tr>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6-Segment Gig-T</td>
<td></td>
</tr>
<tr>
<td>Ports: 12 Fixed RJ-45 copper ports</td>
<td></td>
</tr>
<tr>
<td>Port speed: 10/100/1000 Mbps</td>
<td></td>
</tr>
<tr>
<td>Part Number: TPNN0059/TPNN0196</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> The second slot of the 5500TX device supports only the first four segments of a 6-segment I/O module.</td>
<td></td>
</tr>
<tr>
<td>6-Segment GbE SFP (SFP)</td>
<td></td>
</tr>
<tr>
<td>Ports: 12 SFP ports</td>
<td></td>
</tr>
<tr>
<td>Port speed: 1 Gbps</td>
<td></td>
</tr>
<tr>
<td>Part Number: TPNN0068</td>
<td></td>
</tr>
</tbody>
</table>
Table 4-2: Standard Modules

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> The second slot of the 5500TX device supports only the first four segments of a 6-segment I/O module.</td>
</tr>
<tr>
<td>4-Segment 10GbE SFP+ (SFP+)</td>
</tr>
<tr>
<td>Ports: 8 Fiber SFP+ ports</td>
</tr>
<tr>
<td>Port speed: 10 Gbps</td>
</tr>
<tr>
<td>Part Number: TPNN0060</td>
</tr>
<tr>
<td>1-Segment 40 GbE QSFP+ (QSFP+)</td>
</tr>
<tr>
<td>Ports: 2 Fiber QSFP+ ports</td>
</tr>
<tr>
<td>Port speed: 40 Gbps</td>
</tr>
<tr>
<td>Part Number: TPNN0069</td>
</tr>
</tbody>
</table>

4.7.2. Bypass Modules

The TX-Series devices support a range of Bypass I/O Modules (BIOMs), which combine the segment interfaces with mechanical bypass switches for high-availability purposes. The BIOMs offered for the TX-Series support various interface speed and connectivity types, including copper or fiber. Fiber modules are available with either long-range or short-range transceivers.

The BIOMs can route traffic within the module when the device loses power or when the module is removed from the device. Using the LSM, CLI, or SMS, you can also configure the BIOMs to bypass traffic on a per-module basis.

Table 4-3: Bypass Modules

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-Segment Gig-T</td>
</tr>
<tr>
<td>Ports: 8 copper ports</td>
</tr>
<tr>
<td>Port speed: 10/100/1000 Mbps</td>
</tr>
<tr>
<td>Part Number: TPNN0070</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
</tr>
<tr>
<td>2-Segment 1G Fiber SR</td>
</tr>
<tr>
<td>Ports: 4 Multi-Mode</td>
</tr>
<tr>
<td>Port speed: 1 Gbps</td>
</tr>
<tr>
<td>Part Number: TPNN0071</td>
</tr>
<tr>
<td>2-Segment 1G Fiber LR</td>
</tr>
<tr>
<td>Ports: 4 Single-Mode Fiber</td>
</tr>
<tr>
<td>Port speed: 1 Gbps</td>
</tr>
<tr>
<td>Part Number: TPNN0072</td>
</tr>
<tr>
<td>2-Segment 10G Fiber SR</td>
</tr>
<tr>
<td>Ports: 4 Multi-Mode Fiber</td>
</tr>
<tr>
<td>Port speed: 1/10 Gbps</td>
</tr>
<tr>
<td>Part Number: TPNN0073</td>
</tr>
<tr>
<td>2-Segment 10G Fiber LR</td>
</tr>
<tr>
<td>Ports: 4 Single-Mode Fiber</td>
</tr>
<tr>
<td>Port speed: 1/10 Gbps</td>
</tr>
<tr>
<td>Part Number: TPNN0074</td>
</tr>
<tr>
<td>1-Segment 40G Fiber SR</td>
</tr>
<tr>
<td>Ports: 4 Multi-Mode Fiber</td>
</tr>
<tr>
<td>Port speed: 40 Gbps</td>
</tr>
<tr>
<td>Part Number: TPNN0131</td>
</tr>
<tr>
<td>1-Segment 40G Fiber LR</td>
</tr>
<tr>
<td>Ports: 4 Single-Mode Fiber</td>
</tr>
<tr>
<td>Port speed: 40 Gbps</td>
</tr>
<tr>
<td>Part Number: TPNN0132</td>
</tr>
</tbody>
</table>
4.7.3. General Module Information

- Running “show-mfg” from the Command Line Interface (CLI) will display the model number of the modules that are installed into the appliance. In addition, the model number and description can also be found on the sticker on the bottom of the module itself.

- When the device is managed by the SMS, a delay of up to 1 minute can occur before the SMS recognizes the changed I/O module.

- Hot-swapping I/O modules during system initialization is not supported.

- Hot-swapping I/O modules is only supported with swapping like-for-like I/O modules in the same slot.

- A bypass module that is installed while the system is powered on remains in bypass mode. This way, the network can continue to pass traffic while users configure the number of network ports and their speeds to meet specific requirements. The BIOM must be taken out of bypass mode either administratively (using the CLI or the LSM) or through a reboot.

- Bypass modules should continue to pass traffic even while not connected to the device, or while the device is powered off or administratively placed in bypass mode. If the module does not pass traffic under these conditions, ensure that you have the appropriate cable for your network. In many cases, replacing a straight-through cable with a cross-over cable will resolve link issues.

- Bypass modules contain electromechanical switches that are very sensitive to handling when not installed in the system. Network disruption can occur if handled improperly.

- Best practice calls for network connectivity to be tested in all available modes (inspection, bypass, and transitions) between devices to ensure that cabling mistakes have occurred.

- For more information about deploying I/O modules, refer to the TippingPoint Hardware Specification and Installation Guide found at http://docs.trendmicro.com.
4.7.4. Module Hot-Swapping Guidelines

When hot-swapping I/O modules, note the following administrative guidelines:

- If a slot has always been empty, all possible ports and segments on the slot are absent and unavailable.

- If a slot’s configuration is erased by the user, configuration of that slot’s ports and segments is deleted, and all possible ports and segments on the slot become absent and unavailable. However, any policy-related configuration for these ports does not change when the bay configuration is erased and must be manually cleaned up by the user.

- When a module is inserted into a slot or restarted, the system software performs the following evaluation. When the device boots up, the evaluation is performed for every module installed in a slot:
  - The module is validated.
  - The status of the module (whether there is a module in the slot, what type of module it is, whether it is being used or is in error) is determined.
  - The physical state (present/absent) and availability state (available/unavailable) for each possible port and segment on this slot is determined.
  - The configuration is changed and applied as necessary.
  - A Syslog message is added (depending on whether the module passed validation and the module status check).

- Removing a module from a slot does not change or reapply the configuration. It also does not change the availability state of ports and segments. It will, however, change the physical state to absent. An error-level Syslog message indicates that the module was removed. In addition, users are shown the physical state when viewing configuration and status related to that slot. These changes also occur when the device boots up for every empty slot.

- The following conditions are displayed when the corresponding ports and segments are available and are hidden when they are unavailable:
  - Segment configuration
  - Network port configuration
  - Network port health
  - Network port throughput performance
  - Traffic profile by the network port
4.7.5. What happens when modules are swapped?

1. Swapping like-for-like
   - All configuration is preserved including:
     - Port & Segment configuration (port state, speed / duplex settings, Link Down Sync & L2FB behavior)
     - Inspection Bypass, VLAN translation rules & Filter policy

2. Swapping with a different module type
   - Port & Segment configuration is reset to defaults
   - Inspection Bypass rules & Filter Policy is preserved
   - VLAN translation rules are preserved, but ports are administratively disabled

3. Upgrading from 1G to 10G
   - Swapping 6 segments to 4 segments (standard) or 4 segments to 1 segment (bypass)
   - Behavior is as Example-2, but you will have Filter Policy applied to segments which are no longer physically present
   - Customers will have to manually remove the Filter Policy on the unused segments

4. Hot-inserting a Bypass I/O modules
   - The newly hot-inserted bypass module will remain in bypass until an administrator removes it from bypass or reboots the device

5. Swapping to/from a 40G module or inserting new 40G module
   - Hot-swapping 40G module will require a reboot –full to be placed into service
   - One exception is when you are swapping like for like, which does not require a reboot
4.7.6. Fiber-Optic Connection

The TPS uses fiber-optic connectors with the connector type being a Small Form-Factor Pluggable (SFP) fiber optic connector that is LC-Duplex compatible. The following modules are approved for use in the TX-Series devices:

<table>
<thead>
<tr>
<th>I/O Module P/N</th>
<th>Transceiver P/N</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6-Segment GbE SFP (TPNN0068)</td>
<td>TPNN0054</td>
<td>X126 1G SFP RJ45 T (Copper SFP)</td>
</tr>
<tr>
<td></td>
<td>TPNN0055</td>
<td>X126 1G SFP LC SX 550m 850nm XCVR (1G SFP Short Range / Multi Mode)</td>
</tr>
<tr>
<td></td>
<td>TPNN0056</td>
<td>X126 1G SFP LC LX 10Km 1310nm XCVR (1G SFP Long Range / Single Mode)</td>
</tr>
<tr>
<td>1-Segment 40 GbE QSFP+ (TPNN0069)</td>
<td>TPNN0067</td>
<td>S146 40G QSFP+ SR4 850nm (40G SFP Short Range / Multi Mode)</td>
</tr>
<tr>
<td></td>
<td>TPNN0327</td>
<td>S146 40G QSFP+ LR4 1310nm (40G SFP Long Range / Single Mode)</td>
</tr>
<tr>
<td>4-Segment 10GbE SFP+ (TPNN0060)</td>
<td>TPNN0057</td>
<td>S136 10G SFP+ LC SR (10G SFP Short Range / Multi Mode)</td>
</tr>
<tr>
<td></td>
<td>TPNN0058</td>
<td>S136 10G SFP+ LC LR (10G SFP Long Range / Single Mode)</td>
</tr>
</tbody>
</table>
4.8. Intrusion Detection System (IDS)

When Intrusion Detection System (IDS) mode is enabled, it adjusts the TPS device configuration such that the TPS operates in a manner suitable for intrusion detection scenarios and filter configurations. When in IDS mode the following areas are modified;

- Performance protection is disabled
- Adaptive Filtering is set to manual
- Queue length is increased
- Filters currently set to Block are not switched to Permit, and Block filters can still be set

Procedure:

1. Configure the network device for port mirroring/SPAN mode
2. Connect the TPS device "Segment A" to the network device
3. Enable IDS mode;
   a. **On the LSM;** IDS mode is enabled on the TPS Preferences page (Policy → Settings). When IDS Mode settings are changed, the device must be rebooted for the change to take effect.
      
      **Important:** Changing IDS Mode does not change Performance Protection mode. For best results, when enabling IDS Mode, go to the System > Settings > Log Configuration > Performance Protection page and change Performance Protection to Always log Alert and Block events mode.
   b. **On the SMS;** Go to Devices and then choose your device from the list on the left or the window on the right. Once selected, choose Device Configuration. Another window will pop-up and in this window choose TSE Settings on the left. On the right side click the IDS Mode checkbox and press OK to continue. Once again, this will require a reboot.

Notes:

- Using the TPS device in a mixed configuration is not supported. If the TPS device will be used in an IDS configuration, then it is an IDS device. Use the TPS as either IDS or TPS device but not both. Attempting to run in mixed mode will lead to performance issues.
- Connect the mirrored/span port only to Segment A, leave Segment B open
Definitions:

**Port Mirror / SPAN Mode** - A port mirror is *active* packet duplication, meaning that a network device (switch/router) has to copy packets onto the mirrored port physically. This means that the device has to carry on this task by using some resources (e.g., CPU) and that both traffic directions will be copied into the same port.

**Network TAP** - This entails either electrically or optically copying packets from the tap port.

4.9. SSL Inspection

TPS devices provide in-line, real-time threat protection for inbound SSL traffic to your servers. The TPS manages its own private keys and certificates from the servers it is securing; you can either store them on the device or access them at run-time using the Security Management System (SMS). With access to your server certificate and private key, the TPS is a transparent proxy that receives and decrypts SSL data, inspects it using the Threat Suppression Engine, and then encrypts it before sending it to the actual destination.

SSL inspection is supported on the following TPS devices:
- T-Series (2200T)
- TX Series (5500TX, 8200TX, 8400TX)
- vTPS, when deployed in “Performance Mode.”

**Table 4-5: SSL Deployment Considerations**

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound IPv4 traffic only</td>
<td>The TPS device inspects inbound traffic only to include IPv4, HTTP, and HTTPS traffic. SSL inspection does not support:</td>
</tr>
<tr>
<td></td>
<td>• IPv6 traffic, including IPv4 over IPv6 tunneling</td>
</tr>
<tr>
<td></td>
<td>• Outbound IPv4 traffic and IPv6 traffic</td>
</tr>
<tr>
<td>Quarantine hosts and redirecting HTTP traffic</td>
<td>When configuring an Action Set to quarantine hosts, if you also configure the response to redirect traffic to an HTTP server, the device redirects the HTTP traffic from the quarantined host but does not redirect the HTTPS traffic.</td>
</tr>
<tr>
<td>to another site</td>
<td></td>
</tr>
</tbody>
</table>
### Table 4-5: SSL Deployment Considerations

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Tunneled traffic** | Supported SSL encapsulations:  
  - GRE (Generic Routing Encapsulation)*  
  - IPv4 (IP-in-IP)  
  - One layer of tunneling only for both GRE and IPv4-in-IPv4. SSL inspection does not include support for GTP or IPv6 encapsulations.  
  *GRE support includes the mandatory GRE fields. Optional GRE key configuration is also supported but requires the key to be the same value for both directions. SSL inspection does not support other optional GRE fields, such as GRE sequence number. |
| **Filter Precedence** | The TPS processes filters in the following order of precedence:  
  1. Inspection Bypass Rules  
  2. Traffic Management Filters  
  3. RepDV  
  4. Quarantine  
  5. Digital Vaccine Filters  
  When encrypted traffic is routed through the device, and SSL inspection is configured, the order of precedence applies to the decrypted traffic. The device does not quarantine or apply Digital Vaccine filters to traffic without first decrypting the traffic.  
  If SSL inspection is not configured, the device applies Inspection Bypass, Traffic Management, RepDV, and quarantine filtering against the encrypted traffic. The device applies Digital Vaccine filters, but they do not match against encrypted payload. |
Table 4-5: SSL Deployment Considerations

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Non-encrypted traffic when SSL is configured** | The TPS device drops non-encrypted traffic flows that match a configured SSL server tuple (destination port and destination IP address) in the SSL profile but send clear text traffic before starting an SSL handshake.  
The TPS device drops non-encrypted traffic flows that match a configured SSL server tuple (destination port and destination IP address) in the SSL profile due to the lack of an SSL handshake. |
| **Traffic Management filters - Trust action** | The TPS device continues to proxy the SSL session between the client and the server when HTTPS traffic matches a traffic management filter that is set to Trust (incoming traffic is trusted and not inspected). |
| **Packet trace**                        | Packet Trace as an action includes the decrypted traffic.                                                                                   |
| **Traffic capture**                     | Traffic capture by tcpdump does not include the decrypted contents.                                                                             |
| **L2FB/ZPHA**                           | The TPS device clears proxied SSL sessions when the device enters Intrinsic HA Layer-2 Fallback or Zero Power High Availability (ZPHA).         |
| **SSL v3.0 with TLS,**                  | If you need to configure SSL v3.0 with TLS, always configure all TLS protocols, including TLS v1.0, TLS v1.1, and TLS v1.2. You must enable all SSL protocols between the configured lowest-strength and highest-strength SSL protocols. |
| **SSL Certificate**                     | When configuring SSL, make sure that you update both the device certificate and the SSL webserver certificate before they expire. If the certificates expire or become out of sync, the SSL connections might fail. |
5. System Administration

5.1. How to turn off SMS Management of the device

Issue the following command at the command line:

```
sms unmanage
```

To re-enable SMS management issue the following CLI command:

```
sms manage
```

You can also turn SMS management on or off by using the LSM via System ➔ SMS.

After the TPS is managed by an SMS, you can view the SMS information from the CLI of the TPS. Type in the following to get information on which SMS is managing your device:

```
show sms
```

This will display the SMS Serial number, the SMS version, SMS IP address, as well as the SMS Port.

5.2. Management port

TippingPoint recommends configuring the management port on the TPS to use a non-routed IP address from the RFC-1918 Private Address space. This helps to prevent a direct attack on the management port from the Internet. Additionally, the management port IP Address filter feature should be used to limit access to the management port. Only addresses defined by the command will be allowed to access the TPS. Host IP filters are essentially ACLs on the management port of the TPS.

When the TPS is initially configured, the default security policy is set to permit any connection. Once you establish a host IP filter, whether it is a permit or deny, then the default IP filter becomes deny any, the old legal idea of the inclusion of one is to the exclusion of all others). If you are doing this via SSH (not the console), the first thing you must do is a permit rule for the IP address you are on, or you will deny your IP access to the management port inadvertently.

“Management interface under attack” This message appears when too much of the traffic sent to the management port wasn’t meant for the management IP address - too much broadcast traffic for instance.
**Note:** The TPS must not be under SMS control when doing this. If the device is currently managed, you may use the CLI command “sms unmanage” to temporarily unmanage the TPS. To resume SMS management, use the CLI command “sms manage.”

You can use the following CLI commands to configure the management port:

```plaintext
{running-mgmt} ip-filter (allow | deny) (https | icmp | snmp | ssh | ip) [ip]
```

For example, issue the following command to limit management port access to one host:

```plaintext
{running-mgmt} ip-filter allow ip 192.168.1.32/24
```

If you require more than one address, then create a host ip-filter for all IP addresses or the subnet that is allowed to access the device. For example, if the legal machines are on the 192.168.10.X subnet, enter the following CLI command:

```plaintext
{running-mgmt} ip-filter allow ip 192.168.1.0/24
```

To change the default action back to "permit any" enter the following command:

```plaintext
{running-mgmt} ip-filter allow default
```

### 5.3. Reports available via the Local Security Manager (LSM)

The TPS itself has basic reporting capabilities via the LSM interface. Apart from the top-level display that shows Top 10 Filters, Filters by Severity, Filters by Action, and Filters by Protocol, the reports available on the **Reports** page, you can also access reporting information on the Dashboard and Monitor pages. The **Dashboard** provides information in the form of graphs on device performance. The **Monitor** page provides additional graphical reports on system health.

The following reports are available via the **Reports** tab on the LSM.

- **Activity** - Contain information about network traffic and network activity, including reports on Rate Limiters, Traffic Profile, and SSL Connections.

- **Security** - Contain information about the performance and activity for the device, including reports for Adaptive filter control, DDoS, Quarantines, and Top filter matches.

The following report is available via the **Tools** tab on the LSM.

- **Tech Support Report** - Use the Technical Support Report page to arrange for the LSM to send you a status report in an email based on the email server settings you configured.
5.4. Authentication Levels

Restrictions on username and password values for user accounts are determined by the Security Level preference setting configured on the Preferences page. Username and password requirements are the same for local users and TOS users. There are three possible security levels available on the TPS:

Table 5-1: Authentication Levels and Password Requirements

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| None   | • User names must be at least six characters in length  
         • A password does NOT have to be defined  
         • If you choose to define a password, it must contain at least 8 and no more than 32 characters without spaces |
| Low    | • User names must be at least six characters in length  
         • Passwords must contain at least 8 and no more than 32 characters without spaces |
| Medium | • User names must be at least six characters in length  
         • Passwords must contain at least 8 and no more than 32 characters without spaces  
         • Must contain at least two alphabetic characters  
         • Must contain at least one numeric character  
         • Must contain at least one non-alphanumeric character (E.g. ! ? $ * #). |
| High   | • User names must be at least six characters in length  
         • Passwords must contain at least 15 and no more than 32 characters without spaces  
         • Must contain at least two alphabetic characters  
         • Must contain at least one numeric character  
         • Must contain at least one non-alphanumeric character (E.g. ! ? $ * #).  
         • Contains at least one uppercase character  
         • Contains at least one lowercase character  
         • At least half the characters cannot occupy the same positions as the current password. |
5.5. How to Recover the TPS device SuperUser Password?

You cannot recover the SuperUser password of a TPS device, but you can reset it to a new value or create a new login with SuperUser privileges.

⚠️ **Caution:** This procedure requires a reboot operation which will disrupt traffic!

Connect to the TPS device via the console serial port using a null-modem cable. The terminal emulator software must be set to 115200bps, 8 Data Bits, No Parity, 1 Stop Bit. (115200,8,N,1)

1. Reboot the TPS device.

2. As the device is rebooting, watch for the word "Loading." You should see something similar to the following:

```
Mounting system disk.................................[ OK ]
Initializing hardware clock........................[ OK ]
Creating device nodes...............................[ OK ]
Configuring fast path...............................[ OK ]
Loading kernel modules............................[ OK ]
Checking firmware...................................[ OK ]
Starting syslog daemon.............................[ OK ]
Configuring system.................................[ OK ]
Configuring system firewall.......................[ OK ]
Starting platform daemons.........................[ OK ]
Starting keystore...................................[ OK ]
Starting health monitoring........................[ OK ]
Starting fast path...................................[ OK ]
Starting TippingPoint OS...........................[ OK ]
Starting segments..................................[ OK ]
Starting XMS......................................[ OK ]
Starting certificate status monitoring..........[ OK ]
Loading configuration............................[ OK ]
Starting process monitoring......................[ OK ]
Updating boot counts.............................[ OK ]
```

**Loading....**
3. Type the word **mkey** within 3 seconds of seeing the word "Loading" and press <Enter>.

   **Note**: if you do not type **mkey** before the dots "..." appear after the word **Loading**, you will have to reboot the device and try again.

4. If successful, you will see the following prompts;

   ```
   Welcome to Super User Password Recovery

   Please enter the Super User account username and password. Password recovery will create a new super user account or will reset the password on an existing super user account.

   Spaces are not permitted in username or password.

   Minimum password requirements currently configured on the system are:

   Maximum: The password must contain 8 characters or more, at least 2 alpha characters, at least 1 digit, and at least 1 non-alphanumeric character
   ```

5. **Enter Super User username**: Type the account name you would like to reset or type a new account name and press <Enter>.

6. **Enter SuperUser password**: Enter your new password and press<Enter>.

7. **Verify SuperUser password**: Re-type the password to verify and press <Enter> again.

8. After entering the new password, you will see the following screen.
9. Log in to the system with the new credentials

5.6. **How to Reset a TPS device to Factory Settings?**

**WARNING:** The TPS will reboot during this procedure and will interrupt traffic flow through the TPS. When the TPS finishes the process of resetting to factory defaults, the TPS will need to be reconfigured using the Out-of-Box-Experience at the serial console.

Be aware that the TPS will revert to the original TOS shipped with the device and that the Digital Vaccines (DVs) will be deleted. System logs, snapshots, and other system data will not be deleted, but they will not be visible until you restore the TOS version that created them.

To factory reset your TPS enter the following command at the CLI interface;

```
debug factory-reset
```
5.7. What are Inspection Bypass rules?

Inspection Bypass rules enable administrators to configure rules that, in effect, will allow traffic to bypass the TPS inspection engine. Any traffic that matches an inspection bypass rule is directed through the TPS without further inspection. Also, traffic that is passed with an inspection bypass rule does not count against the maximum traffic capacity of the device. Inspection bypass rules can be created to take into account any of the following criteria:

- CIDR
- VLAN
- Source IP Address
- Destination IP Address
- Port or Protocol
- Tunneling Traffic

**Note:** TPS devices support up to 32 inspection bypass rules per device; this feature cannot be enabled on vTPS devices.

**Note:** Best practice dictates to utilize inspection bypass rules to bypass encrypted traffic. This is recommended because the TPS cannot inspect encrypted traffic and attempting to do so can impact performance and cause unnecessary CPU processing load.

5.8. System Upgrades

Hitless upgrades are available for TPS devices. To completely reboot or do a full reboot, non-hitless, type the following at the CLI:

```
TPS# reboot full
```

**Note:** If possible, connect to the console port during a TOS upgrade so that you can watch the status and catch any errors. Always update the DV after a TOS upgrade since the TOS will include a DV from the period in which the TOS file was generated.

5.9. Traces and Email Notifications

When troubleshooting, use packet traces and email notifications sparingly and remember to revert to normal after your “forensics” analysis is finished.

5.10. Maximum Frame Sizes

TPS family of devices support a Maximum Transmission Unit (MTU) size of up to 9050 bytes. This includes the 14-byte Ethernet header, 9032 bytes of payload data, and the 4-byte
Ethernet checksum, which helps accommodate for VLAN traffic. Use a TPS device to monitor jumbo frames. Jumbo frames are not supported on vTPS devices. vTPS MTU is 1500.

5.11. TPS Storage Devices

TPS devices have both internal and external storage devices. The internal storage device (CFast card) contains the TippingPoint Operating System (TOS), Digital Vaccine, Malware Filters, and the running configuration. The external device (CFast/SSD) is used to store system logs, snapshots, and other system data. By removing the external storage device, all customer-specific data is removed from the system.

The user can remove and insert the external storage device while the device is running; however, the user must be sure to issue the appropriate CLI command. The device will continue to perform correctly if the external storage device is not available. However, if you attempt to take a system snapshot, the operation will fail, and an error will be recorded in the system log.

Notes:

- External storage devices are required to stay with the customer if performing an RMA. The replacement RMA unit does not come with an external storage device.

- Commercially available External storage devices are not supported. If a new device is required, ensure that you contact the TippingPoint Technical Assistance Center (TAC) for a replacement.

- Ejecting a compact flash card may fail after a 30-second timeout if the card is in use. The most common cause for failure is if a snapshot is being written to the card when the Eject command is issued.

5.12. Performance Protection

During high traffic inspection timeframes, the TPS device will send notifications to the SMS. These notifications take up valuable CPU cycles which should be used for traffic inspection. System notifications can be suspended automatically if the system is experiencing congestion.

Performance Protection settings:

- Logging Mode: Always log / Disable if congested
- Congestion Percentage: Default:1.0% – Range: 0.1% to 99.9%
- Disable Time: How long to suppress notifications, 600 seconds by default
5.13. Link-Down Synchronization (LDS)

Industry-standard routing protocols like Open Shortest Path First (OSPF), Virtual Router Redundancy Protocol (VRRP) and Hot Standby Router Protocol (HSRP) utilize “path down” detection technology to detect when a network path is down and thus initiate a switch to a redundant default path. Link-Down Synchronization, also called Sympathetic HA, allows you to configure the device to force both ports down on a segment when the device detects a link-state of down on one of the ports. When Link-Down Synchronization is enabled, the device monitors the link state for both ports on a segment.

If the link goes down on either port, both ports on the segment are disabled. This functionality propagates the link-state across the device. In the case of Router, A and Router B, if the link to Router A goes down, then both ports are disabled, resulting in the link to Router B also going down, which Router B then detects. With Link-Down Synchronization, ports respond according to the configured setting. The settings include the following:

- **Hub** - When a port goes down, the system ensures the partner port remains up.
- **Breaker** - When a port goes down, the system disables the partner port until both ports are manually restarted. The breaker option requires manually restarting both ports.
- **Wire** - When a port goes down, the system disables the partner port, automatically restarting both ports when the link is re-established.

In addition to the ability to enable Link-Down Synchronization for each segment, you can change the amount of time after detecting a link is down before forcing both ports down on a segment. The default is one second. You can configure the setting to any number of seconds ranging from zero to 240.

**Note:** Best practice recommendation is to set the time between two and four seconds.

Once you enable Link-Down Synchronization for a segment, monitoring of that segment begins only after link-up is detected on both ports. When Link-Down Synchronization disables the ports on a segment, two audit log messages are generated. The first message in the audit log corresponds to the port with the link down. The second message corresponds to the segment partner. Additionally, an error message is added to the system log indicating which port was detected with the link down, activating Link-Down Synchronization for that segment.

**Recommendation:** We recommend in most network environments to set the link down synchronization to **wire** mode to prevent routing issues.

**Note:** Testing has shown that it can take up to 4 seconds for the partner link to shut down even if the timer is set to less than 4 seconds.

Intrinsic HA, also known as “Layer 2 Fallback” (L2FB), is a mode wherein the TPS will pass traffic from one interface to its partner without inspecting the traffic. If an internal failure is detected, the device goes into L2FB mode and either permits or blocks all traffic on each segment, depending on the preference of the network administrator (see below).

![Figure 5-1: Intrinsic Network HA](image)

Some of the checks, thresholds, and resulting actions can be customized based on each customer’s HA and security requirements. For example, L2FB can be configured to fail open (Permit All) or closed (Block All) on a per-segment basis. L2FB can also be enabled manually (see below). Traffic flowing through each segment on the device will be either blocked or permitted based on the segment configuration. Any permitted traffic will not be inspected. Setting the TPS manually in L2FB is a useful tool for troubleshooting by ruling out the TPS as the device causing the issue (or not).

Notes:

- L2FB only functions as long as the TPS device has power. If you lose power to the device, you will lose connectivity unless the device has a Zero Power High Availability (ZPHA) module.

- To place device in L2FB from the Command Line Interface (CLI), it will be necessary to take the TPS out of SMS control. Otherwise, this can be controlled through the SMS.

- Function not supported by vTPS

5.15. TPS System Backup (Snapshot)

Best practice calls for snapshots to be created each time the TPS device is modified. Whether you distribute a new DV or upgrade the TOS or modify any system configuration, you should perform a snapshot. Snapshots are stored on the external storage device.

If you have an SMS: Through the SMS System Snapshot section, you can manage the snapshots taken of device filters and settings. You can create these snapshots through the Device Configuration screen for a specific device. Creating a new snapshot stores a copy on
the TPS device. Archiving a snapshot stores a copy on the SMS. Deleting a snapshot removes the system snapshot from the device and, if present, the snapshot on the SMS. Snapshots have the option to include LSM created Reputation Entries, as well as Reputation DV and SMS, created Entries.

**Note:** If you perform a TOS upgrade on the TPS, any snapshots taken on a previous version of the TOS will not be visible after the upgrade. However, the snapshots are still saved, and if/or when you perform a rollback, the snapshot will be visible again.

### 5.16. Scan/Sweep Filters

The T/TX-Series support filters to detect and/or block port scans and host sweeps and can be found in the Reconnaissance filter category under Application Protection. The following filters are referred to as the scan/sweep filters:

- 7000: TCP: Port Scan
- 7001: UDP: Port Scan
- 7002: TCP: Host Sweep
- 7003: UDP: Host Sweep
- 7004: ICMP: Host Sweep
- 7016: ICMPv6: Host Sweep

The scan and sweep filters track the number of port scans, and host sweeps attempts from a single source IP address. These filters have threshold values that can be configured per Security Profile and per filter. The filter becomes active when the number of connection attempts from a source IP address exceeds the threshold. Host scans and port sweeps are blocked through the Quarantine feature. Scan and sweep filters only look at connections from the traffic that undergoes TPS inspection. These filters ignore the following types of traffic:

- Blocked or trusted by a Traffic Management filter
- Trusted flow due to Trust as an Action
- Blocked or trusted by IP Reputation
- Matches an inspection-bypass rule

**Best Practice:** Before enabling the scan sweep filters in a **Block+Notify** action set, you should test these filters in a **Permit+Notify** or **Trust+Notify** action set. This should be done as a precaution as several servers will trigger these filters (e.g., Proxy, DNS, Mail). In this fashion, a determination can be made as to what servers will require filter exceptions once these filters are enabled. Once you have added the exceptions, you can then enable the filters as **Block+Notify**.
5.17. Common Pitfalls

**Virus Category** - Turning on all of these filters includes the entire Malware category, which can cause performance issues. Also, they can block all traffic from mail servers, so test before enabling them.

**Security Policy Category** – These filters are provided as additional tools for specific applications that wouldn’t otherwise be allowed in secure environments. They should not, as a rule, be enabled as they will block legitimate traffic.

**Traffic Normalization** – By default, most Traffic Normalization filters are set to Block. We do not recommend using a permit action on these filters as it could introduce vulnerabilities with malformed packets.

**Over Configured Devices** – too many overrides, double/triple inspection – perimeter, core, and DMZ on the same device – use bypass or traffic management or virtual segments if necessary. Too much permit & notify can cause performance issues as it endlessly inspects legitimate packets over and over again. Permit+Notify should be restricted to testing filters and/or limited use for troubleshooting purposes.

<table>
<thead>
<tr>
<th>Table 5-2: Do’s and Don’ts</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Do’s</strong></td>
</tr>
<tr>
<td><strong>Filters</strong></td>
</tr>
<tr>
<td><strong>Bandwidth</strong></td>
</tr>
<tr>
<td><strong>Packet size</strong></td>
</tr>
<tr>
<td><strong>Protocols</strong></td>
</tr>
</tbody>
</table>
Table 5-2: Do’s and Don’ts

<table>
<thead>
<tr>
<th></th>
<th>Do’s</th>
<th>Don’ts</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Trusting SSL or QUIC</strong></td>
<td>Filters 28987 and 29276 are available to trust SSL to avoid inspection or block QUIC traffic to force the use of HTTPS</td>
<td>Do not use these filters without careful monitoring; SSL may fill the ‘Trusted Flows’ table on the device</td>
</tr>
<tr>
<td><strong>Backups</strong></td>
<td>Create regular device snapshots and SMS backups</td>
<td>Do Not forget to ‘archive’ snapshots to your SMS</td>
</tr>
</tbody>
</table>

5.18. TPS Throughput Licensing

Update your license package to assign a product capability that you have purchased, such as an inspection throughput license, to a particular security device. To review and manage the capabilities in your license package, go to the TippingPoint License Manager on the Threat Management Center (TMC). Verify your product license provides sufficient inspection throughput. By default, a TPS security device is unlicensed and provides reduced inspection throughput for testing and evaluation purposes only.

Table 5-3: TPS Throughput Licensing

<table>
<thead>
<tr>
<th>Model</th>
<th>Licensed</th>
<th>Un-Licensed</th>
</tr>
</thead>
<tbody>
<tr>
<td>vTPS</td>
<td>250 Mbps/500 Mbps/1 Gbps/2 Gbps</td>
<td>Trial Mode</td>
</tr>
<tr>
<td>440T</td>
<td>250Mbps/500Mbps/1Gbps</td>
<td>100 Mbps</td>
</tr>
<tr>
<td>2200T</td>
<td>1Gbps/2Gbps</td>
<td>200 Mbps</td>
</tr>
<tr>
<td>1100TX</td>
<td>250Mbps/500Mbps/1Gbps</td>
<td>100 Mbps</td>
</tr>
<tr>
<td>5500TX</td>
<td>1/2/3/5 Gbps</td>
<td>100 Mbps</td>
</tr>
<tr>
<td>8200TX</td>
<td>3/5/10/15/20/30/40 Gbps</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>8400TX</td>
<td>3/5/10/15/20/30/40 Gbps</td>
<td>1 Gbps</td>
</tr>
</tbody>
</table>

**Note:** Making any changes to the licensed throughput will require a reboot of the device.
6. Troubleshooting Commands

Certain performance-related issues can be diagnosed from the CLI. The following commands are useful in determining this:

6.1. show np tier-stats

Displays throughput and efficiency across the different inspection tiers

| Tier 1: |
|-----------------|-----------------|
| Rx Mbps         | 0.0 (0.0)       |
| Tx Mbps         | 0.0 (0.0)       |
| Rx Packets/Sec  | 0.0 (0.0)       |
| Tx Packets/Sec  | 0.0 (0.0)       |
| Bypass Packets/Sec | 0.0 (0.0)   |
| Bypass to Rx Ratio | 0.0%            |
| VLANTrans Packets/Sec | 0.0 (0.0) |
| VLANTrans to Rx Ratio | 0.0%            |
| Avg Bytes/Pkt   | 0.0             |
| CPU Balance (A/B) | 0.0 (A: 0.0 B: 0.0) |
| Utilization     | 0.0% (0.0%)     |
| Ratio to next tier | 100.0% [100.0%] (0.0%) |

**Tier 1:** This inspection tier is responsible for inspection bypass rules and Intrinsic HA L2FB, which prevents network traffic from going to the next tier. This tier is also responsible for the rate limiter, inspection bypass rules, jumbo packet shunting, and the hardware watchdog timer.

- This section shows how much traffic is entering the inspection engine from all the segments. The numbers in the brackets represent the high-level water mark since the TPS was powered on or “tier stats” was reset (Note: The clear np tier-stats CLI command is used to clear out these statistics).

- Bypass Mbps shows the current and max throughput matching an Inspection Bypass rule. Traffic matching an Inspection Bypass rule does not count towards the TPS inspection limits. Inspection bypass rules reduce the value of both “Utilization” and “Ratio to next tier.”

- Utilization is shown as a percentage of rated system throughput and traffic to the next tier
Tier 2:

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Mbps</td>
<td>0.0 (0.0)</td>
</tr>
<tr>
<td>Rx Packets/Sec</td>
<td>0.0 (0.0)</td>
</tr>
<tr>
<td>Tx trust packets/sec</td>
<td>0.0 (0.0)</td>
</tr>
<tr>
<td>Utilization</td>
<td>0.0% (0.0%)</td>
</tr>
<tr>
<td>Ratio to next tier</td>
<td>100.0% [100.0%] (0.0%)</td>
</tr>
</tbody>
</table>

Tier 2: Load balances flows through the KS threads and handles traffic management trusts, and block filters will prevent traffic from proceeding to the next tier. Tier 2 “Ratio to next tier” accounts for Traffic Management Trust and Block rules and Traffic normalization filters. TCP ACKs are trusted by default and reduces Tier 2 ratio to the next tier.

Tier 3:

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Mbps</td>
<td>0.0 (0.0)</td>
</tr>
<tr>
<td>Rx Packets/Sec</td>
<td>0.0 (0.0)</td>
</tr>
<tr>
<td>Tx trust packets/sec</td>
<td>0.0 (0.0)</td>
</tr>
<tr>
<td>Utilization</td>
<td>0.0% (0.0%)</td>
</tr>
<tr>
<td>Ratio to next tier</td>
<td>0.0% [0.0%] (0.0%)</td>
</tr>
</tbody>
</table>

Tier 3: This tier is designed to search for suspicious traffic that needs to undergo deep inspection. This section handles IPv6 + GRE and Mobile IPv4 tunnels. IP reassembly, maintaining connection table, and TCP state tracking is handled here. If triggers are found, it determines what filters need to be checked against the packet or flow than it turns on soft-reroute for the flow, and, if necessary, sends it for deep packet inspection. Shows how much traffic KS threads and IP reassembly will inspect. Ratio to next tier shows what percentage of traffic needs TCP reassembly or is suspicious (matched a trigger).

Tier 4:

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Mbps</td>
<td>0.0 (0.0)</td>
</tr>
<tr>
<td>Rx Packets/Sec</td>
<td>0.0 (0.0)</td>
</tr>
<tr>
<td>Rx due to:</td>
<td></td>
</tr>
<tr>
<td>Trigger match</td>
<td>0.0% (0.0%)</td>
</tr>
<tr>
<td>Reroute</td>
<td>0.0% (0.0%)</td>
</tr>
<tr>
<td>TCP sequence</td>
<td>0.0% (0.0%)</td>
</tr>
<tr>
<td>Protocol decode</td>
<td>0.0% (0.0%)</td>
</tr>
<tr>
<td>Utilization</td>
<td>0.0% (0.0%)</td>
</tr>
<tr>
<td>Ratio to deep</td>
<td>0.0% [0.0%] (0.0%)</td>
</tr>
</tbody>
</table>
**Tier 4:** It performs TCP Reassembly, Threat verification (Header based checks, protocol decoders, content search, and regular expression matching). Also, action handling occurs here whether the packet is dropped, rate-limited, or rate-limited in the connection table.

- This section shows why traffic is going deep. Rx due to TCP sequence - If traffic cannot be reordered by K threads using loopy packet; it must go to Tier 4 for reordering. Trigger match - The percentage shows what traffic has matched a trigger. Rx is due to reroute – when a packet matches a trigger the following packets which belong to the same flow are required for threat verification.

- The “Ratio to next tier” is the percentage of traffic which matched a filter irrespective of Action Set.

Tuning is required if congestion is occurring or if a device is operating close to its maximum rated throughput. The deeper a flow is inspected the more processing is required, so the most performance gains can be attained by optimizing the KS threads at this level (Tiers 3 & 4). The three most process-intensive operations are:

1. IP Reassembly
2. Threat verification
3. TCP Packet reordering

**Note:** The `show np tier-stats` command will also display Stack and SSL information if the system is enabled for those functions.
Stack: Segment Ports

Note: The counter data only displays if the device is “stacked.”

-----------------------------------------------------------
Stack : Segment Ports
-----------------------------------------------------------
Segment Rx Mbps = 2.0 (25.4)
Segment Tx Mbps = 2.0 (25.4)
Stack Balance (A/B) = 22.3% (25.4)
  8400TX-1 Rx Mbps = 0.1 [0.9%]
  8400TX-2 Rx Mbps = 1.5 [6.7%]
Segment ratio to tier 1 = 11.1% [0.4%]

This inspection tier presents the total I/O module throughput for the network segment device as well as the receive rates from the I/O module to each stack member. When stacking is enabled, the following information is displayed:

- **Segment Rx Mbps** displays the aggregate received traffic from all network segments on this device.

- **Segment Tx Mbps** displays the aggregate traffic transmitted from all network segments on this device.

- **Stack Balance (A/B)** displays the load balance percentage, in which 100% equates to perfect balance across the number of devices in the stack. For devices that are Intrinsic HA L2FB, the Rx rate is zero, and this zero value is included in the load balance calculation. This statistic is similar to the A/B/C Balance percentage in Tier 1.

- **<host n> Rx Mbps** displays the traffic balanced from this device's network segments to the other devices in the stack. Note that the number of packets going through each host is flow based, so it is not uncommon to see a slight difference between them.

- **Segment ratio to tier 1** displays the percentage of traffic being inspected by this device as a ratio of the segment Rx traffic.
**Stack: Stack Ports**

**Note:** The counter data only displays if the device is “stacked.”

<table>
<thead>
<tr>
<th>Stack : Stack Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack Rx Mbps = 1.9 (6.7)</td>
</tr>
<tr>
<td>Stack Tx Mbps = 1.5 (15.8)</td>
</tr>
<tr>
<td>Stack Rx &gt; Stack Tx Mbps = 0.0 (0.0)</td>
</tr>
<tr>
<td>Stack Rx &gt; Seg Tx Mbps = 1.9 (6.7)</td>
</tr>
<tr>
<td>Stack Rx &gt; Tier 1 = 0.0 (0.0)</td>
</tr>
</tbody>
</table>

This inspection tier presents stacking port throughput, including through traffic and return traffic rates. When stacking is enabled, the following information is displayed:

- **Stack Rx Mbps** displays the aggregate received traffic from both stacking ports.
- **Stack Tx Mbps** displays the aggregate traffic that is transmitted from both stacking ports.
- **Stack Rx > Stack Tx** displays the total amount of transit, or through traffic on the stacking ports, for example, traffic received on Stack port 1 which is forwarded by the switch to stack port 2.
- **Stack Rx > Seg Tx** displays the amount of return traffic coming in on a stacking port that is returning to the outbound network segment.
- **Stack ratio to tier 1** displays the percentage of traffic being inspected by this device as a ratio of the stack Rx traffic.

**SSL Statistics**

**Note:** The following data only displays if the device is licensed for SSL.

<table>
<thead>
<tr>
<th>Tier 5:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Mbps = 0.0 (0.0)</td>
</tr>
<tr>
<td>Rx Packets/Sec = 0.0 (0.0)</td>
</tr>
<tr>
<td>Utilization = 0.0% (0.0%)</td>
</tr>
</tbody>
</table>
6.2. show np rule-stats

- Shows top 20 triggering filters, and whether they are successful

<table>
<thead>
<tr>
<th>Filter</th>
<th>Flows</th>
<th>Success</th>
<th>% Total</th>
<th>% Success</th>
</tr>
</thead>
<tbody>
<tr>
<td>4810</td>
<td>7722</td>
<td>0</td>
<td>13</td>
<td>0.00</td>
</tr>
<tr>
<td>2802</td>
<td>7722</td>
<td>0</td>
<td>13</td>
<td>0.00</td>
</tr>
<tr>
<td>2753</td>
<td>7722</td>
<td>0</td>
<td>13</td>
<td>0.00</td>
</tr>
<tr>
<td>2443</td>
<td>7722</td>
<td>0</td>
<td>13</td>
<td>0.00</td>
</tr>
<tr>
<td>2441</td>
<td>7722</td>
<td>0</td>
<td>13</td>
<td>0.00</td>
</tr>
<tr>
<td>2419</td>
<td>7722</td>
<td>0</td>
<td>13</td>
<td>0.00</td>
</tr>
<tr>
<td>2445</td>
<td>7722</td>
<td>0</td>
<td>13</td>
<td>0.00</td>
</tr>
<tr>
<td>1130</td>
<td>249</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>1129</td>
<td>249</td>
<td>249</td>
<td>0</td>
<td>100.00</td>
</tr>
<tr>
<td>1279</td>
<td>249</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>1287</td>
<td>249</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>1733</td>
<td>249</td>
<td>249</td>
<td>0</td>
<td>100.00</td>
</tr>
<tr>
<td>1117</td>
<td>249</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>2435</td>
<td>249</td>
<td>249</td>
<td>0</td>
<td>100.00</td>
</tr>
<tr>
<td>1109</td>
<td>249</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>1335</td>
<td>249</td>
<td>249</td>
<td>0</td>
<td>100.00</td>
</tr>
<tr>
<td>1079</td>
<td>249</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>2538</td>
<td>249</td>
<td>249</td>
<td>0</td>
<td>100.00</td>
</tr>
<tr>
<td>495</td>
<td>249</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>234</td>
<td>249</td>
<td>249</td>
<td>0</td>
<td>100.00</td>
</tr>
</tbody>
</table>

Total of 57540 flows

Pay close attention to filters that have a high percentage total but not percentage success. These filters are possible candidates to be disabled if optimization is required.

Any filter that has a success rate greater than 0% is matching against a filter. A success rate of 100% means each time a filter is triggered, a threat is found. These filters should not be disabled in this case. If you have an excessive amount of notifications changing this filter to block only will alleviate this issue. **Note:** To reset these counters, issue the `clear np rule-stats` command at the CLI.
### 6.3. `debug np congestionx`

This command shows where and how many packets dropped due to congestion since you last ran the command. Very useful for troubleshooting latency as it tells you where exactly in hardware is the congestion is occurring.

<table>
<thead>
<tr>
<th>Device</th>
<th>Bypassed</th>
<th>Dropped</th>
<th>Out of</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCOM</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FPGA Ingress</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NIC Ingress</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CPU Ingress</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CPU Egress</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NIC Egress</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FPGA Egress</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>F thread</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>K thread</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>L thread</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>L Held Descriptor Limit Drops</td>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>L Flow Queue Limit Drops</td>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>L Reroute Fail Drops</td>
<td></td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
6.4.  `debug np regex show average`

This CLI command outputs the maximum, average, and total microseconds of processing time required to perform threat verification by filter number. The output highlights the filters with the highest amount of time spent processing and therefore shows the filters that when disabled, would provide the greatest performance improvement to the inspection engine. For tuning, the focus of this output would be on filters with the highest values for Max and Avg. times.

“Evals” is a count of the number of times a filter triggered (initial, rough inspection) on tier 3 and “Matches” is a count of the number of those flows that matched the filter’s full inspection on tier 4. A filter with “Matches” could be left enabled since it has successfully provided network protection (in the case of a block action).

<table>
<thead>
<tr>
<th>Filter</th>
<th>CRC</th>
<th>Flag</th>
<th>Max(us)</th>
<th>Avg(us)</th>
<th>Evals</th>
<th>Matches</th>
<th>Total (us)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1109</td>
<td>0x18b5a170</td>
<td>R</td>
<td>30</td>
<td>18</td>
<td>17775</td>
<td>17775</td>
<td>313244</td>
</tr>
<tr>
<td>234</td>
<td>0xea960ed1</td>
<td>R</td>
<td>21</td>
<td>12</td>
<td>17775</td>
<td>17775</td>
<td>214347</td>
</tr>
<tr>
<td>1279</td>
<td>0x6671dd10</td>
<td>R</td>
<td>13</td>
<td>8</td>
<td>17775</td>
<td>17775</td>
<td>136034</td>
</tr>
<tr>
<td>1279</td>
<td>0xfd292919</td>
<td>R</td>
<td>12</td>
<td>7</td>
<td>17775</td>
<td>17775</td>
<td>120524</td>
</tr>
<tr>
<td>495</td>
<td>0x043cb005</td>
<td>R</td>
<td>6</td>
<td>2</td>
<td>17775</td>
<td>17775</td>
<td>43382</td>
</tr>
</tbody>
</table>

**Note:** To reset these counters issue the command:

`debug np regex clear` at the CLI
### 6.5. debug np port show

This command is useful in diagnosing issues with network connectivity to the TPS’ connected ports/segments.

**PORT status:**

Local Device 0 (switch in NORMAL mode)  
--- I/O Bay 1 --- 1Gx12 Copper ---

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Admin</th>
<th>Status</th>
<th>Speed/Duplex</th>
<th>AutoNeg</th>
<th>Mode</th>
<th>MTU</th>
<th>Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1A</td>
<td>1</td>
<td>Enabled</td>
<td>DOWN</td>
<td>auto</td>
<td>SGMII</td>
<td>9050</td>
<td>Copper</td>
</tr>
<tr>
<td>1-1B</td>
<td>2</td>
<td>Enabled</td>
<td>DOWN</td>
<td>auto</td>
<td>SGMII</td>
<td>9050</td>
<td>Copper</td>
</tr>
<tr>
<td>1-2A</td>
<td>3</td>
<td>Enabled</td>
<td>DOWN</td>
<td>auto</td>
<td>SGMII</td>
<td>9050</td>
<td>Copper</td>
</tr>
<tr>
<td>1-2B</td>
<td>4</td>
<td>Enabled</td>
<td>DOWN</td>
<td>auto</td>
<td>SGMII</td>
<td>9050</td>
<td>Copper</td>
</tr>
<tr>
<td>1-3A</td>
<td>5</td>
<td>Enabled</td>
<td>DOWN</td>
<td>auto</td>
<td>SGMII</td>
<td>9050</td>
<td>Copper</td>
</tr>
<tr>
<td>1-3B</td>
<td>6</td>
<td>Enabled</td>
<td>DOWN</td>
<td>auto</td>
<td>SGMII</td>
<td>9050</td>
<td>Copper</td>
</tr>
<tr>
<td>1-4A</td>
<td>7</td>
<td>Enabled</td>
<td>DOWN</td>
<td>auto</td>
<td>SGMII</td>
<td>9050</td>
<td>Copper</td>
</tr>
<tr>
<td>1-4B</td>
<td>8</td>
<td>Enabled</td>
<td>DOWN</td>
<td>auto</td>
<td>SGMII</td>
<td>9050</td>
<td>Copper</td>
</tr>
<tr>
<td>1-5A</td>
<td>9</td>
<td>Enabled</td>
<td>DOWN</td>
<td>auto</td>
<td>SGMII</td>
<td>9050</td>
<td>Copper</td>
</tr>
<tr>
<td>1-5B</td>
<td>10</td>
<td>Enabled</td>
<td>DOWN</td>
<td>auto</td>
<td>SGMII</td>
<td>9050</td>
<td>Copper</td>
</tr>
<tr>
<td>1-6A</td>
<td>11</td>
<td>Enabled</td>
<td>DOWN</td>
<td>auto</td>
<td>SGMII</td>
<td>9050</td>
<td>Copper</td>
</tr>
<tr>
<td>1-6B</td>
<td>12</td>
<td>Enabled</td>
<td>DOWN</td>
<td>auto</td>
<td>SGMII</td>
<td>9050</td>
<td>Copper</td>
</tr>
</tbody>
</table>

--- I/O Bay 2 --- 10Gx4 SR Bypass ---

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Admin</th>
<th>Status</th>
<th>Speed/Duplex</th>
<th>AutoNeg</th>
<th>Mode</th>
<th>MTU</th>
<th>Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-1A</td>
<td>13</td>
<td>Enabled</td>
<td>DOWN 10Gbps</td>
<td>none</td>
<td>XGMII</td>
<td>9050</td>
<td>*Fiber</td>
</tr>
<tr>
<td>2-1B</td>
<td>14</td>
<td>Enabled</td>
<td>DOWN 10Gbps</td>
<td>none</td>
<td>XGMII</td>
<td>9050</td>
<td>*Fiber</td>
</tr>
<tr>
<td>2-2A</td>
<td>15</td>
<td>Enabled</td>
<td>DOWN 10Gbps</td>
<td>none</td>
<td>XGMII</td>
<td>9050</td>
<td>*Fiber</td>
</tr>
<tr>
<td>2-2B</td>
<td>16</td>
<td>Enabled</td>
<td>DOWN 10Gbps</td>
<td>none</td>
<td>XGMII</td>
<td>9050</td>
<td>*Fiber</td>
</tr>
</tbody>
</table>

--- System Ports ---

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Admin</th>
<th>Status</th>
<th>Speed/Duplex</th>
<th>AutoNeg</th>
<th>Mode</th>
<th>MTU</th>
<th>Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>fpga0</td>
<td>50</td>
<td>Fpga-HG2</td>
<td>40Gbps full</td>
<td>none</td>
<td>XGMII</td>
<td>9070</td>
<td>Fiber</td>
</tr>
<tr>
<td>fpga1</td>
<td>51</td>
<td>Fpga-HG2</td>
<td>40Gbps full</td>
<td>none</td>
<td>XGMII</td>
<td>9070</td>
<td>Fiber</td>
</tr>
<tr>
<td>byp0</td>
<td>52</td>
<td>Fpga-BYP</td>
<td>40Gbps full</td>
<td>none</td>
<td>XGMII</td>
<td>9054</td>
<td>Fiber</td>
</tr>
<tr>
<td>byp1</td>
<td>53</td>
<td>SSL-uplk</td>
<td>40Gbps full</td>
<td>none</td>
<td>XGMII</td>
<td>9054</td>
<td>Fiber</td>
</tr>
<tr>
<td>sp0</td>
<td>54</td>
<td>Disabled</td>
<td>DOWN 40Gbps</td>
<td>none</td>
<td>XGMII</td>
<td>9070</td>
<td>Fiber</td>
</tr>
<tr>
<td>sp1</td>
<td>55</td>
<td>Disabled</td>
<td>DOWN 40Gbps</td>
<td>none</td>
<td>XGMII</td>
<td>9070</td>
<td>Fiber</td>
</tr>
</tbody>
</table>
6.6. **debug np port diags <port#>**

This command is useful in diagnosing issues with network connectivity to the TPS connected ports/segments.

<table>
<thead>
<tr>
<th>Port:</th>
<th>1-1A (uport 1; port 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MDIO bus:</td>
<td>4</td>
</tr>
<tr>
<td>PHY address:</td>
<td>0x01</td>
</tr>
<tr>
<td>Enable state:</td>
<td>Enabled</td>
</tr>
<tr>
<td>Link status:</td>
<td>DOWN</td>
</tr>
<tr>
<td>Laser status:</td>
<td>Linkscan mode: SW</td>
</tr>
<tr>
<td>Auto-negotiated:</td>
<td>(no link)</td>
</tr>
<tr>
<td>Port ability:</td>
<td>fd = 10MB,100MB,1000MB</td>
</tr>
<tr>
<td></td>
<td>hd = &lt;none&gt;</td>
</tr>
<tr>
<td></td>
<td>intf = mii,gmii,sgmii</td>
</tr>
<tr>
<td></td>
<td>medium = &lt;none&gt;</td>
</tr>
<tr>
<td></td>
<td>pause = pause_tx,pause_rx,pause_asym</td>
</tr>
<tr>
<td></td>
<td>lb = none,MAC,PHY</td>
</tr>
<tr>
<td></td>
<td>flags = autoneg</td>
</tr>
<tr>
<td>Advertised ability:</td>
<td>fd = 10MB,100MB,1000MB</td>
</tr>
<tr>
<td></td>
<td>hd = &lt;none&gt;</td>
</tr>
<tr>
<td></td>
<td>intf = &lt;none&gt;</td>
</tr>
<tr>
<td></td>
<td>medium = &lt;none&gt;</td>
</tr>
<tr>
<td></td>
<td>pause = &lt;none&gt;</td>
</tr>
<tr>
<td></td>
<td>lb = &lt;none&gt;</td>
</tr>
<tr>
<td></td>
<td>flags = &lt;none&gt;</td>
</tr>
<tr>
<td>STP mode:</td>
<td>Forward</td>
</tr>
<tr>
<td>Learn mode:</td>
<td>FWD</td>
</tr>
<tr>
<td>Untag priority mask:</td>
<td>0</td>
</tr>
<tr>
<td>Multicast flood (pfm):</td>
<td>FloodNone</td>
</tr>
<tr>
<td>Interface:</td>
<td>SGMII</td>
</tr>
<tr>
<td>Phy master mode:</td>
<td>Auto</td>
</tr>
<tr>
<td>Max_frame size:</td>
<td>9050</td>
</tr>
<tr>
<td>MDIX mode:</td>
<td>Auto, Xover</td>
</tr>
<tr>
<td>Medium:</td>
<td>Copper</td>
</tr>
</tbody>
</table>