© Copyright 2020 Trend Micro.

Trend Micro Incorporated ("Trend Micro") makes no warranty of any kind with regard to 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 set forth 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. Intrusion Prevention System (IPS) ........................................................................................................ 6
   2.1. Architecture and Background Information .......................................................................................... 6
   2.2. NX-Platform Engine Enhancements ..................................................................................................... 6
      2.2.1. Threat Digital Vaccine (ThreatDV) .................................................................................................. 7
   2.3. IPS System Architecture ......................................................................................................................... 7
      2.3.1. TSE Connection Table – Blocked Streams ....................................................................................... 8
      2.3.2. TSE Connection Table Timeout ........................................................................................................ 8
      2.3.3. TSE Asymmetric/Symmetric Mode .................................................................................................... 8
      2.3.4. TSE Adaptive Filtering .................................................................................................................... 9
      2.3.5. TSE Adaptive Aggregation ............................................................................................................. 9
   2.4. VLAN Translation ................................................................................................................................... 10
   2.5. IPS Elements .......................................................................................................................................... 10
      2.5.1. Filtering Concepts ............................................................................................................................. 10
      2.5.2. Filter Precedence ............................................................................................................................. 11
      2.5.3. Flow Inspection Filters ..................................................................................................................... 11
      2.5.4. Trust as an Action Set ...................................................................................................................... 11
      2.5.4.1. Traffic Management Filters ......................................................................................................... 11
      2.5.4.2. Flow Management Filters ........................................................................................................... 13
   2.6. IPS Deployment Considerations ............................................................................................................... 14
      2.6.1. Deployment Guidelines ................................................................................................................... 14
      2.6.2. IPS Positioning ................................................................................................................................... 14
      2.6.3. Physical Connections ........................................................................................................................ 15
      2.6.4. Cabling Requirements ..................................................................................................................... 15
      2.6.5. Transparent High Availability (TRHA) ............................................................................................ 16
   2.7. NX Modules .......................................................................................................................................... 17
      2.7.1. Standard Modules ............................................................................................................................ 17
      2.7.2. Bypass Modules ............................................................................................................................... 18
      2.7.3. I/O Modules General Information .................................................................................................. 19
      2.7.4. I/O Module Hot-Swapping Guidelines ............................................................................................ 20
      2.7.5. What happens when modules are swapped? .................................................................................. 21
      2.7.6. Fiber-Optic Connection ................................................................................................................... 22
   2.8. Stacking ................................................................................................................................................... 23
   2.9. Intrusion Detection System (IDS) ......................................................................................................... 25
   2.10. System Administration ......................................................................................................................... 26
      2.10.1. IPS Management port .................................................................................................................... 26
      2.10.1.1. Reports available via the Local Security Manager (LSM) ................................................................ 27
      2.10.2. IPS Security Levels ....................................................................................................................... 28
      2.10.3. How to Recover the IPS SuperUser Password? ........................................................................... 29
      2.10.4. How to Reset an IPS to Factory Settings? ..................................................................................... 30
      2.10.5. How to Turn Off SMS Management on the IPS ........................................................................... 30
      2.10.6. What are Inspection Bypass rules? ............................................................................................... 31
4.4. debug np congestionx ............................................................................................................................ 51
4.3. debug np rule-stats .................................................................................................................................. 50
4.2. show np rule-stats .................................................................................................................................. 46
4.1. show np tier-stats .................................................................................................................................... 46
3.2. NX Platform IPS at a glance .................................................................................................................... 42
3.1. System Architecture ................................................................................................................................. 43
3. Power Information ....................................................................................................................................... 42
2.1. System Architecture ............................................................................................................................... 43
2.2. NX Platform IPS at a glance .................................................................................................................... 42
2.1. Power Information ....................................................................................................................................... 42
2. NX-Platform System descriptions ......................................................................................................... 42
1. System Architecture .................................................................................................................................. 43

LIST OF TABLES

Table 2-1: NX-Platform Standard Modules .................................................................................................. 17
Table 2-2: NX-Platform Bypass Modules .................................................................................................... 18
Table 4-4: NX-Series Approved Interfaces .................................................................................................. 22
Table 2-4: NX-Platform Security Levels and Password Requirements ....................................................... 28
Table 2-5: Inspection-Bypass CLI Commands .............................................................................................. 31
Table 2-6: NX-Platform Configuration Parameters ..................................................................................... 38
Table 3-1: NX-Platform IPS System ............................................................................................................ 42

LIST OF FIGURES

Figure 2-1: TRHA Configuration .................................................................................................................. 16
Figure 2-2: NX-Platform resilient stack configuration ................................................................................. 24
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-3</td>
<td>Logging Mode Settings</td>
<td>34</td>
</tr>
<tr>
<td>2-4</td>
<td>Link-Down Synchronization</td>
<td>35</td>
</tr>
<tr>
<td>2-5</td>
<td>Intrinsic Network HA</td>
<td>35</td>
</tr>
<tr>
<td>2-6</td>
<td>Intrinsic Network HA (LSM)</td>
<td>36</td>
</tr>
</tbody>
</table>
1. Introduction

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

2. Intrusion Prevention System (IPS)

2.1. Architecture and Background Information

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

- Inline - All traffic passes through the IPS making blocking possible and minimizing latency.
- High availability – the IPS must be very stable and continue to perform even under increased traffic volumes.
- Accuracy – the IPS must accurately detect attacks. It must be able to filter out just the attack traffic and leave innocuous traffic through without issue. Conversely, the IPS cannot have false negatives otherwise attacks will get through.
- Usability – The IPS 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 a very powerful architecture consisting of both custom hardware and software elements. This section describes the architecture and the key functions and features implemented.

2.2. NX-Platform Engine Enhancements

The following enhancements have been made to the NX-Platform architecture:

- IPv6 inspection
- Jumbo frame packet inspection for frames up to 9234 bytes. This includes 14 bytes of Ethernet header, 9216 bytes of payload data (including tunneling encapsulations if any) and 4 bytes of FCS.
- Inspection of tunneled traffic
  - GRE
  - Mobile IPv4 (IP-in-IP)
  - IPv6 (6-in-4, 4-in-6, 6-in-6)
  - Authentication Header (AH) tunnels
  - Arbitrary tunnel nesting up to 10 tunnels deep (or max header size)
  - GPRS
  - GTP-U (v1) only – GTP-C and GTP is not supported. No ability to support TCP resets or quarantine on GTP packets.
- Traffic Normalization filters work on all inspected traffic
• Inspection Bypass Rules.
  \textbf{Note:} The NX-Platform IPS devices (2600NX, 5200NX, 6200NX, 7100NX and 7500NX) support up to a maximum of 8 rules per device.
• Most filters will work on both IPv4 and IPv6 traffic (unless specified e.g. IPv6 only)
• Best Effort Mode
• Trust as an Action
• SYN Proxy
• VLAN Translation

\subsection{2.2.1. Threat Digital Vaccine (ThreatDV)}

Reputation Feed (formerly known as RepDV) is now part of the Threat Digital Vaccine (ThreatDV) product, which is a premium subscription service that includes both the reputation database and the new Malware Filter Package.

The Reputation Feed identifies and delivers suspect IPv4, IPv6 and Domain Name System (DNS) security intelligence feeds from a multi-vendor, global reputation database so that customers can actively enforce and manage reputation security policies using the TippingPoint Next Generation Intrusion Prevention System (NGIPS) Platform. The addresses are tagged with reputation, geographic, and other identifiers for ready and easy security policy creation and management. The Reputation Feed provides the addresses and tags multiple times a day (two hours on average) in the same manner as standard Digital Vaccines.

\subsection{2.3. IPS System Architecture}

The TippingPoint IPS’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 re-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 IPS. A flow is uniquely identified by the port on which it was received and its packet header information, referred to as the “\textit{flow-tuple}”:\begin{itemize}
\item IP protocol (ICMP, TCP, UDP, other)
\item Source IP address
\item Source ports (TCP or UDP)
\item Destination IP address
\item Destination ports (TCP or UDP)
\item VLAN ID
\end{itemize}

Once classified, each packet is inspected by the appropriate set of protocol and application filters. The IPS 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.

2.3.1. TSE Connection Table – Blocked Streams

All packets received by the IPS 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.

2.3.2. 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 IPS 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.

2.3.3. 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 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 IPS filters are flow based (meaning state kept per flow versus per session), attacks are detected in either send or receive directions.

By default, the IPS is shipped with Asymmetric mode enabled. This means that the IPS only sees one side of the TCP connection. When using Advanced Distributed Denial of Service (DDoS)
protection filters, you must place the IPS 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 IPS 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 nameservers, 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 NX-Platform IPS devices only support **SYN Proxy**. In order 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 be proxied to the protected server.

### 2.3.4. TSE Adaptive Filtering

The IPS Adaptive Filtering feature is designed to protect the IPS from poorly performing filters. When the IPS 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 IPS will initiate AFC on that filter.

• **When a Filter is creating congestion and not firing.** It is possible that the traffic is passing certain filters’ early inspection functions but failing the later inspection functions. If the IPS is experiencing continued congestion, the recommendation is to look for these filters and consider disabling them. See the **Filtering Concepts** section, for more information on the different filtering mechanisms within the IPS.

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.

### 2.3.5. 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 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.

### 2.4. VLAN Translation

The NX-Platform IPS is 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.

- Support “IPS on a Stick” with Commercial Off the Shelf (COTS) Switches
- 96 VLAN translations (192 bidirectional VLAN pairs)
- Increase port density options by leveraging switches as port aggregation point
- Only supports policy by VLAN as received by IPS
- All policy, security, events, etc. happen on ingress VLAN id only
  - VLAN Translation will strip all VLAN tags and inspect the traffic payload, once inspection is completed, all VLAN tags will be reinserted except the outer most VLAN tag will be change 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 IPS won’t be able to translate the return traffic
- Command Line interface
  - `conf t vlan-translation add <port> <ingress-vlan> <egress-vlan> [-both-directions]`
  - `conf t vlan-translation remove <port> <ingress-vlan>`

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

### 2.5. IPS Elements

#### 2.5.1. Filtering Concepts

The IPS 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.
2.5.2. Filter Precedence

The IPS processes filter in the following order of precedence;
1. Inspection Bypass Rules
2. Traffic Management Filters
3. RepDV
4. Quarantine
5. Digital Vaccine filters

2.5.3. Flow Inspection Filters

The flow inspection filters are the most common type of filter used by the IPS. 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 in order for the filter to “fire.”

2.5.4. 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 IPS uninspected until the trusted stream times out (default 30 minutes). Trusted streams are also shared with the partner IPS in a TRHA configuration.

2.5.4.1. 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 IPS 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 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 IPS (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 IPS. They may generate very large packets, which are fragmented at the IP layer. The IPS 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 throughput of this application.

**Note:** As indicated above, a TMF filter set to trust will cause the IPS 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.

**2.5.4.2. 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 afterwards will follow the TMF recommendations for trust.

Flow Management Filters are available on the N-Platform (660N, 1400N, 2500N, 5100N, 6100N), the NX-Platform (2600NX, 5200NX, 6200NX, 7100NX, 7500NX) and the S-Series (S10, S110, S330; running TOS v3.2.2+) IPS devices. Only one TCP and/or one UDP filter should be enabled.

<table>
<thead>
<tr>
<th>Flow Management Filters</th>
<th>TCP Flow Management</th>
<th>UDP Flow Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>7620</td>
<td>(5MB)</td>
<td>(5MB)</td>
</tr>
<tr>
<td>7621</td>
<td>(10MB)</td>
<td>(10MB)</td>
</tr>
<tr>
<td>7622</td>
<td>(100MB)</td>
<td>(100MB)</td>
</tr>
<tr>
<td>7623</td>
<td>(500MB)</td>
<td>(500MB)</td>
</tr>
<tr>
<td>7624</td>
<td></td>
<td>(5MB)</td>
</tr>
<tr>
<td>7625</td>
<td></td>
<td>(10MB)</td>
</tr>
<tr>
<td>7626</td>
<td></td>
<td>(100MB)</td>
</tr>
<tr>
<td>7627</td>
<td></td>
<td>(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:** via TRUSTED STREAMS table via the Devices->"IPS"->Events->Trusted Streams tab
2. **LSM:** via Events->Managed Streams->Trusted Streams

### 2.6. IPS Deployment Considerations

#### 2.6.1. Deployment Guidelines

The TippingPoint IPS 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, baseline configuration of an SMS or IPS 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 IPS configuration parameters.

#### 2.6.2. IPS Positioning

The most common IPS deployment is at the customer network perimeter, which is those links connecting the customer network to the Internet. Although the IPS 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 IPS. With the introduction of the NX-Platform 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 IPS protection if one unit is bypassed for maintenance. In most cases user traffic can pass through as many as three IPS’s before any cumulative latency is noticed.
2.6.3. Physical Connections

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

2.6.4. Cabling Requirements

The IPS ships with the following cables:

• Two (2) AC power cables for the redundant power supplies
• Serial cable (RJ45, DB-9 FM) for (COM) port
2.6.5. Transparent High Availability (TRHA)

TRHA is a redundancy option for two IPS devices installed on parallel network paths. TRHA requires configuring two IPS devices with the same TRHA settings. Enabling this option configures the IPSs 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 IPS, causes network traffic to be routed to the IPS on the redundant path.

Note: Both IPS devices must be from the same product family and running the same TOS version.

What is shared between TRHA pairs?
- Blocked flows
- Rate limited flows
- Quarantined flows
- SYN proxy sequence number

What isn’t shared?
- TCP state
- TCP reassembly information
- Information about flows that aren’t being blocked or rate limited.

Figure 2-1: TRHA Configuration
2.7.  NX Modules

2.7.1.  Standard Modules

The NX-Platform IPS support up to four I/O modules, which enable the user to customize the device to suit the needs of the network. Each NX 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 2-1: NX-Platform Standard Modules

<table>
<thead>
<tr>
<th>Description</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>6-Segment Gig-T NX (Gig-T)</td>
<td>JC768A / TPNN0059</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>6-Segment GbE SFP NX (SFP)</td>
<td>JC769A / TPNN0068</td>
</tr>
<tr>
<td>Ports: 12 SFP ports</td>
<td></td>
</tr>
<tr>
<td>Port speed: 1 Gbps</td>
<td></td>
</tr>
<tr>
<td>4-Segment 10GbE SFP+ NX (SFP+)</td>
<td>JC770A / TPNN0060</td>
</tr>
<tr>
<td>Ports: 8 Fiber SFP+ ports</td>
<td></td>
</tr>
<tr>
<td>Port speed: 10 Gbps</td>
<td></td>
</tr>
<tr>
<td>1-Segment 40 GbE QSFP+ NX (QSFP+)</td>
<td>JC771A / TPNN0069</td>
</tr>
<tr>
<td>Ports: 2 Fiber QSFP+ ports</td>
<td></td>
</tr>
<tr>
<td>Port speed: 40 Gbps</td>
<td></td>
</tr>
</tbody>
</table>
### 2.7.2. Bypass Modules

The NX-Platform IPS support a range of Bypass I/O Modules (BIOMs), which combine the IPS segment interfaces with mechanical bypass switches for high-availability purposes. The BIOMs offered for the NX-Platform support various interface speed and connectivity types, including copper or fiber (1Gbps) or fiber (10Gbps). Fiber modules are available with either long range or short range transceivers.

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

#### Table 2-2: NX-Platform Bypass Modules

<table>
<thead>
<tr>
<th>Description</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>NX IPS 4-Segment Gig-T Bypass Module</td>
<td>JC877A / TPNN0070</td>
</tr>
<tr>
<td>Ports: 8 copper ports</td>
<td></td>
</tr>
<tr>
<td>Port speed: 10/100/1000 Mbps</td>
<td></td>
</tr>
<tr>
<td>NX IPS 2-Segment 1G Fiber SR</td>
<td>JC878 / TPNN0071</td>
</tr>
<tr>
<td>Ports: 4 Multi-Mode (LC type)</td>
<td></td>
</tr>
<tr>
<td>Port speed: 1 Gbps</td>
<td></td>
</tr>
<tr>
<td>NX IPS 2-Segment 1G Fiber LR Bypass Module</td>
<td>JC879A / TPNN0072</td>
</tr>
<tr>
<td>Ports: 4 Single-Mode Fiber (LC type)</td>
<td></td>
</tr>
<tr>
<td>Port speed: 1 Gbps</td>
<td></td>
</tr>
<tr>
<td>NX IPS 2-Segment 10G Fiber SR</td>
<td>JC880A / TPNN0073</td>
</tr>
<tr>
<td>Ports: 4 Multi-Mode Fiber (LC type)</td>
<td></td>
</tr>
<tr>
<td>Port speed: 1/10 Gbps</td>
<td></td>
</tr>
<tr>
<td>NX IPS 2-Segment 10G Fiber LR Bypass Module</td>
<td>JC881A / TPNN0074</td>
</tr>
<tr>
<td>Ports: 4 Multi-Mode Single-Mode Fiber (LC type)</td>
<td></td>
</tr>
<tr>
<td>Port speed: 1/10 Gbps</td>
<td></td>
</tr>
</tbody>
</table>
2.7.3. I/O Modules General Information

- Running “show-mfg” from the NX Command Line Interface (CLI) will display the model number of the modules (bypass or otherwise) 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.

- Hot-swapping I/O modules on the NX-Platform devices is only supported with TOS v3.6.0 or higher. Hot-swapping modules without adverse reactions, only works by swapping like-for-like I/O modules in the same slot.

- Hot-swapping I/O modules on the NX-Platform running TOS v3.5.x is not supported. If you must remove and replace an NX I/O module, shut down the system, replace the module and re-start the system.

- Bypass modules are only compatible with the NX-Platform IPS devices running TOS v3.6.0 and higher.

- 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 NX-Platform 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 electro mechanical 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. This should be done in order to ensure that no cabling mistakes have occurred.

- For more information about deploying NX I/O modules, refer to the TippingPoint NX-Platform Hardware Installation and Safety Guide.
2.7.4. I/O 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 IPS 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 or Absent) and availability state (Available or 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 IPS 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 network port
2.7.5. 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 may 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
2.7.6. Fiber-Optic Connection

The IPS 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 NX-Platform devices:

**Table 2-3: NX-Series Approved Interfaces**

<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>
2.8. Stacking

The TOS v3.9.0, has introduced a new feature for the NX-Platform 7100NX or 7500NX IPS devices called stacking. Stacking enables you to increase the overall inspection capacity of your TippingPoint Intrusion Prevention System (IPS) by grouping multiple NX-Platform devices and pooling their resources. You can configure up to five NX-Platform devices in a stack. The stack operates as a single device that you manage on the TippingPoint Security Management System (SMS). In-line inspection capacity increases with each device that you add to the stack. Stacking support allows for a higher inspection throughput.

- Increased inspection capacity for 7100NX (30Gb-75Gb)
- Increased inspection capacity for 7500NX (40Gb-100Gb)

Stacking requirements

- TippingPoint 7100NX or 7500NX device (each member of the stack must be the same model).
- One TippingPoint 40 GbE QSFP+ I/O module for each device (installed in slot 4).
- One TippingPoint 40G QSFP+ Active Optical Cable (AOC) for each device. **Note:** 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 module.
- TOS v3.9.0, or later installed on all devices.
- SMS v4.5.0, or later.

Important Notes

- Prior to installing TOS v3.9.0 for the purpose of stacking, you must perform a factory reset.
- The same Digital Vaccine must be distributed to all devices in the stack, failure to do this will result in errors from the stack.
- The I/O modules should be installed 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 do install additional I/O modules on the other devices in the stack, they must match the I/O modules in the network segment device and they can only be used for the same network (redundancy).
Figure 2-2: NX-Platform resilient stack configuration
2.9. Intrusion Detection System (IDS)

When Intrusion Detection System (IDS) mode is enabled, it adjusts the IPS device configuration such that the IPS 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 IPS device "Segment A" to network device
3. Enable IDS mode;
   a. **On the LSM;** IDS mode is enabled on the IPS Preferences page (IPS ➞ Preferences) under the Configure Threat Suppression Engine section. When IDS Mode settings are changed, the device must be rebooted for the change to take effect.
   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 windows will pop-up and in this window choose TSE Settings on the left. On the right side click the IDS Mode check box and press OK to continue. Once again this will require a reboot.

**Note 1:** Using the IPS device in a mixed configuration is not supported. If the IPS device will be used in an IDS configuration, then it is an IDS device. Use the IPS as either IDS or IPS device but not both. Attempting to run in mixed mode will lead to performance issues.

**Note 2:** 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 physically copy packets onto the mirrored port. 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.
2.10. System Administration

2.10.1. IPS Management port

TippingPoint recommends configuring the management port on the IPS to use a non-routed IP address from the RFC-1918 Private Address space. This helps to prevent 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 IPS. Host IP filters are essentially ACLs on the management port of the IPS.

When the IPS is initially configured, the default security policy is set to permit any. 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 IPS must not be under SMS control when doing this. If the device is currently managed, you may use the CLI command conf t no sms to temporarily unmanage the IPS. To resume SMS management, use the CLI command conf t sms.

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

```
conf t host ip-filter (permit | deny) ip
```

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

```
conf t host ip-filter permit ip 192.168.10.45/24
```

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:

```
conf t host ip-filter permit ip 192.168.10.0/24
```

To reverse the effect of the previous command, issue the following command:
conf t host no ip-filter permit ip 192.168.0.24

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

conf t host ip-filter permit any ip

To view current ip-filters, use the show host -details CLI command:

#show host -details

IP Address           Action      # Hits
==================== ====== =========
192.168.10.45        permit      38

2.10.1.1. Reports available via the Local Security Manager (LSM)

The IPS itself has basic reporting capabilities via the LSM interface. Apart from the top level display that shows the number of attacks by severity, there are several useful displays for indicating general information such as relative amounts of TCP/UDP/ICMP as well as specific security reports.

The following are the types of reports available via the LSM.

- Filter Matches
- Rate Limits
- Traffic
  - Transmission Type (Unicast, Broadcast, Multicast, etc.)
    - Traffic Profile by Transmission Type (Unicast, Multicast, Broadcast)
      - This report can be very useful when troubleshooting – if you see a disproportionate amount of multicast and broadcast traffic, you may find that you are just seeing router control traffic, such as OSPF or EIGRP multicast HELLO traffic, RIP updates or Cisco discovery protocol (CDP).
  - Protocol (ICMP, UDP, TCP, etc.)
  - Frame Size
    - Traffic Profile by Frame Size - According to CAIDA (http://www.caida.org/) the average packet size on the Internet is very small, in part due to the dominance of TCP traffic, which generates a
large number of very small packets (e.g. SYN and SYN+ACK for the connection establishment). In a real network with a reasonable amount of HTTP and FTP, the number of large packets will be substantial. If only small packets are present, there is usually something wrong. The NX-Platform tracks jumbo packets as well.

- Port (traffic by segment)
  - DDoS
  - Quarantine
  - Adaptive Filter
  - 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.

### 2.10.2, IPS Security 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 IPS:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 0 – Low/No Security</td>
<td>• A password does NOT have to be defined. If you choose to define a password, any length and format is allowed. A password can NOT contain spaces.</td>
</tr>
<tr>
<td>Level 1 - Medium Security</td>
<td>• Passwords must contain at least 8 characters without spaces.</td>
</tr>
</tbody>
</table>
| Level 2 - High Security (default) | • Passwords must contain at least 8 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. A non-alphanumeric character includes any character that is not a digit or a letter. Do not use spaces in the password. |
2.10.3. How to Recover the IPS SuperUser Password?

Q: Can you recover a SuperUser lost password?

A: You cannot recover the SuperUser password of an IPS, but you can reset it to a new value or create a new login with SuperUser privileges.

Note: This procedure requires a reboot operation which will disrupt traffic!

1. Connect to the IPS via the console port. The serial port connection settings are as follows:  
   Speed: **115200** - Databits: **8** - Parity: **None** - Stop bits: **1**

2. Reboot the IPS.

3. After the IPS completes its initial startup screens the TippingPoint splash screen is displayed in ASCII characters. You should see something similar to the following:

   Initialize Audit log....................[OK]
   Initialize Block Log....................[OK]
   Initialize Alert Log....................[OK]
   Initialize SNMP.........................[OK]
   Initialize Email.........................[OK]
   Initialize Remote Syslog...............[OK]
   Validating Certificate...............[OK]

   ____________________________________________________________________________
   Loading . . .

   TippingPoint Technologies, Inc.

   TippingPoint - Austin, Texas, USA - www.tippingpoint.com
   TOS Version     : X.X.X.XXXX      Build  : XXX XX XXXX, XX:XX:XX
   Digital Vaccine : X.X.X.XXXX      Serial : X-XXXX-XXXX-XXXX
   Hardware Rev    : X

4. Type the word **mkey** (lower case) within 3 seconds of seeing the word "Loading."

   Note: If you don't type **mkey** before the three dots "..." appear after the word "Loading" you will have to restart and try again.

5. If you were successful, then you will be prompted to specify the security level for the initial “SuperUser” account and password creation.

6. Enter the desired username for the SuperUser account.
**Note:** If you use the existing SuperUser account user name, you will be resetting the previous password for that user. If you use a different user name you will be creating a new super-user account.

7. Enter your new password. Once the new username and password has been accepted, the IPS will complete the boot process and you will be able to login to the IPS with the new credentials.

### 2.10.4. How to Reset an IPS to Factory Settings?

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

Be aware that the IPS will revert to the original TOS shipped with the device and that the Digital Vaccines (DV$s) 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.

In order to factory reset your IPS enter the following command at the CLI interface;

```
dump factory-reset
```

### 2.10.5. How to Turn Off SMS Management on the IPS

Issue the following command at the command line:

```
configure terminal no sms
```

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

```
configure terminal sms
```

You can also turn SMS management on or off by using the LSM via **Configure ➔ NMS Management**.

After the IPS is managed by an SMS, you can view the SMS information from the CLI of the IPS. 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.
What are Inspection Bypass rules?

An Inspection Bypass rule is a feature available in the NX-Platform (2600NX, 5200NX, 6200NX, 7100NX and 7500NX) IPS devices. This feature enables administrators to configure rules that in effect will allow traffic to bypass the IPS inspection engine. Any traffic that matches an inspection bypass rule is directed through the IPS without further inspection. In addition, traffic that is passed with an inspection bypass rules do 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
- IPS Port Number
- Protocol Port Number
- Tunneling Traffic

The NX-Platform IPS devices support up to a maximum of 8 inspection bypass rules per device.

The `conf inspection-bypass` CLI command is used to manage inspection bypass rules. The rules are identified by an ID number that is generated by the IPS when the rule is created with the `conf inspection-bypass add` command. You can view a list of current inspection bypass rules with the `show inspection-bypass` command.

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

**Parameters:** The `conf inspection-bypass` command uses the following parameters:

<table>
<thead>
<tr>
<th>Subcommand</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Adds an inspection bypass rule.</td>
<td><code>conf inspection-bypass add</code></td>
</tr>
<tr>
<td>clear-stats</td>
<td>Clears statistics associated with an inspection bypass rule.</td>
<td><code>conf inspection-bypass clearstats &lt;rule_ID&gt;</code></td>
</tr>
<tr>
<td>Enable</td>
<td>Enables an inspection bypass rule.</td>
<td><code>conf inspection-bypass enable &lt;rule_ID&gt;</code></td>
</tr>
<tr>
<td>disable</td>
<td>Disables an inspection bypass rule.</td>
<td><code>conf inspection-bypass disable &lt;rule_ID&gt;</code></td>
</tr>
<tr>
<td>remove</td>
<td>Removes an inspection bypass rule.</td>
<td><code>conf inspection-bypass remove &lt;rule_ID&gt;</code></td>
</tr>
</tbody>
</table>

**Note:** Inspection Bypass rules can also be configured via the Security Management System (SMS).
2.10.7. System Upgrades

Hitless upgrades are available for the NX-Platform (2600NX, 5200NX, 6200NX, 7100NX and 7500NX). To completely reboot or do a full reboot, non-hitless, type the following at the CLI:

*IPS*# 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 time period in which the TOS file was generated.

2.10.8. Traces and Email Notifications

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

2.10.9. Maximum Frame Sizes

NX-Platform devices (2600NX, 5200NX, 6200NX, 7100NX and 7500NX) support 1548 bytes’ frame inspection with jumbo frame inspection (up to 9234 bytes).

2.10.10. Compact Flash

The NX-Platform ships with a pre-formatted external variant of a compact flash (Cfast) and an internal compact flash. The external compact flash is inserted in the front of the NX-Platform IPS. Only approved Compact Flash cards are supported by TippingPoint.

The compact flash card is used to store system logs, snapshots, packet traces, and other system data. The user can remove and insert the compact flash card while the device is running; however, the user must ensure to issue the appropriate command from the Command Line Interface (CLI). The device will continue to perform correctly if the compact flash card is not available.

2.10.10.1. External Compact Flash Commands

Remove media command: *compact-flash unmount*

Format new (blank) media command: *compact-flash format*

The IPS will automatically mount the newly formatted media

Authenticate mode
Enable command:

```
conf t compact-flash operation-mode authenticate
```

Must be super-user in order to mount compact flash media

Mount new media command:

```
compact-flash mount
```

If no external compact flash is present, the IPS can still capture packet traces by storing them on the internal compact flash by issuing the following command:

```
depug mod ini-cfg user Flogger PACKET_CAPTURE_DRIVE SYSTEM
```

### 2.10.10.2. Internal Compact Flash

To maximize reliability no periodic data will be written to the internal compact flash. The following are the only writes that are allowed:
- TOS and DV updates
- Configuration settings (INI and filter)

### 2.10.11. Performance Protection (Logging Mode)

During high traffic inspection timeframes, the IPS 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
2.10.12. Link-Down Synchronization

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.

**Figure 2-4: Link-Down Synchronization**

**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.

**2.10.13. Intrinsic Network High Availability (HA)**

Intrinsic HA, also known as “Layer 2 Fallback” (L2FB), is a mode wherein the IPS 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 2-5: Intrinsic Network HA**

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 IPS
manually in L2FB is a useful tool for troubleshooting by ruling out the IPS as the device causing the issue (or not).

![Intrinsic Network HA (LSM)](image)

**Figure 2-6: Intrinsic Network HA (LSM)**

**Note:** L2FB only functions as long as the IPS 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.

In order to do this from the Command Line Interface (CLI) it will be necessary to take the IPS out of SMS control. Otherwise this can be controlled through the SMS. The command to initiate L2FB is:

```
IPS# high-availability force fallback
```

Typing in:

```
IPS# show high
```

This will display the current HA state of the box.
2.10.14. IPS System Backup (Snapshot)

Best practice calls for snapshots to be created each time the IPS 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 compact flash, so ensure that your flash card is installed.

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 places, a copy on the IPS device. Archiving a snapshot places, a copy on the SMS. Deleting a snapshot removes the system snapshot from the device and, if present, the snapshot on the SMS. Snapshots for NX-Platform devices 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 IPS, 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.

2.10.15. Scan/Sweep Filters

The NX-Platform 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 traffic that undergoes IPS 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:** Prior to 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 a number of servers will actually 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**.

### 2.10.16. Configuration Parameters

**Table 2-6: NX-Platform Configuration Parameters**

<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Default</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td></td>
<td>Use names consistent with customer network naming standards and practices.</td>
</tr>
<tr>
<td>Location</td>
<td></td>
<td>Use this to identify where the IPS is located. For large deployments, this may identify the rack and position.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Assigned by TippingPoint</td>
<td></td>
</tr>
<tr>
<td>Model</td>
<td></td>
<td>Ensure model supports required throughput.</td>
</tr>
<tr>
<td><strong>Management Interface</strong></td>
<td></td>
<td>If the management network is not isolated from the general user population, consider using “host ip filters” to restrict access. These are described in a later section.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the IPS’s management port.</td>
<td>Must be reachable by the SMS. Can either be IPv6, IPv4 address or both.</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>Mask for the IPS’s management port IP address</td>
<td></td>
</tr>
<tr>
<td>Gateway</td>
<td>IP address of the default gateway for the IPS management port.</td>
<td></td>
</tr>
<tr>
<td>DNS 1</td>
<td>IP address of a DNS server.</td>
<td></td>
</tr>
<tr>
<td>DNS 2</td>
<td>IP address of a DNS server.</td>
<td></td>
</tr>
<tr>
<td>DNS Domain</td>
<td>Required when using DNS (according to SMS)</td>
<td></td>
</tr>
<tr>
<td>Time Zone</td>
<td>Time zone in which the IPS is located</td>
<td></td>
</tr>
<tr>
<td>SNTP Primary</td>
<td>Time server IP address.</td>
<td>If the IPS is managed by an SMS, then the SMS will serve as the IPS’s time server.</td>
</tr>
<tr>
<td>SNTP Secondary</td>
<td>IP address of a secondary time server</td>
<td></td>
</tr>
<tr>
<td>Audit Log Syslog</td>
<td>The IPS may be configured to send its audit log to a remote Syslog server. Be sure to configure the remote Syslog server appropriately.</td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Log Syslog</td>
<td>The IPS may be configured to send its system log to a remote Syslog server. Be sure to configure the remote Syslog server appropriately.</td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 2-6: NX-Platform Configuration Parameters

<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Default</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Management System</td>
<td></td>
<td>The IPS may be configured to send SNMP traps to a network management system.</td>
</tr>
<tr>
<td>Community String</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trap IP Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trap Port</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email Server</td>
<td></td>
<td>The IPS may be configured to send email notification that a filter has fired. This feature should be used sparingly.</td>
</tr>
<tr>
<td>Default &quot;To&quot; address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>From email address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>From email domain</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMTP server IP address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transparent HA partner IP Address</td>
<td></td>
<td>This is the IPS address of the IPS that will be used in the transparent HA configuration.</td>
</tr>
<tr>
<td>Segment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Segment 1, Segment 2, ...</td>
<td>Name segments in accordance with site practices. Segment names are propagated to the SMS and are used in Reporting, Events and other features.</td>
</tr>
<tr>
<td>Media (Copper / Fiber)</td>
<td></td>
<td>Determined by the IPS model but can include both types.</td>
</tr>
<tr>
<td>Speed / Duplex</td>
<td>Auto</td>
<td></td>
</tr>
<tr>
<td>Auto-negotiate / MDI/MDX settings</td>
<td>Auto</td>
<td>Physical interface settings should be consistent with the site standard practices.</td>
</tr>
<tr>
<td>Segment Group (SMS)</td>
<td>Default</td>
<td>If the IPS is being managed by an SMS, each segment will be assigned to a Segment Group. The Segment Groups are used in Profile distribution and Reporting functions.</td>
</tr>
<tr>
<td>Layer-2 Fallback Setting</td>
<td>Permit</td>
<td>An IPS will go into Layer-2 fallback if it detects an internal error or there is excessive congestion. Each segment may be configured to pass traffic (permit), uninspected or to block traffic under this condition. If a segment is part of an iLink group (in a Core Controller configuration), the segments should be set to Block. This way the Core Controller heartbeats will fail and the CC will take that segment out of the group and not forward traffic to it.</td>
</tr>
</tbody>
</table>
Table 2-6: NX-Platform Configuration Parameters

<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Default</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Link Down Synchronization Mode       | Hub     | Each segment consists of two Ethernet links. The Link Down Synchronization parameter specifies what the IPS is to do with the second link in the event the first link goes down. Under Hub mode, the second link remains up.
Under Wire and Breaker modes, the second link is taken down. If the IPS is in a HA configuration, Wire mode is commonly used. The network infrastructure will determine the link is down (remember the IPS is a “bump in the wire” and the network has no knowledge of its existence) and route traffic around the failed link.
When the failed link is restored, under Wire mode the IPS will restore the second link automatically. Under Breaker mode, both links must be manually restored from the SMS or LSM. |
| Threat Suppression Engine            |         |          |
| Connection Table Timeout            | 1800 seconds | A blocked flow (6-tuple) is automatically released from the connection table after 1800 seconds on inactivity. This parameter is rarely modified.
In demonstrations, this parameter is frequently set to 30 seconds so that the connection table does not have to be manually cleared for the next scenario. |
| Asymmetric Network                  | Asymmetric | “Asymmetric” must be used if the IPS will not see both sides of the TCP connection. |
| Logging Mode                        | Disable | If the IPS experiences congestion exceeding the Congestion % parameter, it will suspend logging activities. This feature may be enabled by the user. |
| Congestion %                        | 1.00%   | Congestion percentage to disable logging. |
| Time                                | 600 seconds | Time which the logging is disabled |
| AFC Mode                            | Auto    | If the IPS determines that a filter is performing poorly, it will disable the filter. This feature may be disabled at the global level here, or disabled on a filter by filter basis in the profile. |
| Log severity                        | WARN    | If a filter is disabled using AFC, a system log entry is generated with this severity. |
### Table 2-6: NX-Platform Configuration Parameters

<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Default</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Health Monitoring</strong></td>
<td></td>
<td>These are parameters that govern when system log messages are generated if resource consumption becomes too high. These are typically left in their default values. Health monitor has been greatly expanded compared to previous hardware releases. You can now monitor fan speed, voltage, and more detailed disk usage to name a few.</td>
</tr>
<tr>
<td><strong>Auto DV</strong></td>
<td></td>
<td>If the IPS is not managed by an SMS, it may be configured to contact the TMC periodically and download an updated Digital Vaccine. This, of course, requires that the management port have access to the Internet. If this feature is used, care should be taken to ensure the management port is not exposed and subject to attacks. TippingPoint does have an IPS whose management port is exposed to the Internet for demonstration purposes. This port is constantly under brute force attacks.</td>
</tr>
<tr>
<td></td>
<td>Disabled</td>
<td>Auto DV configured</td>
</tr>
<tr>
<td>Frequency</td>
<td>60 minutes</td>
<td>Time after which an idle LSM session will be terminated.</td>
</tr>
<tr>
<td></td>
<td>30 seconds</td>
<td>Certain LSM pages have automatic refreshes.</td>
</tr>
<tr>
<td></td>
<td>2 - Maximum</td>
<td>The security level specifies the length and general format of IPS user id’s and passwords.</td>
</tr>
<tr>
<td></td>
<td>90 Days</td>
<td>Password Expiration Action Force user to change password</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>Max Login Attempts Lockout account for 5 minutes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failed Login Action Lockout account for 5 minutes</td>
</tr>
</tbody>
</table>
3. NX-Platform System descriptions

3.1. Power Information

The NX-Platform unit contains two 750W power supplies equipped with two AC input modules, with either capable of supplying full power (2n redundancy) giving the unit a total of 2560 BTU/hr.

3.2. NX Platform IPS at a glance

<table>
<thead>
<tr>
<th>Model</th>
<th>Throughput</th>
<th>Segments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2600NX</td>
<td>3.0Gbps</td>
<td>Every NX chassis supports up to 4 hot-swappable NX I/O modules</td>
</tr>
<tr>
<td>5200NX</td>
<td>5.0Gbps</td>
<td>With the NX chassis populated with 4 of the SFP+ NX I/O modules, you can</td>
</tr>
<tr>
<td>6200NX</td>
<td>10.0Gbps</td>
<td>achieve inspection of up to 16 segments of 10GbE, or a combination of</td>
</tr>
<tr>
<td>7100NX</td>
<td>15.0Gbps</td>
<td>1GbE, 10GbE, and 40GbE segments.</td>
</tr>
<tr>
<td>7500NX</td>
<td>20.0Gbps</td>
<td></td>
</tr>
</tbody>
</table>
3.1. System Architecture

Control Plane
- Dedicated Management / Control Plane CPU

CFAST
- Internal: 32GB, TOS, DV, running configuration
- External: 32GB, user logs, snapshots, traces
  - Hot swappable
  - Device can operate without it

Broadcom Switch ASIC
- Used as a MUX not a switch
- L2FB, Hitless Reboot / Upgrade
- Inspection Bypass
- VLAN translation
ZEUS - FPGA
- Load balance flows to XLR’s
- Hardware acceleration
  - Header parsing
  - Trigger searching
- Inspection Bypass (when Broadcom can’t support)
- Hardware watchdog
  - Loops back traffic (L2FB) if MGMT CPU dies

MERCURY – FPGA
- Multiplexer
- ZEUS still makes Load Balancing decision
**XLR**
- Heart of the data-plane (IPS engine runs here)
- 3rd XLR gives 50% improvement over N-Platform
- 8 Cores per XLR, 4 hw Threads per Core
- 24 Cores / 96 hw Threads per system

**Tier 1:**
- Inspection Bypass and L2FB prevent traffic proceeding to next tier

**Tier 2:**
- Load balances flows to KS Threads
- Traffic Management Trust and Block Filters prevent traffic proceeding to next tier

**Tier 3:**
- IP Reassembly, TCP State Tracking, Blocked / Rate-limited streams, Trigger Matching
- Traffic going to next tier is a function of Trigger hits & out of order packets

**Tier 4:**
- TCP Reassembly & Threat Verification
4. **NX-Platform Troubleshooting Commands**

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

4.1. **show np tier-stats**

- Displays throughput and efficiency across the different inspection tiers

<table>
<thead>
<tr>
<th>Stack: Segment Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Segment Rx Mbps       = 2.0 (25.4)</td>
</tr>
<tr>
<td>Segment Tx Mbps       = 2.0 (25.4)</td>
</tr>
<tr>
<td>Stack Balance (A/B)   = 22.3% (25.4)</td>
</tr>
<tr>
<td>7500NX-1 Rx Mbps      = 0.1 [0.9%]</td>
</tr>
<tr>
<td>7500NX-2 Rx Mbps      = 1.5 [6.7%]</td>
</tr>
<tr>
<td>Segment ratio to tier 1 = 11.1% [0.4%]</td>
</tr>
</tbody>
</table>

<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>

**Note:** The stacking information is only displayed for devices that have stacking enabled

**Stack: Segment Ports:**

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/C) displays the load balance percentage, in which 100% equates to perfect balance across the number of devices in the stack. For devices that are in 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:

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.

------------------------------------------------------------------------------
Tier 1: 

------------------------------------------------------------------------------

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
<th>High-Level Water Mark</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Mbps</td>
<td>979.6</td>
<td>(1,972.8)</td>
</tr>
<tr>
<td>Tx Mbps</td>
<td>462.4</td>
<td>(1,956.9)</td>
</tr>
<tr>
<td>Rx packets/sec</td>
<td>133,496.0</td>
<td>(277,733.0)</td>
</tr>
<tr>
<td>Tx packets/sec</td>
<td>77,514.0</td>
<td>(266,671.0)</td>
</tr>
<tr>
<td>Bypass Mbps</td>
<td>0.0%</td>
<td></td>
</tr>
<tr>
<td>A/B/C Balance</td>
<td>0.9%</td>
<td>(A: 240,992.0 B: 236,863.0 C: 61,308.0)</td>
</tr>
<tr>
<td>Utilization</td>
<td>6.2%</td>
<td>(12.6%)</td>
</tr>
<tr>
<td>Ratio to next tier</td>
<td>100.0%</td>
<td>[81.2%]</td>
</tr>
</tbody>
</table>

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 IPS 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 IPS inspection limits.

- A/B/C Balance displays how well the flows are being balanced between the XLRs. 100% indicates even balance 33/33/33 split, which is ideal. 0% means that all traffic is going to a single XLR. Note that the number of packets going thru the each XLR is flow based, so it is not uncommon to see a slight difference between them.

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

- Inspection bypass rules reduces the value of both “Utilization” and “Ratio to next tier”

```
Tier 2:

Tx trust packets/sec = 0.0 (0.0)
Utilization = 45.7% (69.1%)
Ratio to next tier = 66.5% [52.2%]
```

**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 next tier.

```
Tier 3:

Rx Mbps = 1,440.7 (2,167.3)
Rx packets/sec = 130,766.0 (198,777.0)
Tx trust packets/sec = 0.0 (0.0)
Utilization = 44.9% (67.6%)
Ratio to next tier = 1.6% (22.1%)
```

**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>Tier 4</th>
<th>Tier 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Mbps</td>
<td>23.7 (62.9)</td>
<td></td>
</tr>
<tr>
<td>Rx packets/sec</td>
<td>2,124.0 (26,115.0)</td>
<td></td>
</tr>
<tr>
<td>Rx due to:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trigger match</td>
<td>0.2% (50.0%)</td>
<td></td>
</tr>
<tr>
<td>Reroute</td>
<td>99.7% (100.0%)</td>
<td></td>
</tr>
<tr>
<td>TCP sequence</td>
<td>0.0% (50.0%)</td>
<td></td>
</tr>
<tr>
<td>Tx trust packets/sec</td>
<td>0.0 (0.0)</td>
<td></td>
</tr>
<tr>
<td>Ratio to next tier</td>
<td>0.6% (9.4%)</td>
<td></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 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 an IPS is being operated 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
4.2. **show np rule-stats**

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

```
# sh np rule

<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 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:** In order to reset these counters, issue the `clear np rule-stats` command at the CLI.
### 4.3. `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>Shunted</th>
<th>Dropped</th>
<th>Out Of</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCOM</td>
<td>0</td>
<td>0</td>
<td>3689827523</td>
</tr>
<tr>
<td>XAUI1</td>
<td>0</td>
<td>0</td>
<td>3689828804</td>
</tr>
<tr>
<td>Spi4A</td>
<td>0</td>
<td>0</td>
<td>1724841692</td>
</tr>
<tr>
<td>Spi4B</td>
<td>0</td>
<td>0</td>
<td>1964987119</td>
</tr>
<tr>
<td>System RL</td>
<td>0</td>
<td>0</td>
<td>3689163038</td>
</tr>
<tr>
<td>XlrA F</td>
<td>0</td>
<td>0</td>
<td>1964987377</td>
</tr>
<tr>
<td>XlrA KS</td>
<td>0</td>
<td>0</td>
<td>1259101896</td>
</tr>
<tr>
<td>XlrA L</td>
<td>0</td>
<td>0</td>
<td>60933135</td>
</tr>
<tr>
<td>XlrB F</td>
<td>0</td>
<td>0</td>
<td>1724842442</td>
</tr>
<tr>
<td>XlrB KS</td>
<td>0</td>
<td>0</td>
<td>1101670370</td>
</tr>
<tr>
<td>XlrB L</td>
<td>0</td>
<td>0</td>
<td>58726968</td>
</tr>
<tr>
<td>XlrC F</td>
<td>0</td>
<td>0</td>
<td>1884842462</td>
</tr>
<tr>
<td>XlrC KS</td>
<td>0</td>
<td>0</td>
<td>1121670380</td>
</tr>
<tr>
<td>XlrC L</td>
<td>0</td>
<td>0</td>
<td>59826990</td>
</tr>
</tbody>
</table>
4.4. debug information dp-ps

This command shows all threads for XLR-A, XLR-B, and XLR-C. Pay close attention to the Q lengths, look for evenly distributed depth. The Max LLQ length is 64 packets and the maximum Q is 1511 packets. This command output includes the eight L queues. The L queue was designed to focus on traffic that takes more time to process, thus allowing clean traffic to flow through the IPS with less latency. Below are the output results from issuing this command:

<table>
<thead>
<tr>
<th>NAME</th>
<th>TIME(tics)</th>
<th>DATA</th>
<th>Q</th>
<th>MAX</th>
<th>CONTROL</th>
<th>Q</th>
<th>MAX</th>
<th>CPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>D0</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>I0</td>
<td>1516314</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>126278736</td>
<td>0</td>
<td>3</td>
<td>0%</td>
</tr>
<tr>
<td>R0</td>
<td>12740</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>518070</td>
<td>0</td>
<td>1</td>
<td>0%</td>
</tr>
<tr>
<td>X0</td>
<td>2061043</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>63180118</td>
<td>0</td>
<td>7</td>
<td>0%</td>
</tr>
</tbody>
</table>

RUN(T1)
<table>
<thead>
<tr>
<th>NAME</th>
<th>TIME(tics)</th>
<th>DATA</th>
<th>Q</th>
<th>MAX</th>
<th>CONTROL</th>
<th>Q</th>
<th>MAX</th>
<th>CPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>X1</td>
<td>116661</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>2590351</td>
<td>0</td>
<td>1</td>
<td>0%</td>
</tr>
<tr>
<td>f0</td>
<td>659018</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2%</td>
</tr>
<tr>
<td>f1</td>
<td>657669</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2%</td>
</tr>
<tr>
<td>f2</td>
<td>625581</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2%</td>
</tr>
<tr>
<td>f3</td>
<td>654374</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2%</td>
</tr>
<tr>
<td>f4</td>
<td>624097</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2%</td>
</tr>
<tr>
<td>f5</td>
<td>659287</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2%</td>
</tr>
<tr>
<td>f6</td>
<td>615336</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2%</td>
</tr>
<tr>
<td>f7</td>
<td>669098</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2%</td>
</tr>
<tr>
<td>k0</td>
<td>221788</td>
<td>19475846</td>
<td>0</td>
<td>12</td>
<td>8289123</td>
<td>0</td>
<td>3</td>
<td>0%</td>
</tr>
<tr>
<td>k1</td>
<td>214283</td>
<td>19255942</td>
<td>0</td>
<td>10</td>
<td>8289123</td>
<td>0</td>
<td>3</td>
<td>0%</td>
</tr>
<tr>
<td>k2</td>
<td>211924</td>
<td>19089179</td>
<td>0</td>
<td>9</td>
<td>8289122</td>
<td>0</td>
<td>3</td>
<td>0%</td>
</tr>
<tr>
<td>k3</td>
<td>215170</td>
<td>19285301</td>
<td>0</td>
<td>10</td>
<td>8289124</td>
<td>0</td>
<td>3</td>
<td>0%</td>
</tr>
<tr>
<td>k4</td>
<td>215621</td>
<td>19430623</td>
<td>0</td>
<td>9</td>
<td>8289123</td>
<td>0</td>
<td>3</td>
<td>0%</td>
</tr>
<tr>
<td>k5</td>
<td>215095</td>
<td>19430704</td>
<td>0</td>
<td>9</td>
<td>8289122</td>
<td>0</td>
<td>3</td>
<td>0%</td>
</tr>
<tr>
<td>k6</td>
<td>213783</td>
<td>19362142</td>
<td>0</td>
<td>11</td>
<td>8289123</td>
<td>0</td>
<td>3</td>
<td>0%</td>
</tr>
<tr>
<td>k7</td>
<td>216109</td>
<td>19452018</td>
<td>0</td>
<td>10</td>
<td>8289123</td>
<td>0</td>
<td>3</td>
<td>0%</td>
</tr>
<tr>
<td>k8</td>
<td>213464</td>
<td>19201821</td>
<td>0</td>
<td>9</td>
<td>8289123</td>
<td>0</td>
<td>3</td>
<td>0%</td>
</tr>
<tr>
<td>l0</td>
<td>564904</td>
<td>6834973</td>
<td>0</td>
<td>5</td>
<td>3108420</td>
<td>0</td>
<td>3</td>
<td>3%</td>
</tr>
<tr>
<td>l1</td>
<td>563358</td>
<td>6827187</td>
<td>0</td>
<td>6</td>
<td>3108420</td>
<td>0</td>
<td>3</td>
<td>4%</td>
</tr>
<tr>
<td>l2</td>
<td>563364</td>
<td>6831457</td>
<td>0</td>
<td>6</td>
<td>3108420</td>
<td>0</td>
<td>3</td>
<td>3%</td>
</tr>
<tr>
<td>l3</td>
<td>562005</td>
<td>6826049</td>
<td>0</td>
<td>6</td>
<td>3108420</td>
<td>0</td>
<td>3</td>
<td>3%</td>
</tr>
<tr>
<td>l4</td>
<td>562593</td>
<td>6834450</td>
<td>0</td>
<td>6</td>
<td>3108420</td>
<td>0</td>
<td>3</td>
<td>4%</td>
</tr>
<tr>
<td>l5</td>
<td>562556</td>
<td>6828993</td>
<td>0</td>
<td>6</td>
<td>3108420</td>
<td>0</td>
<td>3</td>
<td>3%</td>
</tr>
<tr>
<td>l6</td>
<td>562861</td>
<td>6826882</td>
<td>0</td>
<td>6</td>
<td>3108420</td>
<td>0</td>
<td>3</td>
<td>4%</td>
</tr>
<tr>
<td>l7</td>
<td>560500</td>
<td>6822526</td>
<td>0</td>
<td>6</td>
<td>3108420</td>
<td>0</td>
<td>3</td>
<td>2%</td>
</tr>
<tr>
<td>r0</td>
<td>44083</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>53128</td>
<td>0</td>
<td>1</td>
<td>0%</td>
</tr>
<tr>
<td>r1</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0%</td>
</tr>
<tr>
<td>w0</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>157</td>
<td>0</td>
<td>1</td>
<td>0%</td>
</tr>
</tbody>
</table>

Totals:
<table>
<thead>
<tr>
<th>DATA</th>
<th>CONTROL</th>
<th>DROPPED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other:</td>
<td>0</td>
<td>192620561</td>
</tr>
<tr>
<td>F:</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>K:</td>
<td>1932586902</td>
<td>828912285</td>
</tr>
<tr>
<td>L:</td>
<td>54634317</td>
<td>24867360</td>
</tr>
</tbody>
</table>
4.5. **debug np regex show**

**Debug np regex show** 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
```

4.6. **Best Effort Mode**

Best Effort mode is a feature, which can be enabled in NX-Platform appliances, that allows the appliance to favor network latency performance (voice, video). The NX-Platform is architected as a collection of parallel network processor threads. Each of these threads implements the security protection that is configured by the user. When processing traffic, the network flows are load balanced among all of the available threads in the system.

In infrequent cases, the traffic directed to a single processor thread can exceed the level that thread can manage, causing the appliance to drop the overflow traffic. If Best Effort mode is enabled, then the appliance simply forwards the overflow packets, instead of dropping them. The forwarded traffic is only related to the specific processing thread; all other threads would be unaffected. This feature was designed to protect latency sensitive applications.

Best Effort mode is enabled using a CLI command, allowing the user to specify the amount of latency that can be allowed, before deciding to forward a packet. If latency exceeds a configured threshold the packet will be shunted. By default, this command is not enabled. The following is the syntax used in order to implement this configuration. It can only be executed from the IPS CLI.

```
IPS# debug np best-effort enable –queue-latency –recover-percent
```
Queue latency (microseconds) defines when the Best Effort will start working. Percent of queue latency defines when Best Effort mode will exit. **Note:** Setting the queue latency to 100µs or lower will probably enable this feature too often and it’s not recommended. Use of the default is highly recommended.

4.7. **Troubleshooting Network Connectivity**

4.7.1. `debug np port diags <port#>`

This command is useful in diagnosing issues with network connectivity to the IPS' connected ports/segments. (Note: the syntax of this command has changed. You will now have to specify by port e.g. 1A, 1B, etc. Slots are no longer used e.g. 3 1). Incorrect duplex settings will be displayed here.

When a port is down you will get the following output:

Port number: 9  
PHY address: 9  
PHY: FIBER interface  
Auto Negotiation: Supported  
Auto-Negotiation: Enabled  
Link: DOWN  
Advertised Capabilities:  
1000BASE-X full-duplex capable  
1000BASE-X half-duplex capable

When a port is enabled and plugged in you will get the following output:

Port number: 11  
PHY address: 11  
PHY: COPPER interface  
Auto Negotiation: Supported  
Auto-Negotiation: Enabled  
Link: UP  
Auto-Negotiation: Completed  
Duplex mode: FULL  
Speed: 1Gbps  
Advertised Capabilities:  
1000BASE-T full-duplex capable  
1000BASE-T half-duplex capable  
100BASE-T half-duplex capable  
100BASE-T full-duplex capable  
10BASE-T half-duplex capable  
10BASE-T full-duplex capable  
Link Partner Capabilities:  
Remote receiver OK
1000BASE-T half-duplex capable
1000BASE-T full-duplex capable
10BASE-T half-duplex capable
10BASE-T full-duplex capable
100BASE-T half-duplex capable
100BASE-T full-duplex capable
Pause operation capable
Received link code word
Next Page ability supported
Auto-Negotiation Capable

### 4.7.2. `debug np port show`

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

<table>
<thead>
<tr>
<th>Admin</th>
<th>Status</th>
<th>Negotiate</th>
<th>Type</th>
<th>MTU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port 0: Enabled</td>
<td>DOWN</td>
<td>auto incomp</td>
<td>Fiber</td>
<td>9234</td>
</tr>
<tr>
<td>Port 1: Disabled</td>
<td>DOWN</td>
<td>auto incomp</td>
<td>Fiber</td>
<td>9234</td>
</tr>
<tr>
<td>Port 2: Enabled</td>
<td>DOWN</td>
<td>auto incomp</td>
<td>Fiber</td>
<td>9234</td>
</tr>
<tr>
<td>Port 3: Disabled</td>
<td>DOWN</td>
<td>auto incomp</td>
<td>Fiber</td>
<td>9234</td>
</tr>
<tr>
<td>Port 4: Enabled</td>
<td>DOWN</td>
<td>auto incomp</td>
<td>Fiber</td>
<td>9234</td>
</tr>
<tr>
<td>Port 5: Disabled</td>
<td>DOWN</td>
<td>auto incomp</td>
<td>Fiber</td>
<td>9234</td>
</tr>
<tr>
<td>Port 6: Enabled</td>
<td>DOWN</td>
<td>auto incomp</td>
<td>Fiber</td>
<td>9234</td>
</tr>
<tr>
<td>Port 7: Disabled</td>
<td>DOWN</td>
<td>auto incomp</td>
<td>Fiber</td>
<td>9234</td>
</tr>
<tr>
<td>Port 8: Enabled</td>
<td>DOWN</td>
<td>auto incomp</td>
<td>Fiber</td>
<td>9234</td>
</tr>
<tr>
<td>Port 9: Disabled</td>
<td>DOWN</td>
<td>auto incomp</td>
<td>Fiber</td>
<td>9234</td>
</tr>
<tr>
<td>Port 10: Enabled</td>
<td>DOWN</td>
<td>auto incomp</td>
<td>Copper</td>
<td>9234</td>
</tr>
<tr>
<td>Port 11: Disabled</td>
<td>DOWN</td>
<td>auto incomp</td>
<td>Copper</td>
<td>9234</td>
</tr>
<tr>
<td>Port 12: Enabled</td>
<td>DOWN</td>
<td>auto incomp</td>
<td>Copper</td>
<td>9234</td>
</tr>
<tr>
<td>Port 13: Disabled</td>
<td>DOWN</td>
<td>auto incomp</td>
<td>Copper</td>
<td>9234</td>
</tr>
<tr>
<td>Port 14: Enabled</td>
<td>DOWN</td>
<td>auto incomp</td>
<td>Copper</td>
<td>9234</td>
</tr>
<tr>
<td>Port 15: Disabled</td>
<td>DOWN</td>
<td>auto incomp</td>
<td>Copper</td>
<td>9234</td>
</tr>
<tr>
<td>Port 16: Enabled</td>
<td>DOWN</td>
<td>auto incomp</td>
<td>Copper</td>
<td>9234</td>
</tr>
<tr>
<td>Port 17: Disabled</td>
<td>DOWN</td>
<td>auto incomp</td>
<td>Copper</td>
<td>9234</td>
</tr>
<tr>
<td>Port 18: Disabled</td>
<td>DOWN</td>
<td>auto incomp</td>
<td>Copper</td>
<td>9234</td>
</tr>
<tr>
<td>Port 19: Disabled</td>
<td>DOWN</td>
<td>auto incomp</td>
<td>Copper</td>
<td>9234</td>
</tr>
<tr>
<td>Port 24: Disabled</td>
<td>DOWN</td>
<td>none</td>
<td>Fiber</td>
<td>9234</td>
</tr>
<tr>
<td>Port 25: Disabled</td>
<td>DOWN</td>
<td>none</td>
<td>Fiber</td>
<td>9234</td>
</tr>
<tr>
<td>HG 26: Enabled</td>
<td>DOWN</td>
<td>none</td>
<td>XAUI</td>
<td>9254</td>
</tr>
<tr>
<td>HG 27: Enabled</td>
<td>UP</td>
<td>10Gbps full</td>
<td>none</td>
<td>XAUI</td>
</tr>
<tr>
<td>MGMT  : Enabled</td>
<td>UP</td>
<td>100Mbps full</td>
<td>auto</td>
<td>Copper</td>
</tr>
</tbody>
</table>