TippingPoint Operating System Release Notes

V 2.5.4

Part Number: TECHD-0000000254
Publication Control Number: 080808:1520

TippingPoint Technologies, Inc. reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of TippingPoint Technologies, Inc. to provide notification of such revision or change.

TippingPoint Technologies, Inc. provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms, or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. TippingPoint Technologies, Inc. may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document.

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

United States Government Legend: All technical data and computer software is commercial in nature and developed solely at private expense. Software is delivered as Commercial Computer Software as defined in DFARS 252.227-7014 (June 1995) or as a commercial item as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in TippingPoint's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with guide.

Table of Contents

Release Notes

Overview

This document contains information about the V 2.5.4 release of the TippingPoint Operating System. It also includes information about the new and changed features that were released with TOS V 2.5.3.

Note: To ensure that you have the most current version of the Release Notes and other product documentation, download the documents from the TippingPoint Threat Management Center (TMC) at http://tmc.tippingpoint.com.

The Release Notes contain the following major sections:

For additional information or assistance, contact TippingPoint Customer Support:

Telephone

North America:	+1 866 681 8324
International:	+1 512 681 8524
Australia:	800 783 933
New Zealand:	0800 852 300

E-mail

support@tippingpoint.com

Important Notices

For complete documentation refer to the following publications available from the TippingPoint Threat Management Center (TMC) at http://tmc.tippingpoint.com:

- *TippingPoint Local Security Manager User's Guide* or *LSM Online Help*
- *IPS Hardware Installation and Safety Guide*
- *Command Line Interface Reference*

Release Restrictions

The following restrictions apply to this release.

The following features and changes apply only to the TippingPoint 600E/1200E/2400E/5000E:

- "CPU Temperature Reporting" on page 5
- "Filter Changes on 600E/1200E/2400E/5000E" on page 9

In addition, VoIP and SCADA filters are available only on the TippingPoint 600E/1200E/2400E/5000E.

SMS Version Support

If you use the TippingPoint Security Management System (SMS) to manage your IPS device, TOS V 2.5.4 requires you to install SMS V 2.5.2 and above on your management device before you upgrade the IPS to TOS V 2.5.4. Prior versions of the SMS will not support TOS V 2.5.4. For more information about migration, see "Migration and Upgrades" on page 11.

Custom Shield Writer (CSW) Filters

Only filters created by CSW 2.5 will operate on TOS V 2.5.4. Filters written with earlier versions of CSW will not load.

TippingPoint Operating System V 2.5.4 Updates

The following changes have been made in TOS V 2.5.4.

Hitless Reboot on 600E/1200E/2400E/5000E

Rebooting a 600E/1200E/2400E/5000E device is now hitless by default. A complete reboot can be performed with the `reboot -full` command.

Improved Recovery from "Receive No Transmit"

TOS V 2.5.4 improves the fix implemented in TOS V 2.5.3 for the "Receive No Transmit" issue. Instead of placing the IPS in Layer-2 Fallback (L2FB) when this condition occurs, TOS V 2.5.4 automatically corrects the problem and continues to inspect traffic normally. A warning will be logged in the system log when or if this happens.

For network ports running at 10/100 Mbps, there will be a link flap while the system corrects the issue. When the link is re-established, traffic will be inspected normally.

The improved recovery applies to the TippingPoint 600E/1200E/2400E/5000E IPS devices. Other models will continue to go into L2FB if this condition occurs.

Known Issues

The following issues have been identified in TOS V 2.5.4.

- "Delayed Removal of IP Addresses From Quarantine" on page 6
- "Invalid Characters in Profiles Created in the CLI" on page 7
- "Redefining DDoS Exception Filters" on page 8
- "Upgrade Issues Betweeen TOS V 2.5.3 to V 2.5.4" on page 12

Resolved Issues

The following issues have been resolved in TOS V 2.5.4.

- "Closed Port Shows Activity After Reboot" on page 9
- "Host Name and IP Address Retained in Snapshots" on page 10
- "Traffic Congestion Issues" on page 11

What's New (Version 2.5.3)

This section describes new features that were introduced with version 2.5.3 of the TOS.

TippingPoint 210E

TippingPoint introduces the TippingPoint 210E IPS, which ships with the following pre-installed components:

- One custom processor card with 10 Ethernet ports
- Host processor to control, configure, monitor, and store network traffic
- One power supply module
- Redundant fan cooling with speed control
- 1GB Compact Flash Drive
- 32-character LCD Display

The TippingPoint 210E supports traffic up to 200 Mbps per port. For more detailed TippingPoint 210E information, consult the *TippingPoint Hardware Installation and Safety Guide* and *Quick Start TippingPoint 210E*.

TippingPoint 210E and ZPHA

The TippingPoint 210E includes an integrated Zero-Power High Availability (ZPHA) module. The ZPHA module provides a network bypass for Ethernet traffic in the event that the IPS fails. If all segments are configured to Permit, a failure will put the TippingPoint 210E into ZPHA mode.

When Layer 2 Fallback is activated, the link will briefly go offline and come online again. This behavior is normal.

When you install and configure the TippingPoint 210E, be sure to follow ZPHA best practices.

- Between similar ports (DTE-DTE or DCE-DCE), a connection should be crossed.
- Between dissimilar ports (DCE-DTE), the connection should be straight-over.
- Ensure that all IPS interfaces and connected switches have the same linespeed and duplex settings.

Support for the 600E/1200E/2400E/5000E

TOS V 2.5.3 added the following TOS V 2.5.1 functionality to the TippingPoint 600E/1200E/2400E/5000E IPS devices.

- Virtual ports and VLAN awareness
- Security Profiles and Traffic Management Profiles
- IPS filter configuration with Security Profiles
- Enhanced IPS filter search
- Quarantine tracking and threshold configuration and Quarantine reports
- Support for Firefox v1.5+, Mozilla v1.7+, and Netscape v8.1+
- New category settings
- Modified log files
- Automatic negotiation, linespeed, and duplex settings for the management port
- Power supply monitoring
- New CLI commands

For detailed information about TOS 2.5.1, refer to the *TippingPoint Operating System Release Notes V 2.5.1*, available at http://tmc.tippingpoint.com.

TOS Hitless OS Update

On the TippingPoint 600E/1200E/2400E/5000E IPS models, TOS V 2.5.3 provided the ability to perform a TOS software update without interrupting traffic through IPS data ports. During the reboot process, each segment continues to handle traffic based on the Intrinsic Network HA: Layer-2 Fallback settings configured for the segment (Permit All or Block All). However, no IPS filtering functions are performed on the traffic during the update process.

Updates from TOS V 2.5.2 to V 2.5.3 are hitless on copper ports. Updates from TOS V 2.5.2 to V 2.5.3 are **not** hitless on fiber ports, but V 2.5.3 to V 2.5.4 and other future versions will be hitless. Rollbacks to earlier TOS versions are not hitless.

LSM Support for Internet Explorer 7

The LSM includes support for Internet Explorer 7.

Performance Protection Filters

New features have been added to Performance Protection filters. Performance Protection filters include the IM, P2P, and Streaming Media filter sub-categories.

- You can assign any action set that uses a **Permit** action to Performance Protection filters.
- Per-filter exceptions are now supported on Performance Protection filters.

For detailed information about working with Performance Protection Filters, refer to the “Tipping Point Local Security Manager User’s Guide 2.5.2 Addendum” in the *TippingPoint Local Security Manager User’s Guide.*

What’s Changed (Version 2.5.3)

The following feature changes were introduced in TOS V 2.5.3.

Digital Vaccine Support

TippingPoint made enhancements to the Digital Vaccine packages in V 2.5.2 and V 2.5.3. Digital Vaccine packages that support V 2.5.2 and V 2.5.3 will not work on older versions of the TOS.

CPU Temperature Reporting

On the TippingPoint 600E/1200E/2400E/5000E, the method for polling and reporting CPU temperature changed. The reported CPU temperature in V 2.5.3 and later versions is higher than the reported CPU temperature in V 2.2.5.

If you have modified the default threshold CPU temperature values, the modified thresholds will be set to the default thresholds (Major: 69 C, Critical: 72 C) when you upgrade from V 2.2.5 to V 2.5.3 or V 2.5.4. If you roll back to V 2.2.5 from V 2.5.3 or V 2.5.4, modified thresholds will be retained and adjusted during rollback.

Known Issues

Cache Settings and Cookies in Internet Explorer

Set your cache setting in Internet Explorer for enhanced browser performance. Open the Internet Options for your browser (**Tools —> Internet Options**). On the General tab, select the Settings option for Temporary Internet Files. In the Check for new versions section, select **Every visit to the page**. Save these settings.

Cookies for previous versions of the LSM may conflict with cookies in the updated version. If the browser receives 404 Page Not Found errors or displays blank LSM frames, the cookies on the computer may be out of sync. To remedy this, delete the existing cookies and open a new session. On the General tab of the Internet Options dialog, click **Delete Cookies**. Restart Internet Explorer, connect to the LSM and continue as before.

Delayed Removal of IP Addresses From Quarantine

When an IPS is experiencing a heavy traffic load, removal of IP addresses from the quarantine table may take longer than the configured amount of time.

Digital Vaccine Messages

When you push a new Digital Vaccine (DV) version to the IPS, the following errors may be generated on a per-filter basis:

```
ERR UDM isValid: Signature [XXX-XXX-XXX-XXX-XXX] does not exist for
policy

ERR UDM parseOnePolicy: Invalid policy [XXX-XXX-XXX-XXX-XXX]
```

These errors occur when filters have been removed from that version of the DV and when there are synchronization variances between the IPS and the SMS. Depending on the number of filters that have been changed or removed, a large number of alerts may be sent to the console. This does not impact or reduce the IPS's security posture.

Double Quotes in Passwords

Although you can create passwords that contain double quotes ("), SSH will not support them, and you will not be able to log in over SSH. You can still access the device through direct console access or through the LSM. TippingPoint recommends that you do not create passwords that contain double quotes.

Filter Configuration for Traffic Management, Traffic Threshold and DDoS

When you define a Traffic Management Profile, Traffic Threshold or DDoS filter, the specified virtual segment must also have a Security Profile explicitly assigned to it. If a Security Profile is not defined, the traffic on the virtual segment will not be inspected by the IPS device. For example, if the only

Security Profile configured on a device is the default (*ANY* <==> *ANY*) and you create a Traffic Threshold profile to apply to traffic on the virtual segment 1A ==> 1B, you must create a Security Profile that explicitly applies to the 1A ==> 1B segment, or add this virtual segment to an existing Security Profile. If a Security Profile for a virtual segment is missing, the *Virtual Segments* table on the *LSM Security Profiles* page table displays the following error message:

```
No security profile is assigned to the in/out pair. Traffic will NOT be
inspected against DV filter policies
```

Invalid Characters in Profiles Created in the CLI

It is possible to create profile names in the CLI that contain invalid characters. These profiles prevent the LSM profile display from functioning correctly. The names of these profiles must be changed in the CLI with the following command:

```
conf t profile [old_name] rename [new_name]
```

Line Speed Settings

The IPS does not support manual configuration of copper ports to a line speed of 1000 Mbps, and the LSM will not permit this action. However, the CLI still appears to permit you to set the line speed at 1000 Mbps. This action should be avoided, as it will lead to link issues and inconsistencies between the settings displayed in the LSM and CLI.

Layer-2 Fallback and Ports Configured to Block

The following issues have been identified with Layer-2 Fallback (L2FB) and ports that have been configured to block traffic while in L2FB state:

- When a segment is configured to block traffic when in L2FB, the port is shut down. However, the LSM and the CLI command **show interface ethernet** show the port status as **Up**. Use the command **debug np port show** to display the port status correctly.
- After performing a TOS update, ports that have been configured to block traffic when in L2FB will not re-establish the network connection when you reboot the device. Use the LSM or the CLI to restart the port.

Receive No Transmit

Note: TippingPoint 600E/1200E/2400E/5000E IPS devices feature an improvement to the management of this issue in V 2.5.4. For more information, see "Improved Recovery from "Receive No Transmit"" on page 3. This improvement is available **only** for TippingPoint 600E/1200E/2400E/5000E IPS devices.

Under certain rare circumstances an IPS device with TOS versions prior to V 2.5.3 may cease to pass traffic without notification. Should the condition occur in V 2.5.3, the device will go into Layer-2 Fallback.

Redefining DDoS Exception Filters

After upgrading to TOS V 2.5.4, any DDoS exception filters should be deleted and redefined.

Resetting Filters

The *Reset* button (labeled *Reset Filters* in TOS V 2.5.2 and earlier) resets security profiles, action sets, notifications, DDOS and traffic threshold filters, traffic management profiles, and virtual ports.

If you want to reset your filter settings, TippingPoint recommends that you remove the relevant security profile instead of using the *Reset* button. If you do use the *Reset* button, use the CLI to capture virtual port configuration.

Capturing Virtual Port Configuration

1. In the CLI, enter the command **show conf virtual-port**.
2. Select and copy the user-defined virtual port information from the generated output.
3. Reset the filters.
4. In the CLI, type the command **conf t** and paste in the output generated in steps 1 and 2. The virtual port configuration is restored.

Note: The copy-and-paste process will insert line breaks on wrapped lines. Before copying the output, ensure that your terminal screen is wide enough to accommodate the lines without breaks.

Rollback from TOS V 2.5.4 to V 2.2

If you rollback an IPS running TOS V 2.5.4 or later to V 2.2.5 or earlier, the following error message may appear in the system log during the TSE firmware rollback:

```
tptPumaCheckXgmiiDll: Puma XGMII Clock DLL failed to lock.
```

This error message is caused by a temporary incompatibility between the V 2.5.4 FPGA and the earlier version of the TOS software installed during the rollback process. The incompatibility will not affect the IPS after the TOS rollback is complete. This message may be ignored.

Note: TippingPoint IPS devices that ship with V 2.5.4 cannot be rolled back to V 2.2.

Resolved Issues

This section documents issues resolved in TOS V 2.5.2, TOS V 2.5.3, and TOS V 2.5.4. For issues resolved in V 2.5.1, refer to the *TippingPoint Operating System Release Notes V 2.5.1*, available at http://tmc.tippingpoint.com.

Closed Port Shows Activity After Reboot

After you close a port through the LSM or CLI and reboot the device, the port link light correctly indicates that the port is inactive and not passing traffic.

CPU Reporting High Utilization

In previous versions of the TOS, the CPU would inaccurately report high utilization levels. This issue has been resolved, and CPU utilization is now reported correctly.

Device Stops Passing Traffic in Layer-2 Fallback

In cases of the loss of a link partner, the IPS would go into Layer-2 Fallback and stop passing traffic. This issue has been resolved, and the device now passes traffic correctly in Layer-2 Fallback mode.

Dropped Packets During Hitless Updates

During hitless updates, some fiber-port devices could drop packets. This issue has been resolved, and the hitless updates are now completed correctly.

Engine Memory Leak

Certain patterns of fragmented IP traffic could cause memory leaks. This issue has been resolved.

False Errors in the CLI

The **clear configuration** command in the CLI no longer generates false “Unknown notification contact” errors.

File Descriptor Leak (38337)

A file descriptor leak could interrupt device management. This issue has been resolved.

Filter Changes on 600E/1200E/2400E/5000E

When a Digital Vaccine update changed certain filters on the TippingPoint 600E/1200E/2400E/5000E IPS models, error messages could appear in the system log. These messages were similar to the following messages:

```
7377,2007-06-26 12:24:33,ERR ,NP ,"Attempt to delete active hre rule
0x36596d50."

7378,2007-06-26 12:24:33,ERR ,NP ,"freeRuleInternals: Failed to
release rule data for rule pointer 0x107f0314."
```

If subsequent traffic matched any of the affected filters after the DV upgrade, the device could experience a page fault or other failure condition and go into Layer 2 Fallback mode. This issue has been resolved.

Host Name and IP Address Retained in Snapshots

System snapshots no longer retain the host name and IP address of the device on which the snapshot was created. When you apply a snapshot to a device different from the one on which it was created, you are no longer required to update the host name and IP address after you install the snapshot.

Intrinsic Network High Availability State

When you forced a device into Layer-2 Fallback, the High Availability indicator would show the INHA state as "None". The state now correctly shows Layer-2 Fallback.

Long Filter Descriptions

Filter descriptions of more than 2000 characters could cause errors. This issue has been resolved.

Page Faults in TOS V 2.5.2

Under certain circumstances, page faults could occur in IPS devices running TOS V 2.5.2. This issue has been resolved.

Password Auto-Complete Disabled

Password auto-complete has been disabled on the LSM login page.

Port Settings

When the user changed auto-negotiation, duplex, or port speed settings, the port could be disabled when the device was rebooted. This issue has been resolved.

Saving Adaptive Filter Files

You can now save adaptive filter dump files through the LSM.

SMS Management Errors

Under certain circumstances, updates initiated by the SMS would not get propagated to the IPS, requiring the user to disable and re-enable SMS management on the IPS. This issue has been resolved.

Snapshot Imports

Attempts to import large snapshots would result in errors. Snapshots now import correctly.

System Log Search and Daylight Savings Time

During Daylight Savings Time, the System Log search results now display correctly.

TSE Failures

Under certain circumstances, an IPS device would go into Layer-2 Fallback mode due to TSE failures. This issue has been resolved.

Traffic Congestion Issues

Improvements to the IPS engine mitigate congestion issues, improving throughput and performance.

Wildcards in IP Addresses

When you search for an IP address with wildcard characters, such as `192.168.*.*`, the results now appear correctly.

Migration and Upgrades

To migrate your IPS device from V 2.2 to V 2.5.4, download and install the TOS V 2.5.4 software package. Then, download and install a V 2.5.4 DV package. You can install the updated packages from the LSM (System > Update). For details, see *TippingPoint Local Security Manager User's Guide* or *LSM Online Help*.

When you migrate from V 2.2 to V 2.5.4, all global filters will be migrated to the Default Security Profile that includes the virtual segment ANY <==> ANY. All segmental filters will be migrated to a Security Profile that includes two virtual segments, one for each direction, matching the segment to which they apply (1A ==> 1B and 1B ==> 1A, for example).

All IPS filter block events in the V 2.2 Misuse and Abuse log will be migrated to the IPS Block Log.

Note: If you use the SMS to manage your IPS device, the SMS must be updated to SMS 2.5.2 before you upgrade the IPS to TOS V 2.5.4.

Migration Issues Between TOS V 2.2.+ and V 2.5.4

Before migrating your IPS device from TOS V 2.2+ to V 2.5.4, review the following migration issues to determine whether your system requires any configuration adjustments before or after migration.

Note: Migration issues do not apply to devices that ship with V 2.5.4 installed.

Port Scan/Host Sweep Filters

If your IPS device has global Port Scan/Host Sweep filters configured, you must re-configure these filters after you upgrade to V 2.5.4. Port Scan/Host Sweep filter overrides applied to individual segments will migrate without any issues.

Traffic Threshold Filters

Error Message: Traffic threshold profile cannot be assigned to a virtual segment

If you see the following message in the system log after migration, verify the Traffic Threshold filter configuration on the IPS device and update the configuration as required:

```
Traffic threshold profile cannot be assigned to a virtual segment
```

Error Message: Parsing failed for profile map

If you have traffic threshold filters configured on an IPS device running TOS V 2.2, and you migrate to TOS V 2.5.3, you may see the following error message in the system log after migration:

```
ERR UDMparseOneProfileMap: Parsing failed for profile map
```

The traffic threshold filter will function correctly, but you will see the error message in the system log whenever you update the software or DV package for the IPS device. To get rid of the error message, identify the segments that the Traffic Threshold filters apply to (1A ==>1B, for example), delete the Security Profiles containing those segments, and re-configure them.

Alert and Block Logs

All IPS filter block events in the V 2.2 Misuse and Abuse log will be migrated to the Block Log.

If you upgrade an IPS device from a V 2.2+ TOS release to the V 2.5.3 release and subsequently roll back to the 2.2 release, you will lose the data in the Alert and Block logs. This occurs because the log formats for V 2.5.4 have changed from the V 2.2 releases. To save the Alert and Block Log data from V 2.5.4, download and save the log files before rolling back to the earlier release.

Upgrade Issues Betweeen TOS V 2.5.3 to V 2.5.4

When upgrading the TOS from V 2.5.3 to V 2.5.4 with the SMS or when performing the upgrade as a high-priority process, place the IPS into Layer-2 Fallback before performing the upgrade. This applies only to TippingPoint 50, 100E, 200E, and 210E IPS models.