SOURCEFIRE 3D SYSTEM RELEASE NOTES

Version 5.2.0.9

Original Publication: June 1, 2015

These release notes are valid for Version 5.2.0.9 of the Sourcefire 3D System. Even if you are familiar with the update process, make sure you thoroughly read and understand these release notes, which describe supported platforms, new and changed features and functionality, known and resolved issues, as well as product and web browser compatibility. They also contain detailed information on prerequisites, warnings, and specific installation and uninstallation instructions for the following appliances:

- Series 3 managed devices supported for this release

  (the 3D7010, 3D7020, 3D7030, 3D7110, 3D7120, 3D8120, 3D8130, 3D8140, 3D8250)

IMPORTANT!   This update is **not** supported on virtual managed devices.

To update appliances running at least Version 5.2 of the Sourcefire 3D System to Version 5.2.0.9, see the procedures outlined in

IMPORTANT!   You must reimage appliances running Version 4.10.x of the system to Version 5.2 before you install this update. For more information and reimage instructions, see the *Version 5.2 Sourcefire 3D System Release Notes* and the *Sourcefire 3D System Installation Guide*.

TIP! For detailed information on the Sourcefire 3D System, refer to the online help or download the *Sourcefire 3D System User Guide* from the Support Site.

For more information, see the following sections:

Before You Begin: Important Update and Compatibility Notes

Before you begin the update process for Version 5.2.0.9, you should familiarize yourself with the behavior of the system during and after the update process, as well as with any compatibility issues or required pre- or post-update configuration changes.

IMPORTANT!   This update is **not** supported on virtual managed devices.

WARNING!   Cisco **strongly** recommends you perform the update in a maintenance window or at a time when the interruption will have the least impact on your deployment.

For more information, see the following sections:

Configuration and Event Backup Guidelines

Before you begin the update, Cisco **strongly** recommends that you back up current event and configuration data to an external location. This data is **not** backed up as part of the update process.

Use the Defense Center to back up event and configuration data for itself and the devices it manages. For more information on the backup and restore feature, see the *Sourcefire 3D System User Guide*.

IMPORTANT!   The Defense Center purges backups from previous updates. To retain archived backups, store the backups externally.

Traffic Flow and Inspection During the Update

The update process (and any uninstallation of the update) reboots all appliances. Depending on how your devices are configured and deployed, the following capabilities are affected:

- traffic inspection, including application awareness and control, URL filtering, Security Intelligence, intrusion detection and prevention, and connection logging
- traffic flow, including switching, routing, NAT, VPN, and related functionality
- link state

Note that when you update clustered or clustered stacked devices, the system performs the update one device or stack at a time to avoid traffic interruption.

Traffic Inspection and Link State

In an inline deployment, your managed devices (depending on model) can affect traffic flow via application control, user control, URL filtering, Security Intelligence, and intrusion prevention, as well as switching, routing, NAT, and VPN. In a passive deployment, you can perform intrusion detection and collect discovery data without affecting network traffic flow. For more information on appliance capabilities, see the *Sourcefire 3D System Installation Guide*.

The following table provides details on how traffic flow, inspection, and link state are affected during the update, depending on your deployment. Note that regardless of how you configured any inline sets, switching, routing, NAT, and VPN are **not** performed during the update process.

Network Traffic Interruption

DEPLOYMENT	NETWORK TRAFFIC INTERRUPTED?
Inline with configurable bypass (**Failopen** option enabled for inline sets)	Network traffic is interrupted at two points during the update: • At the beginning of the update process, traffic is briefly interrupted while link goes down and up (flaps) and the network card switches into hardware bypass. Traffic is not inspected during hardware bypass. • After the update finishes, traffic is again briefly interrupted while link flaps and the network card switches out of bypass. After the endpoints reconnect and reestablish link with the sensor interfaces, traffic is inspected again. **IMPORTANT!** The configurable bypass option is **not** supported on virtual devices, non-bypass NetMods on 8000 Series devices, or SFP transceivers on 71xx Family devices.
Inline	Network traffic is blocked throughout the update.
Passive	Network traffic is not interrupted, but also is not inspected during the update.

Network Traffic Management

Managed devices do **not** perform switching, routing, NAT, VPN, or related functions during the update. If you configured your devices to perform only switching and routing, network traffic is blocked throughout the update.

Product Compatibility

You must use at least Version 5.2 of the Defense Center to manage Version 5.2.0.9 devices. Defense Centers running Version 5.2.0.9 can manage devices running Version 5.2 or greater.

Web Browser Compatibility

Version 5.2.0.9 of the web interface for the Sourcefire 3D System has been tested on the browsers listed in the following table.

Web Browser Compatibility

BROWSER	REQUIRED ENABLED OPTIONS AND SETTINGS
Firefox 37	JavaScript, cookies, Secure Sockets Layer (SSL) v3
Microsoft Internet Explorer 9, 10, and 11	JavaScript, cookies, Secure Sockets Layer (SSL) v3, 128-bit encryption, **Active scripting** security setting, Compatibility View, set **Check for newer versions of stored pages** to **Automatically**

Screen Resolution Compatibility

Cisco recommends selecting a screen resolution that is at least 1280 pixels wide. The user interface is compatible with lower resolutions, but a higher resolution optimizes the display.

Updating Your Appliances

The following sections help you prepare for and install the Version 5.2.0.9 update:

- Planning the Update on page 5
- Updating Managed Devices on page 7

WARNING! Do **not** reboot or shut down your appliances during the update until after you see the login prompt. The system may appear inactive during the pre-checks portion of the update; this is expected behavior and does not require you to reboot or shut down your appliances.

Planning the Update

Before you begin the update, you must thoroughly read and understand these release notes, especially Before You Begin: Important Update and Compatibility Notes on page 2. To ensure a smooth update process, you must also read the following sections.

IMPORTANT!   You must reimage appliances running Version 4.10.x of the system to Version 5.2 before you install this update. For more information and reimage instructions, see the *Version 5.2 Sourcefire 3D System Release Notes* and the *Sourcefire 3D System Installation Guide*.

Sourcefire 3D System Version Requirements

To update to Version 5.2.0.9, an appliance must be running at least Version 5.2. If you are running an earlier version, you can obtain updates from the Sourcefire Support Site.

A Defense Center must be running at least Version 5.2. to update its managed devices to Version 5.2.0.9.

The closer your appliances' current version to the release version (Version 5.2.0.9), the less time the update takes.

Virtual Appliance Operating System Requirements

You can host 64-bit virtual Sourcefire appliances on the following hosting environments:

- VMware ESX/ESXi 4.1
- VMware vSphere Hypervisor 5.0
- VMware vSphere Hypervisor 5.1

For more information, see the *Sourcefire 3D System Virtual Installation Guide*.

Time and Disk Space Requirements

The following table provides disk space and time guidelines for the Version 5.2.0.9 update. Note that when you update a managed device with the Defense Center, the Defense Center requires additional disk space on its `/Volume` partition.

Do **not** restart the update or reboot your appliance at any time during the update process. Sourcefire provides time estimates as a guide, but actual update times vary depending on the appliance model, deployment, and configuration. Note that the system may appear inactive during the pre-checks portion of the update and

after rebooting; this is expected behavior. If you encounter issues with the progress of your update, contact Sourcefire Support.

Time and Disk Space Requirements

APPLIANCE	SPACE ON /	SPACE ON /VOLUME	SPACE ON /VOLUME ON MANAGER	ESTIMATED TIME
Series 3 managed devices	32 MB	7175 MB	866 MB	44 minutes

Configuration and Event Backup Guidelines

Before you begin the update, Cisco **strongly** recommends that you back up current event and configuration data to an external location. This data is **not** backed up as part of the update process.

You can use the Defense Center to back up event and configuration data for itself and the devices it manages. For more information on the backup and restore feature, see the *Sourcefire 3D System User Guide*.

IMPORTANT!   Sourcefire does not support updating or reimaging appliances with more than one hard drive. You must remove additional hard drives before beginning the update.

When to Perform the Update

Because the update process may affect traffic inspection, traffic flow, and link state, Cisco **strongly** recommends you perform the update in a maintenance window or at a time when the interruption will have the least impact on your deployment.

Installation Method

Use the Defense Center's web interface to perform the update. Update the Defense Center first, then use it to update the devices it manages.

Although you can install a managed device update from its local web interface, Cisco strongly recommends using the Defense Center, especially for older or less powerful managed device models.

Order of Installation

Update your Defense Centers before you update the devices they manage.

Installing the Update on Clustered Devices

When you install an update on clustered devices, the system performs the update on the devices one at a time. When the update starts, the system first

applies it to the secondary device, which goes into maintenance mode until any necessary processes restart and the device is processing traffic again. The system then applies the update to the primary device, which follows the same process.

Installing the Update on Stacked Devices

When you install an update on stacked devices, the system performs the updates simultaneously. Each device resumes normal operation when the update completes. Note that:

- If the primary device completes the update *before* all of the secondary devices, the stack operates in a limited, mixed-version state until all devices have completed the update.
- If the primary device completes the upgrade *after* all of the secondary devices, the stack resumes normal operation when the update completes on the primary device.

Installing the Update on Clustered Stacks

When you install an update on a clustered stack, the system performs the update one stack at a time. When the update starts, the system first applies it to the secondary stack, which goes into maintenance mode until any necessary processes restart and the stack is processing traffic again. The system then applies the update to the primary stack, which follows the same process.

After the Installation

After you perform the update on either the Defense Center or managed devices, you **must** reapply device configuration and access control policies. Applying an access control policy may cause a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected. For more information, see the *Sourcefire 3D System User Guide*.

There are several additional post-update steps you should take to ensure that your deployment is performing properly. These include:

- verifying that the update succeeded
- making sure that all appliances in your deployment are communicating successfully
- updating your vulnerability database (VDB), if necessary

The next sections include detailed instructions not only on performing the update, but also on completing any post-update steps. Make sure you complete all of the listed tasks.

Updating Managed Devices

Although this release does not contain an update for Defense Centers, Cisco **strongly** recommends that you use them to update the devices they manage. A Defense Center must be at least Version 5.2 to update its managed devices.

Updating managed devices is a two-step process. First, download the update from the Support Site and upload it to the managing Defense Center. Next, install the software. You can update multiple devices at once, but only if they use the same update file.

For the Version 5.2.0.9 update, managed devices reboot. Managed devices do **not** perform traffic inspection, switching, routing, NAT, VPN, or related functions during the update. Depending on how your devices are configured and deployed, the update process may also affect traffic flow and link state. For more information, see Traffic Flow and Inspection During the Update on page 3.

WARNING!   Before you update a managed device, use its managing Defense Center to reapply the appropriate access control policy. Otherwise, the managed device update may fail.

WARNING!   Do **not** reboot or shut down your appliances during the update until after you see the login prompt. The system may appear inactive during the pre-checks portion of the update; this is expected behavior and does not require you to reboot or shut down your appliances.

To update managed devices:

1. Read these release notes and complete any required pre-update tasks.

    For more information, see Before You Begin: Important Update and Compatibility Notes on page 2 and Planning the Update on page 5.

2. Download the appropriate update from the Sourcefire Support Site:
    -   for Series 3 managed devices:
        ```
        Sourcefire_3D_Device_S3_Patch-5.2.0.9-4.sh
        ```

    IMPORTANT!   Download the update directly from the Support Site. If you transfer an update file by email, it may become corrupted.

    ---

3. Upload the update to the Defense Center by selecting **System > Updates**, then clicking **Upload Update** on the **Product Updates** tab. Browse to the update and click **Upload**.

    The update is uploaded to the Defense Center.

4. Make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

5. Click the install icon next to the update you are installing.

    The Install Update page appears.

6. Select the devices where you want to install the update.

    If you are updating a stacked pair, selecting one member of the pair automatically selects the other. You must update members of a stacked pair together.

7. Click **Install**. Confirm that you want to install the update and reboot the devices.

    The update process begins. You can monitor the update's progress in the Defense Center's task queue (**System > Monitoring > Task Status**).

    > **WARNING!**   If you encounter issues with the update (for example, if the task queue indicates that the update has failed or if a manual refresh of the task queue shows no progress for several minutes), do **not** restart the update. Instead, contact Support.

8. Select **Devices > Device Management** and confirm that the devices you updated have the correct software version: Version 5.2.0.9.

9. Verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

10. Reapply device configurations to all managed devices.

    > **TIP!**   To reactivate a grayed-out **Apply** button, edit any interface in the device configuration, then click **Save** without making changes.

11. Reapply access control policies to all managed devices.

    Applying an access control policy may cause a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected. For more information, see the *Sourcefire 3D System User Guide*.

Uninstalling the Update

The following sections help you uninstall the Version 5.2.0.9 update from your appliances:

Planning the Uninstallation

Before you uninstall the update, you must thoroughly read and understand the following sections.

Uninstallation Method

You must uninstall updates locally. You **cannot** use a Defense Center to uninstall the update from a managed device.

For all physical appliances and virtual Defense Centers, uninstall the update using the local web interface. Because virtual managed devices do not have a web interface, you must use the shell to uninstall the update.

Order of Uninstallation

Uninstall the update in the reverse order that you installed it. That is, first uninstall the update from managed devices, then from Defense Centers.

Uninstalling the Update from Clustered or Paired Appliances

Clustered devices and Defense Centers in high availability pairs must run the same version of the Sourcefire 3D System. Although the uninstallation process triggers an automatic failover, appliances in mismatched pairs or clusters do not share configuration information, nor do they install or uninstall updates as part of their synchronization. If you need to uninstall an update from redundant appliances, plan to perform the uninstallations in immediate succession.

To ensure continuity of operations, uninstall the update from clustered devices and paired Defense Centers one at a time. First, uninstall the update from the secondary appliance. Wait until the uninstallation process completes, then immediately uninstall the update from the primary appliance.

WARNING! If the uninstallation process on a clustered device or paired Defense Center fails, do **not** restart the uninstall or change configurations on its peer. Instead, contact Support.

Uninstalling the Update from Stacked Devices

All devices in a stack must run the same version of the Sourcefire 3D System. Uninstalling the update from any of the stacked devices causes the devices in that stack to enter a limited, mixed-version state.

To minimize impact on your deployment, Cisco recommends that you uninstall an update from stacked devices simultaneously. The stack resumes normal operation when the uninstallation completes on all devices in the stack.

Uninstalling the Update from Clustered Stacks

All devices in a clustered stack must run the same version of the Sourcefire 3D System. Uninstalling the update from any of the clustered, stacked devices causes the devices in that stack to enter a limited, mixed-version state.

To minimize impact on your deployment, Cisco recommends that you uninstall the update from all devices in a stack simultaneously. First, uninstall the update from the devices in the secondary clustered stack. Wait until the uninstallation process completes, then immediately uninstall the update from the devices in the primary clustered stack.

Uninstalling the Update from Devices Deployed Inline

Managed devices do **not** perform traffic inspection, switching, routing, NAT, VPN, or related functions while the update is being uninstalled. Depending on how your devices are configured and deployed, the uninstallation process may also affect traffic flow and link state. For more information, see Traffic Flow and Inspection During the Update on page 3.

After the Uninstallation

After you uninstall the update, there are several steps you should take to ensure that your deployment is performing properly. These include verifying that the uninstall succeeded and that all appliances in your deployment are communicating successfully.

The next sections include detailed instructions not only on performing the update, but also on completing any post-update steps. Make sure you complete all of the listed tasks.

Uninstalling the Update from a Managed Device

The following procedure explains how to use the local web interface to uninstall the Version 5.2.0.9 update from managed devices. You **cannot** use a Defense Center to uninstall the update from a managed device.

Uninstalling the Version 5.2.0.9 update results in a device running Version 5.2.0.8. For information on uninstalling a previous version, refer to the release notes for that version.

All managed devices reboot when uninstalling the Version 5.2.0.9 update. Managed devices do **not** perform traffic inspection, switching, routing, NAT, VPN, or related functions during the update. Depending on how your devices are configured and deployed, the update process may also affect traffic flow and link state. For more information, see Traffic Flow and Inspection During the Update on page 3.

To uninstall the update:

1. Read and understand Planning the Uninstallation on page 10.

2. On the managing Defense Center, make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

3. On the managed device, view the task queue (**System > Monitoring > Task Status**) to make sure that there are no tasks in progress.

   Tasks that are running when the uninstallation begins are stopped, become failed tasks, and cannot be resumed; you must manually delete them from the task queue after the uninstallation completes. The task queue automatically refreshes every 10 seconds. You **must** wait until any long-running tasks are complete before you begin the uninstallation.

4. Select **System > Updates**.

   The Product Updates tab appears.

5. Click the install icon next to the uninstaller that matches the update you want to remove, then confirm that you want to uninstall the update and reboot the device.

   The uninstallation process begins. You can monitor the uninstallation progress in the task queue (**System > Monitoring > Task Status**).

   WARNING!   Do **not** use the web interface to perform any other tasks until the uninstallation has completed and the device reboots. Before the uninstallation completes, the web interface may become unavailable and the device may log you out. This is expected behavior; log in again to view the task queue. If the uninstallation is still running, do **not** use the web interface until the uninstallation has completed. If you encounter issues with the uninstallation (for example, if the task queue indicates that the update has failed or if a manual refresh of the task queue shows no progress for several minutes), do **not** restart the uninstallation. Instead, contact Support.

6. After the uninstallation finishes, clear your browser cache and force a reload of the browser. Otherwise, the user interface may exhibit unexpected behavior.

7. Log in to the device.

8. Select **Help > About** and confirm that the software version is listed correctly: Version 5.2.0.8.

9. On the managing Defense Center, verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Issues Resolved in Version 5.2.0.9

You can track defects resolved in this release using the Cisco Bug Search Tool (https://tools.cisco.com/bugsearch/). A Cisco account is required. To view defects addressed in older versions, refer to the legacy caveat tracking system. The following issues are resolved in Version 5.2.0.9:

- **Security Issue** Resolved an issue where certain rare, high availability packets caused traffic inspection to stop while components restarted. (CSCuu10871)

Issues Resolved in Previous Updates

Previously resolved issues are listed by version.

Version 5.2.0.8

- **Security Issue** Addressed multiple vulnerabilities in SSLv3 that allowed external attacks on client connections as described in CVE-2014-3566.
- **Security Issue** Addressed a vulnerability in Linux and other third party products. The fix is addressed in CVE-2007-6750.
- Resolved an issue where multiple network address translation (NAT) requests caused a disruption in traffic. (141861/CSCze93346)
- Resolved multiple issues that resulted in system issues on stacked devices. (142097/CSCze93525, 143490/CSCze94894)
- Resolved an issue where two conflicting static network address translation (NAT) rules caused system issues. (142153/CSCze93418)
- Resolved an issue where, if you clustered your Series 3 devices without connecting the high availability link interface using a cable and then restarted the system, the device's high availability link interface erroneously appeared to be active even if it was not. (142241/CSCze93447)
- Resolved an issue where manually placing a Series 3 device running Version 5.2.0.7 or earlier with an inline set into hardware bypass prior to updating to a new version caused the system to experience traffic disruption. (142322/CSCze93431)
- Resolved an issue where the Defense Center's web interface displayed only 50 user roles even if there were more than 50 valid user roles available. (142627/CSCze93599)
- Resolved an issue where the modbus preprocessor failed to generate events. (142758/CSCze93162)
- Improved data pruning. (142948/CSCze94297)
- Resolved an issue where access control rules containing web application conditions were incorrectly interpreted as case sensitive domain names and caused the system to ignore web application traffic that did not contain exact matches. (143069/CSCze94529)

- Resolved an issue where, if the system attempted to save multiple scheduled reports to remote storage, reports saved to local storage instead. (143707/CSCze94120)
- Resolved an issue where you could not switch between the months on the Scheduling page. (143788/CSCze94220)
- Resolved an issue where the primary and secondary devices in a clustered stack were unable to reestablish high availability link connectivity if the system experienced a loss of high availability link. (143906/CSCze94080)
- Resolved an issue where, during the processing of retransmitted transmission control protocol (TCP) packets, the devices could experience additional latency. (144222/CSCze94683)
- Resolved an issue where the system experienced a FSIC failure. (144878/CSCze95325)
- Resolved an issue where the 40GB fiber NetMod traffic statistics was incorrectly logged traffic on the wrong 40GB port. (145515/CSCze95830)
- Resolved an issue where you were unable to configure your Defense Center as the network time protocol (NTP) source. (CSCus75305).

Version 5.2.0.7

- Security Issue Addressed an arbitrary injection vulnerability allowing unauthenticated, remote attackers to execute commands via Bash. The fix addresses CVE-2014-6271 and CVE-2014-7169. For more information, refer to the Cisco Security Advisory page at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140926-bash. (144861/CSCze95469, 144940/CSCze95446, 144947/CSCze96152)

Version 5.2.0.6

- Security Issue Addressed multiple cross-site scripting (XSS) vulnerabilities.
- Security Issue Addressed multiple cross-site request forgery (CSRF) vulnerabilities.
- Security Issue Addressed multiple injection vulnerabilities, including HTML and command line injections.
- Security Issue Addressed multiple vulnerability issues in Linux, strongSwan, and Wireshark, including those described in CVE-2013-2237, CVE-2013-5718, CVE-2013-5719, CVE-2013-5720, CVE-2013-5721, CVE-2013-5722, and CVE-2013-2338.
- Resolved an issue where, if you modified the interface type on a routed or switched interface associated with a hybrid interface, applying the device configuration failed. (132221/CSCze88314)
- Resolved an issue where, if you configured Simple Network Management Protocol (SNMP) polling on a Series 3 managed device, the system retrieved non-compliant RFC data. (135323/CSCze89413)

- Resolved an issue where, if you configured a custom table populated with data from either the correlation events table or the applications table, then selected **Source IP** as a common field, updates to Version 5.3 failed. (135735/CSCze89511)

- Improved memory usage of the Sourcefire Data Correlator. (135868/CSCze89437, 138800/CSCze91288)

- Improved the performance of the Rule Management page (**Policies > Correlation > Rule Management**). (137905/CSCze91247)

- Resolved an issue where, if you created a backup file for configuration data, the system included extraneous geolocation data and increased the size of the backup file. (137976/CSCze90600)

- Resolved an issue where the system provided incorrect speed data for fiber interfaces with speeds of 4GB and faster. (138072/CSCze90543)

- Resolved an issue where, if you applied an access control rule with end-of-connection logging enabled on a Series 3 managed device, large quantities of traffic caused system issues. (139931/CSCze91584)

- Improved the firmware on 8000 Series and 3D9900 devices to optimize resource usage for packet processing. (140166/CSCze91569)

- Resolved an issue where, in rare cases, the system generated health alert emails containing indecipherable messages. (140442/CSCze92157)

- Resolved an issue where scheduled vulnerability database (VDB) updates failed if Greenwich Mean Time (GMT, also known as UTC) was not your local time zone. (140464/CSCze91826)

- Resolved an issue where, if you registered more than 100 managed devices to a Defense Center, the Defense Center experienced system issues. (140512/CSCze92416)

- Resolved an issue where creating a new scheduled task on the Scheduling page (**System > Tools > Scheduling**) caused the system to display an authorization error message. (140556/CSCze92060)

Version 5.2.0.5

- Security Issue Eliminated a cross-site scripting (XSS) vulnerability (CVE-2014-2012) in the intrusion rule editor pages that could allow an attacker to access and disclose information, imitate user actions and requests, or execute arbitrary JavaScript. Special thanks to Liad Mizrachi Check Point Security Research Team for reporting this issue. (136539)

- Security Issue Eliminated a cross-site request forgery (CSRF) vulnerability (CVE-2014-2011) in the User Configuration page that could allow an attacker to add or edit user accounts. Special thanks to Liad Mizrachi Check Point Security Research Team for reporting this issue. (136910)

- Security Issue Eliminated a CSRF vulnerability (CVE-2014-2028) in the User Management page that could allow an attacker to activate, deactivate, edit, or delete user accounts. Special thanks to Liad Mizrachi Check Point Security Research Team for reporting this issue. (136913)

- Security Issue Eliminated an XSS vulnerability (CVE-2014-2275) in the Scheduling page, Health Monitor page, and event viewers that could allow an attacker to access and disclose information, imitate user actions and requests, or execute arbitrary JavaScript. Special thanks to Adi Volkovitz Check Point Security Research Team for reporting this issue. (137849, 137852, 137855)

Version 5.2.0.4

- Resolved an issue where, in some cases, NAT rule validation failed if you configured a static NAT rule with an original destination network that overlapped the translated source network on a dynamic NAT rule in the same NAT policy. (131490)

- Resolved an issue where, after you selected **Logarithmic** as the Vertical Scale for the Intrusion Event dashboard widget, the system refreshed the widget and instead displayed the data using the default **Linear** Vertical Scale. (132203)

- Improved the stability of host data queries to the eStreamer client. (132239, 134244, 134295)

- Improved the stability of connection event processing if your correlation policy contained a rule based on a connection event and specified a **NETBIOS Name** rule condition. (132562)

- Resolved an issue where the eStreamer client omitted intrusion rule name metadata for intrusion events if you associated a Sourcefire-provided intrusion policy with an access control rule on a Defense Center running Version 5.2.0.2. (132667)

- Improved system stability in cases where you applied an access control policy revision that changed the file inspection options in an access control rule. (132741)

- Resolved an issue where setting the maximum transmission unit (MTU) of an inline set on a Series 2 or a virtual device to a value below 1518 caused a disruption in traffic. (134256)

Version 5.2.0.3

- Resolved a NTP time synchronization issue between managed devices and Defense Centers. (121909)

- Resolved an issue where, in some cases, FireSIGHT rule state recommendations did not generate if an intrusion rule variable contained a network object. (125910)

- Resolved an issue where, in some cases, the eStreamer client failed to deserialize network discovery user events and the system generated an error message. (126827)

- Resolved an issue where, after updating an appliance running Version 5.1.x of the Sourcefire 3D System and Version 2.0.3 of the Sourcefire User Agent to Version 5.2 of the Sourcefire 3D System, the system generated an extraneous health alert. (127082, 127265, 127724)

- Resolved an issue where, if the system logged the only intrusion event associated with a connection as `would have dropped`, the associated connection logged with the incorrect action of `Block`. (127141)

- Resolved an issue where, in rare cases, the system detected a user login through network discovery but the Defense Center incompletely logged the user data. (127274)

- Improved the stability of custom application detectors. (127309)

- Resolved an issue where you could not replace one NetMod with another on devices managed by Defense Centers in a high availability configuration. (128091)

- The system now notifies you upon intrusion policy commit if your intrusion policy contains invalid system default variable configurations. (129105)

- Resolved an issue where changes to the system variable set from within an intrusion policy were not applied if the default action of your access control policy was a Sourcefire authored policy. (129179)

- Improved the stability of the `byte_extract` keyword and the HTTP inspect preprocessor. (129329, 129843, 130005)

- Resolved a hardware issue that, in rare cases, could cause a disruption in traffic. (130055)

- Resolved a memory leak on managed devices that, in some cases, necessitated a system reboot. (130198)

- Resolved a memory leak within the eStreamer client. (130478)

- Security Issue Eliminated a vulnerability that could allow a remote attacker to execute unauthorized IPMI commands if Lights-Out Management was enabled on a Series 3 appliance. For more information, log in to the Customer Center and access the KB article at https://na8.salesforce.com/articles/Informational/000002045. (131040)

- Security Issue Resolved an issue where the Sourcefire 3D System web server had the potential to execute system commands as root. Special thanks to Detmar Liesen and Christian Rahmen at Information und Technik Nordrhein-Westfalen (IT.NRW) for reporting this issue. (131737)

- Security Issue Eliminated a vulnerability that could allow an attacker to execute Linux commands via the filter search field on the System Log page. For more information, log in to the Customer Center and access the KB article at https://na8.salesforce.com/articles/Informational/000002058. (131738)

Version 5.2.0.2

- Resolved an issue where, in some cases, if you configured passive interfaces and assigned them to a passive security zone in the object manager, the device configuration apply failed. (125119)

- Resolved an issue where, in rare cases, the system did not provide **URL Category** or **URL Reputation** values for unknown URLs. (125151)

- Resolved a hardware issue where a virtual switch did not pass IPv6 traffic if you did not configure IPv6 support on the connected hybrid interface. (125306)

- Resolved an issue where, in some cases, the system triggered false positive intrusion events on the SMTP preprocessor rules 124:1 and 124:3. (124688)

- Resolved an issue where traffic matched an access control policy block rule and the system evaluated it against the access control policy default action configured as an intrusion policy. (124732)

- Resolved a synchronization issue where, in rare cases, clusters lost their clustered status. (125497)

- Resolved an issue where accessing the intrusion rule editor from the packet view (**Analysis > Intrusion > Events**) caused the system to display an error message and log the attempt as an unauthorized action. (125770)

- Resolved an issue with the Sourcefire Data Correlator where complex queries slowed the system's ability to process new connection events. (125754)

- Updated Sourcefire documentation to reflect that when you reimage a device with interfaces configured to fail open, they will revert to a non-bypass (fail closed) configuration at first boot and remain closed until you configure bypass mode for them. (125957)

- Improved performance statistics logging to more accurately reflect packet counts per time interval. (126437)

- Resolved an issue where the device management page showed managed devices running an outdated version. (126564)

- Resolved an issue where, in some cases, system updates failed to download when you used a NLTM authenticated proxy server. (126872)

Version 5.2.0.1

- The About page (**Help > About**) and Advanced display option for the Appliance Information dashboard widget now show the current version of Snort running on a Defense Center. (121228, 123403, 124615)

- Resolved an issue where, during an update, a device in a clustered, inline deployment could fail over incorrectly. (123239)

- Resolved an issue where, in some cases, device configuration apply to a stack failed if it contained a NAT policy that referenced invalid interfaces. (123540)

- Resolved an issue where, in some cases, intrusion events displayed incorrect VLAN ID information. (123696)

- Resolved an issue where, in some cases, access control policy apply did not succeed on a cluster with both state sharing and **Inspect Local Router Traffic** enabled. (123710)

- Resolved an issue where the intrusion policy comparison view stalled if the option to update the base policy with intrusion rule updates was disabled in the base intrusion policy. (123739)

- Resolved an issue where, in some cases, adding two or more detection patterns to an application protocol detector drained system resources. (123767)

- Resolved a firmware issue where NAT, access control, or system policy apply could fail on 3D7010, 3D7020, or 3D7030 managed devices configured with NAT policies. (123920)

- Resolved an issue where you could not break clusters or stacks from the command line interface (CLI) on the primary device if the managing Defense Center was unavailable. (123932)

- Improved the accuracy of the FireSIGHT host limit count. (124091)

- The Product Updates widget now displays the correct geolocation update version running on the Defense Center. (124616)

- Improved the reliability of the Context Explorer when accessed from the dashboard. (124638)

- Resolved an issue where, after completing the update to Version 5.2, Snort did not load if an intrusion policy contained invalid local rules. (124935)

- Resolved an issue where, in some cases, configuration backups failed after the system included extraneous geolocation and Security Intelligence statistics. (125131)

- Resolved an issue where Snort did not load on managed devices if an intrusion policy contained a network object used as a variable value and an SRU or custom rule file was installed. (125139)

Version 5.2

- The command line interface (CLI) command `show traffic-statistics` now displays statistics for virtual as well as physical interfaces. (102347)

- Resolved an issue where clicking the evaluate icon to evaluate an application detector with a packet capture prevented you from activating the detector. (102464)

- Added, modified, and removed numerous preprocessor rules. (102633, 104588, 111941, 113970, 118178, 118500, 118553, 122038)

- Resolved an issue where the intrusion event views incorrectly displayed XFF data. (102655, 110873, 113369)

- Improved the use of colors throughout the user interface. (104562, 112517)

- Report text now supports the ASCII code 8217 quotation mark. (105857)

- When navigating from a Custom Analysis dashboard widget to an event viewer page, a message now appears to clarify any potential event count differences between the two pages. (106867)

- Resolved an issue where, in some cases, the system generated errors on packets when an interface returned to a routed configuration after being temporarily configured as a switched interface. (106986)

- Improved the system's ability to identify intrusion policy validation errors. (107105)

- Resolved an issue where, in some cases, intrusion policies did not save when inline normalization allowed TCP options that contained both commas and blank spaces. (108289)

- Status icons on the Device Management page (**Devices > Device Management**) now indicate whether a device in a clustered configuration is in a degraded state. (108908)

- Improved the performance of the `content` keyword in intrusion rules. (109059, 118112)

- Resolved an issue where custom HTTP response pages for Interactive Block access control rules did not appear consistently or allow users to bypass successfully. (109186, 110109, 110110, 111661)

- Resolved an issue where threshold values of 86400 seconds (24 hours) for the packet view in the event viewer could not be saved successfully. (109187)

- Resolved an issue where, in some cases, the system incorrectly identified a correlation policy as active. (110111)

- Added a new troubleshooting option to the Performance Statistics configuration. (110470)

- Resolved an issue where intrusion rules did not generate events if they defined SIP methods in the `sip_method` keyword that were not already defined in the SIP preprocessor. (110532)

- Resolved an issue where two passive interfaces on appliances with identical access control policy and rule settings, but in different security zones, could produce different connection events from the same traffic. (110575)

- Resolved an issue where, after completing an access control or intrusion policy apply, the system generated extraneous process status health alerts. (110578, 120317)

- Resolved an issue where, in some cases, the primary device in a stack appeared perpetually active in the device management portion of the user interface. (110702)

- Resolved an issue where, in some cases, the system experienced issues with task status reporting during access control policy apply on a Defense Center managing clustered devices. (110704)

- Resolved an issue where reports generated graphs and charts without labels for portscan events. (110828)

- The audit log (**System > Monitoring > Audit**) now provides details about settings that changed during edits to the system policy. (110860)

- Resolved an issue where managed devices continued to store user data purged from their managing Defense Center. (111234)

- Resolved a display issue on the intrusion policy comparison page. (111350)

- Improved accuracy of intrusion policy comparison reports. (111396)

- Resolved an issue where, in some cases, two interfaces viewing the same network traffic experienced issues with application detection. (111554)

- Improved performance of the TCP stream preprocessor. (111871, 120171, 122391)

- Resolved an issue where negated predefined search objects lost the negation after the search was saved. (111912)

- Added an alert to notify users that accented characters may not display properly in custom login banners. (111957)

- Improved performance of custom workflows based on the hosts table. (112204)

- Optimized database queries to improve performance of the connection events table. (112506, 117165)

- Resolved an issue where, in some cases, intrusion events generated from reassembled traffic did not contain packet data. (112519)

- Resolved an issue where physical appliances experienced system issues after running continuously for a minimum of 208 days. (112556, 112765, 112766)

- Improved accuracy of operating system identification in the network map. (112843)

- Resolved an issue where, in some cases, the host profile showed inactive ports and services as pending. (113213)

- Resolved an issue where, in rare cases, the system omitted the first line of text from an uploaded list of security intelligence objects encoded in UTF-8. (113578)

- Resolved an issue where the eStreamer service returned events from before the specified start time if the event request did not contain the `FLAG_DETAIL_REQUEST` flag. (113599)

- Resolved an issue where, in some cases, the system incorrectly sorted the **Status** column of custom report templates created based on the health events table. (113618)

- Improved connection tracking to identify a separate ICMP session for each ICMP type in a packet. (113663)

- If you use a Serial Over LAN (SOL) connection to restore a 3D7010, 3D7020, or 3D7030 managed device to factory settings, and a Lights-Out Management (LOM) user is logged in when you begin the restore, that LOM user is now correctly disconnected and deleted. (113706, 113824)

- Resolved an issue where, in some cases, the system failed to email reports. (114256)

- The system now allows users with either a FireSIGHT license or a RNA Host license to enable FireSIGHT recommendations. The system can alert users if they attempt to enable FireSIGHT recommendations without available hosts. (114430)

- Resolved an issue where, in some cases, the system omitted NetBIOS information from the host profile. (115291)

- Resolved an issue where the system generated health alerts about nonexistent issues with discovery event generation. (115308)

- Resolved an issue where uploading a text file to create a new Security Intelligence list caused the system to identify IP addresses as invalid. (115489)

- Resolved an issue where, in some cases, setting thresholds or suppressions from the intrusion event table caused system errors. (115950)

- Improved the performance of the context menu accessed from the intrusion event views. (116165)

- Resolved an issue where, in passive deployments, the system did not perform network discovery on traffic for networks where you constrained the associated discovery rule by security zone. (116462)

- Resolved an issue where the system restarted during intrusion policy apply due to detected SMTP preprocessor changes, even if there were no changes to the SMTP preprocessor. (116830)

- Resolved an issue where the system incorrectly identified versions of Internet Explorer while the browser operated in compatibility mode. (117530)

- Resolved an issue that prevented you from suppressing a GID 134 rule. (117593)

- Resolved an issue where drilling down to the operating systems table view from the **Network Information** graph in the Context Explorer improperly constrained the data. (117996)

- Improved the performance of the HTTP inspect preprocessor. (118025, 118713, 119009)

- Improved the performance of incident generation and reporting in intrusion policies. (118096, 118121)

- Improved the performance of line charts in dashboard widgets. (118173)

- Resolved an issue where, in rare cases, end-of-connection events were not logged. (118688)

- Resolved an issue where the system truncated text in long syslog messages. (118816)

- Resolved an issue where some TCP connections detected by virtual devices were not logged to the Defense Center. (118827)

- Resolved an issue with the formatting of text files sent with email alerts by the Defense Center. (119267)

- Improved the IP defragmentation preprocessor to avoid a possible evasion using packet fragments. (119531)

- Resolved an issue where TCP connections that were reset took a long time to generate connection events. (119557)

- Resolved an issue where the system experienced issues with packet reassembly when the port configuration in an applied intrusion policy differed from the base intrusion policy. (119714)

- Improved functionality of access control rules with user conditions. (119962)

- Resolved an issue where intrusion rules using the `file_data` keyword did not drop traffic if **Drop when Inline** was disabled in the base intrusion policy. (120156)

- Resolved an issue where the TCP stream preprocessor did not correctly identify the server in HTTP traffic when detected midstream. (120170)

- Improved Teredo traffic decoding. (120292)

- Resolved an issue where, in some cases, intrusion events generated during a network discovery policy apply were associated with incorrect security zones. (120316)

- Resolved an issue with high availability configurations where you could not change the secondary Defense Center to the primary role if the original primary Defense Center was offline. (120327)

- Improved logging of Security Intelligence decisions to the syslog. (120564, 120565, 121050)

- Resolved an issue where, in some cases, URL filtering database updates were not synchronized from the Defense Center to managed devices. (120572)

- Resolved an issue where access control policy apply failed when the default action was **Block All Traffic** and the HOME_NET variable was `any`. Because this combination is invalid, the system now warns you if you attempt to configure it. (120578)

- Resolved an issue where fragmented IP traffic that would normally match a **Trust** access control rule and pass without further inspection was instead evaluated by the intrusion policy associated with the default action. (120734)

- Resolved an issue where, in some cases, changing the dashboard widget time range caused the widget to display incorrect event statistics. (121009)

- Resolved an issue where the system did not log correlation rules that referenced user logins. (121129)

- Resolved an issue where the system did not detect files transferred in HTTP POST requests. (121204)

- Resolved an issue where, in some cases, intrusion email alerts did not associate events with the correct managed device. (121278)

- Resolved an issue where, in rare cases, very large troubleshooting files did not download successfully. (121471)

- Resolved an issue where, in some cases, adding an interface to a security zone caused access control policy apply to fail. (121511)

- Resolved an issue where, in some cases, eStreamer reported incorrect data for intrusion event record type 207. (121555)

- When viewing packet information for intrusion events, the timestamp now reports the correct time in all cases. (121685)

- Resolved an issue where, in some cases, the Intrusion Events by Impact report template preset reported incorrect impact flag data. (121864)

- When you view intrusion events with a search constraint of **Source IP**, this constraint now appropriately changes to **Sending IP** if you navigate to the Malware or Files tabs. (122034)

- Resolved an issue where, in rare cases, devices failed to process packets and log intrusion events. (122130)

- Improved performance of the Context Explorer when handling large datasets. (122276)

- Resolved an issue where, in some cases, eStreamer logged packets before their associated event records. (122365)

- Resolved an issue where, in some cases, the system did not enable traffic profiles with inactive periods. (122440)

- Resolved an issue in network discovery policies where changes to user protocol detection configuration did not take effect. (122763)

- Improved the system's reporting of error messages generated by the eStreamer client. (122859)

- Resolved an issue with the eStreamer client where SHA-256 values were incorrectly reported by the Defense Center. (122869)

- Resolved an issue where users were not prompted to enable the TCP stream preprocessor when saving an intrusion policy with the rate-based attack prevention preprocessor enabled and the TCP stream preprocessor disabled. (122905)

- Resolved an issue where, in rare cases, intrusion rules that triggered on pruned sessions applied the rule action to current sessions. (122990)

Known Issues

The following new known issues are reported in Version 5.2.0.9:

- In some cases, if you attempt to import a policy referenced by another policy as a shared layer or as a base policy, importing the policy may fail. (144946/CSCze96151)

- In some cases, managed devices stop processing traffic when the Defense Center updates a large Security Intelligence Feed referenced in an access control policy during a policy apply. As a workaround, reapply the policies containing Security Intelligence Feeds. (CSCus19921)

- In some cases, if your system includes an SSL Visibility Appliance (SSLVA) or a Cisco SSL appliance and you create a file policy containing a Web Application category condition and a Block Malware rule, your first attempt to download a file identified as malware over HTTPS may fail. As a workaround, disable the file policy. (CSCus72505)

Known Issues Reported in Previous Releases

The following is a list of known issues that were discovered in previous releases of the Sourcefire 3D System:

- You must use the Defense Center's web interface to unregister a managed device. If you unregister a device using either the device's web interface or its command line interface (CLI), it is not removed from the Defense Center. (112659)

- The system will generate a health alert if the Defense Center is unable to connect to the Sourcefire cloud. To troubleshoot, ensure the connection from the Defense Center to the Sourcefire cloud (`54.243.248.19` and `54.243.248.162`) on port 32137 is working properly. (112708)

- If multiple files are attached to a single email, the system may incorrectly identify files after the first. (114523)

- If you attempt to create multiple static NAT rules with the same original values, the system may experience issues with traffic mapping. (116148)

- In some cases, the Defense Center may show a cluster in a degraded state when it has already recovered, generating extraneous system alerts. (118122)

- When Lights-Out Management is enabled, the system also enables a web server in the background. The web server does not drain system resources and has no known exploits. (119456)

- Sourcefire documentation currently does not reflect that, on a Series 3 device, TCP connections matching a Trust access control rule on the first packet generate different events depending on the presence of a Monitor rule. If an active Monitor rule is present, the system generates both a beginning and end-of-connection event, as expected. If no monitor rule is active, the system does not generate a beginning-of-connection event. (121060)

- Do not name security zone objects using the pound sign (#); it may cause errors during device reconfiguration. (121514)

- If you attempt to break a stack that was registered using DNS during a period when DNS is disabled, you will experience system issues. Do **not** attempt this. (122709)

- In some cases, intrusion event counts in the dashboard may not match the counts in the event viewer. (122743, 123040, 122936)

- When creating stacks of devices from different device groups, the secondary device in the stack both retains membership in its original group and becomes associated with the stack's primary group. The user interface does not alert the user to this behavior. (122802)

- In some cases, your network discovery policy may not function as expected if you apply two or more network discovery rules that apply to the same zones and networks but are configured to discover different hosts, users, and applications. (122853)

- In rare cases, the system may require up to 3 hours to complete an update or uninstall to Version 5.2 of the Sourcefire 3D System on a 3D7110 or 3D7120 managed device. Do **not** interrupt the update; allow the post-update reboot to finish completely. (124148)

- If a device group contains an inactive managed device, you may be unable to edit the device group. (124286)

- In some cases, if you begin installing an intrusion rule update during a system update, the intrusion rule update fails. To avoid this, do **not** attempt to install an intrusion rule update during system update. (124290)

- You can not use IPv6 addresses to configure connections to Sourcefire User Agents (**Policies > Users**). As a workaround, configure the connection using the associated IPv4 addresses instead. (124377)

- In some cases, the system may trigger false positive events on the SMTP preprocessor rule124:10. (125449)

- In rare cases, the system does not terminate a rule update installation if the installation fails in an early stage. If this occurs, you should attempt a rule update reinstallation and contact Support if the issue persists. (125368)

- In some cases, enabling sensitive data detection in your intrusion policy may not generate events for all packets containing sensitive data. (125588)

- If you create a custom analysis dashboard widget based on a saved connection event search that uses data in fields without an asterisk (*****), the widget displays incorrect data. Only the fields that constrain connection summaries can constrain custom analysis dashboard widgets based on connection events. (127324, 127327)

- If you apply a VPN deployment on a stack, cluster, or clustered stack and then unregister the stack, cluster, or clustered stack from its managing Defense Center, the VPN deployment remains active on the stack, cluster, or clustered stack when you register the appliances to another Defense Center. Additionally, you cannot manage the VPN deployment from the new Defense Center. As a workaround, remove the VPN deployment from the stack, cluster, or clustered stack before unregistering it from the Defense Center. (128816, 130728)

- In some cases, the system experiences issues with user account management if devices running Version 5.1.1.x are managed by a Defense Center running Version 5.2.x.x. As a workaround, update your managed devices to Version 5.2. (130024)

- If a managed device processes traffic only from the initiator of a TCP connection, the system does not log a connection event at the end of the connection. (126040)

- If you create a custom saved search for intrusion events with the **Generator** (GID) field populated, the search returns empty. (126109)

- In some cases after completing a scheduled rule update import and subsequent intrusion policy reapply, Defense Centers in a high availability configuration may incorrectly show intrusion policies as out-of-date. (126670)

- If you register a managed device as the only device on a Defense Center with an existing custom network discovery policy configuration, the device does not detect hosts or users until you edit, modify, and reapply the existing network discovery policy. (127633)

- If you modify the device configuration on a clustered stack and immediately apply your changes, the apply fails and the system displays an error message in the task status queue. The device configuration apply succeeds after a second attempt. (121625)

- In some cases, custom intrusion rule classifications referenced by correlation rules revert to predefined rule classifications after you install an intrusion rule update. (122163)

- If you configure a custom analysis dashboard widget based on the Connection Summary Data table and the **Ingress Interface**, **Ingress Security Zone**, **Egress Interface**, or **Egress Security Zone** fields, the widget displays no data. (122857)

- If you edit and save your access control policy ten or more times without applying the changes to your devices and then install a new version of the Sourcefire 3D System, the system shows your access control policy as unapplied. To avoid this issue, apply access control policies completely before installing system updates. (123003)

- If the DNS entries in your network environment for your LDAP server's hostname and IP address do not match, LDAP authentication may fail. (123447)

- In rare cases, the Defense Center may not back up events onto remote storage. (124350)

- In some cases, if you set an operating system identity from the host profile or network map, the system displays **Please wait, loading…** even after the pop-up window has loaded completely. (124918, 128594)

- In some cases, executing large Nmap scans may cause system issues. As a workaround, reduce the size of the Nmap scans to include fewer targets. (124999)

- If you attempt to install a version of the Sourcefire Geolocation Database (GeoDB) that is already installed on your system, the system does not inform you that the update failed because the GeoDB version was already installed. (125183)

- If you configure an Nmap scan and specify a device in the **Remote Device Name** field, the system runs the scan from the device even if you are using a remediation where **Scan from reporting device** is disabled. (125608)

- In some cases after importing a new intrusion rule update, the number of imported rules in the intrusion policy may not match the number of rules in the import log. (125900)

- In some cases, the system may not log connection events for IPv6-in-IPv4 traffic if the access control policy contains an access control rule with connection event logging enabled and any of the following ports selected: `IP 0`, `IP-ENCAP 4`, `IPv6 41`, `IPv6-ROUTE 43`, `IPv6-FRAG 44`, `GRE 47`, `ESP 50`, or `IPv6-OPTS 60`. (126117, 126746)

- In some cases, if you configure a syslog alert response to send connection events to the syslog, the system may omit data from the **Initiator Country**, **Responder Country**, **Client Version**, **Application Risk**, **Business Relevance**, **Intrusion Events**, **Files**, **TCP Flags**, **NetBIOS Domain**, **Initiator Packets**, **Responder Packets**, **Initiator Bytes**, or **Responder Bytes** fields. (127682)

- If you configure a traffic profile and a correlation rule to trigger on traffic spikes at or above two standard deviations, the system may not generate a correlation event. (128107)

- In rare cases, the 3D8120, 3D8130, 3D8140, and 3D8250 may experience system issues that require you to reboot the appliance. (128689)

- If you disable **ldap protocol detection** in your network discovery policy, the Defense Center stops logging user agent login data. (128741)

- In some cases, if you schedule an automatic LDAP user data retrieval, you cannot perform on-demand user data retrieval and download. (128962)

- In rare cases, automatic application bypass (AAB) activates during network discovery policy apply. (129230)

- Critical Issue After completing an event-only backup, the backup process enters an unrecoverable state. Do **not** attempt an event-only backup. As a workaround, back up both configurations and events. (129231)

- In some cases, if you view reviewed intrusion events and drill down to the packet view, there are no visible events and the reviewed constraint is removed. (129257)

- In rare cases, installing Version 5.2 or later on a 3D6500 managed device may cause system issues. (129561)

- In some cases, the system incorrectly identifies SMTP and generates a connection event with missing application information if the SMTP server responds with a connection error. (130085)

- In rare cases, the system may generate critical health alert emails containing indecipherable messages. (130518)

- In some cases, the system may incorrectly sort values in the **Type** column or omit names from the **Security Zones** column on the security zones page in the object manager. (130569, 130631, 130632)

- In some cases, drilling down in a custom workflow may redirect you to the incorrect packet view page for an intrusion event. (130620)

- In some cases, the system restore boot option does not output to the serial port on managed devices even if you selected **Physical Serial Port** as the remote console access option. (130772)

- In several places, the documentation incorrectly indicates that you can add IP address ranges to network objects. The Sourcefire 3D System currently supports adding individual IP addresses or address blocks to network objects, not ranges. (130821, 130992)

- In some cases, 3D8250, 3D8260, 3D8270, and 3D8290 managed devices with 10G or 40G NMSB may experience compatibility issues with 10G NFTW NetMods. To be compatible with 10G NFTW Netmods, 10G NMSB must be revision 7 or later and 40G NMSB must be revision 8 or later. (131189)

- In rare cases, the table view of servers (**Analysis > Hosts > Servers**) may duplicate servers and produce inaccurate server counts. (131329)

- The eStreamer client omits file policy UUID metadata from type 502 intrusion events. (131362)

- If you schedule multiple simultaneous reporting tasks when using remote storage, the system may fail to send all reports to the selected remote storage location. As a workaround, schedule report generation tasks in 30-minute intervals. (131805)

- Sourcefire documentation does not reflect that you must disable Spanning Tree Protocol (STP) on any third-party switching equipment connected to a device's management interface before connecting to a Series 3 appliance using LOM/SOL. (132488)

- Configuring a proxy server to authenticate with a Message Digest 5 (MD5) password encryption for malware cloud lookups is not supported. (135279)

- If Greenwich Mean Time (GMT, also known as UTC) is not your local timezone, scheduled geolocation database (GeoDB) updates may fail. If your local timezone is +X number of hours from GMT, schedule GeoDB updates for `x:00` or later. If your local timezone is -X number of hours from GMT, schedule GeoDB updates for `(24:00 - x)` or earlier. For example, if your local timezone is UTC-5, schedule updates before `19:00` local time. (135756)

- The documentation incorrectly states the following: `If a secondary device fails, the primary device continues to sense traffic, generate alerts, and send traffic to all secondary devices. On failed secondary devices, traffic is dropped. A health alert is generated indicating loss of link.`

  The documentation should specify that, if the secondary device in a stack fails, inline sets with configurable bypass enabled go into bypass mode on the primary device. For all other configurations, the system continues to load balance traffic to the failed secondary device. In either case, a health alert is generated to indicate loss of link. (138269)

- The documentation does not reflect that, if you enable an intrusion rule that checks for a flowbits state on traffic over a port, and enable at least one other rule that affects assigning the same flowbits state for traffic over the same port, when you apply or reapply the policy, the system does not automatically enable any other rule within the policy that affects assigning that flowbits state. (138507, 141143)

- In an access control policy, the system processes certain Trust rules before the policy's Security Intelligence blacklist. Trust rules placed before either the first Monitor rule or before a rule with an application, URL, user, or geolocation-based network condition are processed before the blacklist. That is, Trust rules that are near the top of an access control policy (rules with a low number) or that are used in a simple policy allow traffic that should have been blacklisted to pass uninspected instead. (138743, 139017)

- Security Issue Sourcefire is aware of a vulnerability inherent in the Intelligent Platform Management Interface (IPMI) standard (CVE-2013-4786). Enabling Lights-Out Management (LOM) on an appliance exposes this vulnerability. To mitigate the vulnerability, deploy your appliances on a secure management network accessible only to trusted users and use a complex, non-dictionary-based password. To prevent exposure to the vulnerability, do not enable LOM. If you enable LOM and expose this vulnerability, change the complex password every three months. (139286, 140954)

- The documentation does not reflect that, if you register a cluster, stack, or clustered stack of devices to a Defense Center, you may have to manually reapply the device configuration. (142411, 141602)

- In some cases, if you generate a report from a report template, reports only display the IP address if the system cannot resolve the IP address to a host name. (142640)The documentation does not reflect that Lights-Out Management (LOM) users on 7100 Family devices must limit their password to 16 characters rather than 20 characters. (142752)

Features Introduced in Previous Versions

Functionality described in previous versions may be superseded by other new functionality or updated through resolved issues.

5.2.x.x

No new features were introduced in Versions 5.2.0.1, 5.2.0.2, 5.2.0.3, 5.2.0.4, 5.2.0.5, 5.2.0.6, 5.2.0.7, or 5.2.0.8.

5.2

The following new features and functionality were introduced in Version 5.2:

Advanced Malware Protection

Version 5.2 adds two new features to enhance the malware protection capabilities of the Sourcefire 3D System: malware blocking and network file trajectory.

Malware Blocking

The Sourcefire 3D System network-based advanced malware detection capabilities added in Version 5.1.1 identifies individual files as they enter your network, creates a fingerprint of each file, checks the fingerprint against the Sourcefire cloud to determine the disposition of the file, and alerts you to files identified as malware.

With the addition of malware blocking in Version 5.2, the Sourcefire 3D System now provides advanced malware protection (AMP). You can now configure file policies to block transfer of known malware files.

Based on the disposition of each detected file and the rules you set in your file policies, the Defense Center instructs a managed device either to block the file or to allow its upload or download. To improve performance, if the system already knows the disposition for a file based on its SHA-256 hash value, the Defense Center uses a cached disposition rather than querying the Sourcefire cloud.

If necessary, you can override dispositions from the cloud on a file-by-file basis with the global malware whitelist. If a file has a disposition in the cloud that you know to be incorrect, you can add the file's SHA-256 value to the whitelist. When the system detects a file from the whitelist, it does not perform a malware lookup or block the file as malware. You can enable use of the global malware whitelist on a per-file-policy basis.

Several analysis tools let you track AMP events, including the Context Explorer, the dashboard, the event views, and the network file trajectory view. Connection, file, and malware events all reflect when a file is blocked because of malware.

You can perform AMP, which requires Protection and Malware licenses, using any Series 3 managed device or virtual device. You can manage an AMP deployment using any Series 3 or Series 2 Defense Center, except a DC500.

Network File Trajectory

The network file trajectory feature provides a visual, interactive representation of the path an infected file takes across your network, to help you understand the broader impact, context, and spread of malware across the network and endpoints. This view depicts point of entry, propagation, protocols used, and the users or endpoints involved in the transfer. You can use the map to determine which hosts may have transferred malware or are at risk and to observe file transfer trends.

File trajectory information provides standard information about the file (the file name, type, disposition, actions taken by the system, and so on) as well as when it was first and last seen, the number of hosts associated with the file, and the name of any associated threats. The trajectory of a file through your network is illustrated in visual form on the File Trajectory page. You can access the File Trajectory page directly (**Analysis > Files > Network File Trajectory**) or from the Context Explorer, dashboard, or event views of connection, file, or malware events.

You can view network file trajectories on any file where a malware cloud lookup occurred using AMP or on any file detected or quarantined by FireAMP, Sourcefire's endpoint-based advanced malware analysis and protection solution.

Next-Generation Firewall (NGFW)

Several new device management features were added in Version 5.2: high availability state sharing, gateway VPN configuration, policy-based configuration of network address translation (NAT), and clustered stacking.

Clustered State Sharing

The clustered state sharing feature, also referred to as high availability (HA) state sharing, allows clustered devices or clustered stacks to synchronize their states so that, if either device or stack in the cluster fails, the other peer can take over with no interruption to traffic flow. This provides improved failover capability for strict TCP enforcement, unidirectional access control rules, and blocking

persistence. Clustered state sharing is supported for VPN and NAT configurations.

With state sharing, devices in the cluster allow TCP sessions to continue after failover without having to reevaluate the connection against your access control rules, even if strict TCP enforcement is enabled.

State sharing also allows the system to transfer the status of allowed connections matching unidirectional access control rules during failover. Without state sharing, if an allowed connection is still active following a failover and the next packet is seen as a response packet, the system denies the connection. With state sharing, a midstream pickup matches the existing connection and the connection continues to be allowed.

Another advantage of state sharing is that while many connections are blocked on the first packet based on access control rules or other factors, there are cases where the system allows some number of packets through before determining that the connection should be blocked. With state sharing, the system immediately blocks the connection on the peer device or stack as well.

You can enable state sharing on clustered Series 3 managed devices with a Control license enabled.

Gateway VPN

You can now configure the Sourcefire 3D System to build secure Virtual Private Network (VPN) tunnels between virtual routers on Sourcefire managed devices and a remote device. After the VPN connection is established, the hosts behind the local gateway can connect to the hosts behind the remote gateway through the secure VPN tunnel.

The Sourcefire 3D System builds tunnels using the Internet Protocol Security (IPSec) protocol suite. The system uses the IKE protocol to mutually authenticate the two gateways against each other as well as to negotiate the security association (SA) for the tunnel. Packets across a VPN tunnel are supported for both the Authentication Header (AH) and Encapsulating Security Payload (ESP) security protocols.

The system supports three types of VPN deployments: point-to-point, star, and mesh.

In a point-to-point VPN deployment, two endpoints communicate directly with each other.

In a star VPN deployment, a central endpoint (hub node) establishes a secure connection with multiple remote endpoints (leaf nodes). Star deployments commonly represent a VPN that connects an organization's main and branch office locations using secure connections over the Internet or other third-party network. Star VPN deployments provide all employees with controlled access to the organization's network.

In a mesh VPN deployment, all endpoints can communicate with every other endpoint by means of an individual VPN tunnel. The mesh deployment offers

redundancy so that when one endpoint fails, the remaining endpoints can still communicate with each other. This type of deployment commonly represents a VPN that connects a group of decentralized branch office locations.

Note that this feature is only available on Series 3 devices. To deploy VPN, you must enable Protection, Control, and VPN licenses on each of the managed devices used for the VPN.

Policy-Based NAT

Version 5.2 introduces the ability to create a network address translation (NAT) policy. A NAT policy determines how the system performs routing with NAT.

You can now create and use both static and dynamic NAT rules for further flexibility and granular control of NAT configuration. Policy-based NAT supports the following types of rules:

- static, which provide one-to-one translations on destination networks and optionally port and protocol
- dynamic IP, which translate many-to-many source networks, but maintain port and protocol
- dynamic IP and port, which translate many-to-one or many-to-many source networks and port and protocol

You can configure NAT policies in different ways to manage specific network needs:

- to expose an internal server to an external network
- to allow an internal host or server to connect to an external application
- to hide private network addresses from an external network by using a block of IP addresses
- to hide private network addresses from an external network using a limited block of IP addresses and port translation

In previous versions, you could configure NAT through device-based NAT rules. Policy-based NAT replaces that functionality. When you update managed devices to Version 5.2, the device-based NAT rules for that device (formerly configured under **Devices > Device Management > Edit**) become a NAT policy (under the **Devices > NAT** tab on the Defense Center) with equivalent rules.

You can use policy-based NAT on Series 3 managed devices with a Control license enabled.

Clustered Stacking

In addition to the ability to create clustered configurations of managed devices, you can now establish redundancy of networking functionality and configuration data between two identically configured peer device stacks. Just as with paired individual devices in a cluster, clustered stacks provide a backup option if one stack fails. As in the existing clustering feature, all devices in the configuration must have identical licenses and must have Control licenses. When you register

or unregister any device in a clustered stack with a Defense Center, the entire clustered stack is registered or unregistered as a group.

All Series 3 devices that support stacking are supported for this feature. However, stacked 3D9900 devices are not supported.

Drop BPDUs Support

The drop Bridge Protocol Data Units (BPDUs) configuration added in Version 5.2 allows you to set up an inline configuration that operates over a single physical link. You can now configure a virtual switch with two logical interfaces; each interface must have a different configured VLAN tag. Additionally, on a third-party switch or other supported device, you must configure two VLANs and two logical interfaces; each interface must be in a different VLAN but configured on the same physical port.

Series 2 Device Reimaging

Series 2 appliances are the second series of Sourcefire physical appliances, which includes the following appliance models:

- 3D500/1000/2000
- 3D2100/2500/3500/4500
- 3D6500
- 3D9900
- DC500/1000/3000

Version 5.2.0.9 of the Sourcefire 3D System can now run on Series 2 appliances. Previously, Series 2 devices supported only 4.x versions of the Sourcefire 3D System. Note that Series 2 devices running Version 5.2.0.9 must be managed by a Defense Center; they no longer have standalone capabilities. For more information, see the *Sourcefire 3D System User Guide*.

To update any Series 2 appliance to Version 5.2.0.9 from Version 4.x, you must reimage the appliance, which discards all events and configuration data stored on those appliances. For more information about reimaging, see the *Sourcefire 3D System Installation Guide*.

Geolocation

The geolocation feature enhances Sourcefire 3D System analysis tools with data about the geographical sources of routable IP addresses (the country, continent, and so on). You can use this data to determine if, for example, connections originate from or terminate in countries unconnected with your organization.

Geolocation information is available in intrusion events, connection events, file events, malware events, host profiles, and user profiles. The Context Explorer and the dashboard can also now include geolocation information.

After you install a geolocation database (GeoDB) update, you can view granular information available for an IP address, such as postal code, coordinates, time zone, Autonomous System Number (ASN), internet service provider (ISP), use type (home or business), organization, domain name, connection type, and proxy

information. Note that the system does not retroactively generate data for events logged before the update. You can also pinpoint the detected location with any of four third-party map tools. Note that without a GeoDB update, only the flag icon and ISO3 alpha country code appear.

Network Discovery

Two new areas of functionality have been added to network discovery for Version 5.2: IPv6 support for network discovery and support for user logoff events generated by Version 2.1 of the Sourcefire User Agent.

IPv6 Support

Version 5.2 introduces extensive support for IPv6 addresses in features that were previously limited (partially or completely) to IPv4 addresses. These include adaptive profiles, auditing compliance, correlation, custom fingerprinting, FireSIGHT recommendations, host profiles, intrusion events, IP packet defragmentation, network discovery, the network map, network objects, and the User Agent.

Hosts on your monitored network may now have multiple associated IP addresses (both IPv4 and IPv6). Most parts of the system coordinate data for each of a host's IP addresses to give a full picture of the host's activity and to allow you to take action against an entire host easily.

Sourcefire User Agent Logoff Detection

User Agents monitor users as they log into the network or when accounts authenticate against Active Directory credentials for other reasons and maps users to host IP addresses, to support user access control.

Version 2.1 of the Sourcefire User Agent also now detects logoffs of active directory users. When the agent checks a host and discovers that the expected user is no longer logged in, the agent generates a logoff for that user. When the Defense Center receives the logoff, it unmaps the user from the previously associated IP address.

Access Control

Version 5.2 also adds new functionality in the access control policy: support for source ports and ICMP types and codes in port conditions in access control rules and support for blocking encrypted application traffic using either application conditions or URL conditions.

Source Ports in Access Control Rules

You can now specify source ports as a condition for access control rules; this expands upon the existing capability to specify destination ports. The source ports you specify must be TCP or UDP ports.

ICMP Types and Codes in Access Control Rules

You can now use Internet Control Message Protocol (ICMP) types and codes in access control rules, correlation rules, and port objects. You can also now view ICMP types and codes for all relevant events in the event viewer.

SSL Application Detection

Version 5.2 adds many new application detectors for applications in SSL traffic, allowing you to identify, and optionally block, encrypted application sessions based on the common name from the SSL client certificate used in the session.

URL Blocking based on SSL Common Name

You can now block encrypted application traffic using a URL based on the common name in an SSL certificate.

Updates to API Support

Version 5.2 introduces the ability to request intrusion rule documentation using either eStreamer or the database access feature. In addition, several structures were updated for new features.

eStreamer and Database Access Updates

Version 5.2 contains several data structures updated for IPv6 address support, geolocation changes, changes to support malware blocking, ICMP type and code support, and bug fixes. For more information, see the *Sourcefire 3D System eStreamer Integration Guide* and *Sourcefire 3D System Database Access Guide* for Version 5.2.

Extended Rule Documentation

You can now request intrusion rule documentation using eStreamer. You can also use the database access feature to query intrusion rule documentation.

For Assistance

If you are a new customer, thank you for choosing Sourcefire. Please visit https://support.sourcefire.com/ to download the Sourcefire Support Welcome Kit, a document to help you get started with Sourcefire Support and set up your Customer Center account.

If you have any questions or require assistance with the Sourcefire Defense Center or managed devices, please contact Sourcefire Support:

- Visit the Sourcefire Support Site at https://support.sourcefire.com/.
- Email Sourcefire Support at support@sourcefire.com.
- Call Sourcefire Support at 410.423.1901 or 1.800.917.4134.

Thank you for using Sourcefire products.

Legal Notices

Cisco, the Cisco logo, Sourcefire, the Sourcefire logo, Snort, the Snort and Pig logo, and certain other trademarks and logos are trademarks or registered trademarks of Cisco and/or its affiliates in the United States and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

The legal notices, disclaimers, terms of use, and other information contained herein (the "terms") apply only to the information discussed in this documentation (the "Documentation") and your use of it. These terms do not apply to or govern the use of websites controlled by Cisco or its subsidiaries (collectively, "Cisco") or any Sourcefire-provided or Cisco-provided products. Sourcefire and Cisco products are available for purchase and subject to a separate license agreement and/or terms of use containing very different terms and conditions.

The copyright in the Documentation is owned by Cisco and is protected by copyright and other intellectual property laws of the United States and other countries. You may use, print out, save on a retrieval system, and otherwise copy and distribute the Documentation solely for non-commercial use, provided that you (i) do not modify the Documentation in any way and (ii) always include Cisco's copyright, trademark, and other proprietary notices, as well as a link to, or print out of, the full contents of this page and its terms.

No part of the Documentation may be used in a compilation or otherwise incorporated into another work or with or into any other documentation or user manuals, or be used to create derivative works, without the express prior written permission of Cisco. Cisco reserves the right to change the terms at any time, and your continued use of the Documentation shall be deemed an acceptance of those terms.

© 2004 - 2015 Cisco and/or its affiliates. All rights reserved.

Disclaimers

THE DOCUMENTATION AND ANY INFORMATION AVAILABLE FROM IT MAY INCLUDE INACCURACIES OR TYPOGRAPHICAL ERRORS. CISCO MAY CHANGE THE DOCUMENTATION FROM TIME TO TIME. CISCO MAKES NO REPRESENTATIONS OR WARRANTIES ABOUT THE ACCURACY OR SUITABILITY OF ANY CISCO-CONTROLLED WEBSITE, THE DOCUMENTATION AND/OR ANY PRODUCT INFORMATION. CISCO-CONTROLLED WEBSITES, THE DOCUMENTATION AND ALL PRODUCT INFORMATION ARE PROVIDED "AS IS" AND CISCO DISCLAIMS ANY AND ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING BUT NOT LIMITED TO WARRANTIES OF TITLE AND THE IMPLIED WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL CISCO BE LIABLE TO YOU FOR ANY DIRECT,

INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING BUT NOT LIMITED TO PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF DATA, LOSS OF PROFITS, AND/OR BUSINESS INTERRUPTIONS), ARISING OUT OF OR IN ANY WAY RELATED TO CISCO-CONTROLLED WEBSITES OR THE DOCUMENTATION, NO MATTER HOW CAUSED AND/OR WHETHER BASED ON CONTRACT, STRICT LIABILITY, NEGLIGENCE OR OTHER TORTUOUS ACTIVITY, OR ANY OTHER THEORY OF LIABILITY, EVEN IF CISCO IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES/JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU..