This document describes how to load and install patch 7.0.0.06 (the GeoLocation, TrustedSource, and SSH Proxy patch) on a Sidewinder® appliance.

This patch was released on April 7, 2008. **One year from this release date, support for the previous release, 7.0.0.05, will end.** By April 7, 2009, all systems must be at a supported version greater than 7.0.0.05. For more information, see [www.securecomputing.com/goto/eol](http://www.securecomputing.com/goto/eol).

**Contents...**

About this patch ........................................................................................................................................2
Before installing patch 7.0.0.06 ..............................................................................................................7
After installing patch 7.0.0.06 ...............................................................................................................9
Loading and installing this patch ............................................................................................................10
  Procedure 1 — Identify the location of the patch ..............................................................................10
  Procedure 2 — Download the patch .................................................................................................10
  Procedure 3 — Install the patch .......................................................................................................11
Patch 7.0.0.05 ....................................................................................................................................15
Patch 7.0.0.04 ....................................................................................................................................20
Patch 7.0.0.03 ....................................................................................................................................30
Patch 7.0.0.02 ....................................................................................................................................33
Patch 7.0.0.01 ....................................................................................................................................39
About this patch

Sidewinder patch 7.0.0.06 (the GeoLocation, TrustedSource, and SSH Proxy patch) provides the following benefits:

Patch 7.0.0.06 fixes and enhancements

Patch 7.0.0.06 provides the following benefits:

Kernel/OS features

- Removes support for older embedded Broadcom NICs: bge driver for 5700, 5701, and 5702.
- Adds supports for next generation Sidewinder E model appliances.
- Clears QoS filter rules and statistics so they are no longer reported when a profile is deactivated/deleted.
- Improves handling of UDP sockets closures on SMP systems.
- Corrects an issue with the em driver, which will improve multicast routing.
- Adjusts TCP connection timeouts to improve handling of TCP traffic on networks that have very short roundtrip times.
- Increases the number of interfaces (VLANs or physical) that can join a multicast group to 64.
- Removes forwarding restrictions for IPv4 link-local subnet (169.254.0.0/16).

Proxies

- Introduces a new SSH decrypting proxy. For more information, see the “Application Defenses” chapter of the Sidewinder Administration Guide, rev. D.
- Introduces a new SMTP proxy. Upgrades will migrate and accommodate old proxy configuration settings in the new proxy. For more information, see the “Application Defenses” chapter of the Sidewinder Administration Guide, rev. D.
- HTTP
  - Adds support for URI translation (similar to a Classic/TSP feature) for incoming non-transparent HTTP connections. This allows one external IP address on the Sidewinder appliance to map to multiple internal server addresses for inbound traffic. Redirection is configurable, using request data to determine the server address to reflect internal network characteristics. For more information, see the “Services” chapter of the Sidewinder Administration Guide, rev. D.
  - Improves close handling of connections when the client connection closes before the server connection is done sending data.
  - Prevents configuration of upstream proxy on a transparent HTTPS Application Defense.
  - Ensures correct address is used for a session when the proxy gets multiple addresses returned from a DNS query.
  - Improves the downloading of large files.
  - Fixes an issue with FTP requests through the HTTP proxy to an FTP server that does not respond to the SIZE command. Also, improves support for FTP requests through the HTTP proxy to an FTP server that rejects the SIZE command.
  - Improves URL auditing so long URLs are audited in the information field of the audit record, which can be split across multiple audits.
  - Corrects logic in the HTTP Application Defense to accept all URLs in a specified URL whitelist.
  - Improves proxy interoperability with SmartFilter when configured to reject all requests when SmartFilter is unavailable.
  - Fixes the proxy’s handling of delayed responses from SmartFilter.
  - Corrects an issue with posting large files through the decrypting proxy.
  - Removes use of the identity value on the Transfer-Encoding header on FTP responses through the HTTP proxy.
- SIP
  - Adds support for port ranges.
  - Enhances the SIP proxy to examine additional types of messages for possible session descriptions.
- FTP — Adds logic to successfully establish the connection when a client or server is not listening immediately after it passes the port number.
About this patch

- **SNMP** — Corrects NAT issue when supporting multiple SNMP servers residing in a single burb.
- **H.323** — Addresses call manager interoperability issues.
- **DNS** — Prevents the DNS proxy from being misconfigured to listen on the firewall burb.
- **Ping** — Improves handling of ping requests to IP addresses that have the host portion set to zero (for example, x.x.x.0).

**Packet filter**

- Improves packet filter rule recheck processing.
- Improves traffic processing when both packet filter and proxy rules were using the same port and the traffic matched the packet filter rule.
- Corrects packet filter rule processing to ignore data with a query reply that is irrelevant to its processing.

**IPS**

- Adds a number of IPS related enhancements. For more information, see the “Content Inspection” chapter of the *Sidewinder Administration Guide*, rev. D; also see Knowledge Base article 6600.
- Corrects an error in the IPS download e-mail notification processing.
- Improves scanning engine performance by tuning engine scan traffic streams to omit scans in contexts of no interest and by improving multi-slash encoding detection.

**Policy**

- Introduces new GeoLocation processing. This enhances policy rules to support specifying GeoLocation source and destination restrictions. For more information, see the “General Policy Configuration,” “Network Objects and Time Periods,” and “Content Inspection” chapters of the *Sidewinder Administration Guide*, rev. D.
- Introduces TrustedSource IP reputation in the policy engine. This enhances policy rules to support specifying cross-protocol TrustedSource IP reputation thresholds on rules. For more information, see the “Quick Deployment,” “Rules,” and “Content Inspection” chapters of the *Sidewinder Administration Guide*, rev. D.
  - Successful relicensing is required before using TrustedSource. See “After installing patch 7.0.0.06” on page 9 for information.
  - TrustedSource reports are not supported in SecurityReporter v4.6.4.1 or earlier. TrustedSource reports will be supported in a future release of SecurityReporter.
  - For other requirements and dependencies, refer to “Before installing patch 7.0.0.06” on page 7.

**System features**

- Introduces a DHCP Relay agent to allow systems in a network accessible from one burb to obtain IP addresses from a DHCP server connected through a different burb. For more information, see the “Services” chapter of the *Sidewinder Administration Guide*, rev. D.
- Introduces an interface failover capability that allows a user to group two interfaces while specifying one of them as a redundant, failover interface. For more information, see the “Burbs, Interfaces, and Quality of Service” chapter of the *Sidewinder Administration Guide*, rev. D; also see Knowledge Base article 10760.

  **Caution:** Do not enable an additional interface until it is connected to a network cable and ready to use. The monitor link status function is enabled by default and will cause a failover event if an enabled interface is not connected.

- Introduces a default route failover capability that allows sites with multiple ISPs (or ways to reach their ISP) to redirect traffic to the other ISP if the interface to the primary ISP fails, without manually resetting the default route. For more information, see the “Routing” chapter of the *Sidewinder Administration Guide*, rev. D; also see Knowledge Base article 10762.
- Adds support for hyphen '-' and underscore '_' characters in burb names.
- Ensures the number of multicast destination addresses configurable per rule (via cf) matches the supported limits. This also prohibits configuration of multicast and non-multicast addresses on the same packet filter rule.
- Updates time zone information for New Zealand and Chatham.
• Improves handling of large configuration changes that are interrupted by a user before the changes are finished.
• Improves handling of expired ACL cache processing.
• Improves ACLd performance by eliminating host object and DNS lookups when the query is against localhost.
• Adds auto-binding for SSHD local addresses. If one or more ListenAddress keywords are configured in sshd_config, SSHD will bind only to those addresses, otherwise it will automatically bind to all interface aliases for the current burb.
• Corrects an issue in processing vif xxx entries in the xorp configuration file when interfaces are swapped.
• Ensures that static routes created by the administrator are also configured correctly when dynamic routing protocols are being used.
• Includes improvements to daemond health monitoring.
• Automates recovery procedure on boot if system finds file system corruption after a hard shutdown.
• Adds SNMP queries that will show the total number TCP, UDP, and packet filter session counts on the appliance.
• Adds last changed by and last changed date information to cf_policy rule queries.
• VLAN names and NIC group names and designations are now consistent through policy and interface configuration changes.

High Availability
• Introduces failover reset capability. The primary of a High Availability cluster that has failed over to the secondary will automatically resume its active role in the cluster when communication between cluster members is restored.
• Introduces better load-sharing HA interoperability with some Cisco routers. This eliminates the need to define static ARP entries on the appliance.
• Ensures that SSHd accepts connections from both native and cluster IP addresses following a reboot when the cluster address was manually configured in sshd_config as a ListenAddress.
• Corrects an issue with passport data conversion sent from HA primary to secondary that interrupted authenticated web traffic after a failover event.
• Improves reliability of failover processing in environments with many interfaces and VLANs configured.
• Adds capability for cf_failover to unassign the backup_heartbeat_burb after removal of secondary from a cluster.
• Adds checks to HA registration to ensure there are a minimum number of burbs (two for OTM and three for HA), and that all burb names match.
• Ensures traffic is not shared with peer in a load-sharing HA pair when the peer is in failure mode.
• Ensures SNMP trap events are sent when the failover heartbeat interface is downed.
• Corrects an issue so that cluster addresses and static ARP entries persist after reboot on a load-sharing secondary.

Admin Console
• Introduces Admin Console support for Windows Vista™ systems.

Note: The Home Basic version of Windows Vista™ is not supported.
• Introduces the ability to assign a description/tag to a set of configuration changes. For more information, see the “Administrator Basics” and “Auditing” chapters of the Sidewinder Administration Guide.
• Introduces the capability of configuration tracking and rollback. A set of configuration changes can be tracked and automatically stored in a configuration backup. The configuration rollback capability is accessible from the Configuration Backup window on the Admin Console. For more information, see the “Administrator Basics” and “Auditing” chapters of the Sidewinder Administration Guide.
• Introduces the ability to modify objects referenced in a rule while editing the rule.
• Introduces a DNS address lookup button to assist administrator with input for fields that
require an IP address. When this button is clicked, it brings up a small box. If there was a
name in the IP address field before clicking the button, a lookup is done and the field is
automatically filled in. If multiple addresses are returned, the administrator can select an
entry from the list to populate the IP address field.
• Eliminates an unnecessary reverse DNS lookup during Admin Console login, allowing
quicker connection when a DNS server is not available to the appliance.
• Corrects an issue in saving changes made in the Reconfigure DNS tool when static ARP
entries are configured in rc.local.
• Adds negotiated interface speed and mode to interface status display.
• Adds GMT (UTC) as an available time zone in the Admin Console.
• Adds a warning when Application Defense level is set to None on HTTP, HTTPS, FTP, T120,
H.323, SOCKS, or SIP proxies. This warns the administrator that there are affects of this
setting that may not be obvious. For more information, see the “Rules” chapter: “Creating,
modifying, and duplicating” rules section of the Sidewinder Administration Guide.
• Improves handling of missing or incorrect data entered in the VPN Properties window.
• Adds support for the /nn IP address mask length syntax to network objects and other areas.
Netmasks tied to an IP address or subnet address can now support the /nn mask length
syntax in the several places that previously required the 255.255.255.0 netmask syntax.
• Corrects issue with CPU percentage calculation used by the Dashboard and System
Resources dialog box.
• Updates the audit level options for the ISAKMP server.
• Corrects processing of the Enter key when editing a text cell within a grid — it now stops cell
edit without discarding changes or closing the window.
• Corrects an issue encountered with the Service Status window when viewing status of a
manual key VPN that was created from the command line.
• Adds Update Bandwidth and Simulate Bandwidth buttons in the Quality of Service window.
• Corrects dialog box always remaining open issue in DNS configuration screens when DNS
resource record was changed and the server type is changed from split DNS to use an
Internet server.
• Corrects an issue preventing an administrator from reversing, once configured, the signing of
configuration backups from the Audit Management window.
• Adds support for longer lists in TCP/UDP port entries in Services dialog box, increasing the
length of lists configurable from the Admin Console for packet filter TCP and UDP ports.
• Adds multiple Admin Console enhancements to improve Rules window performance for sites
with very large rule sets.
• Synchronizes the acceptable TCP and UDP idle timeout range (0–2147483647) with the
command line interface.

Quick Start Wizard
• Adds capability to configure an administrator e-mail address in the Quick Start Wizard.
• Adds the capability to specify internal and external burb names in the Quick Start Wizard.
• Enhances handling of input data to avoid potential errors, and to better handle errors that are
encountered.

Auditing and Reporting
• Enhancements to auditing to support new configuration change identification and
configuration tracking and rollback features.
• Adds audit when the date command is used to change the date — the previous and the new
dates are included in the audit record.
• Modifies type enforcement access permissions to audit.raw. Now use audit_clean command
to delete audit files. For more information, see Knowledge Base article 10755.
• Allows an administrator (read/write or read-only) to use acat on raw audit files that were
moved out of /var/log.
• Correct audit inconsistency in some VPN auditing of reporting local and remote networks, local and remote gateway information.
• Improves checking and handling of large data fields added to audit.
• Addresses auditbot processing issues when the system time is changed.

**Backup and restore**
• Adds `cf config contents` command to list files contained within a backup without doing a restore. See man `cf_config` for details.
• Retains the original license if the master key data in a restored backup is invalid for the current hardware. This will allow administrators to restore a configuration backup on different, but previously licensed, hardware without losing their valid license.

**Package management**
Enhances package management to attempt a cleanup of any temporary package directories created under both `/vcd/packages/` under `/var/packages/` directories if a download error occurs.

**Cryptographic components**
• Introduces a new `cf` area to support hardware crypto accelerators. This configuration is no longer part of `cf_interface`.
• Corrects IKEv2 NAT-T detection processing when NAT is not being used.
• Improves Sidewinder and SnapGear VPN interoperability.

**URL filtering**
Upgrades SmartFilter to v4.2.1.
• SmartFilter Admin Console plugin policy adds support for filtering action per individual SmartFilter policy rule (block, warn, coach, delay, etc) for uncategorized URLs.
• Allows the user to configure the Action Page when a URL is blocked by the policy because it is uncategorized. The options available include block page text, URL redirect, etc. Uncategorized warn text can also be modified.
• The supported maximum user group name length is now 128.
• The supported maximum directory server hostname length within both the Authentication Server and all plugins is now 255.

**Mail filters**
Adds audit and prevents keyword scan when keyword filter has an empty keyword table.
Before installing patch 7.0.0.06

To determine if you need to take any action before installing patch 7.0.0.06, review the following topics:

- Version requirements must be met.
- [TrustedSource users only] Determine if a hotfix is required.
- Manually added static routes must be valid.
- [SmartFilter users only] SmartFilter Administration Software must be updated.
- NICs based on BCM5700, BCM5701, or BCM5702 hardware must be disabled.

Version requirements must be met

Patches must be installed sequentially and cannot be skipped. If your Sidewinder appliance is at version 7.0.0.02 or higher, you can simultaneously install patches 7.0.0.03, 7.0.0.04, 7.0.0.05, and 7.0.0.06 as required (the appliance will install these patches in the correct order).

If your appliance is at a version earlier than 7.0.0.02, you must first install the appropriate patches to reach 7.0.0.02. After the appliance reboots, continue patching to 7.0.0.06.

[TrustedSource users only] Determine if a hotfix is required

Patch 7.0.0.06 introduces support for TrustedSource, which requires either specific license features or a hotfix. Use these steps to determine if your appliance requires the hotfix to use TrustedSource:

1. In the Admin Console, select Maintenance > License to view your appliance’s licensed features.
2. In the Current Features table, determine if the following features are licensed:
   - Strong Cryptography
   - SSL Decryption
   - If one or both of these features are not licensed, your appliance requires hotfix 7.0.0.06.H01 to use TrustedSource. If your appliance requires hotfix 7.0.0.06.H01, it can be installed at a later time but TrustedSource will not function until it is installed.

Manually added static routes must be valid

If you have manually added static routes to the /etc/gateways file, you must make sure that these routes are valid before you install this patch.

- Route entries must be formatted correctly. See the route man page (man route) for information on static route syntax.
- Route entries cannot be duplicated.
- Route entries must be valid for your network, for example, a gateway must be reachable on a local subnet.
- Network route entries must include the netmask.

Example:

route add -net 10.1.2.0 192.168.1.2
must be converted to

route add -net 10.1.2.0 192.168.1.2 -netmask 255.255.255.0
[SmartFilter users only] SmartFilter Administration Software must be updated

To manage the SmartFilter plugin on Sidewinder version 7.0.0.06, you must update your SmartFilter Administration software to version 4.2.1.

After your Sidewinder appliance and SmartFilter Administration Software have been updated, deploy the SmartFilter policy to the Sidewinder appliance.

To download the update, see: www.securecomputing.com/goto/smartfilter/downloads.

NICs based on BCM5700, BCM5701, or BCM5702 hardware must be disabled

Driver support has been removed for unsupported NICs based on BCM5700, BCM5701, or BCM5702 hardware. If your Sidewinder appliance is one of the affected models, you must disable the unsupported NICs and their properties before installing this patch.

The following appliances are affected:

• All 4150 models
• Some 2100 models
• Some 2150 models

If you have a 2100 or 2150 model appliance, run the following command to determine if your appliance is affected:

`pciconf -l | egrep "0x164514e4|0x164414e4"`

If the above command runs and produces no output, your appliance is not affected.

The following example output is from a system with two BCM5701-based NICs:

```
bge0@pci4:6:0: class=0x020000 card=0x01211028 chip=0x164514e4 rev=0x15 hdr=0x00
bge1@pci4:8:0: class=0x020000 card=0x01211028 chip=0x164514e4 rev=0x15 hdr=0x00
```

To disable a NIC and its properties, select Network > Interfaces and then do the following:

1. From the list of interfaces, select the NIC that you need to disable.
2. In the Enable area, select Off.
3. In the IP Address and Network Mask fields, enter 0.0.0.0.
4. In the Burb drop-down menu, select Select A Burb.
5. Save your changes.
After installing patch 7.0.0.06

To determine if you need to take any action after installing patch 7.0.0.06, review the following topics:

**Auto-activation must be successful to use TrustedSource feature**

After patch 7.0.0.06 is installed, your Sidewinder appliance is automatically relicensed to add a certificate and Certificate Authority used by the new TrustedSource feature. If you want to use TrustedSource and the auto-activation fails, you must manually relicense your appliance.

To verify whether auto-activation was successful:

1. Select **Maintenance > Certificate/Key Management**. The Certificate/Key Management window appears.
2. Click the **Firewall Certificates** tab and verify that a TrustedSource certificate appears in the Certificates list: **TS_Cert_[serial number]**.
3. Click the **Certificate Authorities** tab and verify that a TrustedSource Certificate Authority appears in the Cert Authorities list: **TrustedSource_CA**.

If these items do not appear and you want to use TrustedSource, follow these steps to manually relicense your appliance:

1. Select **Maintenance > License**.
2. Click the **Firewall** tab.
3. Click **Submit Data**.

**Note:** If you will not use TrustedSource, you do not need to relicense your appliance.
Loading and installing this patch

You install the patch in three steps:

1. Identify the location of the patch.
2. Load the patch onto the appliance.
3. Install the loaded patch.

*Note:* Make a configuration backup before beginning the patch update.

**Procedure 1 — Identify the location of the patch**

The 7.0.0.06 patch is located on Secure Computing’s FTP site. Patches are downloaded from this site.

- If you will always download patches from Secure Computing’s FTP site, you do not have to make changes to this window.
- You can configure your appliance to download packages automatically using the Automatically check for and load packages option.
- You can configure a different location to load packages from if you have appliances on an isolated network, or to speed up downloads to several appliances.

To identify the patch location:

1. In the Admin Console, select Maintenance > Software Management.
2. Click the Load Packages tab.
3. Verify or configure the patch site:
   - **Load using** — Select the protocol used to transport the package. The default is FTP.
   - **Directory** — The path name on the site where the package is located. The default is packages/sidewinder/7.0.
   - **Host** — The host name of the site where the package is located. The default is downloads.securecomputing.com.
   - **User Name** — The user account defined on the site. The default is anonymous.
   - **Port** — The number of the port used to access the site. The default is 21.
   - **Password** — The password to validate you to the site. No password is required for Secure Computing’s FTP site.
   - **Confirm Password** — Verify the password.

*Note:* To restore the system default values to these fields, click Restore Defaults.

4. Save your changes.

Continue with “Procedure 2 — Download the patch” on page 10.

**Procedure 2 — Download the patch**

Downloading the patch moves it from the FTP site to the appliance, but does not install it.

*Note:* If your appliance is configured to download packages automatically, go to “Procedure 3 — Install the patch” on page 11.

To download the patch from the network:

1. Select Maintenance > Software Management.
2. Click the Manage Packages tab.
3. To display the available patches, click Check for Updates. Packages appear in the table with a status of Available. These packages are available for downloading from the Secure Computing FTP site. (You can configure this action to happen automatically on the Load Packages tab.)
4 In the Manage Packages table, select **70006**.
5 On the toolbar, click **Download**. Click **Yes** to confirm.

A “successfully loaded” message appears and the package status changes to **Loaded**.

Continue with “Procedure 3 — Install the patch” on page 11.

---

**Procedure 3 — Install the patch**

Perform the appropriate procedure to install the 7.0.0.06 patch:

- “Install the patch on a Sidewinder appliance” on page 11
- “Install the patch on an existing HA pair” on page 13
- “Install the patch in a One-to-Many cluster” on page 14
- “Install the patch on CommandCenter managed appliances” on page 14

**Install the patch on a Sidewinder appliance**

Perform this procedure to install patch 7.0.0.06 on a Sidewinder appliance.

- The appliance will reboot during the patch installation.
- This patch also includes a separate Admin Console update.
- Perform a configuration backup of your current system before installing the patch: Select **Maintenance > Configuration Backup**.

To install this patch on a Sidewinder appliance:

1 Select **Maintenance > Software Management**.
2 Click the **Manage Packages** tab.
3 In the Package Name list, select **70006**.
4 On the toolbar, click **Install**. The Install window appears.

5 Select **Install now**.
6 Click **OK**.

A warning appears stating that the appliance will reboot after the patch is installed.
7 Click **Yes**.

The patch is installed, and then an Error message appears stating that the connection to the server has been lost.
8 Click **OK**.

The Admin Console is disconnected and the Sidewinder appliance reboots.
9 Re-connect the Admin Console to the appliance.

A message appears prompting you to install an Admin Console update.
10 Click Yes.
  The Admin Console update is downloaded, and then a message appears asking if you want to install the package now.

11 Click Yes. The Sidewinder 7 InstallShield Wizard Welcome window appears.

Note: If you are upgrading from Admin Console 4.05, a Diagnostic Window also appears.

Close the open windows:
  • Click Continue to close the Diagnostic Window.
  • Click Cancel to close the Password Authentication window.
  • From the File menu, select Exit to close the Admin Console.

12 In the Sidewinder 7 InstallShield Wizard Welcome window, click Next.
  A progress bar appears while the Admin Console update is installed. When the installation is complete, the Update Complete window appears.

13 Click Finish. The Admin Console opens.

14 Re-connect the Admin Console to the Sidewinder appliance.

15 Select Maintenance > Software Management.

16 On the Manage Packages tab, verify that the status for 70006 is Installed.

Note: If the patch status is still Loaded, call Technical Support.

You can also click View Package Details or View Log to see information about the installation.

The patch is now installed.
Installing and installing this patch

**Install the patch on an existing HA pair**

**Note:** The minimum network outage in this procedure is the duration of the take-over time (typically under one minute). Systems that have different take-over times will require two outages.

To install patch 7.0.0.06 on Sidewinder appliances that belong to an HA pair:

1. Using the Admin Console, connect to the secondary-standby and install the patch and the Admin Console update using the instructions in “Install the patch on a Sidewinder appliance” on page 11.

2. Install the patch on the primary in one of the following ways:
   - If you want to install the patch on the primary immediately: Connect to the primary and install the patch using the instructions in “Install the patch on a Sidewinder appliance” on page 11.
   - If you want to evaluate this patch on a single Sidewinder appliance before upgrading both of your HA pair appliances, perform [Conditional] Evaluate the patch on a single Sidewinder appliance below to assign the secondary (now running at 7.0.0.06) as the primary appliance.

[Conditional] Evaluate the patch on a single Sidewinder appliance

To evaluate the patch on a single Sidewinder appliance, assign the 7.0.0.06 appliance as the primary:

1. [Conditional] If you have a primary/standby HA configuration, temporarily convert to a peer-to-peer HA configuration: In the Admin Console, expand the **High Availability** branch and select the primary (currently at version 7.0.0.05). In the Mode field, select **Standby**, set the Takeover Time value to the same value as your secondary, and then click the **Save** icon. (To determine the takeover time of the secondary, select the secondary appliance icon and select the Mode field.)

2. Reboot the current primary (at version 7.0.0.05).

3. When the primary is rebooted, the secondary (at version 7.0.0.06) will detect that the primary is unavailable and take over as the primary. Evaluate the patch 7.0.0.06 Sidewinder appliance as needed.

   **Note:** Configuration changes made to the primary will not be synchronized with the standby when they are at different versions.

4. When you are finished evaluating the patch 7.0.0.06 Sidewinder appliance, upgrade your second HA appliance to patch 7.0.0.06.

   **Important:** You cannot schedule an upgrade for a second HA appliance. You must select **Install now** in the Install window when upgrading the second appliance.

5. [Conditional] If you changed your HA configuration from primary/standby to peer-to-peer, reset your appliances to their previous primary/standby configuration.

Once both Sidewinder appliances have been rebooted, both appliances will be functioning at the same patch level and the HA cluster will be synchronized.
Install the patch in a One-to-Many cluster

Perform these steps to install a patch on Sidewinder appliances that belong to a One-to-Many cluster.

1. Using the Admin Console, connect to the primary and install the patch using the instructions in “Install the patch on a Sidewinder appliance” on page 11.

2. One at a time, select each secondary node beneath the Maintenance > Software Management primary node and install the patch using the instructions in “Install the patch on a Sidewinder appliance” on page 11.

Once the secondaries have been rebooted, the One-to-Many cluster will have an up-to-date policy and all Sidewinder appliances will be functioning at the same patch level.

Install the patch on CommandCenter managed appliances

Managed Sidewinder appliances must be upgraded using the CommandCenter Software Updates tool. Do not install a patch directly on a managed appliance.

- Verify that a Sidewinder patch can be managed by your version of CommandCenter. See CommandCenter release notes for version compatibility information and installation instructions.

- You can also use the Sidewinder Admin Console to determine if a Sidewinder patch can be managed by CommandCenter.
  a. Select Maintenance > Software Management.
  b. Click the Manage Packages tab.
  c. Click Check for Updates to see the latest package information. The CommandCenter Management column shows the CommandCenter version that can manage that patch.

Rolling back the patch

If the installed patch does not work to your satisfaction, you can use the Rollback feature to restore the appliance to a previous state. Select Maintenance > Software Management, then click the Rollback tab.

- Any configuration changes made after the patch was installed are lost. A rollback reverts the appliance to the state just before the patch was installed. Therefore, rolling back is a recommended recovery option for only a short time after a patch installation.

- A rollback always requires a reboot.
Patch 7.0.0.05

Sidewinder patch 7.0.0.05 (the QoS Support, SNMPv3, Performance Improvements, and Miscellaneous Fixes patch) provides the following benefits:

Patch 7.0.0.05 fixes and enhancements

Patch 7.0.0.05 provides the following benefits:

Kernel/OS features

- Adds support for Quality of Service (QoS) traffic shaping using the class-based queuing (CBQ) method. For details, see the “Burbs and Interfaces” chapter of the Sidewinder Administration Guide and KB article 9984.
- Upgrades to several operating system components including editors, drivers, shells, etc.
- Adds several networking performance enhancements.

System features

Adds new health check mechanism between daemon and key proxies to ensure failure conditions are quickly detected and resolved.

SNMP agent

- Upgrades the SNMP agent to support SNMP v3.
- Corrects an issue with SNMP Get requests, ensuring that the value for TCP currently established connections is correctly calculated before return.

Proxies

Improves performance in the HTTP, HTTPS, and Generic TCP proxies by integrating the kqueue kernel event notification mechanism for socket read/write multiplexing.

- HTTP
  - Adds HTTP proxy enhancements from Classic and TSP.
    - Strips out java applet object tags as well as applet tags.
    - Enforces strict header parsing.
    - Removes second header if duplicate content-length headers; if headers differ, then the message is rejected.
    - Rejects request with binary data in header when feature is enabled.
    - Allows the administrator to specify a list of headers and matching values to block.
    - In non-transparent mode, when a DNS lookup for a URL has multiple entries, the proxy will now attempt to connect to each IP address until successful.
    - Guards against “..” entries in URLs that would lead to a path above the server root directory.
    - Drops blank continuation lines to help prevent request splitting attacks and to support recommended behavior described in the RFC.
    - Supports forwarding of requests with arbitrary schemes if the schemes are configured in the upstream proxy table.
    - Improves flexibility and control on specified URL matches, allowing the customer to specify contains, begins with (anchor left), and ends with (anchor right).
      - When relax protocol enforcements is enabled in the application defense, the body after a 304 response from servers is truncated rather than disallowing the connection.
      - Improves detection of transparent vs. non-transparent HTTP connections when the TCP connection is addressed to the firewall. This allows transparent redirect rules to work even when the request uses a fully qualified URI.
      - Enables use of a host name in SSO redirects in place of an IP address.
      - Improves the downloading of large files.
      - Improves the processing of fragmented messages.
  - FTP
    - Adds Symantec™ syntax support to the FTP proxy for establishing transparent and non-transparent authenticated sessions. See Knowledge Base article 9420 for more information.
    - Allows user to configure non-transparent FTP username and authentication data prompt.
– Adjusts processing of server responses when virus scanning to ensure all clients properly display scanning results.
– Sends *keep-alives* when virus scanning large files to avoid client timeout.

**SNMP**
– Modifies SNMP OID filtering to properly forward SNMP v1 traps.
– Corrects SNMP trap processing when the source burb was set to something other than *Any*.
– Corrects audit to accurately identify SNMP version number.

**H.323**
– Corrects an initial connection timeout issue on slow networks.
– Adds support for H.323 gatekeeper clients to optionally call by name or H.323 alias (rather than having to use the IP address of the callee).

**SIP** — Adds several SIP proxy enhancements, including support for event notification, additional SIP devices, and calls between phones in the same burb.

**SOCKS** — Fixes DNS access issue preventing connection completion.

**DNS**
– Improves connection cleanup processing when encountering an invalid DNS header.
– Fixes issue with source and destination burb IDs being reversed in nettraffic audits.

**Telnet**
– Improves handling of requests to unreachable hosts.
– Adds ability to configure the destination prompt for non-transparent telnet connections. See Knowledge Base article 9420 for more information.

**UDP Generic Proxy** — Enhances proxy connection processing to eliminate some intermittent connection failures.

**IPS**
Adds signature name (msg field) to IPS audits.

**Admin Console**
– Correctly preserves the NAT and Redirect settings when selecting a different service on a rule (rather than resetting to the defaults).
– Adds support for scheduling configuration backups. See the “General Maintenance Tasks” chapter of the *Sidewinder Administration Guide* for details.
– Adds Audit Management screen to the Admin Console to support managing (exporting, rolling, etc.) audit logs. See the “Auditing” chapter of the *Sidewinder Administration Guide* for details.
– Adds a *Last modified* field to the Rules window showing when the rule was last changed and who made that change.
– Adds Admin Console support to configure application defense groups on single service rules.
– Adds the capability to duplicate existing IPS signature groups or response mappings.
– Adds right-click menu option to view audit when a rule is selected.
– Adds up/down buttons to the Authenticators window to allow easier change of rank on the Servers list.
– Adds a confirmation dialog when exiting the Admin Console if there are unsaved changes pending.
– Corrects an error when adding NS records to DNS subdomains from the Admin Console.
– Removes liberal burb default value in the Rules window.
– Synchronizes the acceptable TCP idle timeout range (1-65535) with the command line interface.
– Enables finer granularity for specifying the number of proxy instances to improve performance tuning capability.
– Adds capability for read-only administrator to update their Admin Console.
– Increases the Services port definition field to allow up to 10,000 characters.
• Adds help links for the following routing services: bgpd, ospfd, pimd and ripd.
• Corrects an error in the main Service Status window when a server was not configured to run in all burbs — the screen showed servers as “running with error” when they were actually running normally in all configured burbs.
• Eliminates erroneously reported error condition on the Service Status window regarding the snmpd service.
• Corrects an issue with sshd port configuration from the Admin Console when a ListenAddress already exists in the configuration file.
• Fixes an issue with the Certificate Management window when the Audit Level value on the Certificate Server tab is of an unexpected format or is unset.

Auditing and Reporting
• Improves audit viewing for time zones with greater than three character abbreviations.
• Corrects an audit viewing issue at the calendar year transition that prevented viewing of the previous year’s audit.
• Corrects processing that resulted in TE errors from rollaudit.
• Corrects an issue with exporting multiple files to some directly connected FTP servers that prevented more than one file transfer.
• Adds support to cf_export for absolute path names and special characters in user names and passwords.
• Fixes formatting of WELF audit data by correctly applying quotes to rule names that contain spaces.

Backup and restore
• Adds support for optionally adding password-protected encryption to disaster recovery USB sticks.
• Removes obsolete packages from disaster recovery USB stick when writing new recovery media.
• Ensures that, when restoring a system in an HA cluster, policy is synchronized before the restored system reboots, to ensure that the cluster is working with the latest policy when the restore is complete.
• Corrects handling of CRLF when parsing XML in configuration backups.

Package management
• Adds support to optionally separate patch installation and patch activation so the patch activation (which might require a system reboot) can be delayed. See the “General Maintenance Tasks” chapter of the Sidewinder Administration Guide for details.
• Adds numerous patch process enhancements including automatic configuration backup prior to package install/uninstall, verbose logging in cf_package, time-stamped package logs, and error message improvements.
• Corrects an issue that allowed an older patch to be installed over a newer patch during a bulk installation of updates.

Authentication
• Adds support for external groups for RADIUS authenticators and optional internal groups for LDAP and SafeWord authenticators. Now includes the option to use internal groups, Sidewinder-defined groups, or external groups for the LDAP, RADIUS, and SafeWord authenticators. See the “Authentication” chapter of the Sidewinder Administration Guide for details.
• Cleans up warder shutdown process to allow clean recovery after configuration changes.
• Enhances LDAP warder password processing.

DNS
Enhances resolver processing when there are unresponsive DNS servers.

Anti-Spam
Clarifies sendmail audit messages to clearly state if the message was rejected or if it was tagged as spam yet still allowed through (since the spam score was above the spam threshold but below the rejection threshold).
Mail filters
Corrects an issue in keyword search filtering (KMV), which was causing failure to pass large files.

Cryptographic components
• Corrects netmask handling for IKEv2 VPN processing to allow non-zero netmasks.
• Adds capability to restart cmd from cf_daemond to support situations where the Admin Console is not available.
• Corrects issue with reported VPN status information.

High Availability
• Enhances VPN policy synchronization in a High Availability load-sharing environment to include the synchronization of dynamic IP VPNs.
• Corrects an issue that breaks the Admin Console connection to the secondary member of an HA pair when the administrator performs an action that causes an email notification to be sent.
• Corrects an issue on HA cluster secondaries when the cluster is configured with multicast rules.
• Corrects an issue that caused excessive IGMP traffic on the heartbeat burb when the internal burb was used for heartbeat verification and intraburb forwarding and multicast routing were both configured.
• Corrects an issue with applying sendmail configuration changes from primary to standby.
• Improves HA ipfilter state session management so that sessions no longer accumulate on the standby.
• Corrects a problem with IP Source Check in a failover environment.

Miscellaneous system
• Eliminates an unnecessary "reboot needed" notification when setting the host name during the initial configuration.
• Corrects an issue adding static ARP entries at reboot.
• Corrects an issue when UPS signals a shutdown.
• When using ipconfig, the native IP addresses are now listed before aliases.
• Corrects an issue processing dynamic host objects in rules in which the host cannot be DNS resolved.
• Adds stability enhancement to multicast routing.

Known issues
Some configurations require extra steps to ensure successful implementation. Review the following issues to determine if you need to take any action before or after installing patch 7.0.0.05.

Before installing patch 7.0.0.05

Custom IPS signatures must include the msg rule option.
If you have defined any custom IPS signatures, they must be modified to include the msg rule option in Snort 2.4.4 rules syntax.

See Knowledge Base article 6600 for information about Snort rules syntax: www.securecomputing.com/goto/kb
After installing patch 7.0.0.05

SIP proxy must be modified to allow VoIP calls through virtual burb VPN sessions.

If you are using a SIP proxy in a virtual burb VPN scenario, default application defense settings prevent completion of the connection.

To allow VoIP calls in this state:

1. Modify the SIP configuration file:
   a. Use the File Editor to open `secureos/etc/proxy/sipp.conf`.
   b. Change the following variable from `true` to `false`:
      `media_streams_must_match_signaling = false`
   c. Save and close the file.
2. Restart the SIP proxy: `cf daemond restart agent=sip_proxy`

[New SmartFilter configurations only] Rules for new SmartFilter configurations must be enabled in sequence.

When enabling SmartFilter and HTTP rules on the Rules window of the Sidewinder Admin Console, you must enable them in this order:

1. Enable the default SmartFilter rule group.
2. Create a rule for HTTP or HTTPS traffic that you want SmartFilter to monitor and create or select the appropriate application defense.

Reversing the order will result in denied access to allowed sites.

Stateful packet inspection must be disabled for multicast routing using the PIM-SM protocol.

When you create a rule to enable multicast traffic, you must disable stateful packet inspection in the TCP/UDP Packet Filter service for that rule.

To create the packet filter service:

2. Click New Service. The New Service window appears.
3. Enter a name and description that easily identifies the service.
4. From the Agent drop-down list, select TCP/UDP Packet Filter.
5. In the UDP ports field, select the UDP ports your multicast applications will be using.
6. Clear the Enable stateful packet inspection check box.
7. Select Bi-directional.
8. Make any other changes necessary for your site’s security policy.
9. Click Add and save your changes.

See the “Routing” chapter of the latest Sidewinder Administration Guide for more information.
Patch 7.0.0.04

Sidewinder patch 7.0.0.04 (the CommandCenter Support, Multicast Routing, and SmartFilter upgrade patch) has new features as well as fixes and enhancements. The new features include:

• Support for CommandCenter, a management tool for creating and applying security policies across multiple security appliances.
• Support for the Sendmail implementation SMTP over TLS.
• PIM-SM protocol and multicast routing

See “Patch 7.0.0.04 new features” for details.

Patch 7.0.0.04 fixes and enhancements

Patch 7.0.0.04 provides the following benefits:

Proxies

• HTTP Proxy
  – Corrects a transparent NTLM authentication issue where the proxy incorrectly returns a failed Authentication notice after the user has already properly authenticated.
  – Modifies the Relax enforcement processing to better handle HTTP server 304 or 205 responses.
  – Improves aborted session handling when SmartFilter processing is involved.
  – Accommodates IE7 idiosyncrasy to enable IE7 to connect to Windows Update through a non-transparent HTTP connection.
• PFTP — Improves ACL request/response processing when acld restarts.
• H.323 — Corrects an issue with enable/disable configuration processing using the Admin Console.
• UDP — Corrects an issue with proxy names in configuration processing for generic UDP proxies.
• SOCKS — Updates the proxy processing to ensure all data gets delivered to the client before the session is closed.
• Citrix, MS-SQL, SOCKS, SMTP — Adds the ability to create multiple proxy instances for greater connectivity.
• Generic proxy agent — Increases the maximum concurrent connections a single proxy instance can handle to 32,000.

Packet Filter

Corrects kernel contention issue processing the IPFilter session table.

IPS

Corrects handling with duplicate signature categories, improves detection rate, reduces false positives, and adds new evasion detection handling.

Admin Console

• Adds window for registration to CommandCenter.
• Enables selection of multiple entries in the Host Enrollment List.
• Modifies Restart button on the Service Status window to distinguish between the need to restart vs. the need to re-enable a failed service.
• Restores license import capability.
• Corrects an issue loading packages from a file in the Admin Console.
• Improves data parsing in /etc/services.
• Adds Sidewinder/CommandCenter version compatibility information to the Software Management window.
Quick Start Wizard
Adds Rapid Deployment capability for registration to CommandCenter in the initial configuration process.

Auditing and Reporting
- Adds port and protocol information to audit records written in WELF format.
- Corrects an issue with acat -W (Webtrends reports) parsing smtp proxy nettraffic audits.
- Fixes acat -W (Webtrends reports) to output the correct firewall hostname specified (fw=).
- Corrects auditd and acat SEF output issue when processing large audit messages.
- Corrects issue sending Syslog events primarily interfacing with SecurityReporter.

Package management
Fixes manual loading of local packages (residing in a local Sidewinder file) from the Admin Console.

DNS
Adds specific bug fixes from 9.3.4 to update bind processing.

Anti-Virus
- Improves auto-download processing to avoid notifying the engine when no new updates are available.
- Adds the executable group option and the namespace support options to those that are turned on by the `scan-all` in the scanner configuration.

URL Filter
- Updates SmartFilter to v4.2, which includes support for the new SmartFilter XL Internet Database, TrustedSource Web reputation filtering, ability to enforce safe search for Google and Yahoo!, ability to scan embedded URLs, and other enhancements.
- Allows SmartFilter to download control list on ports other than 80.

Hosted Sendmail
Adds support for STARTTLS in Sendmail.

Cryptographic components
- Corrects kernel notification issue when IKE gets restarted.
- Corrects an issue dropping traffic when multiple destination networks are defined.
- Improve AES processing.
- Adds IPSec support for Explicit Congestion Notification (ECN).
- Improves IKEv2 processing for better interoperability (ICSA 2.1 certification requirements).
- Improves ISAKMP processing to add some dead peer detection (DPD) processing in IKEv2 sessions.

High Availability
- Corrects faild issue mapping interfaces with unused burbs.
- Ensures static routes are added after primary-standby failover event.

Miscellaneous system
- Adds stratum option as an optional key for the NTP server commands.
- Allows NTP server configuration using either an IP address or a host name.
- Properly drops packets when `Hide port unreachable` is set for a specific burb.
- Fixes `cf config` to unmount USB flash drives.
• Fix `cf policy export` report to display rules properly.
• Supports multicast traffic over VLAN interfaces.
• Eliminates the potential for creating duplicate user IDs after upgrade to Sidewinder 7.

**Patch 7.0.0.04 new features**

Patch 7.0.0.04 introduces these new features:

• Support for CommandCenter
• Sendmail TLS
• PIM-SM protocol and multicast routing

**Support for CommandCenter**

Secure Computing CommandCenter™ is an enterprise-class management tool for creating and applying security policies across multiple security appliances. It centrally manages policy, software updates, reports, and monitoring of your organization’s Sidewinder appliances.

The CommandCenter appliance is part of a three-tier system that includes a workstation installed with the Client Suite, the CommandCenter with its enterprise-wide database, and the managed Sidewinder appliances. You configure and manage a CommandCenter appliance from a Windows workstation. The Client Suite CD provides the programs needed to prepare the initial configuration and manage your CommandCenter and its registered security devices after installation.

Patch 7.0.0.04 enables a Sidewinder appliance to be managed by a CommandCenter appliance.

• A Sidewinder appliance can be registered with CommandCenter in these two ways:
  – Registering with CommandCenter using the Quick Start Wizard
  – Registering with CommandCenter using the Admin Console

  **Note:** A Sidewinder administrator account named `ccfwadmin` is automatically created when you register with CommandCenter. If you already have an administrator account with that name, it will be overwritten.

• A Sidewinder appliance must be at version 7.0.0.04 or higher to be managed by CommandCenter. See “Managing versions of Sidewinder software” on page 24 for more information about supported versions.

• The `smgrd` (Secure Manager Server) service name has changed to `ccmd` (CommandCenter Management Server). It is used in registration and CommandCenter Management daemon communication among the CommandCenter and managed Sidewinder appliances.
Registering with CommandCenter using the Quick Start Wizard

CommandCenter’s rapid deployment option allows an administrator to enroll multiple security appliances using a streamlined enrollment process.

Figure 1: Quick Start Wizard: CommandCenter Management window

1. Begin the Sidewinder Quick Start Wizard.
   On the CommandCenter Registration window, select the **Auto-register to CommandCenter** check box. Complete these fields:
   a. **Primary Server host name** — Enter the fully qualified domain name of the Management Server. If you are using a High Availability Management Server configuration, use the fully qualified domain name of the active Management Server.
   b. **Primary Server IP address** — Enter the IP address of the Management Server.
   c. **Sign Up password** — Create a password that will be used when enrolling this Sidewinder with the CommandCenter Configuration Tool. The password must be a minimum of 8 characters and a maximum of 256 characters.

2. Complete this appliance’s initial configuration.
   Use the Sign Up Firewalls dialog in the CommandCenter Configuration Tool to initiate rapid deployment. See the *CommandCenter Startup Guide* for more information.

Registering with CommandCenter using the Admin Console

You can use the Admin Console to register a single configured appliance.

1. Select **Maintenance > CommandCenter Registration**. The CommandCenter Registration window appears.

2. In the **Name** field, enter the fully qualified domain name of the Management Server that will manage this appliance. If you are also using backup servers, use the fully qualified domain name of the active Management Server.

3. In the **IP Address** field, enter the IP address of the Management Server.

4. Click **Register with the CommandCenter Now**. Click **Yes** to confirm your changes. The Authentication window appears.
5 Enter the user name and password of the CommandCenter administrator. These are the
user name and password created when initially configuring the CommandCenter
Management Server.

A "registration succeeded" message appears.

6 Click **OK**.

To complete registration, use the Management Server Configuration Tool. See the
*CommandCenter Startup Guide* for more information.

**Managing versions of Sidewinder software**

The Software Management window has been updated to show whether a Sidewinder version
can be managed by CommandCenter.

On the Admin Console tree, select **Maintenance > Software Management**.

On the Manage Packages tab, the new CommandCenter Management column displays one of
the following values:

- **4.0.0.00** — The version(s) of CommandCenter software that the selected Sidewinder patch
  is compatible with.
- **Not Supported** — A version of CommandCenter software that can manage the selected
  Sidewinder patch has not yet been released.
- **Not Applicable** — The selected Sidewinder patch does not affect CommandCenter
  management.
- **Never Supported** — Support for CommandCenter management will never be available for
  the selected Sidewinder patch/version.

**Sendmail TLS**

The Sendmail implementation of RFC 2487, SMTP over TLS, is now supported.

Sendmail can act as either a client or server in a TLS session:

- When acting as the server, it advertises the STARTTLS feature in the response to the EHLO
  command, then responds positively to the subsequent STARTTLS command.
- When acting as the client, it issues the STARTTLS command if the remote server advertises
  STARTTLS on the EHLO response.

In both cases, after the STARTTLS command and positive response, the client and server
negotiate a TLS session.

*Note: As part of the implementation, Sendmail TLS also enforces FIPS mode.*

For more information, see the Sendmail TLS app note at

**PIM-SM protocol and multicast routing**

*Multicast* is communication between a single or multiple senders and multiple receivers on a
network. The Sidewinder appliance uses a XORP routing package and IGMP and PIM-SM
protocols to route multicast traffic:

- The Internet Group Management Protocol (IGMP) is used by hosts and adjacent routers to
  establish multicast group memberships. IGMP tells routers that a host wants to receive
  multicast traffic for the specified multicast group.
- The Protocol Independent Multicast - Sparse Mode (PIM-SM) protocol sets up a multicast
  forwarding table in routers. Multicast traffic is directed to a Rendezvous Point (RP), which
  distributes it toward PIM-registered receivers.
When a host wants to join a multicast session, IGMP sends a join request to its gateway router for a multicast group. Since the gateway router doesn't have information about the source address, it will send a PIM join back to the RP, which will contain the source information.

Once a gateway router with direct connection to the receiver’s network has received traffic from the source, the gateway router might start a process to build a direct path from the sender to the source.

To configure a Sidewinder appliance to route multicast traffic using PIM-SM, you must perform the following procedures:

1. Create policy rules for the following:
   a. Enable the pimd (XORP server) service.
   b. Enable PIM traffic forwarding to RPs and bootstrap routers.
   c. Allow multicast traffic.

2. Configure the pimd (XORP server) service.

3. Configure IGMP.

4. Configure PIM-SM.
   a. Specify which interfaces are expected to receive multicast traffic.
   b. Configure the rendezvous point (RP).

5. Restart the pimd (XORP server) service.

It is recommended that you make all of these configuration changes at one time, since you must restart the pimd service to initialize your changes.

**Note:** When making subsequent changes to PIM-SM, there are two types of changes that require different procedures. See “Exceptions to making PIM-SM changes” for more information.

Create a rule to enable the pimd (XORP server) service

2. Click New Rule.
3. Enter a name and description that quickly identifies this as the rule that enables the pimd (XORP server) service.
4. In the Service field, select pimd from the drop-down list.
5. Set both the Source Burb and the Destination Burb fields to Any.
6. Configure the other Source and Destination fields as necessary to enforce your PIM-SM security policy.
7. Save your changes.
Create a rule to enable PIM traffic forwarding to RPs and bootstrap routers

1. Create a packet filter service for the rule:
   b. Click New Service. The New Service window appears.
   c. Enter a name and description that easily identifies the service.
   d. From the Agent drop-down list, select Other Protocol Packet Filter.
   e. From the Protocol drop-down list, select 103 - pim.
   f. Select Bi-directional.
   g. Click Add and save your changes.

2. Create a rule using the service:
   b. Click New Rule.
   c. Enter a name and description that quickly identifies this as the rule that enables PIM traffic forwarding.
   d. In the Service field, select the new traffic forwarding service.
   e. Set both the Source Burb and the Destination Burb fields to Any.
   f. Configure the other Source and Destination fields as necessary to enforce your PIM-SM security policy. Include all RP and bootstrap routers within the PIM network.
   g. Click Add and save your changes.

Create a rule to enable multicast traffic

1. Create a packet filter service for the rule:
   b. Click New Service. The New Service window appears.
   c. Enter a name and description that easily identifies the service.
   d. From the Agent drop-down list, select TCP/UDP Packet Filter.
   e. In the UDP ports field, select the UDP ports your multicast applications will be using.
   f. Select Bi-directional.
   g. Make any other changes necessary for your site’s security policy.
   h. Click Add and save your changes.

2. Create a rule using the service:
   b. Click New Rule.
   c. Enter a name and description that quickly identifies this as the rule that enables multicast traffic forwarding.
   d. In the Service field, select the new multicast traffic service.
   e. Set both the Source Burb and the Destination Burb fields to Any.
   f. Configure the other Source and Destination fields as necessary to enforce your multicast security policy. Include the multicast groups in the Destination Endpoint field.
   g. Click Add and save your changes.
Configure the pimd (XORP server) service

1 Select **Network > Routing > Dynamic Routing > PIMSM**.
2 Click **Edit**. The xorp configuration file opens in the File Editor.
3 Verify that the interface names in the file are correct.
4 Remove the comments for these parameters:
   - Interfaces you want to run multicast over. *default-system-config* causes pimd to use the interface configuration from the system kernel.
   - *mfea4* identifies which interfaces are being used for multicast traffic.
   - *register_vif* is necessary for XORP processing.
   - *fea* tells pimd how to locate unicast routes.
   - *fib2mrib* tells PIM-SM to use the unicast routing table to find a route to the rendezvous points and to the sender.
5 Save your changes.

Configure IGMP

1 If necessary] Select **Network > Routing > Dynamic Routing > PIMSM** and click **Edit** to open the xorp configuration file.
2 Add an IGMP clause to the configuration file, specifying the interfaces to networks where hosts are receiving multicast packets. See the example below.

![Figure 3: IGMP added to the xorp configuration file](image)

*Note:* To disable IGMP, remove the *igmp* section, then restart the pimd service.

3 Save your changes.
Configure PIM-SM

You need to perform two tasks to configure PIM-SM:

• Specify interfaces you expect to receive multicast traffic.
• Configure the rendezvous points.

To specify interfaces:

1 [If necessary] Select Network > Routing > Dynamic Routing > PIMSM and click Edit to open the xorp configuration file.

2 Configure these parameters:
   • Interfaces that will run PIM-SM.
     • For each interface, an interface statement within the pimsm4 section of the config file must be included.
     • register_vif must be included.
   • Bootstrap router information. The bootstrap router selects the rendezvous points.
   
   **Note:** You cannot change the bsr-priority (bootstrap router priority) setting in this file. If you need to change this setting, see "Changing the bsr-priority setting" for instructions.

3 Save your changes.

To configure rendezvous points:

1 [If necessary] Select Network > Routing > Dynamic Routing > PIMSM and click Edit to open the xorp configuration file.

2 Remove the comments from the bootstrap router and rendezvous points.
   • cand-bsr is the bootstrap protocol that selects a bootstrap router. The bootstrap router tells all PIM-SM routers what the rendezvous points are.
   • cand-rp tells the bootstrap router that it is a candidate to be an RP.

3 Save your changes.

**Restart the pimd (XORP server) service**

You must restart the pimd (XORP server) service to initialize your configuration changes.

1 Select Policy > Rules.
2 Select the rule that uses the pimd service and click Modify.
3 Clear the Enable box.
4 Click OK and save your changes.
5 Select the rule that uses the pimd service and click Modify.
6 Select the Enable box.
7 Click OK and save your changes.

**Viewing the PIM-SM configuration**

You can use the PIMSM window on the Admin Console to view different segments of the PIM-SM configuration, and to view the running configuration.

1 Select Network > Routing > Dynamic Routing > PIMSM. The PIMSM window appears.
2 Select an option from the list and then click Retrieve.
Exceptions to making PIM-SM changes

The procedures in this document explain how to configure the XORP server using the Sidewinder Admin Console. To configure the XORP server through a command line interface, you use the XORP command shell xorpsh.

The Admin Console’s PIMSM window, xorpsh, and any file editor open the same config.boot file (/secureos/etc/xorp/config.boot). However, the PIMSM editor and xorpsh interact, which can cause conflicts.

To avoid conflicts, there are two types of changes to PIM-SM that require different procedures:

• Disabling and enabling PIM-SM
• Changing the bsr-priority setting

Disabling and enabling PIM-SM

You cannot use xorpsh to enable or disable PIM-SM. To avoid an error message, you must enable or disable the rule that uses the pimd service.

1 Select Policy > Rules.
2 Select the rule that uses the pimd service and click Modify.
3 Make the appropriate action:
   • To disable the pimd (XORP server) service, clear the Enable box.
   • To enable the pimd (XORP server) service, select the Enable box.
4 Click OK and save your changes.

Changing the bsr-priority setting

You cannot change the bsr-priority (bootstrap) parameter using the Edit function on the PIMSM window. To avoid an error message, you must stop the XORP server, change the parameter, and restart the XORP server.

To change the bsr-priority parameter:

1 Stop the XORP server:
   a Select Policy > Rules.
   b Select the rule that uses the pimd service and click Modify.
   c Clear the Enable box.
   d Click OK and save your changes.
2 Change the bsr-priority parameter:
   a Select Maintenance > File Editor and open the following firewall file:
      /secureos/etc/xorp/config.boot
   b Make the desired change to the bsr-priority parameter.
   c Save your changes and close the File Editor.
3 Start the XORP server:
   a Select Policy > Rules.
   b Select the rule that uses the pimd service and click Modify.
   c Select the Enable box.
   d Click OK and save your changes.
Patch 7.0.0.03

Sidewinder patch 7.0.0.03 (the New Dynamic Routing and various improvements patch) provides the following benefits:

Patch 7.0.0.03 new features

Patch 7.0.0.03 introduces these new features:

• Supports dynamic routing protocols – Quagga routing suite: RIPv2, OSPF, BGP. See the “Routing” chapter of the updated Sidewinder Administration Guide for details.
• Adds support for multicast ranges and subnets to TCP/UDP Packet Filter services.
• Adds ability to export rules from the Active Rules window.

Patch 7.0.0.03 fixes and enhancements

Patch 7.0.0.03 provides the following benefits:

Proxies

• HTTP Proxy
  – Corrects an issue that could cause incorrect informational audits when ActiveX filtering is enabled.
  – Improves handling of allowed data when ActiveX or Java Applets are filtered.
  – Enhances proxy to accommodate a benign idiosyncrasy in a popular Web site.
  – Enhances SmartFilter redirect, making address configurable.
  –Corrects an issue in handling the presence of both a Connection header and a Proxy-Connection header in the server’s response.
  – Improves handling of virus scanning on persistent HTTP connections.
  – Improves error handing and recovery in the proxy.
  – Prevents unwarranted timeout upon FTP request through the HTTP proxy for zero length file.
  – Improves proxy delayed acl response handling when SmartFilter is enabled.
• H.323
  – Corrects issue preventing H.323 call completion in H.245 routed mode with both endpoints in the same burb.
  – Corrects an issue that could prevent H.245 connection acceptance through a VPN.
  – Corrects an issue with three burb H.323 traffic configuration, with the gatekeeper and call terminals all in different burbs.
• SNMP — Corrects processing of uptime value from external load balancing system.
• RTSP — Improves memory management of the proxy.

Packet Filter

Improves handling of ICMP message filtering rules.

Admin Console

• Relaxes restrictions on server names when adding a new server using the Admin Console. Initial definition now allows spaces, periods, underscores, and many other characters. This change also allows renaming a server (as long as you’re not connected to it).
• The Load Packages window now automatically searches the correct directory when loading packages from CD-ROM.
• The State Change Wizard has been renamed the Cluster Wizard, and is now found at Maintenance > Cluster Wizard. It can no longer be accessed from the Dashboard or from the toolbar.

Quick Start Wizard

Corrects an issue with the Quick Start Wizard initial configuration time zone changes for countries containing only a single time zone.
Auditing & Reporting

- E-mail group support is added to IPS Attack Responses and System Responses.
- Adds support for exporting audit with SCP to `cf export`.
- Improves efficiency of audit daemon handling of log rolling.
- Adds `report_name=all` feature to `cf_reports` report generation.
- Includes packet filter rule usage in rule usage report.
- Improves dashboard monitoring when blackholing attacking hosts in an IPS Attack Response.

Authentication

Adds audit if appliance cannot resolve its own hostname. This provides a tool to debug an operational dependency of some RADUIS servers.

Anti-Virus

Improves error handling during the downloading of a new signature file.

Hosted Sendmail

- Improves handling of connections that are terminated before the message is complete.
- Corrects an issue preventing configuration of mail filtering in burbs with index greater than 9.

URL Filter

Enhances SmartFilter operation in an HA load-sharing environment.

Configuration Backup/Restore

- Adds audit at start as well as completion of a configuration restore.
- Improves error feedback when user attempts to restore a configuration to an incompatible Sidewinder version.

Miscellaneous System

- Corrects issue causing spurious error audits during burb add/delete and config/restore operations.
- The "login" service, used to control console access, can no longer be included in service groups. Since it does not involve network traffic, it cannot be logically grouped with network-based services.
- Adds support into Intel® driver for new dual port NICs on 510D appliances.
- Adds the ability to use source port NAT on the primary firewall IP instead of just on aliases — allows VPN both through, and to, the appliance on a single IP.
- Corrects TCP SYN response negotiated windows size to improve interoperability with some older web servers.
- Ensures that communications internal to the appliance will not be inadvertently blocked by policy.
- Improves Kernel burb index parsing algorithm.
- Corrects an issue caused by use of an empty netgroup as a destination on a proxy rule.
- Prevents creation of empty domain objects.
- Prevents package installation on an incorrect base revision.
Administration Guide

An updated version of the Sidewinder Administration Guide is available on the Secure Computing web site: www.securecomputing.com/goto/manuals. Revision B includes the following new or updated information:

- Changes from patches 1 and 2 are incorporated into guide.
- The “Routing” chapter has been updated to reflect the Quagga implementation of routing protocols.
- The “VPN” chapter includes a section explaining how to use rules to filter traffic bound for a VPN.
- The “Auditing” chapter includes an expanded list of supported formats.
- The “Basic Troubleshooting” appendix has added instructions on using the Backup Builder application to create disaster recovery media.
- Various other enhancements and fixes.
Patch 7.0.0.02

Sidewinder patch 7.0.0.02 (the IPS and Blackhole Dashboard patch) provides the following benefits:

- For fixes and enhancements, see the following section.
- For new features, see page 36.

Patch 7.0.0.02 fixes and enhancements

Patch 7.0.0.02 provides the following benefits:

Intrusion Prevention System (IPS)

Updates default IPS signature groups to provide more guidance about how to make the best use of signature-based IPS capabilities.

Proxies

- HTTP Proxy
  - Corrects an issue with SSO authentication through the HTTP proxy when using SmartFilter and LDAP.
  - Improves performance of anti-virus processing of HTTP 1.1 pipelined responses.
  - Improves session cleanup processing when the server-side session unexpectedly closes the connection.
  - Corrects handling of abbreviated and mismatched case authenticators specified during login.
  - Improves handling of client close requests sent in rapid succession.
  - Improves handling of anti-virus scanning when the server immediately closes the connection.

- FTP
  - Corrects reply that prevents `ftp -n` from some Unix clients from working with a non-transparent proxy.

- SIP
  - Improves the proxy’s ability to scale connections under heavy load.

- RTSP
  - Improves session close processing.
  - Adds support for updated protocol behavior in some new clients and servers.

Packet Filter

- Improves IP Filter idle time-out reset processing on redirected connections.
- Corrects unnecessary source IP address translation on ICMP packets processed through IP Filter.

Admin Console

- Adds ability to manage blackhole lists from the Dashboard.
- Adds columns to the main Rules window to show the current IPS group and response settings.
- Adds SIP proxy process to the Service Status window for proxy status reporting.
- Corrects an issue with application of source and destination burb restrictions to the rule editor service source and destination dialogs, and includes the Firewall burb option in the menus.
- Corrects Admin Console handling of an HA primary demotion to stand-alone appliance. The connection is now properly maintained and the address on the main connection window correctly reverts to the standalone address.
Quick Start Wizard

- Allows the underscore '_' character in host names.
- Introduces the ability to save a configuration if the Quick Start Wizard is unable to connect to the appliance via the serial port. When the failure message appears, click Save and then follow the on-screen instructions.
- Improves error notification when a user tries to push a configuration when HyperTerminal is simultaneously connected using the same serial connection.

Licensing

Corrects a problem where an appliance boot message incorrectly complains that SecureOS is not licensed.

Auditing and Reporting

- Corrects an issue sometimes causing reports with unrealistic traffic byte counts.
- Corrects Sendmail auditing if the client sends a MAIL FROM: command that includes a SIZE= parameter with a value that is greater than the SIZE on the EHLO response.
- Corrects an issue preventing forwarding of WELF format audit via syslog.
- Adds support for transmitting multiple syslog streams using different audit message formats.
- Corrects a case where a 0-byte traffic audit was be issued for a connection denied by policy.

IPsec VPN

- Removes VPN dependency on existence of a default route.
- Adds capability to duplicate and rename defined VPN security associations from the Admin Console. See “VPN Definitions rename and search functionality” on page 37 of these Release Notes for details.
- Corrects an issue that could have prevented users from selecting some VPN definitions for editing in the Admin Console.
- Improves processing when changing the termination burb of an active VPN.
- Corrects a number of IKEv2 interoperability issues discovered during multi-vendor IKEv2 testing.

Anti-spam

Corrects error in an audit message for some non-spam messages that incorrectly labeled them as spam in the audit, even though message processing and handling was correct.

SmartFilter

- Supports operation of SmartFilter on appliances with an SSL acceleration adapter.
- Corrects an issue that required a manual SmartFilter agent restart to enable a SmartFilter admin connection to an HA secondary after pushing a new configuration to the agent.

Hosted Sendmail

- Updates sidfilter (Sender ID) to v0.2.14.
- Extends the allowable maximum configurable DNS time-out value for sidfilter.
- Adds explanation string to Sender ID rejection response. For example, response changed from Diagnostic-Code: SMTP; 554 5.7.1 Command rejected to Diagnostic-Code: SMTP; 550 5.7.1 Rejected due to SPF policy for sender test@pilsner.a.com.
- Improves processing of multiple messages received in the same connection. See Knowledge Base article #5067 for details.
- Corrects a problem that could cause large messages to stay in the queue for too long.
**Configuration Backup/Restore**
- Corrects an issue during a configuration restore when the physical interface associated with a VLAN is missing (removed from the system).
- Corrects an issue when backing up a configuration on appliances where `named.conf.*` files included sortlist entries.

**DNS**
Adds a popup reminder that, when reconfiguring DNS (transparent, single server, or split DNS), a reboot is necessary for the changes to take effect.

**High Availability and OTM**
- A newly enabled sshd on a load-sharing cluster now immediately locks to the primary node.
- Changes warning message displayed when modifying cluster common HA settings to direct the user to reboot all members of a cluster to get the cluster common settings to take effect on all nodes.

**Miscellaneous System**
- Adds capability to remove packages that are loaded, but not installed. Also adds capability to view descriptions of packages on CD-ROM.
- Corrects an issue in handling of `routed.conf` files during burb configuration changes and configuration restore operations.
- Corrects an issue in ACL cache management.
- Corrects an issue that prevented SSH from using some ports in its allowed range as an alternate port.
- Corrects an issue that prevented `cf policy export` from working.
Patch 7.0.0.02 new features

Patch 7.0.0.02 introduces these new features:

- “IPS instructions and enhancements” on page 36
- “VPN Definitions rename and search functionality” on page 37
- “Blackholed IPs list management” on page 37

IPS instructions and enhancements

The Sidewinder Intrusion Prevention System (IPS) license and signature files are now widely available. Read this section for important information on purchasing the IPS add-on module and IPS Engine with ASIC hardware acceleration, activating the IPS features and installing the latest signature files, and IPS-related enhancements to the main Rules window.

- **Purchasing** — If you have not yet purchased an IPS add-on module or the IPS Engine with ASIC hardware acceleration, and would like to use these Sidewinder IPS features, contact your Secure Computing channel partner or sales representative. To find Sales contact information, visit [www.securecomputing.com](http://www.securecomputing.com) and select an option from the Try/Buy menu.

- **Activating and installing** — Carefully follow the instructions in these Release Notes for licensing the IPS and IPS Signatures features, downloading and installing patch 7.0.0.02, and downloading and installing the newest signatures. These steps must be completed in the following order:

  Note: Complete these steps, even if you previously installed 70001H01 and downloaded a signature file at that time.

  a. License the IPS feature: Once you have purchased the IPS add-on module, select Maintenance > License, and then click the Firewall tab. Click Submit Data to obtain the updated license.

  b. [Conditional] Install the IPS Engine with ASIC hardware acceleration: For instructions, go to [www.securecomputing.com/supportkb.cfm](http://www.securecomputing.com/supportkb.cfm) and see Knowledge Base article #5379.

  c. Download and install patch 7.0.0.02: See “Loading and installing this patch” on page 10.

  d. Download and install the most recent signatures.

  **Tip:** If you accidentally install this patch and the signatures before updating your license, IPS will not be properly enabled. To manually enable IPS, use a command line session and run `cf ips reload`.

- **Displaying IPS information on rules** — The main Rules window has added two new columns: IPS Response and IPS Signature Group. These columns display a rule’s selected IPS response mapping and signature groups. These columns are displayed by default, but you must scroll to the right to see them.

  To move these columns, select Policy > Rules and then click Columns. Select the column you want to move and then use the Up and Down buttons to change the column order.

  ![Figure 4: Rules window with IPS columns displayed](image)
**VPN Definitions rename and search functionality**

The main VPN Definitions window (Network > VPN Configuration > VPN Definitions) has added three new features:

- **Duplicate** — To create a duplicate of an existing VPN definition, select the original VPN definition and click **Duplicate**. The default name of the new item is `Copy_of_x`, where `x` is the original definition’s name.

- **Rename** — To rename a VPN definition, select an existing definition and then click **Rename**. Type the new name in the pop-up window and click **OK**.

- **Find** — To find a VPN definition, enter a character string related to the definition you are searching for in the **Find** field. The Find function searches all columns, and filters as you type. Clear this field to see the complete list again.

**Blackholed IPs list management**

The Blackholes IPs window allows you to view and manage the currently blackholed IP addresses.

To access this window, select the **Dashboard** and then click the **Blackholed IPs** link.

Clicking this link opens the Blackholed IPs pop-up, shown in Figure 7 on the following page.
Each entry in the table displays the IP address, burb, and the date and time at which the IP address will no longer be blackholed. You can perform the following actions in this window:

- **Add an IP address to blackhole** — To add an IP address to this list, click **Add**. In the Add Blackhole IP pop-up window, enter the IP address you want to blackhole and how long, in seconds, before the appliance will accept and respond to traffic from that IP address. This address is then automatically blackholed on all configured burbs.

- **Delete one or more entries** — To remove one or more entry from the list, highlight the row you want to delete and click **Delete**. To select multiple rows, press and hold the **Ctrl** key as you select the items.

- **Delete all IP entries** — To remove all of the entries that are listed in the table, click **Delete All**.

- **Update the window** — To retrieve an updated list of blackholed IP addresses, click the **Refresh now** icon. The date and time when displayed data was captured is listed in the upper portion of the window.

Click **Close** to exit the window. Change are saved automatically.
Sidewinder patch 7.0.0.01 (the Various Kernel, VoIP, and Other Proxy Enhancements patch) provides the following benefits:

- For fixes and enhancements, see the following section.
- For new features, see page 41.

### Patch 7.0.0.01 fixes and enhancements

Patch 7.0.0.01 provides the following benefits:

#### Proxies

- **SIP proxy** — Improves SIP (Session Initiation Protocol) proxy capabilities. The proxy now supports direct endpoint-to-endpoint calls, as well as calls involving a SIP proxy server on one or both sides of the Sidewinder appliance. For information on configuring the SIP proxy in a load sharing environment, see Knowledge Base article #5066.
- **H.323 Gatekeeper proxy** — Improves support in the H.323 proxy to support Gatekeeper transactions. This allows the Sidewinder appliance to interact with H.323 call requests from a Gatekeeper on one or both sides of the firewall. Routed and direct mode calls are supported.
- **HTTP proxy** — Improves SmartFilter URL response processing when the session is unexpectedly closed.

#### Packet Filter

- Restores intra-burb packet forwarding. Packet filter processing can now forward packets to another destination (VLAN or interface) in same burb on which they arrived. Intra-burb forwarding is configured on the Packet Filter rule Properties pop-up.
- Corrects an issue with rules using an `sw-all` packet filter.

#### Licensing

Corrects an issue where the Admin Console would not immediately reflect license changes when submitting a new serial number for the secondary member of a peer-to-peer High Availability cluster.

#### Auditing and Reporting

- Allows configuration of IPS attack responses to use blackhole processing based on a source IP address when there is no attacker IP recorded in the audit. The administrator can set a threshold where an excessive number of policy violations (for example, netprobes) trigger blackhole packet processing of the source IP for a defined period of time.
- Adds support for the command line `gen_reports` tool for read-only users.
- Adds man page for `cf_reports`.

#### IPsec VPN

Improves support for simultaneous operation of password and certificate VPN tunnels between the same endpoints.

#### Anti-Virus

Corrects mail scanning to properly process encrypted attachments when `Reject All files if scanning is unavailable` is checked in the application defense.

#### Anti-Spam

- Improves performance by correcting several issues where the engine would scan a message twice or otherwise consume unnecessary resources.
- Improves memory management when using a very large number of white list entries.

#### Disaster Recovery

Improves handling of restoration from a disaster recovery USB stick created on a different hardware platform.
**Policy rules**
Corrects a validation error that allowed an object to be renamed to a name which is already in use.

**Intrusion Prevention System (IPS) Processing**
- Various improvements made to IPS processing:
  
  **Note:** Small instabilities persist. A Hotfix will be available shortly to correct these issues. It is strongly recommended this feature not be enabled until the Hotfix is installed.

  - Signatures are categorized based on the type of traffic to which they apply and the type of attack activity.
  - Signatures to be applied and actions to be taken upon signature matches can be configured on proxy and packet filter policy rules. This allows the user to avoid false positives and to apply the correct signatures to known protocols running on unusual ports.
  - Response actions include auditing, denying or dropping the connection, and blackholing the attack address. Signatures are grouped in IPS and IDS categories, making it easy to limit severe responses to IPS signatures while auditing IDS-level activity.
  - Signature updates can be downloaded manually or on an automated periodic basis. New signatures will be applied to the current policy based on their categorization and the system configuration.
  - More information can be found in the Sidewinder Administration Guide.

- IPS is a licensed feature. Contact your sales representative or reseller for more information.
Patch 7.0.0.01 new features

Patch 7.0.0.01 introduces these new features:

- “Intra-burb forwarding” on page 41
- “Blackhole network probe attacks” on page 42

Intra-burb forwarding

Patch 7.0.0.01 re-implements the intra-burb forwarding option using packet filtering. Use this option to forward traffic between network interfaces located within the same burb.

At Sidewinder G2, intra-burb forwarding was managed at the burb level. At Sidewinder 7, it is enforced on a per-rule basis when these conditions are met:

- The rule’s source and destinationburbs are the same.
- The rule’s service uses the TCP/UDP Packet Filter agent
- The Allow intra-burb forwarding option is enabled on the TCP/UDP Packet Filter agent's Global Properties window.

To enable the intra-burb forwarding option:

2. Click New Service. The New Service window appears.
3. From the Agent drop-down list, select TCP/UDP Packet Filter.
4. Click Properties.
5. Select Allow intra-burb forwarding.

6. Click OK, and then configure and save the service.
8. Create a rule that:
   a. has the same source and destination burb
   b. uses a server based on the TCP/UDP Packet Filter agent.

Intra-burb forwarding now applies to that rule’s traffic.
**Blackhole network probe attacks**

By default, the IPS Attack Responses Strikeback® feature can only blackhole IP addresses found in the Attack IP field of an audit message. An Attack IP field indicates both that the activity from the audit is likely to be malicious or to violate policy, and that the IP address has been confirmed via a TCP 3-way handshake and thus is unlikely to be forged. When an audit message does not have an Attack IP field, the traffic from the attacking host cannot be blackholed.

The **Blackhole source IP if attack IP cannot be confirmed** option makes it possible to blackhole the attacking host even when the related audit message does not have an Attack IP field by blackholing the source IP instead. This can be used to enforce thresholds on otherwise allowed behaviors (for example, limiting a connection rate for SSH traffic). This feature can also be used to configure blackholing on netprobes, UDP attacks, and SYN attacks (all audit messages that do not contain an Attack IP field).

> **Caution:** For netprobes, UDP attacks, and SYN attacks, it is possible for the attacker to forge the source IP address. A configuration which blackholes source addresses found in these audits may allow an attacker to trigger a blackhole for an unrelated third party, potentially interrupting desired traffic.

To change the default behavior so that all IPS attack responses that encounter audit messages that do not have an Attack IP field then blackhole on the source IP address:

1. Select **Monitor > IPS Attack Responses** and click the **Response Settings** button. The Global Attack Response Setting window appears.
2. Select **Blackhole source IP if attack IP cannot be confirmed**.

No connections will be accepted from the IP address originating the attack.