FORCEPOINT

Sidewinder

Hardware Migration Guide

Sidewinder S model to Stonesoft NGFW

Revision B

Table of contents

1 Introduction....................3

2 Prepare to upgrade....................4

Create a Sidewinder configuration backup....................4

Download Stonesoft NGFW product documentation....................5

Obtain licenses....................6

Download Stonesoft NGFW and SMC....................6

Install and configure SMC....................6

3 Upgrade to Stonesoft NGFW....................7

Create the initial configuration....................7

Install Stonesoft NGFW....................7

Transfer the initial configuration....................9

4 Complete post-upgrade tasks....................13

Introduction

This document explains the process of upgrading an existing Forcepoint™ Sidewinder® S model appliance to run as a Stonesoft® Next Generation Firewall by Forcepoint (Stonesoft NGFW) appliance.

Note: We strongly recommend that you read the entire document before beginning the upgrade process.

You can use the upgraded Sidewinder appliance in one of the following Stonesoft NGFW roles.

- **Firewall/VPN** — Layer 3 firewall with IPsec VPN and SSL VPN capabilities
- **Layer 2 Firewall** — Fully transparent layer 2 firewall

The role is assigned during the initial configuration of the appliance. For more information about the roles, see the *Stonesoft Next Generation Firewall Product Guide*.

Note: You cannot use the migrated Sidewinder appliance as a Stonesoft NGFW appliance in the IPS role.

About Stonesoft Management Center

Stonesoft® Management Center (SMC) is the management component of the Stonesoft NGFW system. The Management Client is the user interface for the SMC. You use the Management Client for all configuration and monitoring tasks. You can install the Management Client locally as an application, or you can start the Management Client with a web browser using the Java Web Start feature.

The Management Client allows you to handle various tasks in one place:

- Manage engines
- Manage all licenses
- Create administrator accounts with various levels of permissions
- Create policy templates and policy elements
- Install a policy on multiple engines
- Produce data visualizations of traffic patterns and events that you can export
- Create API Clients, virtual private networks (VPNs), self-signed certificates, and more

Upgrade process

Upgrading your Sidewinder appliance involves these high-level steps:

1. Prepare for the upgrade by making a Sidewinder backup.
2. Install SMC.
3. Create the initial configuration for the Stonesoft NGFW engine in the Management Client.
4. Install the Stonesoft NGFW engine image on the appliance.
5. Transfer the initial configuration to the appliance.

Prepare to upgrade

If you want to transfer elements from the Sidewinder configuration to Stonesoft NGFW, convert and export the configuration before you begin the Sidewinder appliance upgrade.

Note: If you only want to upgrade the Sidewinder appliance hardware, it is not necessary to convert and export the configuration.

Follow these general steps to export the Sidewinder configuration in a format that is compatible with Stonesoft NGFW.

For detailed instructions, see the *Stonesoft NGFW Migration Tool Guide*.

1. Using the Stonesoft NGFW Migration Tool, convert and export the Sidewinder configuration.
2. Import the configuration into the SMC.

Create a Sidewinder configuration backup

Backing up the Sidewinder appliance configuration provides a way to restore the appliance to be used as a Sidewinder appliance if you want to undo the upgrade.

The Sidewinder appliance configuration backup can only be used to restore a Sidewinder appliance. The Sidewinder backup does not contain the configuration information that is needed to convert the Sidewinder configuration for use in the SMC. You cannot transfer the Sidewinder backup to a Stonesoft NGFW appliance.

CAUTION: Do not save the configuration backup on the Sidewinder appliance. Save the configuration backup in another location. The upgrade process erases existing information from the appliance.

Create a backup for an unmanaged firewall

You can back up configuration files to the computer where you use the Admin Console or to a remote system.

Before starting the backup, determine if the firewall has a customized /secureos/etc/config.conf file. We recommend creating a manual backup of any files defined by the custom entries.

1. In the Admin Console, select **Maintenance** > **Configuration Backup**.
2. If the **Backup** tab is not selected, click the **Backup** tab.
3. In the **Backup Sidewinder Configuration** options, select where to save the backup file.
   - To save the backup on computer where you use the Admin Console, select **Client system** .
   - To save the backup on another Sidewinder appliance or a remote system, select **Remote system (SCP)**.
4. If you selected **Client system** , save the backup on the Admin Console computer.
   1. Click **Backup Now**.
      The **Save Configuration Backup** window appears.
   2. Specify the destination path, file name, and the file type, then click **Save**.
      The **Filename and encryption** window appears.
   3. (Optional) If you want to encrypt the configuration backup file, enter and verify an encryption key. Otherwise, continue to the next step.

      Valid values include alphanumeric characters, periods (.), dashes(-), underscores (_), and spaces ( ).

    > ⚠ **CAUTION:** If you encrypt the configuration backup file, you must have this key to restore the configuration backup file. The key is not automatically saved.

    4. Click **OK**.
       A "Configuration backup successful" message appears.
    5. Click **OK**.
       The configuration backup file stored on the on the computer where the Admin Console is installed.

5. If you selected **Remote System (SCP)**, save the backup on a remote system using Secure Copy (SCP).
    1. Enter the remote system access information.
    2. Click **Backup Now**.
       The **Filename and encryption** window appears.
    3. (Optional) In the **Filename** field, enter a name for this configuration backup for your own reference.

       A default name consisting of the firewall name plus the current date automatically populates this field.
    4. (Optional) If you want to encrypt the configuration backup file, enter and verify an encryption key. Otherwise, continue to the next step.

       Valid values include alphanumeric characters, periods (.), dashes(-), underscores (_), and spaces ( ).

       > ⚠ **CAUTION:** If you encrypt the configuration backup file, you must have this key to restore the configuration backup file. The key is not automatically saved.
    5. Click **OK**.
       A "Configuration backup successful" message appears.
    6. Click **OK** to close the message.

You have finished backing up a configuration file to the firewall.

Create a backup for a managed firewall

For managed firewalls, the configuration backup must be created in the Control Center Client.

1. In the navigation pane of the Control Center Client, select **Maintenance**.
2. In the **Firewall Maintenance** tree, double-click the **Configuration Backup** node. The **Firewall Configuration Backup** window is displayed.
3. Select one or more firewalls for which to create a backup of the configuration data.
4. Click **Create Backup(s)** to store a backup copy of the firewall configuration for the selected firewalls on the Management Server. The **Confirm Backup** window is displayed.
5. Edit the description or accept the default value.
6. Click **OK** to confirm this backup.
   A message appears indicating that this request has been sent to the firewall.

After the backup is complete, the **Description**, **Last Backup Date**, and **Last Backup By** column values appear.

Download Stonesoft NGFW product documentation

Review the Stonesoft NGFW documentation for the appliance.

1. Go to https://support.forcepoint.com.
2. Download Stonesoft NGFW documentation, including these documents.
    - *Stonesoft Next Generation Firewall Product Guide*
    - *Stonesoft Next Generation Firewall Installation Guide*

- *Stonesoft Next Generation Firewall Release Notes*
- *Stonesoft Management Center Release Notes*

Obtain licenses

You must purchase a license for SMC and an upgrade license for each appliance.

> **Note:** Your existing Sidewinder appliance must have a valid license to be eligible for upgrade.

Download Stonesoft NGFW and SMC

Download the Stonesoft NGFW image and SMC software from https://support.forcepoint.com/Downloads.

1. Go to https://support.forcepoint.com/Downloads, enter your logon credentials, then navigate to the appropriate product and version.
2. Download the 64-bit installation media.

   You need these files:

   - smc_<version>.<build>.zip or smc_<version>.<build>.iso
   - sg_engine_<version>.<build>_x86-64.iso

   > **Note:** If you use a USB drive for the Stonesoft NGFW engine .iso file, the .iso file must be converted to a bootable format on the USB drive.

Install and configure SMC

SMC is required to manage the upgraded appliance.

You must have the license files available to complete the installation.

1. Start the SMC installation.
   - **.zip file** — Extract and run the setup.exe (Windows) or setup.sh (Linux) file.
   - **.iso file** — Create an installation DVD or USB drive using the ISO image. Then insert the DVD or USB drive in the Windows or Linux server and run the setup executable.
2. Follow the on-screen instructions to configure and install the SMC components.

   > **Note:** Configuring the Web Portal Server is optional and requires a separate license.
3. Start the Management Client using the shortcut icon created during the installation.
4. When prompted, accept the SMC server certificates, and install the licenses for the SMC servers.
5. (Optional) Install the Management Client on several computers, or use Java Web Start to distribute Management Clients from the Management Server or a web server.

   By default, a Management Client is installed on the same computer where you installed SMC. You can optionally install more Management Clients on other computers.

   To distribute Management Clients from the Management Server using Java Web Start, see the *Stonesoft Next Generation Firewall Product Guide*.
6. (Optional) Set up accounts for other administrators.

You are now ready to upgrade to Stonesoft NGFW.

Upgrade to Stonesoft NGFW

Upgrading the Sidewinder appliance to a Stonesoft NGFW appliance requires several installation and configuration tasks.

Create the initial configuration

Create the initial configuration in the Management Client, then transfer the configuration to the appliance.

Before you create the initial configuration, install and configure SMC, then import the license for the engine.

These are the high-level steps for creating the initial configuration. See the *Stonesoft Next Generation Firewall Installation Guide* for complete instructions.

1. Create a Firewall or Layer 2 Firewall element.
2. (Clusters only) Add all cluster nodes.
3. Define the interfaces and their properties.
4. (Optional) Set the global interface options.
5. Bind the licenses to the Firewall or Layer 2 Firewall element.
6. Save the initial configuration in the Management Client.

After the Stonesoft NGFW engine image is installed, the initial configuration is transferred to the appliance. There are two options:

- Transfer the initial configuration with a USB drive. To save the initial configuration on a USB drive, see the *Stonesoft Next Generation Firewall Installation Guide*.
- Transfer the initial configuration manually through the NGFW Initial Configuration Wizard.

Related tasks

Transfer the initial configuration on page 9

Install Stonesoft NGFW

We recommend that you install Stonesoft NGFW following the normal full installation process.

Note: During the installation, the hard drive is partitioned and all existing information is deleted from the hard drive.

If the Sidewinder S appliance was part of a high availability (HA) cluster, prepare the appliance according to the cluster type:

- **Failover** cluster — Upgrade the secondary (standby) cluster node first.
- **Load Sharing** cluster — Use the soft shutdown option on the appliance to minimize service disruption for the users of the cluster.

1. Insert the Stonesoft NGFW engine media into the appliance.
2. Restart the appliance.
3. Press the appropriate key to interrupt the BIOS.

Table 1: S model Boot menu keys by appliance

Sidewinder appliance model	Boot menu key
S1104	**F7**

Sidewinder appliance model	Boot menu key
S2008 S3008 S4016 S5032 S6032	**F6**

4. Select the boot device.

   > **Tip:** If the boot device menu does not list the media, validate that the media used is formatted correctly, then restart.

5. Type YES to accept the EULA.

   To read each screen, press **Space** to advance to the acceptance page. If you prefer to skip the pages, press **Q** to advance to the acceptance page.

   > **Note:** The response is case sensitive.

6. Select the installation mode.

   - Press **1** for normal full installation.

     > **Note:** We recommend this installation method.

   - Press **2** for full installation in expert mode.

   > **Note:** If you install Stonesoft NGFW in expert mode you must partition the hard drive manually. For more information about installation in expert mode, see the *Stonesoft Next Generation Firewall Installation Guide*.

7. Confirm the hard drive partitioning.

   The installation displays the 64-bit installation message and then provides a warning that the full installation erases all existing information from the hard drive. The eUSB image point is unaffected during this process and can be used to re-image the Sidewinder appliance if necessary.

8. When the installation process is complete, remove the installation media. The appliance restarts.

   - If you are transferring the initial configuration using a USB drive, insert the USB drive while the appliance restarts.
   - If a USB drive is not available, use the NGFW Initial Configuration Wizard to manually configure the engine.

> **CAUTION:** For HA installations, when the upgraded appliance is ready to receive the initial policy, you must take the primary Sidewinder node offline. If it is not offline, a network outage can occur because the primary Sidewinder node and the upgraded appliance try to use the same IP addresses.

Related tasks

Download Stonesoft NGFW and SMC on page 6

Transfer the initial configuration using a USB drive on page 9

Transfer the initial configuration manually on page 10

Transfer the initial configuration

You can transfer the initial configuration to the appliance with a USB drive or transfer the initial configuration manually.

Related tasks

Install Stonesoft NGFW on page 7

Transfer the initial configuration using a USB drive

You can transfer the initial configuration from a USB drive to the appliance when the appliance is brought online.

1. After installation while the appliance is restarting, insert the USB drive that contains the initial configuration.
2. Start the NGFW Initial Configuration Wizard.
    1. Press **Enter** to activate the console.
    2. When you are prompted to start the NGFW Initial Configuration Wizard, type Y and press **Enter**.
3. Select the role for the security engine.

    The role must correspond to the engine element (Firewall/VPN or Layer 2 Firewall) that you defined in the Management Client.

    1. Select **Role** and press **Enter**.
    2. Select your choice and press **Enter**.
4. Import the initial configuration.
    1. Highlight **Import** and press **Enter**.
    2. Select **USB Memory** and press **Enter**.
    3. Select the correct initial configuration file.

        These files are specific to each engine node.
    4. Select **Next** and press **Enter** to continue.
5. Define the network interface drivers.
    - If the list populates automatically, make sure that the information is correct and all interfaces have been detected.
    - If the list did not populate automatically, start the autodetect function.
        1. Select **Autodetect** and press **Enter**.
        2. Make sure that the information is correct and all interfaces have been detected.

            Tip: You can use the Sniff option for troubleshooting the network interfaces. Select **Sniff** on an interface to run the network sniffer on that interface.

            If autodetection fails, contact Forcepoint support.
6. Map interfaces to the IDs you defined.

    Upgraded appliances follow the interface mapping pattern shown in the table.

Table 2: Ethernet interface mapping for upgraded appliances

Sidewinder	Stonesoft NGFW	ID
port mgr0	eth0_0	0
port 1–0	eth1_0	1
port 1–1	eth1_1	2
port 1–2	eth1_2	3

Sidewinder	Stonesoft NGFW	ID
port 1–3	eth1_3	4
port 1–4	eth1_4	5
port 1–5	eth1_5	6
port 1–6	eth1_6	7
port 1–7	eth1_7	8

Change the IDs as needed to match the Interface IDs defined for the engine element in the Management Client.

1. Select the **Media** column and press **Enter** to change the settings.
2. Verify that the speed/duplex settings of network cards are identical at both ends of each cable.

   For Layer 2 Firewall engines, make sure that the inline interface speed/duplex settings match for both links in each pair.
3. Select the **Mgmt** column.
4. Press the spacebar to select the correct interface for contact with the Management Server.

   > **Important:** The Management interface must be the same interface on which the control IP address for the corresponding element is configured in the SMC. Otherwise the engine cannot contact the Management Server.

7. On the **Prepare for Management Contact** page, complete the information and make your selections.

   If the initial configuration was imported from a USB drive, most of this information is populated. For more information about how to complete the information, see the *Stonesoft Next Generation Firewall Installation Guide*.

   > **Note:** If there is an intermediate firewall between this engine and the Management Server, the intermediate firewall policy must allow the initial contact and all subsequent communications.

8. Set the password for the root account.

   > **Note:** To access the appliance through the command line, the root account password must be manually set in the Management Client. See the *Stonesoft Next Generation Firewall Product Guide* for more information.

After the appliance successfully contacts the Management Server and restarts, the configuration is complete.

Transfer the initial configuration manually

If a USB drive is not available, you can transfer the initial configuration through the NGFW Initial Configuration Wizard.

> **Tip:** You can run the NGFW Initial Configuration Wizard at any time using the `sg-reconfigure` command on the engine command line.

1. After the appliance restarts, start the NGFW Initial Configuration Wizard.
   1. Press **Enter** to activate the console.
   2. When you are prompted to start the NGFW Initial Configuration Wizard, type Y and press **Enter**.
2. Select the role for the security engine.

   The role must correspond to the engine element (Firewall/VPN or Layer 2 Firewall) that you defined in the Management Client.
   1. Select **Role** and press **Enter**.

    2. Select your choice and press **Enter**.
3. To manually configure the engine's settings, select **Next** and press **Enter**.
4. Set the keyboard layout and local time zone.

   > **Note:** The keyboard layout setting applies only to hardware that you connect to directly with a keyboard and monitor. This setting does not apply if you connect to the hardware only through the serial console port or over the network with SSH.

5. Set these operating system settings.
    1. Enter the name of the engine.
    2. Enter and confirm the password for the user `root`.

       > **Note:** This account is the only one with command-line access to the engine.

    3. (Optional) Select **Enable SSH Daemon** to allow remote access to the engine command line using SSH.
    4. Select **Next** and press **Enter**.
6. Define the network interface drivers.
    - If the list populates automatically, make sure that the information is correct and all interfaces have been detected.
    - If the list did not populate automatically, start the autodetect function.
        1. Select **Autodetect** and press **Enter**.
        2. Make sure that the information is correct and all interfaces have been detected.

           > **Tip:** You can use the Sniff option for troubleshooting the network interfaces. Select **Sniff** on an interface to run the network sniffer on that interface.

        If autodetection fails, contact Forcepoint support.
7. Map interfaces to the IDs you defined.

   Upgraded appliances follow the interface mapping pattern shown in the table.

Table 3: Ethernet interface mapping for upgraded appliances

Sidewinder	Stonesoft NGFW	ID
port mgr0	eth0_0	0
port 1–0	eth1_0	1
port 1–1	eth1_1	2
port 1–2	eth1_2	3
port 1–3	eth1_3	4
port 1–4	eth1_4	5
port 1–5	eth1_5	6
port 1–6	eth1_6	7
port 1–7	eth1_7	8

Change the IDs as needed to match the Interface IDs defined for the engine element in the Management Client.

1. Select the **Media** column and press **Enter** to change the settings.
2. Verify that the speed/duplex settings of network cards are identical at both ends of each cable.

   For Layer 2 Firewall engines, make sure that the inline interface speed/duplex settings match for both links in each pair.
3. Select the **Mgmt** column.

4. Press the spacebar to select the correct interface for contact with the Management Server.

   Important: The Management interface must be the same interface on which the control IP address for the corresponding element is configured in the SMC. Otherwise the engine cannot contact the Management Server.

8. On the **Prepare for Management Contact** page, complete the information and make your selections.

   For more information about how to complete the information, see the *Stonesoft Next Generation Firewall Installation Guide*.

   This information allows the Stonesoft NGFW engine to establish contact with the Management Server. The one-time password is engine-specific and can be used only for one initial contact to the Management Server.

   Note: If there is an intermediate firewall between this engine and the Management Server, the intermediate firewall policy must allow the initial contact and all subsequent communications.

The configuration is complete when the appliance successfully contacts the Management Server and restarts.

Complete post-upgrade tasks

After the appliance installation and initial configuration is complete, the engine is left in the initial configuration state.

You must complete these post-upgrade tasks:

- Configure other interfaces as needed.
- Configure routing for the engine.
- Configure and install a customized policy on the engine or install one of the default policies.

Note: When the engine is in the initial configuration state, it has an initial policy that allows only limited communication to and from the engine. Before the engine can start processing traffic, you must install a policy.

We also recommend completing one or more of these configuration and management tasks:

- Define custom alerts and alert escalation policies.
- Set up automated tasks to manage the log data and prevent the Log Server storage space from filling up with logs.
- Schedule automatic backup tasks to back up the configuration information stored on the Management Server.
- Review settings for automatic updates to keep your system current.

Note: If you are upgrading more than one Sidewinder appliance to Stonesoft NGFW, we recommend completing these optional configuration and management tasks after you have upgraded all Sidewinder appliances.