Common Criteria Certification User's Guide

Legal Information

The use of the products described in these materials is subject to the then current end-user license agreement, which can be found at the McAfee website:
http://www.mcafee.com/us/about/legal/license-agreements.aspx

Revision: SGCC_20140417

Table of Contents

CHAPTER 1

USING STONESOFT DOCUMENTATION

This chapter describes how to use this guide and related documentation. It also provides directions for obtaining technical support and giving feedback on the documentation.

The following sections are included:

Objectives and Audience

This *Common Criteria Certification User's Guide* provides information needed to implement a Stonesoft solution according to Common Criteria (CC) evaluated guidelines. In addition, it provides supplemental user information that is not included in the regular Stonesoft product documentation. This guide is intended to be used in conjunction with the following Stonesoft documentation when installing and configuring a CC certified Stonesoft solution:

- Stonesoft Administrator's Guide
- Stonesoft Firewall/VPN Installation Guide
- Stonesoft Firewall/VPN Reference Guide
- Stonesoft IPS and Layer 2 Firewall Installation Guide
- Stonesoft IPS and Layer 2 Firewall Reference Guide
- Stonesoft Management Center Installation Guide

This guide does not reproduce the above mentioned documentation. Rather, it supplements them by identifying specific configuration criteria that are required for a Common Criteria certified installation. Any configuration that falls outside of the evaluated configuration or security assumptions outlined in this guide should be considered an insecure state with respect to CC certification.

Typographical Conventions

The following conventions are used throughout the documentation:

Table 1.1 Typographical Conventions

Formatting	Informative Uses
User Interface text	Text you see in the User Interface (buttons, menus, etc.) and any other interaction with the user interface are in **bold-face**.
References, terms	Cross-references and first use of acronyms and terms are in *italics*.
`Command line`	File names, directories, and text displayed on the screen are `monospaced`.
`User input`	User input on screen is in **`monospaced bold-face`**.
`Command parameters`	Command parameter names are in *`monospaced italics`*.

We use the following ways to indicate important or additional information:

Note – Notes prevent commonly-made mistakes by pointing out important points.

Caution – Cautions prevent breaches of security, information loss, or system downtime. Cautions always contain critical information that you must observe.

Tip – Tips provide additional helpful information, such as alternative ways to complete steps.

Example Examples present a concrete scenario that clarifies the points made in the adjacent text.

What's Next?

- The *What's Next* lists at the ends of tasks guide you to closely related tasks that you must perform in order to configure features. If several of the procedures listed apply, pick the first one; a new *What's Next* list is available at the bottom of the first task.

Additional Documentation

Stonesoft technical documentation is divided into two main categories: product documentation and support documentation.

Product Documentation

The table below lists the available product documentation.

Table 1.2 Product Documentation

Guide	Description
Reference Guide	Explains the operation and features of the Stonesoft system comprehensively. Demonstrates the general workflow and provides example scenarios for each feature area. Available as separate guides for Stonesoft Management Center and Stonesoft Firewall/VPN, and as a combined guide for Stonesoft IPS and Stonesoft Layer 2 Firewall.
Installation Guide	Instructions for planning, installing, and upgrading a Stonesoft system. Available as separate guides for Stonesoft Management Center and Stonesoft Firewall/VPN, and as a combined guide for Stonesoft IPS and Stonesoft Layer 2 Firewall.
Online Help	Describes how to configure and manage the system step-by-step. Accessible through the Help menu and by using the Help button or the F1 key in any window or dialog. Available in the Stonesoft Management Client and the Stonesoft Web Portal. An HTML-based system is available in the Stonesoft SSL VPN Administrator through help links and icons.
Administrator's Guide	Describes how to configure and manage the system step-by-step. Available as a combined guide for Stonesoft Firewall/VPN, Stonesoft IPS, and Stonesoft Layer 2 Firewall, and as separate guides for Stonesoft SSL VPN and Stonesoft IPsec VPN Client.
User's Guide	Instructions for end-users. Available for the Stonesoft IPsec VPN Client and the Stonesoft Web Portal.
Appliance Installation Guide	Instructions for physically installing and maintaining Stonesoft appliances (rack mounting, cabling, etc.). Available for all Stonesoft hardware appliances.

PDF guides are available at https://www.stonesoft.com/en/customer_care/documentation/current/. The *Stonesoft Administrator's Guide*, and the *Reference Guides* and *Installation Guides* for Stonesoft Management Center, Stonesoft Firewall/VPN, Stonesoft IPS, and Stonesoft Layer 2 Firewall are also available as PDFs on the Management Center DVD.

Support Documentation

The support documentation provides additional and late-breaking technical information. These technical documents support the guide books, for example, by giving further examples on specific configuration scenarios.

The latest technical documentation is available at http://www.stonesoft.com/support/.

System Requirements

The certified platforms for running Stonesoft Firewall or IPS engine software, the hardware and software requirements for the Management Center, and version-specific details for all software products can be found in the *Release Notes* available at http://www.stonesoft.com/en/customer_care/kb/. The Management Center Release Notes are also included on the Management Center DVD.

Supported Features

Not all features are supported on all platforms. See the Appliance Software Support Table at the Stonesoft Support Documentation pages for more information.

Contact Information

For street addresses, phone numbers, and general information about Stonesoft products and Stonesoft Corporation, visit our website at http://www.stonesoft.com/.

Licensing Issues

You can view your current licenses at https://my.stonesoft.com/managelicense.do.

For license-related queries, e-mail order@stonesoft.com.

Technical Support

Stonesoft offers global technical support services for Stonesoft's product families. For more information on technical support, visit http://www.stonesoft.com/support/.

Your Comments

We want to make our products fulfill your needs as well as possible. We are always pleased to receive any suggestions you may have for improvements.

- To comment on software and hardware products, e-mail feedback@stonesoft.com.
- To comment on the documentation, e-mail documentation@stonesoft.com.

Security Related Questions and Comments

You can send any questions or comments relating to the Security Engine inspection features and network security to security-alert@stonesoft.com.

Other Queries

For queries regarding other matters, e-mail info@stonesoft.com.

CHAPTER 2

REQUIREMENTS FOR A COMMON CRITERIA CERTIFIED INSTALLATION

This chapter outlines the specific software, hardware, and network configuration in the Common Criteria evaluated configuration.

The following sections are included:

Certified Software

Caution – It is highly recommended that you check your Stonesoft software prior to installation to ensure its integrity. The checksum for the Stonesoft Security Engine software is provided in this guide. See Obtaining a Common Criteria Certified Product Version (page 20). Also check all Known Issues and possible Security Advisories from http://www.stonesoft.com/en/customer_care/kb/ prior to installation.

Stonesoft Security Engine Software

- The Stonesoft Security Engine software application, version 5.5.4.9869.cc.2.
- The INSIDE Secure QuickSec IPsec Toolkit, version 5.2.

Evaluated Hardware

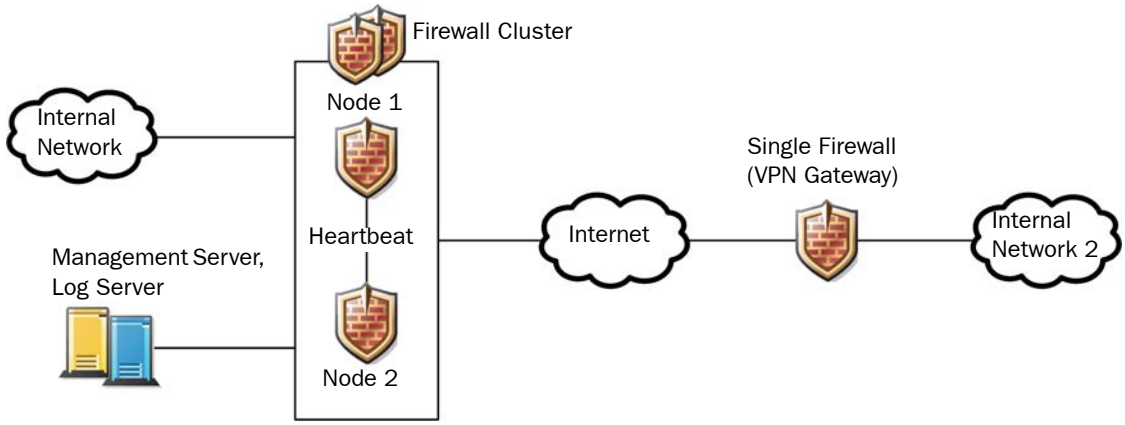
The following Stonesoft appliance models are included within the evaluation scope:

- Stonesoft MIL-320 (Firewall/VPN role only)
- Stonesoft 5206
- Stonesoft 3206
- Stonesoft 3202
- Stonesoft 1402
- Stonesoft 1065
- Stonesoft 1035

Evaluated Network Topology for Stonesoft Firewall/VPN

In its evaluated configuration, Stonesoft Firewall/VPN is installed as a Firewall Cluster, with a VPN created between the cluster and a Single Firewall. The exact network configuration required for certification is detailed in Illustration 2.1.

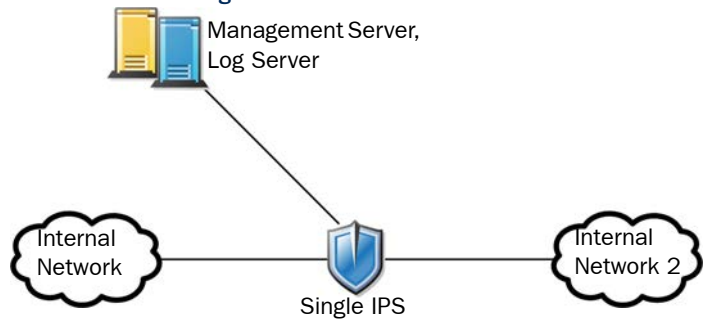
Illustration 2.1 Evaluated Network Configuration for Stonesoft Firewall



Evaluated Network Topology for Stonesoft IPS

In its evaluated configuration, Stonesoft IPS is installed as a Single IPS engine between two networks. The exact network configuration required for certification is detailed in Illustration 2.2.

Illustration 2.2 Evaluated Network Configuration for Stonesoft IPS



Configuration Specifics

A CC certified installation also requires specific configurations as follows:

- Install the Management Server and Log Server on a trusted and separate management network.
- Use only static IPv4 addresses on Ethernet interfaces.
- Use only static routing.
- Set the Failure Mode to **Normal** in the properties of Inline Interfaces on IPS engines.
- Use a dedicated network for the heartbeat between the nodes of the Firewall Cluster.
- Enable **FIPS-Compatible Operating Mode** on the Advanced tab of the Firewall properties and in the command line Engine Configuration Wizard.
- Set the Log Spooling Policy to **Stop Traffic** on the Advanced tab of the engine properties.

Note – If the engine goes to the offline state due to the log spooling policy and it is manually forced back to the online state, the traffic flow through the node will continue. However, in this case no new log entries will be generated until there is enough disk space available.

Note – Access rules (filtering rules) that use ANY as the Destination also include TOE interfaces. If used together with ANY as the Service, this allows access to ports used for TOE management. For a list of open ports on the Firewall and IPS engines, see the section called Security Engine Ports in the *Stonesoft Administrator's Guide*.

- To prevent the possibility of misconfiguration, add the following rule as the first rule of the IPv4 Access rules:
  - **Source**: ANY
  - **Destination**: $$ Local Cluster
  - **Service**: ANY
  - **Action**: Discard

About FIPS-Compatible Operating Mode

By default, Stonesoft Security Engine supports some encryption algorithms that do not have FIPS approval. When FIPS-Compatible Operating Mode is enabled, the following configuration changes are done automatically:

- Access to the command line interface of the engine is disabled
- The cryptographic module is configured to be in FIPS 140-2 mode
- VPN profile options that are not permitted in a FIPS-compatible configuration are disabled.
- FIPS-Compatible Operating Mode restricts the algorithms to FIPS-compatible algorithms.

Only approved cryptographic algorithms are used for communication between engine nodes and the Management Server and Log Server. Only approved cryptographic algorithms are used for the heartbeat communication between the nodes of a Firewall Cluster.

Because MD5 is used for passwords stored in the Management Server's internal LDAP user database, the internal LDAP user database cannot be used to store user passwords when FIPS-Compatible Operating Mode is enabled.

Assumptions About the Intended Environment

This section identifies environmental assumptions that must exist in order to have a secure installation.

Administrator Access

During installation, Administrators can access the Stonesoft Firewall or IPS engine through a command line interface to the engine operating system or through the Management Server. After installation, the command line interface is disabled and Administrators can only access the engine via the Management Server. The Management Server and the Stonesoft Firewall or IPS engine must be on a trusted and separate management network. In addition, identification and authentication must be required to access both the operating system and the Management Client application.

Administrator Attributes

All authorized administrators must be trained, qualified, non-hostile individuals and must follow all instructions and guidance outlined in Stonesoft product documentation.

The administrator has the option of installing or reinstalling the engine in order to detect possible modifications to the Stonesoft Firewall or IPS engine.

If the Stonesoft Firewall or IPS engine is installed by a Value Added Reseller (VAR), the end-user must establish that the VAR fulfills the requirements for trusted administrator attributes as described above.

Environment Audit Procedures

Administrators must ensure that procedures exist to ensure that the audit trails are regularly analyzed and archived.

Audit Support

The IT environment generates audit records for the security functions on which the Stonesoft Firewall or IPS engine depends from its environment. It also provides protected permanent storage of the audit trails generated by the Stonesoft Firewall or IPS engine, including reliable timestamps for the audit records.

Information Flow Control

The IT environment of the engine must ensure that information cannot flow between the internal and external networks unless it passes through the Stonesoft Firewall or IPS engine. In a Firewall Cluster, traffic only needs to pass through one of the cluster nodes.

General IT Environment Support

The Stonesoft Firewall or IPS engines, the Stonesoft Management Server, the Stonesoft Log Server, and the management network must be dedicated to the Firewall or IPS system. This means that they are not used for any purpose other than operating the SMC and the Firewall or IPS engines. Administrators must ensure that all of the above are functioning according to their specifications, are physically secure, and that physical access is only allowed to trusted administrators.

Time Source

The IT environment of the engine must provide a reliable time source to the Stonesoft Firewall or IPS engine and the operating environment.

User Authentication for Information Flow Control

The IT environment must provide a user directory and a user authentication mechanism for the Stonesoft Firewall engine to use when the Firewall Policy requires users to authenticate before information can flow between the internal and external networks.

Trusted VPN Channels

Peer external IT entities in trusted VPN channels must be able to protect the integrity and confidentiality of data transmitted to the Stonesoft Firewall via encryption and provide authentication for such data. Upon receipt of data from the Stonesoft Firewall, the peer external IT entity must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted.

IPS Placement

The IPS must be placed in such a way as to ensure adequate coverage of network segments where critical assets are located.

CHAPTER 3

PREPARING FOR INSTALLATION

This chapter explains how to prepare the operating environment for a Common Criteria certified Stonesoft solution. Installation of the SMC is done in accordance with the instructions provided in the *Stonesoft Management Center Installation Guide*. When doing so, however, refer to this chapter for a detailed explanation of the specific configurations necessary for a certified installation.

The following sections are included:

Configuration Overview

1. Obtain a Common Criteria certified product version. See Obtaining a Common Criteria Certified Product Version.
2. Install the Management Server and Log Server. See Installing the Management Server and Log Server (page 21).
3. Create Firewall and/or IPS engine elements in the Management Client and save the initial configuration (one-time password for Management Contact) for each engine. See the following sections:
   - Defining a Single Firewall Element (page 24)
   - Defining a Firewall Cluster Element (page 25)
   - Defining a Single IPS Element (page 32)
4. Install the Common Criteria certified engine software version. See Installing Stonesoft Security Engines in the Firewall/VPN Role (page 28) and Installing Stonesoft Security Engines in the IPS Role (page 34).

Obtaining a Common Criteria Certified Product Version

The process for ordering, obtaining, and installing a certified product version is as follows:

▼ To obtain a Common Criteria certified product version

1. Order a Common Criteria certified version from Stonesoft.
   - The plastic bag containing the appliance is sealed using security tape.
   - The appliance is delivered with the standard software version that is shipping at the time of the order and a Delivery Pack that includes the information to download the *Common Criteria Certification User's Guide*.
   - Tracking information for the shipment is provided to you.
2. Track the shipment to make sure that the appliance is not lost, or the delivery delayed unnecessarily.
3. When the appliance arrives, verify that the appliance plastic bag and the security tape are intact.
4. Download the Common Criteria certified software at https://my.stonesoft.com/download.do.
   - The Stonesoft Security Engine software may be used either as a Firewall/VPN engine or as an IPS engine. Multiple installations of the same Stonesoft Security Engine software may be used in combination to obtain the functionality of both the Firewall/VPN and the IPS roles. There is no need to separately download the Stonesoft Security Engine software for each engine role.
5. Verify the SHA checksum for the Stonesoft Security Engine software:

Table 3.1 SHA-1 Checksum for the Stonesoft Security Engine Software

File Name	Checksum
sg_engine_5.5.4.9869.cc.2_x86-64.zip	12198db55c734e18956fcb34e0a0b7863557ca8a

What's Next?

▶ Installing the Management Server and Log Server (page 21)

Installing the Management Server and Log Server

This section outlines the specific configuration parameters for the Management Server and Log Server. This section is meant to be used in conjunction with the *Stonesoft Management Center Installation Guide* when installing and configuring the Management Server and Log Server.

▼ To install the Management Server and Log Server

1. Obtain the license files as instructed in the **Obtaining License Files** section of the *Stonesoft Management Center Installation Guide*.
2. Start the installation as instructed in the **Getting Started with Management Center Installation** section of the *Stonesoft Management Center Installation Guide*.
3. Select the appropriate installation options for your environment as instructed in the **Installing Management Center Components** section of the *Stonesoft Management Center Installation Guide*.
4. Configure the Management Server properties for your environment as instructed in the **Installing a Management Server** section of the *Stonesoft Management Center Installation Guide*.
5. Configure the Log Server properties for your environment as instructed in the **Installing a Log Server** section of the *Stonesoft Management Center Installation Guide*.
6. Finish the installation as instructed in the **Finishing the Installation** section of the *Stonesoft Management Center Installation Guide*.

What's Next?

▶ Starting the Management Center (page 22)

Starting the Management Center

When starting the Management Center for the first time, the following steps must be completed:

▼ To start the Management Client

1. Start the Management Center components as instructed in the **Starting the Management Center After Installation** section of the *Stonesoft Management Center Installation Guide*.
2. Start the Management Client as instructed in the **Starting the Management Client** section of the *Stonesoft Management Center Installation Guide*.
3. Log in to the Management Center using the Management Client as instructed in the **Logging in to the Management Center** section of the *Stonesoft Management Center Installation Guide*.
4. Verify and accept the Management Server certificate as instructed in the **Accepting the Management Server Certificate** section of the *Stonesoft Management Center Installation Guide*.
5. Install license files using the Management Client as instructed in the **Installing Licenses** section of the *Stonesoft Management Center Installation Guide*.
6. If you have licenses that are bound to the Management Server's POL code, bind the licenses to the correct components as instructed in the **Binding Management Server POL-Bound Licenses to Servers** section of the *Stonesoft Management Center Installation Guide*.

What's Next?

- ▶ Installing Stonesoft Firewall/VPN (page 23)
- ▶ Installing Stonesoft IPS (page 31)

CHAPTER 4

INSTALLING STONESOFT FIREWALL/VPN

This chapter explains how to install a Common Criteria certified Stonesoft Firewall/VPN. Installation is done in accordance with the instructions provided in the *Stonesoft Firewall/VPN Installation Guide*. When doing so, however, refer to this chapter for a detailed explanation of the specific engine configurations necessary for a certified installation.

The following sections are included:

Defining a Single Firewall Element

This section outlines the specific configuration parameters for the Single Firewall configuration procedure that prepares the Management Center for a Stonesoft Firewall/VPN installation. It is meant to be used in conjunction with the *Stonesoft Firewall/VPN Installation Guide* and the *Stonesoft Administrator's Guide*. The Single Firewall is configured using the Management Client.

▼ To define a Single Firewall

1. Define Single Firewall elements as instructed in the **Adding a Single Firewall Element** section of the *Stonesoft Firewall/VPN Installation Guide*.
2. Define Physical Interfaces as instructed in the **Adding Physical Interfaces** section of the *Stonesoft Firewall/VPN Installation Guide*.
3. (*Optional*) Define VLAN Interfaces as instructed in the **Adding VLANs** section of the *Stonesoft Firewall/VPN Installation Guide*.
4. Define IP Addresses for the Physical Interfaces and VLAN Interfaces as instructed in the **Configuring IP Addresses for Physical, VLAN, ADSL, or SSID Interfaces** section of the *Stonesoft Firewall/VPN Installation Guide*.

Note – Only static IPv4 addresses on Ethernet interfaces are supported in the evaluated configuration.

5. Set interface options as instructed in the **Settings Global Interface Options** section of the *Stonesoft Firewall/VPN Installation Guide*.
6. Switch to the **Advanced** tab of the Firewall Properties.
7. Select **FIPS-Compatible Operating Mode**.

Caution – Selecting this option only disables configuration options that are not available in FIPS-Compatible Operating Mode in the Management Client. It does not enable FIPS-Compatible Operating Mode on the engine. You must enable FIPS-Compatible Operating Mode during the initial configuration of the appliance.

8. Click **Log Handling** and set the Log Spooling Policy to **Stop Traffic**. Click **OK**.
9. Click **OK** in the Firewall Properties dialog. The Firewall element is created.
10. Bind licenses to specific Firewall elements as instructed in the **Binding Engine Licenses to Correct Elements** section of the *Stonesoft Firewall/VPN Installation Guide*.
11. Save the defined configuration for use during Firewall installation as instructed in the **Saving the Initial Configuration** section of the *Stonesoft Firewall/VPN Installation Guide*.

Caution – Handle the configuration files securely. They include the one-time password that allows establishing trust with the Management Server.

What's Next?

- If you are also installing a Firewall Cluster, proceed to Defining a Firewall Cluster Element (page 25).
- Otherwise, proceed to Modifying the Firewall Template for a Common Criteria Installation (page 27).

Defining a Firewall Cluster Element

This section outlines the specific configuration parameters for the Firewall Cluster configuration procedure that prepares the Management Center for a Stonesoft Firewall/VPN installation. It is meant to be used in conjunction with the *Stonesoft Firewall/VPN Installation Guide* and the *Stonesoft Administrator's Guide*. The Firewall Cluster is configured using the Management Client.

▼ To define a Firewall Cluster

1. Define Firewall Cluster elements as instructed in the of the **Adding a Firewall Cluster Element** section of the *Stonesoft Firewall/VPN Installation Guide*.
2. (*Optional*) Add nodes to the Firewall Cluster as instructed in the **Adding Nodes to a Firewall Cluster** section of the *Stonesoft Firewall/VPN Installation Guide*.
3. Define physical interfaces as instructed in the **Adding Physical Interfaces** section of the *Stonesoft Firewall/VPN Installation Guide*.
4. (*Optional*) Define VLAN interfaces as instructed the **Adding VLANs** section of the *Stonesoft Firewall/VPN Installation Guide*.
5. Define CVIs and NDIs as instructed in the **Defining IP Addresses for Cluster Interfaces** section of the *Stonesoft Firewall/VPN Installation Guide*.

Note – Only static IPv4 addresses on Ethernet interfaces are supported in the evaluated configuration.

6. Set interface options as instructed in the **Setting Global Interface Options for Clusters** section of the *Stonesoft Firewall/VPN Installation Guide*.
   - **Packet Dispatch** is the recommended CVI mode. Other CVI modes can be used if necessary.
   - Use a dedicated network for the Heartbeat between the nodes of the Firewall Cluster. In addition to the mandatory **Primary** Heartbeat Interface, we recommend configuring a **Backup** Heartbeat Interface.
7. Switch to the **Advanced** tab of the Firewall Properties.
8. Select **FIPS-Compatible Operating Mode**.

Caution – Selecting this option only disables configuration options that are not available in FIPS-Compatible Operating Mode in the Management Client. It does not enable FIPS-Compatible Operating Mode on the engine. You must enable FIPS-Compatible Operating Mode during the initial configuration of the appliance.

9. Click **Log Handling** and set the Log Spooling Policy to **Stop Traffic**. Click **OK**.

10. Click **Clustering** and verify in the Node Synchronization section that **Sync Security Level** is **Sign** or **Encrypt and Sign**.
    - If necessary, change the Sync Security as instructed in the **Adjusting Firewall Clustering Options** section of the *Stonesoft Administrator's Guide*.
    - When the Sync Security Level is Sign, all synchronization messages are authenticated using a keyed-hash message authentication code and all sensitive messages are also encrypted. The exchange of the key is encrypted and authenticated using digital signatures. This level of security prevents outside injections of connection state information. It is the default security level.
    - When the Sync Security Level is Encrypt and Sign, all messages are both encrypted and authenticated. This level of security increases the overhead compared to the Sign option, but is strongly recommended if the node-to-node are relayed through insecure networks.
11. Click **OK** in the Clustering Properties dialog.
12. Click **OK** in the Firewall Properties dialog. The Firewall Cluster element is created.
13. Bind licenses to each node of the Firewall Cluster as instructed in the **Binding Engine Licenses to Correct Elements** section of the *Stonesoft Firewall/VPN Installation Guide*.
14. Save the defined configuration for use during Firewall installation as instructed in the **Saving the Initial Configuration for Firewall Engines** section of the *Stonesoft Firewall/VPN Installation Guide*.

Caution – Handle the configuration files securely. They include the one-time password that allows establishing trust with the Management Server.

What's Next?

▶ Proceed to Modifying the Firewall Template for a Common Criteria Installation (page 27).

Modifying the Firewall Template for a Common Criteria Installation

The Firewall Template policy must be modified to block Services that are not compatible with a Common Criteria installation.

▼ To modify the Firewall Template for a Common Criteria installation

1. Select **Configuration→Configuration→Security Engine**. The Security Engine Configuration view opens.
2. Browse to **Policies→Firewall Policies→Firewall Template**.
3. Right-click the Firewall Template policy and select **Edit Firewall Template Policy**. The template policy opens for editing.
4. Locate the IPv4 Access rule that has the following properties:

Table 4.1 SG Blacklisting Rule

ID	Source	Destination	Service	Action
7	ANY	$$Local cluster (CVI Addresses Only)	SG Blacklisting	Allow

5. Right-click the ID cell of the rule and select **Delete Rule**.
6. Select **File → Save As** and save this new template under a unique name.

Whenever you create security policies that will be used in FIPS mode, use this newly created template as the template for the new security policies.

What's Next?

▶ Proceed to Installing Stonesoft Security Engines in the Firewall/VPN Role (page 28).

Installing Stonesoft Security Engines in the Firewall/VPN Role

In a Common Criteria certified installation, the Stonesoft Security Engine must be a Stonesoft appliance. In a Firewall Cluster, each node in the cluster must be configured individually.

Upgrading Stonesoft Appliances to the Certified Engine Version in the Firewall/VPN Role

Stonesoft appliances are delivered with the most recent engine software pre-installed. The engine software must be upgraded to the certified engine version before entering FIPS-Compatible Operating Mode. This is necessary even if the same version was installed previously, because the file system checksum is stored during the upgrade process.

▼ To upgrade to the certified engine version

1. Save the Common Criteria certified engine upgrade `.zip` file in the root directory of a USB memory stick or obtain a Common Criteria certified engine upgrade zip file on CD-ROM from Stonesoft support.

Note – The engine upgrade `.zip` file must be in the root directory of the media.

2. Boot up the appliance. The Engine Configuration Wizard starts.
3. Make sure that **Role** is selected on the Welcome page and press Enter. The Security Engine Role dialog opens.
4. Select **Firewall/VPN** as the role for the Security Engine and press Enter. The role-specific Engine Configuration Wizard starts.
5. Select **Upgrade**. The Select Source Media dialog opens.
6. Select **USB Memory** or **CD-ROM**. The upgrade starts.
7. Select **OK**. The engine reboots and the Engine Configuration Wizard starts with the Engine Image Verification dialog shown. Select **Calculate**. The file system checksum is calculated and displayed.
8. Verify the calculated file system checksum depending on the security strength for engine communications and select **OK**:

Table 4.2 File System Checksums

Security Strength	Checksum Type	Checksum
Default	SHA-1	faa6ad4cf73ed388ccb833ac6a18b61b8fd53f95
256-bit Security Strength	HMAC-SHA-256	cd7079ed0d8307510902010aac15573b6d4b5cdb2ab85fe44f58fb10e600d566

9. Select **OK**. The engine reboots.

10. Check the engine version to make sure that the certified version is loaded.

What's Next?

- Proceed to Configuring the Firewall Engine (page 29).

Configuring the Firewall Engine

To configure the Firewall engine

1. Start the Engine Configuration Wizard as instructed in the **Configuring the Engine in the Engine Configuration Wizard** section of the *Stonesoft Firewall/VPN Installation Guide*.

Note – Because the role of the engine was already selected, you are not prompted to select the role again.

2. Configure the Operating System settings as instructed in the **Configuring the Operating System Settings** section of the *Stonesoft Firewall/VPN Installation Guide*.
   - Select **Restricted FIPS-Compatible Operating Mode**. The SSH daemon and root password options are automatically disabled in the Engine Configuration Wizard.
3. Configure the network interfaces according to your environment as instructed in the **Configuring the Network Interfaces** section of the *Stonesoft Firewall/VPN Installation Guide*.
4. Establish contact between the engine and the Management Server as instructed in the **Contacting the Management Server** section of the *Stonesoft Firewall/VPN Installation Guide*.
   - **Enter node IP address manually** is selected by default and other IP address options are disabled when FIPS-Compatible Operating Mode is enabled.

What's Next?

- If you are also installing an IPS engine, proceed to Installing Stonesoft IPS (page 31).
- Otherwise, proceed to Post-Installation Procedures (page 37).

CHAPTER 5

INSTALLING STONESOFT IPS

This chapter explains how to install a Common Criteria certified Stonesoft IPS. Installation is done in accordance with the instructions provided in the *Stonesoft IPS and Layer 2 Firewall Installation Guide*. When doing so, however, refer to this chapter for a detailed explanation of the specific engine configurations necessary for a certified installation.

The following sections are included:

Defining a Single IPS Element

This section outlines the specific configuration parameters for the Single IPS configuration procedure that prepares the Management Center for a Stonesoft IPS installation. It is meant to be used in conjunction with the *Stonesoft IPS and Layer 2 Firewall Installation Guide* and the *Stonesoft Administrator's Guide*. The Single IPS is configured using the Management Client.

▼ To define a single IPS element

1. Define Single IPS elements as instructed in the **Creating Engine Elements** section in the **Defining IPS Engines** chapter of the *Stonesoft IPS and Layer 2 Firewall Installation Guide*.
2. Define Physical Interfaces and optionally VLAN Interfaces for communication with the Management Server and Log Server as instructed in the **Defining System Communication Interfaces for IPS Engines** section of the *Stonesoft IPS and Layer 2 Firewall Installation Guide*.
   - If you define VLAN Interfaces, add IP addresses to the VLAN Interfaces.

Note – Only static IPv4 addresses on Ethernet interfaces are supported in the evaluated configuration.

3. Set interface options as instructed in the **Setting Interface Options for IPS Engines** section of the *Stonesoft IPS and Layer 2 Firewall Installation Guide*.
4. Define Inline Interfaces for traffic inspection as instructed in the **Defining Inline Interfaces** section of the *Stonesoft IPS and Layer 2 Firewall Installation Guide*.
   - Select **Normal** as the Failure Mode for Inline Interfaces.
5. Switch to the **Advanced** tab of the IPS Properties.
6. Click **Log Handling** and set the Log Spooling Policy to **Stop Traffic**. Click **OK**.
7. Make sure that **Bypass Traffic on Overload** is *NOT* selected.
8. Click **OK** in the IPS Properties dialog. The Single IPS element is created.
9. Bind management-bound licenses to specific IPS elements as instructed in the **Binding Engine Licenses to Correct Elements** section of the *Stonesoft IPS and Layer 2 Firewall Installation Guide*.
10. Save the defined configuration for use during IPS installation as instructed in the **Saving the Initial Configuration for Engines** section of the *Stonesoft IPS and Layer 2 Firewall Installation Guide*.

Caution – Handle the configuration files securely. They include the one-time password that allows establishing trust with the Management Server.

What's Next?

▶ Proceed to Modifying the IPS Template for a Common Criteria Installation (page 33).

Modifying the IPS Template for a Common Criteria Installation

The IPS Template policy must be modified to block Services that are not compatible with a Common Criteria installation.

▼ To modify the IPS Template for a Common Criteria installation

1. Select **Configuration→Configuration→Security Engine**. The Security Engine Configuration view opens.
2. Browse to **Policies→IPS Policies→IPS Template**.
3. Right-click the IPS Template policy and select **Edit IPS Template Policy**. The template policy opens for editing.
4. Locate the IPv4 Access rule that has the following properties:

Table 5.1 SG Blacklisting Rule

ID	Logical Interface	Source	Destination	Service	Action
4	System Communications	ANY	$$Local cluster (NDI for management addresses only)	SG Blacklisting	Allow Deep Inspection: off

5. Right-click the ID cell of the rule and select **Delete Rule**.
6. Select **File → Save As** and save this new template under a unique name.

Whenever you create security policies that will be used in FIPS mode, use this newly created template as the template for the new security policies.

What's Next?

▶ Proceed to Installing Stonesoft Security Engines in the IPS Role (page 34).

In a Common Criteria certified installation, the Stonesoft IPS engine must be a Stonesoft appliance.

Upgrading Stonesoft Appliances to the Certified Engine Version in the IPS Role

Stonesoft appliances are delivered with the most recent engine software pre-installed. The engine software must be upgraded to the certified engine version before entering FIPS-Compatible Operating Mode. This is necessary even if the same version was installed previously, because the file system checksum is stored during the upgrade process.

▼ To upgrade to the certified engine version

1. Save the Common Criteria certified engine upgrade `.zip` file in the root directory of a USB memory stick or obtain a Common Criteria certified engine upgrade zip file on CD-ROM from Stonesoft support.

Note – The engine upgrade `.zip` file must be in the root directory of the media.

2. Boot up the appliance. The Engine Configuration Wizard starts.
3. Make sure that **Role** is selected on the Welcome page and press Enter. The Security Engine Role dialog opens.
4. Select **IPS** as the role for the Security Engine and press Enter. The role-specific Engine Configuration Wizard starts.
5. Select **Upgrade**. The Select Source Media dialog opens.
6. Select **USB Memory** or **CD-ROM**. The upgrade starts.
7. Select **OK**. The engine reboots and the Engine Configuration Wizard starts with the Engine Image Verification dialog shown. Select **Calculate**. The file system checksum is calculated and displayed.
8. Verify the calculated file system checksum depending on the security strength for engine communications and select **OK**:

Table 5.2 File System Checksums

Security Strength	Checksum Type	Checksum
Default	SHA-1	faa6ad4cf73ed388ccb833ac6a18b61b8fd53f95
256-bit Security Strength	HMAC-SHA-256	cd7079ed0d8307510902010aac15573b6d4b5cdb2ab85fe44f58fb10e600d566

9. Select **OK**. The engine reboots.
10. Check the engine version to make sure that the certified version is loaded.

What's Next?

▶ Proceed to Configuring the IPS Engine (page 35).

Configuring the IPS Engine

▼ To configure the IPS engine

1. Start the Engine Configuration Wizard as instructed in the **Configuring the Engine in the Engine Configuration Wizard** section of the *Stonesoft IPS and Layer 2 Firewall Installation Guide*.

Note – Because the role of the engine was already selected, you are not prompted to select the role again.

2. Configure the Operating System settings as instructed in the **Configuring the Operating System Settings** section of the *Stonesoft IPS and Layer 2 Firewall Installation Guide*.
   - Select **Restricted FIPS-Compatible Operating Mode**. The SSH daemon and root password options are automatically disabled in the Engine Configuration Wizard.
3. Configure the network interfaces according to your environment as instructed in the **Configuring the Network Interfaces** section of the *Stonesoft IPS and Layer 2 Firewall Installation Guide*.
4. Establish contact between the engine and the Management Server as instructed in the **Contacting the Management Server** section of the *Stonesoft IPS and Layer 2 Firewall Installation Guide*.
   - **Enter node IP address manually** is selected by default and other IP address options are disabled when FIPS-Compatible Operating Mode is enabled.

What's Next?

▶ Proceed to Post-Installation Procedures (page 37).

CHAPTER 6

POST-INSTALLATION PROCEDURES

This chapter explains how to verify that FIPS-Compatible Operating Mode has been activated after installation and how to recover from a FIPS 140-2 self-test failure.

The following sections are included:

Verifying the Activation of FIPS-Compatible Operating Mode

Restricted FIPS-Compatible Operating Mode must be enabled during the initial configuration of the appliance. The following steps describe how to verify that FIPS-Compatible Operating Mode has been activated.

▼ To verify the activation of FIPS-Compatible Operating Mode

1. Verify that the following messages are displayed on the console when the engine restarts:
   - `FIPS: rootfs integrity check OK`
     (displayed after the root file system integrity test has been executed successfully)
   - `FIPS power-up tests succeeded`
     (displayed after the FIPS 140-2 power-up tests have been executed successfully)
2. (*Firewall/VPN role only*) Open the Logs view in the Management Client and verify that the following message is shown in the logs:
   - Started in FIPS 140-2 operating mode.

Caution – If the engine does not enter FIPS-Compatible Operating Mode even though it is configured to do so ("Started in non-FIPS 140-2 approved operating mode" is shown in the logs for an engine in the Firewall/VPN role), or if the power-up tests fail (a power-up test error message is displayed or the success message is not displayed), the appliance must be reset to factory settings and reinstalled as instructed in **Recovering From a FIPS 140-2 Self-Test Failure (page 39)****.**

What's Next?

▶ Continue as instructed in the **After Successful Management Server Contact** section of the *Stonesoft Firewall/VPN Installation Guide* or the *Stonesoft IPS and Layer 2 Firewall Installation Guide*.

Recovering From a FIPS 140-2 Self-Test Failure

If the FIPS 140-2 power-up self-tests fail, or the engine does not enter FIPS-Compatible Operating Mode, the appliance must be reset to factory settings and reinstalled according to these instructions.

▼ To recover from a FIPS 140-2 self-test failure

1. Reboot the appliance and select **System restore options** from the boot menu. Stonesoft Engine System Restore starts.
2. Enter **2** for **Advanced data removal options**.
3. Enter one of the following options:
   - **1** for **1 pass overwrite**.
   - **8** for a **Custom** number of overwrite passes.
4. If you selected **Custom**, enter the number of overwrite passes. A larger number of overwrites is more secure, but it may take a considerable amount of time depending on the appliance storage capacity.
5. Repeat the engine version upgrade as instructed in the following sections:
   - Upgrading Stonesoft Appliances to the Certified Engine Version in the Firewall/VPN Role (page 28).
   - Upgrading Stonesoft Appliances to the Certified Engine Version in the IPS Role (page 34).
6. Configure the engine and enable FIPS-Compatible Operating Mode as instructed in the following sections:
   - Configuring the Firewall Engine (page 29).
   - Configuring the IPS Engine (page 35).
7. Verify that FIPS-Compatible Operating Mode is activated as instructed in Verifying the Activation of FIPS-Compatible Operating Mode (page 38).

CHAPTER 7

IMPLEMENTING USER AUTHENTICATION AND VPNS

This chapter explains how to configure user authentication and Virtual Private Networks (VPNs) in the evaluated configuration.

The following sections are included:

Configuring User Authentication

Because MD5 is used for passwords stored in Stonesoft Management Server's internal LDAP user database, the internal LDAP user database cannot be used to store user passwords when FIPS-Compatible Operating Mode is enabled. Authentication based on username and password requires an external LDAP server, which you can optionally integrate with the Stonesoft Management Server to create different rules for each user. An External RADIUS or TACACS+ Authentication Server can optionally be used for password authentication. Otherwise, authentication is provided by the Firewall.

Note – The optional Stonesoft User Agent component cannot be used for user identification in the evaluated configuration. Do not deploy the Stonesoft User Agent in an evaluated configuration.

This section outlines the specific configuration parameters for user authentication. It is meant to be used in conjunction with the *Stonesoft Administrator's Guide*.

▼ To configure user authentication

1. Configure LDAP integration as instructed in the **Integrating External Directory Servers** section of the *Stonesoft Administrator's Guide*.
2. Define the User Group and User information as instructed in the **Defining User Accounts** section of the *Stonesoft Administrator's Guide*.
3. (*For external authentication server only*) Integrate an external RADIUS Authentication Server or TACACS+ Authentication Server as instructed in the **Defining RADIUS or TACACS+ Authentication Servers** section of the *Stonesoft Administrator's Guide*.
4. (*For external authentication server only*) Define a RADIUS or TACACS+ Authentication Method as instructed in the **Defining Authentication Methods for External Servers** section of the *Stonesoft Administrator's Guide*.
5. Define IPv4 Access rules with authentication requirements as instructed in the **Defining IPv4 Access Rules for Authentication** section of the *Stonesoft Administrator's Guide*.
6. (*Optional*) Enable and configure Browser-Based User Authentication to allow end-users to authenticate using any standard web browser. See the **Enabling Browser-Based User Authentication** section of the *Stonesoft Administrator's Guide*.

What's Next?

- If you want to use VPNs, proceed to Defining and Configuring a Policy-Based VPN (page 43).
- Otherwise, refresh the Firewall Policy to activate the new configuration.

Defining and Configuring a Policy-Based VPN

Only policy-based gateway-to-gateway VPNs in Tunnel Mode are included in the evaluated configuration. The Route-Based VPN is not part of the evaluated configuration. VPN Gateways must use ECDSA or RSA certificates for gateway authentication. Otherwise you may use the product as it is normally supported.

This section outlines the specific configuration parameters for a Stonesoft policy-based VPN in FIPS-Compatible Operating Mode. It is meant to be used in conjunction with the *Stonesoft Administrator's Guide*.

▼ To define and configure a VPN

1. (*Optional*) If you plan to use certificates that are signed by an external certificate authority (CA), define the CA in the system as instructed in the **Defining a VPN Certificate Authority** section of the *Stonesoft Administrator's Guide*.
2. (*Optional*) Adjust performance-related settings of Internal Security Gateways as instructed in the **Advanced VPN Tuning** section of the *Stonesoft Administrator's Guide*.
3. (*Optional*) If you are configuring a VPN with an external gateway and the default profiles are not suitable for your use, create a new Gateway Profile as instructed in the **Defining Gateway Profiles** section of the *Stonesoft Administrator's Guide*.
4. Add the necessary number of Security Gateway elements to represent the physical VPN devices as instructed in the **Defining Security Gateways** section of the *Stonesoft Administrator's Guide*.
5. (*Optional*) Modify the automatically added selection of Sites that define the IP addresses that are routable through the VPN as instructed in the **Defining Sites for VPN Gateways** section of the *Stonesoft Administrator's Guide*.
6. Create a custom VPN Profile as instructed in the **Defining VPN Profiles** section of the *Stonesoft Administrator's Guide*.
   - Configure the following settings on the IKE SA tab:

Table 7.1 IKE SA Settings

Setting	Description
Cipher Algorithms	Select one or more of the following cipher algorithms: AES-128 or AES-256. Deselect any other cipher algorithms.
Message Digest Algorithms	Select **SHA-2**. Select 256 or 384 as the Minimum Length. Deselect any other message digest algorithms.
Diffie-Hellman Groups	Select one or more of the following Diffie-Hellman groups: 14, 19, or 20. Deselect any other Diffie-Hellman groups.
Authentication Method	Select **RSA Signatures** or **ECDSA Signatures**.
SA Lifetime in Minutes	Enter a time in minutes. The maximum lifetime is 1440 minutes (24 hours).
IKEv1 Negotiation Mode	Select **Main**.

- Configure the following settings on the IPsec SA tab:

Table 7.2 IPsec SA Settings

Setting	Description
Cipher Algorithms	Select one or more of the following cipher algorithms: AES-GCM-128 or AES-GCM-256. Deselect any other cipher algorithms.
IPsec Tunnel Lifetime	Enter the lifetime as an amount of traffic in KB or as a time in minutes. If the value is entered as minutes, the maximum lifetime is 480 minutes (8 hours).

7. Create a certificate as instructed in the **Creating and Signing VPN Certificates** section of the *Stonesoft Administrator's Guide*.
   - Select one of the following as the **Key Type**: RSA/SHA-256, ECDSA/SHA256, or ECDSA/SHA384.
   - Enter a **Key Length** of 2048 bits or 3072 bits for RSA certificates. A Key Length of 256 bits or greater is automatically selected for ECDSA certificates.
8. Define a new VPN element as instructed in the **Defining Policy-Based VPNs** section of the *Stonesoft Administrator's Guide*.
   - Select the custom VPN Profile you created as the **Default VPN Profile**.
9. Add the IPv4 Access rules and, if necessary, NAT rules that define which traffic uses the VPN as instructed in the following sections of the *Stonesoft Administrator's Guide*:
   - **Editing Access Rules**
   - **Editing Firewall NAT Rules**

What's Next?

- For VPNs with VPN clients, continue as explained in the **Getting Started With VPN Client Settings** section of the *Stonesoft Administrator's Guide*.
- Otherwise, refresh the policies of all firewalls involved in the VPN to activate the new configuration.