System Configuration

This chapter explains how to configure system configuration settings on the Secure Firewall Management Center.

Requirements and Prerequisites for the System Configuration

Model Support

Management Center

Supported Domains

Global

User Roles

Admin

Manage the Secure Firewall Management Center System Configuration

The system configuration identifies basic settings for the management center.

Procedure

Step 1 Choose **System** (⚙) > **Configuration**.

Step 2 Use the navigation panel to choose configurations to change.

Access Control Preferences

Configure access control preferences on **System** (⚙) > **Configuration** > **Access Control Preferences**.

Requiring Comments on Rule Changes

You can track changes to access control rules by allowing (or requiring) users to comment when they save. This allows you to quickly assess why critical policies in a deployment were modified. By default, this feature is disabled.

Change Reconciliation

To monitor the changes that users make and ensure that they follow your organization's preferred standard, you can configure the system to send, via email, a detailed report of changes made over the past 24 hours. Whenever a user saves changes to the system configuration, a snapshot is taken of the changes. The change reconciliation report combines information from these snapshots to present a clear summary of recent system changes.

The following sample graphic displays a User section of an example change reconciliation report and lists both the previous value for each configuration and the value after changes. When users make multiple changes to the same configuration, the report lists summaries of each distinct change in chronological order, beginning with the most recent.

You can view changes made during the previous 24 hours.

Configuring Change Reconciliation

Before you begin

- Configure an email server to receive emailed reports of changes made to the system over a 24 hour period; see Configuring a Mail Relay Host and Notification Address, on page 4 for more information.

Procedure

Step 1 Choose **System** (⚙) > **Configuration**.

Step 2 Click **Change Reconciliation**.

Step 3 Check the **Enable** check box.

Step 4 Choose the time of day you want the system to send out the change reconciliation report from the **Time to Run** drop-down lists.

Step 5 Enter email addresses in the **Email to** field.

Tip Once you have added email addresses, click **Resend Last Report** to send recipients another copy of the most recent change reconciliation report.

Step 6 If you want to include policy changes, check the **Include Policy Configuration** check box.

Step 7 If you want to include all changes over the past 24 hours, check the **Show Full Change History** check box.

Step 8 Click **Save**.

Related Topics

Using the Audit Log to Examine Changes

Change Reconciliation Options

The **Include Policy Configuration** option controls whether the system includes records of policy changes in the change reconciliation report. This includes changes to access control, intrusion, system, health, and network discovery policies. If you do not select this option, the report will not show changes to any policies. This option is available on management centers only.

The **Show Full Change History** option controls whether the system includes records of all changes over the past 24 hours in the change reconciliation report. If you do not select this option, the report includes only a consolidated view of changes for each category.

Note The change reconciliation report does not include changes to threat defense interfaces and routing settings.

Email Notification

Configure a mail host if you plan to:

- Email event-based reports
- Email status reports for scheduled tasks
- Email change reconciliation reports
- Email data-pruning notifications
- Use email for discovery event, impact flag, correlation event alerting, intrusion event alerting, and health event alerting

When you configure email notification, you can select an encryption method for the communication between the system and mail relay host, and can supply authentication credentials for the mail server if needed. After configuring, you can test the connection.

Configuring a Mail Relay Host and Notification Address

Procedure

Step 1 Choose **System** (⚙) > **Configuration**.

Step 2 Click **Email Notification**.

Step 3 In the **Mail Relay Host** field, enter the hostname or IP address of the mail server you want to use. The mail host you enter **must** allow access from the appliance.

Step 4 In the **Port Number** field, enter the port number to use on the email server.

Typical ports include:

- 25, when using no encryption
- 465, when using SSLv3
- 587, when using TLS

Step 5 Choose an **Encryption Method**:

- **TLS**—Encrypt communications using Transport Layer Security.
- **SSLv3**—Encrypt communications using Secure Socket Layers.
- **None**—Allow unencrypted communication.

Note Certificate validation is not required for encrypted communication between the appliance and mail server.

Step 6 In the **From Address** field, enter the valid email address you want to use as the source email address for messages sent by the appliance.

Step 7 Optionally, to supply a user name and password when connecting to the mail server, choose **Use Authentication**. Enter a user name in the **Username** field. Enter a password in the **Password** field.

Step 8 To send a test email using the configured mail server, click **Test Mail Server Settings**.

A message appears next to the button indicating the success or failure of the test.

Step 9 Click **Save**.

Intrusion Policy Preferences

You can configure the system to track policy-related changes using the comment functionality when users modify intrusion policies. With policy change comments enabled, administrators can quickly assess why critical policies in a deployment were modified.

If you enable comments on policy changes, you can make the comment optional or mandatory. The system prompts the user for a comment when each new change to a policy is saved.

Optionally, you can have changes to intrusion policies written to the audit log.

To get notifications for changes to any *overridden* system-defined rules during LSP updates, ensure that the **Retain user overrides for deleted Snort 3 rules** check box is checked. As a system default, this check box is checked. When this check box is checked, the system retains the rule overrides in the new replacement rules that are added as part of the LSP update. The notifications are shown in the **Tasks** tab under the **Notifications** icon that is located next to **Cog** ().

Network Analysis Policy Preferences

You can configure the system to track policy-related changes using the comment functionality when users modify network analysis policies. With policy change comments enabled, administrators can quickly assess why critical policies in a deployment were modified.

If you enable comments on policy changes, you can make the comment optional or mandatory. The system prompts the user for a comment when each new change to a policy is saved.

Optionally, you can have changes to network analysis policies written to the audit log.