系统配置

以下主题介绍如何在 Cisco Secure Firewall Management Center和托管设备上配置系统配置设置：

系统配置的要求和前提条件

型号支持

管理中心

支持的域

全局

用户角色

管理员

关于系统配置

系统配置设置适用于您的 Cisco Secure Firewall Management Center。

导航 Cisco Secure Firewall Management Center系统配置

系统配置可标识 管理中心 的基本设置。

过程

步骤 1 选择**系统**（⚙）>**配置**。

步骤 2 使用导航面板选择要更改的配置；有关详细信息，请参阅表 1: 系统配置设置 ， 第 2 页。

系统配置设置

请注意，对于受管设备，其中许多配置由从 管理中心应用的 平台设置 策略处理；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 平台设置 。

表 *1:* 系统配置设置

设置	说明
访问控制首选项 (Access Control Preferences)	将系统配置为在用户添加或修改访问控制策略时提示他们添加注释；请参阅策略更改注释 ， 第 4 页。
更改调节	将系统配置为发送过去 24 小时内出现的系统变化的详细报告；请参阅更改调节 ， 第 2 页。
电子邮件通知	配置邮件主机，选择加密方法，并为基于邮件的通知和报告提供身份验证凭证；请参阅邮件通知 ， 第 5 页。
入侵策略首选项 (Intrusion Policy Preferences)	将系统配置为在用户修改入侵策略时提示他们添加注释；请参阅策略更改注释 ， 第 4 页。
网络分析策略首选项 (Network Analysis Policy Preferences)	将系统配置为在用户修改网络分析策略时提示他们添加注释；请参阅策略更改注释 ， 第 4 页。

更改调节

要监控用户进行的更改并确保它们符合您的组织的首选标准，可以将系统配置为通过邮件发送有关过去24小时内进行的更改的详细报告。每当用户保存对系统的配置更改时，就会生成更改快照。更改调节报告将汇总这些快照的信息，以提供最新系统更改的清晰摘要。

以下示例图表显示更改调节报告示例的“用户”部分，并且列出每个配置更改前和更改后的值。如果用户多次更改同一配置，报告会按时间顺序列出每次不同更改的摘要，最近的更改最先列出。

可以查看过去 24 小时内所做的更改。

配置更改调节

开始之前

- 配置邮件服务器，以接收过去24小时对系统进行的更改的报告邮件；有关详细信息，请参阅配置邮件中继主机和通知地址，第 5 页。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击**更改调节**。

步骤 3 选中**启用**复选框。

步骤 4 从**运行时间 (Time to Run)** 下拉列表中选择您希望系统每天发出更改调节报告的具体时间。

步骤 5 在**邮件收件人 (Email to)** 字段中输入邮箱地址。

提示　添加邮箱地址后，点击**重新发送上一报告 (Resend Last Report)** 以向收件人发送另一个最新更改调节报告的副本。

步骤 6 如果要包含策略更改，请选中**包含策略配置 (Include Policy Configuration)** 复选框。

步骤 7 如果要包含过去 24 小时进行的所有更改，请选中**显示完整更改历史记录 (Show Full Change History)** 复选框。

步骤 8 点击**保存 (Save)**。

相关主题

使用审核日志检查更改

更改调节选项

包括策略配置 (Include Policy Configuration) 选项用于控制系统是否在更改调节报告中包括策略更改记录。这包括对访问控制策略、入侵策略、系统策略、运行状况策略和网络发现策略的更改。如果未选择该选项，报告将不会显示对任何策略的更改。此选项仅适用于 管理中心。

显示完整更改历史记录 (Show Full Change History) 选项用于控制系统是否在更改调节报告中包括过去24小时内发生的所有更改的记录。如果未选择该选项，报告仅包括每个类别的更改的整合视图。

注释　更改调节报告不包括对 威胁防御 接口和路由设置的更改。

策略更改注释

当用户修改访问控制、入侵或网络分析策略时，可以配置Firepower系统以使用注释功能跟踪多个与策略相关的更改。

在启用策略更改注释的情况下，管理员可以快速评估修改部署中的关键策略的原因。或者，可以将对入侵策略和网络分析策略的更改写入到审核日志中。

配置跟踪策略更改的注释

可以将系统配置为在用户修改访问控制策略、入侵策略或网络分析策略时提示他们添加注释。可以使用注释来跟踪用户更改策略的原因。如果对策略更改启用了注释功能，则可以将注释设置为可选或必填项。每次保存对策略所作的新更改时，系统都会提示用户输入注释。

过程

步骤 1 选择**系统**（⚙）> **配置**。

系统配置选项显示在左侧导航面板中。

步骤 2 为以下各项配置策略注释首选项：

- 点击**访问控制首选项 (Access Control Preferences)** 为访问控制策略配置注释首选项。
- 点击**入侵策略首选项 (Intrusion Policy Preferences)** 为入侵策略配置注释首选项。
- 点击**网络分析策略首选项 (Network Analysis Policy Preferences)** 为网络分析策略配置注释首选项。

步骤 3 每个策略类型有以下选项：

- **已禁用 (Disabled)** - 禁用更改注释。
- **可选 (Optional)** - 让用户可以根据需要在注释中描述其更改。
- **必需 (Required)** - 要求用户在保存之前在注释中描述其更改。

步骤 4 对于入侵或网络分析策略注释，还可以：

- 选中**将入侵策略中的更改写入审核日志 (Write changes in Intrusion Policy to audit log)** 以将所有入侵策略更改写入审核日志。
- 选中**将网络分析策略中的更改写入审核日志 (Write changes in Network Analysis Policy to audit log)** 以将所有网络分析策略更改写入审核日志。

步骤 5 要在LSP更新期间获取任何 已覆盖的 系统定义的规则更改的通知，请确保选中 **保留已删除的 Snort 3 规则的用户覆盖** 复选框。系统默认情况下，此复选框为选中状态。选中此复选框时，系统会在LSP更新过程中添加的新替换规则中保留规则覆盖。通知显示在 **齿轮** 旁边的 **通知** 图标下的 **任务** 选项卡中（⚙）。

步骤 6 点击**保存 (Save)**。

邮件通知

如果要执行以下操作，请配置邮件主机：

- 通过邮件发送基于事件的报告
- 通过邮件发送有关预定任务的报告
- 通过邮件发送更改调节报告
- 通过邮件发送数据删除通知
- 将邮件用于发现事件、影响标志、关联事件警报，入侵事件警报和运行状况事件警报

配置邮件通知时，可以为系统与邮件中继主机之间的通信选择加密方法，并可根据需要为邮件服务器提供身份验证凭证。配置后，可以测试连接。

配置邮件中继主机和通知地址

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击 **Email Notification**。

步骤 3 在**邮件中继主机 (Mail Relay Host)** 字段中，输入要使用的邮件服务器的主机名或 IP 地址。输入的邮件主机**必须**允许从设备进行访问。

步骤 4 在**端口号 (Port Number)** 字段，请输入邮件服务器上使用的端口号。

典型的端口包括：

- 25，使用加密时
- 465，使用 SSLv3 时
- 587，使用 TLS 时

步骤 5 在**加密方法 (Encryption Method)** 中选择一种加密方法。

- **TLS** - 使用传输层安全加密通信。
- **SSLv3** - 使用安全套接字层加密通信。
- **无 (None)** - 允许未加密的通信。

注释 设备和邮件服务器之间的加密通信不要求进行证书验证。

步骤 6 在**源地址 (From Address)** 字段，输入要将其用作设备发送消息的源邮箱地址的有效邮箱地址。

步骤 7 或者，要在连接到邮件服务器时提供用户名和密码，请选择**使用身份验证 (Use Authentication)**。在**用户名 (Username)** 字段中输入用户名。在**密码 (Password)** 字段中输入密码。

步骤 8 要使用已配置的邮件服务器发送测试邮件，请点击**测试邮件服务器设置 (Test Mail Server Settings)**。

系统会在按钮旁边显示一条消息，以指明测试是否成功。

步骤 9 点击**保存 (Save)**。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。