补救

以下主题包含有关配置补救的信息：

补救措施的要求和前提条件

型号支持

任意

支持的域

任意

用户角色

- 管理员
- 发现管理员

补救简介

补救是一种 Firepower 系统为响应关联策略违规而启动的程序。

当补救程序运行时，系统会生成补救状态事件。补救状态事件包括详细信息，如补救名称、触发补救的关联策略和规则及退出状态消息。

系统支持多种补救模块：

- 思科 ISE 自适应网络控制 (ANC) - 应用或清除关联策略违规中涉及的 ISE 配置的 ANC 策略
- 思科 IOS 空路由 - 在出现关联策略违规的情况下，阻止发送到主机或网络的流量（需要思科 IOS 版本 12.0 或更高版本）
- Nmap 扫描 - 扫描主机以确定运行的操作系统和服务器
- 设置属性值 - 在出现关联策略违规的情况下，设置一台主机的属性。

提示 您可以安装执行其他任务的自定义模块；请参阅《《*Firepower* 系统补救 *API* 指南》》。

实施补救

要实施补救，请先为所选模块创建至少一个实例。您可为每个模块创建多个实例，其中每个实例的配置各不相同。例如，要使用思科 IOS 空路由补救模块与多个路由器通信，请为该模块配置多个实例。

然后，您可以为每个实例添加多个补救，这些补救介绍了违反策略时要执行的操作。

最后，将补救与关联策略中的规则相关联，以便系统启动补救以响应关联策略违规。

补救和多租户

在多域部署中，您可以在任何域级别安装自定义补救模块。系统提供的模块属于全局域。

虽然您无法将补救添加到祖先域中创建的实例，但可以在当前域中创建类似配置的实例，并将补救添加到该实例。您也可以使用祖先域中创建的补救作为关联响应。

相关主题

Cisco Secure Firewall Management Center 警报响应
Nmap 扫描
将响应添加到规则和允许名单

思科 ISE EPS 补救

如果已在 ISE 部署中启用并配置终端保护服务 (EPS)，则可以配置 管理中心以启动使用 ISE 的补救。完全配置时，ISE EPS 补救在涉及关联策略违规的源或目标主机上运行以下**缓解操作 (Mitigation Actions)**：

- **隔离** - 限制或拒绝终端访问网络
- **取消隔离** - 取消终端的隔离状态，允许对网络进行完全访问
- **关闭** - 停用终端的网络附加系统 (NAS) 端口，以将其与网络断开

您还可以免除特定 IP 地址的 ISE EPS 补救。

注释 您的 ISE 版本和配置会影响您使用 ISE 的方式。例如，您不能使用 ISE-PIC 执行 SE EPS 补救。有关详细信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 使用 *ISE/ISE-PIC* 进行用户控制 一章。

有关 ISE EPS 操作的详细信息，请参阅《思科身份服务引擎用户指南》。

配置 ISE EPS 补救

您可以通过在源或目标主机上运行 ISE EPS 补救对关联策略违规做出响应。

注释 ISE-PIC 无法执行 ISE EPS 补救。

开始之前

- 在 ISE 服务器上配置 EPS 操作。
- 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中有关配置 ISE/PIC 的章节。

过程

步骤 1 选择**策略** > **操作** > **实例**。

步骤 2 添加 pxGrid 缓解实例，如添加 ISE EPS 实例，第 3 页中所述。

步骤 3 添加一个或多个 ISE EPS 补救，如添加 ISE EPS 补救，第 4 页中所述。

下一步做什么

- 将补救作为对关联策略违规的响应进行分配，如将响应添加到规则和允许名单中所述。

添加 ISE EPS 实例

创建 ISE EPS 实例以按日志记录类型将单个补救分组。

过程

步骤 1 选择**策略** > **操作** > **实例**。

步骤 2 从**添加新实例 (Add a New Instance)** 列表中，选择 **pxGrid Mitigation(v1.0)** 作为模块类型，然后点击**添加 (Add)**。

步骤 3 输入**实例名称 (Instance Name)** 和**说明 (Description)**。

步骤 4 设置 **启用日志记录** 选项以启用或禁用系统日志记录。

步骤 5 点击**创建**。

下一步做什么

- 创建 ISE EPS 补救，如添加设置属性值补救，第 10 页中所述。

相关主题

Firepower 系统 IP 地址约定

添加 ISE EPS 补救

在实例中创建一个或多个 ISE EPS 补救，以在关联策略违反涉及的源或目标主机上运行**缓解操作 (Mitigation Actions)**。

在多域部署中，无法将补救添加到祖先域中创建的实例。

开始之前

- 创建 ISE EPS 实例，如添加 ISE EPS 实例，第 3 页中所述。

过程

步骤 1 选择**策略** > **操作** > **实例**。

步骤 2 在要向其添加补救的实例旁，点击 **视图**（  ）。

步骤 3 在**已配置补救 (Configured Remediations)** 部分，选择**缓解目标 (Mitigate Destination)** 或**缓解源 (Mitigate Source)**并点击**添加 (Add)**。

如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 输入**补救名称 (Remediation Name)** 和**说明 (Description)**。

步骤 5 选择**缓解操作 (Mitigation Action)**：**隔离 (quarantine)**、**取消隔离 (unquarantine)** 或**关闭 (shutdown)**。

步骤 6 （可选）要免除 IP 地址或范围的补救，请将其输入到 **允许列表** 框中。

步骤 7 依次点击 **Create** 和 **Done**。

下一步做什么

- 分配补救以作为对安全策略违规的响应；请参阅将响应添加到规则和允许名单。

思科 IOS 空路由补救

借助思科 IOS 空路由补救模块，您可以使用思科的“null route”命令阻止某个 IP 地址或地址范围。这会将发送到某主机或网络的所有流量路由到路由器的 NULL 接口，从而丢弃这些流量。不过，这不会阻止从违规主机或网络发送的流量。

注释 不要使用基于目标的补救作为对基于发现或主机输入事件的关联规则的响应。这些事件与源主机关联。

注意 思科 IOS 补救激活后，就不再有超时期限。要解除阻止 IP 地址或网络，必须从路由器手动清除路由更改。

为思科 IOS 路由器配置补救

注释 不要使用基于目标的补救作为对基于发现或主机输入事件的关联规则的响应。这些事件与源主机关联。

注意 思科 IOS 补救激活后，就不再有超时期限。要解除阻止 IP 地址或网络，必须从路由器手动清除路由更改。

开始之前

- 确认思科路由器运行的是思科 IOS 12.0 或更高版本。
- 确认您对路由器具有 15 级管理访问权限。

过程

步骤 1 在思科路由器上启用 Telnet，如思科路由器或 IOS 软件随附的文档中所述。

步骤 2 在 管理中心上，为计划使用的每个思科 IOS 路由器添加思科 IOS 空路由实例；请参阅添加思科 IOS 实例，第 6 页。

步骤 3 根据在违反关联策略时要在路由器上引发的响应类型，为每个实例创建补救。

- 添加思科 IOS 阻止目标补救，第 7 页
- 添加思科 IOS 阻止目标网络补救，第 7 页
- 添加思科 IOS 阻止源补救，第 8 页

- 添加思科 IOS 阻止源网络补救， 第 9 页

下一步做什么

- 分配补救以作为对安全策略违规的响应；请参阅将响应添加到规则和允许名单。

添加思科 IOS 实例

如果具有多个要发送补救的路由器，请为每个路由器创建单独的实例。

开始之前

- 在思科 IOS 路由器上配置 Telnet 访问，如路由器或 IOS 软件随附的文档中所述。

过程

步骤 1 选择**策略** > **操作** > **实例**。

步骤 2 从**添加新实例**列表中，选择**思科 IOS 空路由**并点击**添加**。

步骤 3 输入**实例名称 (Instance Name)** 和**说明 (Description)**。

步骤 4 在**路由器 IP (Router IP)** 字段中，输入要用于补救的思科 IOS 路由器的 IP 地址。

步骤 5 在**用户名 (Username)** 字段中，输入路由器的 Telnet 用户名。该用户必须对路由器拥有 15 级管理访问权限。

步骤 6 在**连接密码 (Connection Password)** 字段中，输入 Telnet 用户的用户密码。

步骤 7 在**启用密码 (Enable Password)** 字段中，输入 Telnet 用户的启用密码。该密码用于进入路由器的特权模式。

步骤 8 在**允许名单** 字段中，输入要免除补救的 IP 地址或范围（每行一个）。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

步骤 9 点击**创建**。

下一步做什么

- 添加要供关联策略使用的特定补救，如添加思科 IOS 阻止目标补救， 第 7 页、添加思科 IOS 阻止目标网络补救， 第 7 页、添加思科 IOS 阻止源补救， 第 8 页和添加思科 IOS 阻止源网络补救， 第 9 页中所述。

相关主题

Firepower 系统 IP 地址约定

添加思科 IOS 阻止目标补救

思科 IOS 阻止目标补救可阻止从路由器发送到关联事件违规中涉及的目标主机的流量。不要使用此补救作为对基于发现或主机输入事件的关联规则的响应。这些事件与源主机关联。

在多域部署中，无法将补救添加到祖先域中创建的实例。

开始之前

- 添加思科 IOS 实例，如添加思科 IOS 实例，第 6 页中所述。

过程

步骤 1 选择**策略** > **操作** > **实例**。

步骤 2 在要向其添加补救的实例旁，点击 **视图**（）。

步骤 3 在**已配置补救 (Configured Remediations)** 部分，选择**阻止目标 (Block Destination)** 并点击**添加 (Add)**。

如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 输入**补救名称 (Remediation Name)** 和**说明 (Description)**。

步骤 5 依次点击 **Create** 和 **Done**。

下一步做什么

- 分配补救以作为对安全策略违规的响应；请参阅将响应添加到规则和允许名单。

添加思科 IOS 阻止目标网络补救

思科 IOS 阻止目标网络补救可阻止从路由器发送到关联事件违规中涉及的目标主机网络的流量。不要使用此补救作为对基于发现或主机输入事件的关联规则的响应。这些事件与源主机关联。

在多域部署中，无法将补救添加到祖先域中创建的实例。

开始之前

- 添加思科 IOS 实例，如添加思科 IOS 实例，第 6 页中所述。

过程

步骤 1 选择**策略** > **操作** > **实例**。

步骤 2 在要向其添加补救的实例旁，点击 **视图**（）。

步骤 3 在**已配置补救**部分，选择**阻止目标网络**并点击**添加**。

如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 输入**补救名称 (Remediation Name)** 和**说明 (Description)**。

步骤 5 在 **Netmask** 字段中，输入子网掩码或使用 CIDR 表示法说明要阻止流量进入的网络。

例如，要在单个主机触发规则时阻止流量进入整个 Class C 网络（不推荐），请使用 `255.255.255.0` 或 `24` 作为子网掩码。

又例如，要阻止流量进入包括触发 IP 地址的 30 条地址，请指定 `255.255.255.224` 或 `27` 作为子网掩码。在这种情况下，如果 IP 地址 `10.1.1.15` 触发补救，则将阻止 `10.1.1.1` 与 `10.1.1.30` 之间的所有 IP 地址。要阻止触发 IP 地址，请将该字段留空，输入 `32` 或 `255.255.255.255`。

步骤 6 依次点击 **Create** 和 **Done**。

下一步做什么

- 分配补救以作为对安全策略违规的响应；请参阅将响应添加到规则和允许名单。

相关主题

Firepower 系统 IP 地址约定

添加思科 IOS 阻止源补救

思科 IOS 阻止源补救可阻止从路由器发送到关联策略违规中涉及的源主机的流量。

在多域部署中，无法将补救添加到祖先域中创建的实例。

开始之前

- 添加思科 IOS 实例，如添加思科 IOS 实例，第 6 页中所述。

过程

步骤 1 选择**策略 > 操作 > 实例**。

步骤 2 在要向其添加补救的实例旁，点击 **视图**（  ）。

步骤 3 在**已配置补救 (Configured Remediations)** 部分，选择**阻止源 (Block Source)**，然后点击**添加 (Add)**。

如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 输入**补救名称 (Remediation Name)** 和**说明 (Description)**。

步骤 5 依次点击 **Create** 和 **Done**。

下一步做什么

- 分配补救以作为对安全策略违规的响应；请参阅将响应添加到规则和允许名单。

添加思科 IOS 阻止源网络补救

思科 IOS 阻止源网络补救可阻止从路由器发送到关联事件违规中涉及的源主机网络的流量。

在多域部署中，无法将补救添加到祖先域中创建的实例。

开始之前

- 添加思科 IOS 实例，如添加思科 IOS 实例，第 6 页中所述。

过程

步骤 1 选择**策略** > **操作** > **实例**。

步骤 2 在要向其添加补救的实例旁，点击 **视图**（  ）。

步骤 3 在**已配置补救**部分，选择**阻止源网络**并点击**添加**。

如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 输入**补救名称 (Remediation Name)** 和**说明 (Description)**。

步骤 5 在 **Netmask** 字段中，输入子网掩码或描述要阻止流量进入的网络 CIDR 表示法。

例如，要在单个主机触发规则时阻止流量进入整个 Class C 网络（不推荐），请使用 `255.255.255.0` 或 `24` 作为子网掩码。

又例如，要阻止流量进入包括触发 IP 地址的 30 条地址，请指定 `255.255.255.224` 或 `27` 作为子网掩码。在这种情况下，如果 IP 地址 `10.1.1.15` 触发补救，则将阻止 `10.1.1.1` 与 `10.1.1.30` 之间的所有 IP 地址。要阻止触发 IP 地址，请将该字段留空，输入 `32` 或 `255.255.255.255`。

步骤 6 依次点击 **Create** 和 **Done**。

下一步做什么

- 分配补救以作为对安全策略违规的响应；请参阅将响应添加到规则和允许名单。

相关主题

Firepower 系统 IP 地址约定

Nmap 扫描补救

Firepower 系统与用于网络探索和安全审核的开源主动扫描程序 Nmap™ 集成。您可以通过 Nmap 补救对关联策略违规做出响应，Nmap 补救会触发 Nmap 扫描补救。

有关 Nmap 扫描的详细信息，请参阅Nmap 扫描。

设置属性值补救

可以响应关联策略违规，只需在触发事件发生的主机上设置主机属性值。对于文本主机属性，可以使用事件说明作为属性值。

配置设置属性补救

过程

步骤 1 选择**策略** > **操作** > **实例**。

步骤 2 创建设置属性实例，如添加设置属性值实例，第 10 页中所述。

步骤 3 添加设置属性补救，如添加设置属性值补救，第 10 页中所述。

下一步做什么

- 分配补救以作为对安全策略违规的响应；请参阅将响应添加到规则和允许名单。

相关主题

预定义主机属性
用户定义的主机属性

添加设置属性值实例

过程

步骤 1 选择**策略** > **操作** > **实例**。

步骤 2 从**添加新实例 (Add a New Instance)** 列表中选择**设定的属性值 (Set Attribute Value)**，然后点击**添加 (Add)**。

步骤 3 输入**实例名称 (Instance Name)** 和**说明 (Description)**。

步骤 4 点击**创建**。

下一步做什么

- 如添加设置属性值补救，第 10 页中所述，创建设定的属性补救。

添加设置属性值补救

设置属性值补救在关联策略违规所涉及的主机上设置主机属性。为要设置的每个属性值创建补救。对于文本属性，可以使用触发事件的说明作为属性值。

在多域部署中，无法将补救添加到祖先域中创建的实例。

开始之前

- 创建设置属性实例，如添加设置属性值实例，第 10 页中所述。

过程

步骤 1 选择**策略** > **操作** > **实例**。

步骤 2 在要向其添加补救的实例旁，点击 **视图**（  ）。

步骤 3 在**已配置补救 (Configured Remediations)** 部分，选择**设置属性值 (Set Attribute Value)**，然后点击**添加 (Add)**。

如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 输入**补救名称 (Remediation Name)** 和**说明 (Description)**。

步骤 5 要使用此补救响应带有源和目标数据的事件，请选择**从事件更新哪些主机 (Update Which Host(s) From Event)** 选项。

步骤 6 对于文本属性，请指定是否要**将事件说明用于属性值 (Use Description From Event For Attribute Value)**：

- 要使用事件说明作为属性值，请点击**打开 (On)** 并在**属性值 (Attribute Value)** 中输入要设置的属性值。
- 要使用补救的**属性值 (Attribute Value)** 设置作为属性值，请点击**关闭 (Off)**。

步骤 7 依次点击 **Create** 和 **Done**。

下一步做什么

- 分配补救以作为对安全策略违规的响应；请参阅将响应添加到规则和允许名单。

管理补救模块

在多域部署中，自定义表会显示在当前域中安装的补救模块，您可以对其进行删除。系统还会显示在祖先域中安装的模块，您不可以对其进行删除。要管理较低域中的补救模块，请切换至该域。

过程

步骤 1 选择**策略** > **操作** > **模块**。

步骤 2 管理补救模块：

- 配置 - 要查看模块的“模块详细信息”页面并配置其实例和补救，请点击 **视图**（  ）。在多域部署中，对于安装在祖先域中的模块，无法在当前域中使用“模块详细信息”(Module Detail) 页

面为其添加、删除或编辑实例。相反，请使用“实例”页面（**策略** > **操作** > **实例**）；请参阅管理补救实例，第 12 页。

- 删除 - 要删除未在使用的自定义模块，请点击 **删除**（）。无法删除系统提供的模块。
- 安装 - 要安装自定义模块，请点击**选择文件 (Choose File)**，浏览至模块，然后点击**安装 (Install)**。有关详细信息，请参阅《*Firepower* 系统补救 *API* 指南》。

管理补救实例

“实例”(Instances) 页面列出了所有补救模块的所有已配置实例。

在多域部署中，系统会显示在当前域中创建的补救实例，您可以对其进行编辑。系统还会显示在祖先域中创建的实例，您不可以对其进行编辑。要管理较低域中的补救实例，请切换至该域。

虽然您无法将补救添加到祖先域中创建的实例，但可以在当前域中创建类似配置的实例，并将补救添加到该实例。您也可以使用祖先域中创建的补救作为关联响应。

过程

步骤 1 选择**策略** > **操作** > **实例**。

步骤 2 管理补救实例：

- 添加 - 要添加实例，请选择要为其添加实例的补救模块，然后点击**添加 (Add)**。对于系统提供的模块，请参阅：
  - 添加 ISE EPS 实例，第 3 页
  - 添加思科 IOS 实例，第 6 页
  - 《Cisco Secure Firewall Management Center 设备配置指南》
  - 添加设置属性值实例，第 10 页

  如需获取添加自定义模块的帮助，请参阅该模块的文档（如有）。
- 配置 - 要配置实例详细信息并添加对实例的补救，请点击 **视图**（）。
- 删除 - 要删除未在使用的实例，请点击 **删除**（）。

管理单个补救模块的实例

“模块详细信息”(Module Detail) 页面显示为特定补救模块配置的所有实例和补救。

在多域部署中，可以访问当前域和祖先域中安装的补救模块的“模块详细信息”(Module Detail) 页面。但是，不能使用“模块详细信息”(Module Detail) 页面为祖先域中安装的模块添加、删除或编辑当前域中的实例。相反，请使用“实例”页面（**策略** > **操作** > **实例**）；请参阅管理补救实例，第 12 页。

过程

步骤 1 选择**策略** > **操作** > **模块**。

步骤 2 在要管理其实例的补救模块的旁边，点击 **视图**（）。

步骤 3 管理补救实例：

- 添加 - 要添加实例，请点击**添加 (Add)**。对于系统提供的模块，请参阅：
  - 添加 ISE EPS 实例，第 3 页
  - 添加思科 IOS 实例，第 6 页
  - 《Cisco Secure Firewall Management Center 设备配置指南》
  - 添加设置属性值实例，第 10 页

  要帮助为自定义模块添加实例，该参阅该模块的文档（如果可用）。
- 配置 - 要配置实例详细信息并添加对实例的补救，请点击 **视图**（）。
- 删除 - 要删除未在使用的实例，请点击 **删除**（）。

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。