管理中心概述

本指南适用于作为主要管理器或仅作为分析管理器的本地设备 Cisco Secure Firewall Management Center。在将 思科安全云控制 (安全云控制) 云交付的 防火墙管理中心 用作主管理器时，您只能使用本地部署 防火墙管理中心 进行分析。请勿将本指南用于 安全云控制 管理；请参阅使用 思科安全云控制 中的云交付的防火墙管理中心来管理 Cisco Secure Firewall Threat Defense 。

Cisco Secure Firewall Management Center是一个功能强大的、基于 Web 的多设备管理器，它在自己的服务器硬件上运行，或者在虚拟机监控程序上作为虚拟设备运行。如果您需要多设备管理器，并且您需要 上的所有功能，则应使用 防火墙管理中心 。防火墙管理中心 还提供强大的流量和事件的分析与监控功能。

注释 如果您有 安全云控制托管设备，并且仅将本地部署 防火墙管理中心 用于分析，则本地部署 防火墙管理中心 不支持策略配置或升级。本指南中的某些相关章节和程序可能不适用于主要管理器为 安全云控制的设备。

用作主用管理器的 防火墙管理中心： 防火墙管理中心 与其他管理器不兼容，因为 防火墙管理中心 拥有 配置，不允许绕过 防火墙管理中心直接配置 。

快速入门：基本设置

Cisco Secure Firewall 功能集足够强大且灵活，可以支持基本和高级配置。使用以下部分快速设置Cisco Secure Firewall Management Center及其受管设备，以开始控制和分析流量。

在物理设备上安装和执行初始设置

过程

使用设备的文档在所有物理设备上安装和执行初始设置：

- 防火墙管理中心
  - 您的硬件型号所对应的Cisco Secure 管理中心入门指南，可从以下网址获取

    《Cisco Secure Firewall Management Center 入门指南》
- 受管设备
  - Cisco Firepower 1010 入门指南
  - Cisco Firepower 1100 入门指南
  - 《Cisco Secure Firewall 3100 入门指南》
  - Cisco Firepower 4100 入门指南
  - 《Cisco Secure Firewall 4200 入门指南》
  - Cisco Firepower 9300 入门指南
  - 《适用于使用 Cisco Secure Firewall Management Center 的 ISA 3000 的 Cisco Secure Firewall Threat Defense 快速入门指南》

部署虚拟设备

如果您的部署包括虚拟设备，请按照下列步骤操作。使用文档路线图查找下列文档：浏览Cisco Secure Firewall Threat Defense 文档。

过程

步骤 1 确定将用于管理中心和设备的支持虚拟平台（可能不相同）。请参阅《*Cisco Secure Firewall* 兼容性指南》。

步骤 2 使用您的环境文档部署虚拟 Cisco Secure Firewall 管理中心：

- Firewall Management Center Virtual 在 VMware 上运行：《思科 *Cisco Secure Firewall Management Center Virtual* 入门指南》
- Firewall Management Center Virtual 在 AWS 上运行：《思科 *Cisco Secure Firewall Management Center Virtual* 入门指南》
- Firewall Management Center Virtual 在 KVM 上运行：《思科 *Cisco Secure Firewall Management Center Virtual* 入门指南》

步骤 3 使用设备的文档部署虚拟设备：

- Firewall Threat Defense Virtual 在 VMware 上运行：《*Cisco Cisco Secure Firewall Threat Defense Virtual for VMware* 入门指南》
- Firewall Threat Defense Virtual 在 AWS 上运行：《思科 *Cisco Secure Firewall Threat Defense Virtual AWS* 入门指南》
- Firewall Threat Defense Virtual 在 KVM 上运行：《*Cisco Cisco Secure Firewall Threat Defense Virtual for KVM* 入门指南》
- Firewall Threat Defense Virtual 在 Azure 上运行：《*Cisco Cisco Secure Firewall Threat Defense Virtual for Azure* 入门指南》

首次登录

在首次登录新的 防火墙管理中心 之前，请按照 在物理设备上安装和执行初始设置，第 2 页 或 部署虚拟设备，第 2 页中的说明准备设备。

第一次登录到新的防火墙管理中心（或新恢复为出厂默认设置的防火墙管理中心）时，请使用CLI或 Web 界面的 **管理员** 帐户，并按照您的 防火墙管理中心 型号的《 思科 *Cisco Secure Firewall* 管理中心入门指南》中的说明进行操作。完成初始配置过程后，系统将配置以下方面：

- 两个**管理员**账户（一个用于 Web 接口访问，另一个用于 CLI 访问）的密码将设置为相同的值，符合防火墙管理中心用户帐户的指南和限制中所述的强密码要求。系统仅在初始配置过程中同步两个 **管理员** 账户的密码。如果您在此后更改任一 **管理员** 账户的密码，两个密码将不再相同，并且强密码要求可以从 Web 接口 **管理员** 账户中删除。(请参阅 添加或编辑内部用户。)
- 防火墙管理中心 用于通过其管理接口 (eth0) 进行网络通信的以下网络设置将设置为默认值或您提供的值：

- 完全限定域名 (<主机名称>.<域>)
- 用于 IPv4 配置的启动协议 (DHCP 或 静态/手动)
- IPv4 地址
- 网络掩码
- 网关
- DNS 服务器
- NTP 服务器

可以通过 防火墙管理中心 Web 接口查看和更改这些设置的值；有关详细信息，请参阅 修改 防火墙管理中心 管理接口 和 时间同步 。

- 默认情况下，Cisco Success Network 和思科支持诊断功能处于启用状态。思科从Cisco Secure Firewall遥测数据，并将其用于客户成功计划。有关思科收集的遥测数据的更多信息，请参阅从管理中心设备收集的 Cisco Success Network 遥测数据。
- 升级或全新安装后，具有**管理员**权限的用户首次登录防火墙管理中心时，系统会一次性提示**管理员**用户提供邮箱地址。提供电子邮件地址是可选的。思科收集并使用电子邮件地址进行销售和产品续约对话、新版本采用新闻通讯，以及共享其他与产品相关的通信。
- 作为初始配置的一部分，系统会安排每周更新 GeoDB。我们建议您查看此任务，并在必要时进行更改，如安排 GeoDB 更新.
- 作为初始配置的一部分，系统会安排每周下载。我们建议您查看此任务，并在必要时进行更改，如自动执行软件下载.

重要事项 此任务仅下载更新。您负责安装此任务下载的任何更新。

- 作为初始配置的一部分， 系统会安排每周仅限配置的 防火墙管理中心 备份（本地存储）。我们建议您查看此任务，并在必要时进行更改，如计划 防火墙管理中心 备份.
- 作为初始配置的一部分，系统会下载并安装最新的VDB。为了让系统保持最新状态，我们建议您安排定期更新，如 漏洞数据库更新自动化.
- 作为初始配置的一部分，系统会安排每日入侵规则更新。我们建议您查看此任务，并在必要时进行更改，如计划入侵规则更新.

完成 防火墙管理中心 初始配置后，Web 接口将显示设备管理页面，如 《Cisco Secure Firewall Management Center 设备配置指南》中所述。

（这只是 **管理员** 用户首次登录时的默认登录页面。 **管理员** 或任何用户后续登录时，默认登录页面将按 指定主页中所述确定。）

完成初始配置时，通过按照设置基本策略和配置 ，第 5 页中的说明配置基本策略，开始控制和分析流量。

设置基本策略和配置

必须配置和部署基本策略，才能在控制面板、情景管理器和事件表中查看数据。

注释 这些并非是对策略或特性功能的全面讨论。有关其他功能和更高级配置的指南，请参阅本指南的其余部分。

开始之前

使用 Web 界面或 CLI 的**管理员**账户登录 Web 接口，并按照适用于您的硬件型号的《思科 *Cisco Secure Firewall* 管理中心入门指南》中所述执行初始配置，可从《安装和升级指南》获取。

过程

步骤 1 为此账户设置时区，如 设置默认时区中所述。

步骤 2 如果需要，请按照 许可证中的说明添加许可证。

步骤 3 如将设备添加到 《Cisco Secure Firewall Management Center 设备配置指南》 中的 防火墙管理中心 中所述，将托管设备添加到部署。

步骤 4 按照以下说明配置受管设备：

- 在 《Cisco Secure Firewall Management Center 设备配置指南》中接口概述，在 设备上配置透明或路由模式
- 在 《Cisco Secure Firewall Management Center 设备配置指南》中接口概述，在 设备上配置接口

步骤 5 配置访问控制策略，如在 《Cisco Secure Firewall Management Center 设备配置指南》中 创建基本访问控制策略 中所述。

- 在大多数情况下，思科建议将**平衡的安全和连接性**入侵策略设置为默认操作。有关详细信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的 访问控制策略默认操作和系统提供的网络分析和入侵策略。
- 在大多数情况下，思科建议启用连接日志记录，以满足组织的安全和合规性需要。在决定要记录哪些连接时，请考虑网络上的流量，以便不会干扰您的显示或系统不堪重负。有关详细信息，请参阅关于连接日志记录。

步骤 6 按照应用运行状况策略中的说明应用系统提供的默认运行状况策略。

步骤 7 自定义一些系统配置设置：

- 如果要允许服务的入站连接（例如，SNMP 或日志），请按照配置访问列表中的说明修改访问列表中的端口。
- 了解并考虑编辑数据库事件限制，如配置数据库事件限制中所述。

- 如果要更改显示语言，请按照设置 Web 接口的语言中的说明编辑语言设置。
- 如果您的组织限制使用代理服务器进行网络访问，请按照 修改 防火墙管理中心 管理接口中的说明编辑代理设置。

步骤 8 自定义网络发现策略，如在 中配置网络发现策略《Cisco Secure Firewall Management Center 设备配置指南》中所述。默认情况下，网络发现策略将分析网络上的所有流量。在大多数情况下，思科建议将发现限制在 RFC 1918 中的地址。

步骤 9 请考虑自定义如下其他常见设置：

- 如果为系统变量自定义默认值，请按照 《Cisco Secure Firewall Management Center 设备配置指南》中的说明了解 变量设置 使用方法。
- 如果要创建进行了本地身份验证的其他用户账号以访问 防火墙管理中心， 请参阅 添加或编辑内部用户。
- 如果要使用 LDAP 或 RADIUS 外部身份验证以允许访问 防火墙管理中心，请参阅 配置防火墙管理中心的外部身份验证。

步骤 10 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》 。

下一步做什么

查看并考虑配置功能， 第 7 页和本指南其余部分中描述的其他功能。

最新设备版本不支持的屏幕

虽然 防火墙管理中心 可以管理运行以前版本的设备（如 Cisco Secure Firewall Threat Defense 兼容性指南 中提供的兼容性矩阵中所述），但本指南仅包括最新版本的设备软件支持的功能。

有关仅在旧设备版本上支持的功能，请参阅与您的版本匹配的指南。

最新设备版本不支持的 Snort 2 屏幕

您已被重定向至此帮助页面，因为此屏幕适用于 Snort 2 功能。威胁防御版本 7.7 及更高版本不支持 Snort 2。有关 7.7 之前版本中支持的 Snort 2 功能的信息，请参阅与您的 版本匹配的 防火墙管理中心 指南。

设备

在典型的部署中，多个流量处理设备向一台 Cisco Secure Firewall Management Center报告，您可以使用它来执行管理、分析和报告任务。

设备是具有NGIPS功能的下一代防火墙(NGFW)。NGFW和平台功能还包括站点间和远程接入VPN、稳健路由、NAT、集群以及应用检查和访问控制中的其他优化功能。

适用于各种物理和虚拟平台。

兼容性

有关管理器设备兼容性的详细信息（包括与特定设备型号兼容的软件、虚拟主机环境、操作系统等），请参阅Cisco Secure Firewall Threat Defense 版本说明、Cisco Secure Firewall Management Center 兼容性指南和Cisco Secure Firewall Threat Defense 兼容性指南。

功能

以下表列出一些常用的 功能。

设备和系统管理功能

要查找文档，请参阅浏览 Cisco Secure Firewall Threat Defense 文档。

如果要...	配置...	如以下所述...
管理登录到Cisco Secure Firewall 设备的用户帐户	设备身份验证	用户和《Cisco Secure Firewall Management Center 设备配置指南》中的设备用户
监控系统硬件和软件的运行状况	运行状况监控策略	关于运行状况监控
备份设备上的数据	备份和恢复	备份/恢复
升级至新版本	系统更新	《适用于管理中心的 Cisco Secure Firewall Threat Defense 升级指南》 Cisco Secure Firewall Threat Defense 版本说明
设置物理设备基准	恢复出厂默认设置（重新映像）	适用于具备威胁防御的 Firepower 1000/2100 和 Cisco Secure Firewall 1200/3100/4200 的思科 FXOS 故障排除指南
更新设备上的VDB、入侵规则更新或GeoDB	漏洞数据库 (VDB) 更新、入侵规则更新或地理定位数据库 (GeoDB) 更新	更新
应用许可证以利用许可证控制的功能	智能许可	关于许可证

如果要...	配置...	如以下所述...
确保设备运行的连续性	受管设备高可用性和/或 防火墙管理中心 高可用性	关于 《Cisco Secure Firewall Management Center 设备配置指南》 中的 *Cisco Secure Firewall* 威胁防御 “高可用性章节” 关于防火墙管理中心高可用性
配置设备，为两个或更多个接口之间的流量提供路由	路由	《Cisco Secure Firewall Management Center 设备配置指南》中的路由参考
在两个或多个网络之间配置数据包切换	设备切换	《Cisco Secure Firewall Management Center 设备配置指南》中的配置网桥组接口
将专用地址转换为公共地址，以进行 Internet 连接	网络地址转换 (NAT)	《Cisco Secure Firewall Management Center 设备配置指南》中的网络地址翻译
在托管 设备之间建立安全隧道	站点间虚拟专用网络 (VPN)	《Cisco Secure Firewall Management Center 设备配置指南》中的*VPN* 概述
在远程用户和托管 设备之间建立安全隧道	远程接入 VPN	《Cisco Secure Firewall Management Center 设备配置指南》中的*VPN* 概述
对受管设备、配置和事件的用户访问进行分段。	使用域的多租户	使用域的多租户简介
使用 REST API 客户端查看和管理设备配置	REST API 和 REST API 管理器	REST API 首选项 《*Cisco Secure Firewall* 管理中心 *REST API* 快速入门指南》
排除问题	不适用	故障排除

检测、防止和处理潜在威胁

要查找文档，请参阅浏览 Cisco Secure Firewall Threat Defense 文档。

如果要...	配置...	如以下所述...
检查、记录和对网络流量进行操作	访问控制策略、其他若干策略的父策略	《Cisco Secure Firewall Management Center 设备配置指南》中的访问控制简介
将指向或来自 IP 地址、URL 和/或域名的连接阻止或监控	访问控制策略中的安全情报	《Cisco Secure Firewall Management Center 设备配置指南》中的关于安全情报
控制用户在网络中可以访问的网站	策略规则中的 URL 过滤	《Cisco Secure Firewall Management Center 设备配置指南》中的*URL* 过滤
监视网络上的恶意流量和入侵	入侵策略	《Cisco Secure Firewall Management Center 设备配置指南》中的*Snort 3* 入侵策略入门
阻止未经检查的加密流量 检查加密或解密的流量	SSL 策略	《Cisco Secure Firewall Management Center 设备配置指南》中的*SSL* 策略概述
通过快速路径对封装的流量进行自定义深度检查并提高性能	预过滤器策略	《Cisco Secure Firewall Management Center 设备配置指南》中的关于预过滤
对访问控制允许或信任的网络流量施行速度限制	服务质量 (QoS) 策略	《Cisco Secure Firewall Management Center 设备配置指南》中的关于 *QoS* 策略
允许或阻止网络上的文件（包括恶意软件）	文件/恶意软件策略	《Cisco Secure Firewall Management Center 设备配置指南》中的网络恶意软件保护和文件策略
处理来自威胁情报源的数据	思科 Threat Intelligence Director (TID)	《Cisco Secure Firewall Management Center 设备配置指南》中的安全防火墙威胁智能导向器 概述
配置被动或主动用户身份验证以执行用户感知和用户控制	用户感知、用户身份、身份策略	《Cisco Secure Firewall Management Center 设备配置指南》中的关于用户身份源 《Cisco Secure Firewall Management Center 设备配置指南》中的关于身份策略

如果要...	配置...	如以下所述...
从网络上的流量中收集主机、应用和用户数据，以执行用户感知	网络发现策略	《Cisco Secure Firewall Management Center 设备配置指南》中的网络发现策略
使用设备以外的工具收集和分析有关网络流量和潜在威胁的数据	集成外部工具	使用外部工具的事件分析
执行应用检测和控制	应用检测器	《Cisco Secure Firewall Management Center 设备配置指南》中的应用检测
排除问题	不适用	故障排除

集成外部工具

要查找文档，请参阅浏览 Cisco Secure Firewall Threat Defense 文档。

如果要...	配置...	如以下所述...
当网络上的条件违反关联策略时自动启动补救	补救	补救简介 《*Firepower* 系统补救 *API* 指南》
将事件数据从 防火墙管理中心 到自定义开发的客户端应用	eStreamer 集成	eStreamer 服务器流传输 *Cisco Secure Firewall* 管理中心 *Event Streamer* 集成指南
使用第三方客户端在 防火墙管理中心 查询数据库表	外部数据库访问	外部数据库访问 *Cisco Secure Firewall* 管理中心数据库访问指南
通过从第三方源导入数据来扩充发现数据	主机输入	《Cisco Secure Firewall Management Center 设备配置指南》中的主机输入数据 《*Firepower* 系统主机输入 *API* 指南》
使用外部事件数据存储工具和其他数据资源调查事件	集成外部事件分析工具	使用外部工具的事件分析
排除问题	不适用	故障排除

搜索防火墙管理中心

您可以使用全局搜索功能快速查找并导航到 Cisco Secure Firewall Management Center 配置的元素。

您可以搜索以下实体的 防火墙管理中心 配置：

- 顶级菜单中 Web 界面页面的名称。（请参阅搜索 Web 接口菜单选项，第 14 页。）
- 对于某些策略类型：
  - 策略名称
  - 策略说明
  - 规则名称
  - 规则注释

  （请参阅搜索策略，第 14 页。）
- 对于某些对象类型：
  - 对象名称
  - 对象说明
  - 配置的值

  (请参阅 搜索对象，第 16 页 。)
- 操作方法逐步指导

  搜索将返回包含搜索词的逐步指导列表，以及指向每个逐步指导的链接。（请参阅搜索如何逐步指导，第 20 页。）

使用全局搜索时，请记住以下几点：

- 当您打开全局搜索工具时，最近十次搜索会显示在搜索文本框下方的历史记录列表中。您可以从此列表中选择一个项目来重新执行搜索。
- 当您键入搜索表达式时，界面会将搜索历史记录替换为在您键入搜索时更新的搜索结果；您不需要按 Enter 键执行搜索。
- 您可以使用鼠标或键盘箭头键和 Enter 键浏览历史记录列表或搜索结果。按 Enter 键可选择搜索结果中当前突出显示的项目。对于 Web 界面页面的结果，这会导致 防火墙管理中心 界面显示突出显示的页面。对于对象和策略，这将显示有关找到的实体的详细信息。
- 搜索不区分大小写。
- 在搜索中，可以使用以下通配符：
  - ? 匹配任意单个字符。
  - * 匹配 0 或多个字符。

- ^ 将其前面的搜索词锚定到匹配实体的开头。
- $ 将其跟随的搜索词锚定到匹配实体的末尾

通配符无法转义。

- 为提高效率，全局搜索不返回间接搜索结果；也就是说，全局搜索不会返回引用找到搜索词的对象的策略或对象。但是，您可以通过在搜索详细信息窗格中查看找到的对象的**使用情况**选项卡来确定哪些策略或对象引用了许多找到的对象。
- 全局搜索返回搜索表达式的排名靠前的结果，具体取决于其与 防火墙管理中心中最常用的配置实体的相关性。如果全局搜索无法返回您希望找到的内容，请尝试细化搜索，尝试使用许多GUI页面顶部显示的搜索或过滤器工具，或者尝试 Web 界面提供的一些特定于配置的搜索功能：
  - 《Cisco Secure Firewall Management Center 设备配置指南》中的搜索规则
  - 《Cisco Secure Firewall Management Center 设备配置指南》中的搜索和过滤 *NAT* 规则表
  - 搜索事件
  - 搜索自定义表

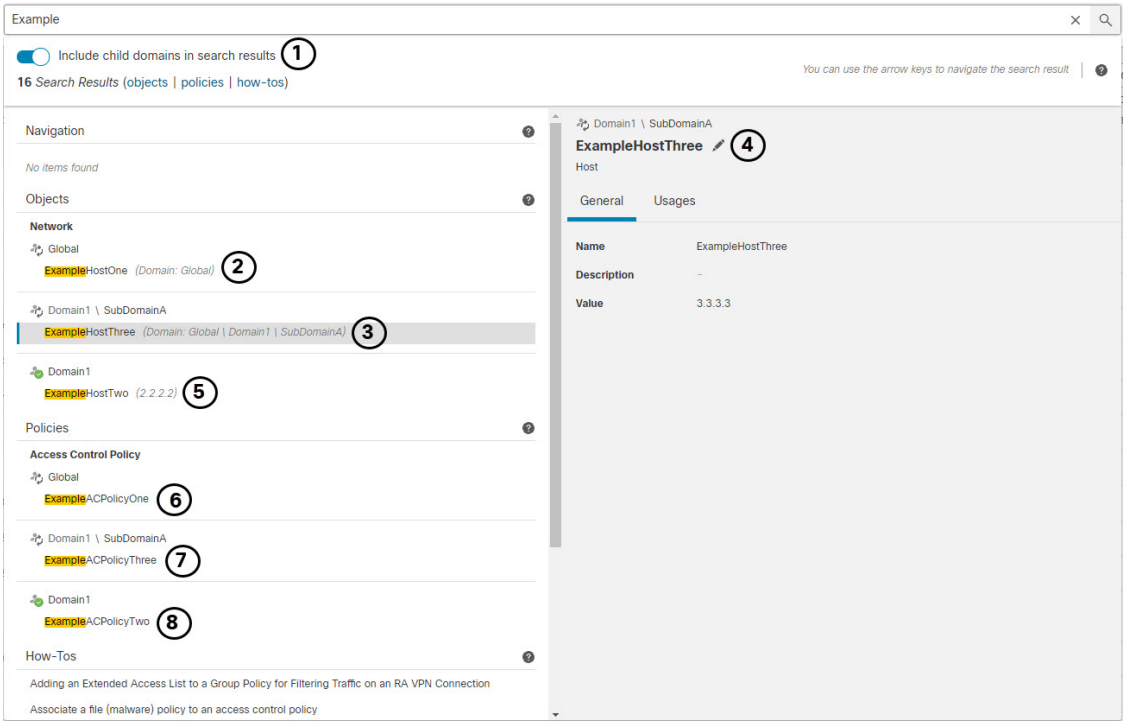
在多域部署中全局搜索

在多域部署中，默认情况下，搜索仅返回当前域及其祖先域中定义的对象和策略。您可以通过切换搜索结果对话框中的选项来查看子域中的对象和策略。

对于对象搜索，如果在当前域以外的域中定义的对象中找到搜索表达式，则搜索结果将显示这些对象所在的域的名称。如果在当前域中定义的对象中找到搜索表达式，则搜索结果会显示对象值。

在下面的示例屏幕截图中，部署包含三个级别的三个域：全局、域 1 和子域 A。当前域为 Domain1 的用户已在祖先域和子域中输入字符串“example”。

图 *1:* 多域环境中的全局搜索示例



1	用户已选择搜索子域 (SubDomainA) 以及当前域 (Domain1) 及其祖先 (Global)。	2	系统将显示父域 Global 中定义的匹配网络对象 ExampleHostOne，其中包含域名和指示用户必须切换域才能编辑详细信息的 **外部域** （） 图标。
3	子域 SubDomainA 中定义的匹配网络对象 ExampleHostThree 将与域名一起显示，并且 **外部域** （） 图标指示用户必须切换域才能编辑详细信息。此对象当前处于选中状态。	4	当前已选择匹配的网络对象 ExampleHostThree，并且右侧窗格中提供了相关信息。 **外部域** （） 图标表示，当用户点击 **编辑** ()时，系统将提示用户确认域更改，然后才允许对对象进行编辑访问。
5	在当前域中定义的匹配网络对象 ExampleHostTwo 与对象值一起显示，并带有指示用户可以编辑此对象而无需切换域的 **当前域** （） 图标。	6	系统将显示父域 Global 中定义的匹配访问控制策略 ExampleACPolicyOne，其中包含域名和指示用户必须切换域才能编辑详细信息的 **外部域** （） 图标。
7	将显示子域 SubDomainA 中定义的匹配访问控制策略 ExampleACPolicyThree，其中包含域名和指示用户必须切换域才能编辑详细信息的图标。 **外部域** （）	8	系统将显示当前域中定义的匹配访问控制策略 ExampleACPolicyTwo，并带有 **当前域** （） 图标，指示用户无需切换域即可编辑详细信息。

搜索 Web 接口菜单选项

您可以搜索以查找 Web 界面顶级菜单中的页面位置。例如，要查看或配置服务质量设置，请搜索 **QoS**。

过程

步骤 1 使用以下两种方法之一启动搜索：

- 在 防火墙管理中心 Web 接口顶部的菜单栏中，点击 **搜索** ( )。
- 将焦点放在文本框外，键入 / （正斜杠）。

步骤 2 输入要查找的菜单选项名称的一个或多个字母。搜索结果显示在文本框下方，并在您键入时更新；您不需要按 Enter 键执行搜索。

步骤 3 搜索结果按类别分组显示。要转到 **导航**下列出的页面，请点击搜索结果列表中的菜单路径。

搜索策略

下表指示可按名称搜索的策略类型：

适用范围	非适用范围
访问控制策略	威胁防御平台设置
预过滤器策略	Firepower 设置策略
威胁防御 NAT 策略	Firepower NAT 策略
入侵类别 • 入侵策略 • Network Analysis Policy	QoS 策略的比较 FlexConfig 策略 DNS 策略 恶意软件与文件策略 (Malware & File Policy) SSL 策略 身份策略 网络发现 应用检测器

适用范围	非适用范围
	关联策略 VPN 类别 • 动态访问策略 • 站点间 • 远程访问

全局搜索返回名称与搜索词匹配的策略，以及使用名称或注释与搜索词匹配的规则的访问控制策略。如果您在搜索结果列表中看到某个访问控制策略的名称与搜索结果不匹配，则表明该匹配是针对该策略中配置的规则的名称或注释进行的。

重要事项 全局搜索返回搜索表达式的排名靠前的结果，具体取决于其与 防火墙管理中心中最常用的配置实体的相关性。您的搜索词可能存在于不属于此搜索功能范围的策略类型中。有关全局搜索功能和替代搜索方法的完整说明，请参阅 搜索 防火墙管理中心。

过程

步骤 1 使用以下两种方法之一启动搜索：

- 在 防火墙管理中心 Web 接口顶部的菜单栏中，点击 **搜索** ()。
- 将焦点放在文本框外，键入 / （正斜杠）。

步骤 2 在搜索文本框中输入搜索表达式。搜索结果显示在文本框下方，并在您键入时更新；您不需要按 Enter 键执行搜索。

步骤 3 （可选）在多域部署中，如果当前域具有后代域，则可以切换 **在搜索结果中包含子域** 以查看这些后代域中的策略。

步骤 4 搜索结果按类别分组显示。在多域部署中，在 **策略** 类别中，搜索结果按定义了找到的策略的域进行分组。在 **策略** 类别下，您可以执行以下操作：

收件人：	执行以下操作：
查看单一策略类型的搜索结果。	点击搜索结果中的策略类型，例如访问控制策略。
查看有关策略的详细信息。	点击搜索结果列表中的策略名称以查看详细信息窗格并显示 **常规** 选项卡。
查看引用入侵和网络分析策略的访问控制策略。	点击搜索结果中的入侵或网络分析策略的名称以查看详细信息窗格并显示 **使用情况** 选项卡。

收件人：	执行以下操作：
在单独的浏览器窗口中打开策略的策略配置页面。	点击搜索结果中的策略名称，然后在详细信息窗格中点击**编辑** (✎)。 在多域部署中，如果您选择编辑未在当前域中定义的策略，系统将提示您更改当前域。

搜索对象

下表指示“对象管理”页面 (**对象** > **对象管理**)上列出的对象类型在全局搜索功能范围内：

适用范围	非适用范围
AAA 服务器类别 • RADIUS 服务器组 • 单点登录服务器 访问列表类别 • 扩展访问列表 • 标准访问列表 地址池类别 • IPv4 池 • IPv6 池 AS 路径 社区列表类别 • 扩展社区 DNS 服务器组 外部属性类别 • 动态对象 • 安全组标记 地理位置 接口类别 • 安全区 • 接口组 密钥链 网络（包括网络、主机、范围、FQDN、网络组） PKI 类别 证书注册	应用过滤器 密码套件列表 社区列表类别 • 社区 可分辨名称类别 • 单独可分辨名称对象 • 可分辨名称对象组 文件列表 FlexConfig 类别 • FlexConfig 对象 • 文本对象 PKI 类别 • 外部证书组 (External Cert Groups) • 外部证书 • 内部 CA 证书 (Internal CA Groups) • 内部 CA • 内部证书组 (Internal Cert Groups) • 外部证书 • 受信任 CA 证书 (Trusted CA Groups) • 受信任 CA 安全智能类别 • DNS 列表和源 • 网络列表和源 • URL 列表和源

适用范围	非适用范围
策略列表 端口（对象和组、TCP、UDP、ICMP、ICMP6、其他） 前缀列表类别 • IPV4 前缀列表 • IPV6 前缀列表 路由映射 SLA 监控器 时间范围 时区 隧道区域 URL（对象、组） VLAN 标记（对象、组） VPN 类别 • 证书映射 • 组策略 • IKEv1 IPSec 提议 • IKEv1 策略 • IKEv2 IPsec 提议 • IKEv2 策略	Sinkhole 变量集 VPN 类别 • 安全客户端 文件 • 自定义属性

全局搜索返回名称或说明与搜索词匹配的对象，以及具有与搜索词匹配的配置值的对象。如果您在搜索结果列表中看到名称与搜索不匹配的对象，则表明该对象的说明或配置的值是匹配的。

重要事项 全局搜索返回搜索表达式的排名靠前的结果，具体取决于其与 防火墙管理中心中最常用的配置实体的相关性。您的搜索词可能不在此搜索功能范围内的对象类型中。有关全局搜索功能和替代搜索方法的完整说明，请参阅 搜索 防火墙管理中心。

当您需要在部署中查找网络信息时，对象搜索尤其有用。您可以在对象名称、说明或配置的值中搜索以下内容：

- IPv4 和 IPv6 地址信息，包括以下格式：

- 完整地址（例如， `194.164.0.23`、 `2001:0db8:85a3:0000:0000:8a2e:0370:7334`。）
- 部分地址（例如， `194.164`、`2001:db8`。）
- 范围（例如， `192.164.1.1-192.168.1.5` 或 `2001:db8::0202-2001:db8::8329`。请勿在连字符前后添加空格。）全局搜索使用与指定范围内的任意地址匹配的网络地址返回对象。
- CIDR 表示法。（例如 `192.168.1.0/24`、 `2002::1234:abcd:ffff:101/64`。）全局搜索使用与指定 CIDR 块中的 any 匹配的网络地址返回对象。

- 端口信息：
  - 端口号（例如， `22` 或 `80`。）
  - 协议 (Protocols)。（例如， `https` 或 `ssh`。）
- 完全限定域名。（例如， `www.cisco.com`。)
- 列表。（例如， `http://www.cisco.com`。)
- 加密标准或散列类型。（例如， `AES-128` 或 `SHA`。）
- VLAN 标记号。（例如， `568`。）

过程

步骤 1 使用以下两种方法之一启动搜索：

- 在 防火墙管理中心 Web 接口顶部的菜单栏中，点击 **搜索** ()。
- 将焦点放在文本框外，键入 / （正斜杠）。

步骤 2 在搜索文本框中输入搜索表达式。搜索结果显示在文本框下方，并在您键入时更新；您不需要按 Enter 键执行搜索。

如果在当前默认域以外的域中定义的对象中找到搜索表达式，则搜索结果将显示这些对象所在的域的名称。如果在当前域中定义的对象中找到搜索表达式，则搜索结果会显示对象值。

步骤 3 （可选）在多域部署中，如果当前域具有后代域，则可以切换 **在搜索结果中包含子域** 以查看这些后代域中的对象。

步骤 4 搜索结果按类别显示。在多域部署中，在 **对象** 类别中，搜索结果按定义找到的对象的域进行分组。在 **对象** 类别下，您可以执行以下操作：

收件人：	执行以下操作：
查看单个对象类型的搜索结果。	点击搜索结果中的对象类型，例如 **网络**。
在搜索结果中查看有关对象的详细信息。	点击搜索结果中的对象名称可查看详细信息窗格并显示 **常规** 选项卡。

收件人：	执行以下操作：
查看使用搜索结果中的对象的策略或对象的列表。	点击搜索结果中的对象名称可查看详细信息窗格并显示 **使用情况** 选项卡。 **注释** 全局搜索不提供所有对象类型的使用信息。
在单独的浏览器窗口中打开对象的对象配置页面。	点击搜索结果中的对象名称，然后在详细信息窗格中点击 **编辑** ()。 在多域部署中，如果您选择编辑未在当前域中定义的对象，系统将提示您更改当前域。

搜索如何逐步指导

您可以搜索解决相关任务的操作方法逐步指导。例如，要查找描述设备设置程序的逐步指导，您可以搜索术语“设备”。

开始之前

此功能在经典主题中不可用。要更改主题，请参阅 更改 Web 接口外观。

过程

步骤 1 使用以下两种方法之一启动搜索：

- 在 防火墙管理中心 Web 接口顶部的菜单栏中，点击 **搜索** ()。
- 将焦点放在文本框外，键入 / （正斜杠）。

步骤 2 输入与您想要查看逐步指导的任务相关联的搜索词。搜索结果显示在文本框下方，并在您键入时更新；您不需要按 Enter 键执行搜索。

步骤 3 搜索结果按类别分组显示。要查看 **操作方法**下列出的逐步指导，请点击搜索结果列表中的逐步指导标题。有关操作方法逐步指导的详细信息，请参阅 联机帮助、操作方法和文档，第 23 页。

切换 Cisco Secure Firewall Management Center 上的域

在多域部署中，用户角色权限确定用户可以访问哪些域，以及用户在其中每个域内具有哪些权限。可以将单个用户帐户与多个域相关联，并在每个域中为该用户分配不同的权限。例如，可以在全局域中为用户分配只读权限，但在后代域中分配管理员权限。

与多个域关联的用户可以在同一 Web 界面会话中的域之间进行切换。

在工具栏中的用户名下，系统会显示可用域的树。树：

- 显示祖先域，但是，可以根据分配给用户帐户的权限禁用对这些域的访问。
- 隐藏用户帐户无法访问的任何其他域，包括同代域和后代域。

在切换到域时，系统会显示：

- 仅与该域相关的数据。
- 由面向该域分配给您的用户角色确定的菜单选项。

过程

在您的用户名下的下拉列表中，选择要访问的域。

情景菜单

Firepower 系统 Web 界面中的某些页面支持右键点击上下文菜单（最常见）或左键点击上下文菜单，可供您用作访问 Firepower 系统中其他功能的快捷方式。上下文菜单的内容取决于您访问菜单时所处的位置 - 不仅是页面，还可以是特定数据。

例如：

- IP 地址热点，提供有关与该地址关联的主机的信息，包括任何可用的 whois 和主机配置文件信息。
- SHA-256 散列值热点，通过其可将文件的 SHA-256 散列值添加到干净列表或自定义检测列表中，或者查看要复制的完整散列值。

在不支持 Firepower 系统上下文菜单的页面或位置上，适用于浏览器的普通上下文菜单将会显示出来。

策略编辑器

许多策略编辑器都包含基于每个规则的热点。您可以插入新规则和类别，剪切、复制和粘贴规则，设置规则状态，以及编辑规则。

入侵规则编辑器

入侵规则编辑器包含基于每个入侵规则的热点。您可以编辑规则，设置规则状态，配置阈值和抑制选项，以及查看规则文档。或者，在点击情景菜单中的**规则文档**后，可以点击文档弹出窗口中的**规则文档**以查看更具体的规则详情。

事件查看器

事件页面（“分析”菜单下的向下钻取页面和表视图）包含基于每个事件、IP地址、URL、DNS查询以及某些文件的SHA-256散列值的热点。查看大多数事件类型时，您可以执行以下操作：

- 在情景管理器中查看相关信息。
- 在新窗口中向下展开到事件信息。
- 查看事件视图中的事件字段包含过长而无法完全显示的文本（例如文件的SHA-256散列值、漏洞说明或URL）的位置的完整文本。
- 使用上下文交叉启动功能打开有关从外部至Firepower源的元素详细信息的Web浏览器窗口。有关详细信息，请参阅使用基于Web的资源的事件调查。

查看连接事件时，您可以将项目添加到默认安全情报阻止和不阻止名单：

- IP地址热点中的IP地址。
- URL热点中的URL或域名。
- DNS查询热点中的DNS查询。

查看捕获的文件、文件事件和恶意软件事件时，您可以执行以下操作：

- 在干净列表或自定义检测列表中添加或删除文件。
- 下载文件的副本。
- 查看存档文件内的嵌套文件。
- 下载嵌套文件的父存档文件。
- 输入文件组成。
- 提交文件以进行本地恶意软件和动态分析。

查看入侵事件时，您可以执行与入侵规则编辑器或入侵策略中的任务类似的任务：

- 编辑触发规则。
- 设置规则状态（包括禁用规则）。
- 配置阈值和抑制选项。
- 查看规则文档。或者，在点击情景菜单中的**规则文档**后，可以点击文档弹出窗口中的**规则文档**以查看更具体的规则详情。

入侵事件数据包视图

入侵事件数据包视图包含IP地址热点。数据包视图使用左键点击上下文菜单。

控制面板

很多控制面板构件都包含热点，用于查看“情景管理器”中的相关信息。控制面板构件还包含IP地址和SHA-256散列值热点。

情景管理器

“情景管理器”包含热点，位于其图表、表格和图形上方。如果您希望以比“情景管理器”允许的更详细的程度来检查图形或列表中的数据，则您可以向下展开到相关数据的表视图。您还可以查看相关的主机、用户、应用、文件和入侵规则信息。

情景管理器使用左键点击上下文菜单，该菜单也包含情景管理器独有的过滤选项及其他选项。

与思科共享数据

Cisco Success Network 和思科支持诊断功能会默认启用。

Cisco Success Network 功能允许思科收集客户使用指标和统计数据，以分析产品使用情况并提升客户对思科产品的体验。要退出向思科发送 Cisco Success Network 遥测数据，请参阅配置 防火墙管理中心 以与思科共享使用情况指标和统计信息。有关思科收集的遥测数据的更多信息，请参阅从管理中心设备收集的 Cisco Success Network 遥测数据。

借助思科支持诊断功能，思科可以从您的设备收集重要信息，为您提供更好的支持体验。要选择不向思科发送思科支持诊断指标，请参阅配置 防火墙管理中心 以与思科共享设备运行状况数据。

您可以选择使用网络分析与思科共享数据。有关详细信息，请参阅Web 分析。

联机帮助、操作方法和文档

可以通过以下方式从 Web 界面访问联机帮助：

- 点击各页面上的上下文帮助链接
- 通过选择**帮助 (Help)** > **页面级帮助 (Page-level Help)**

“操作方法”是一个构件，它提供导航防火墙管理中心上任务的逐步指导。逐步指导将引导您完成每个步骤，依次熟悉可能必须导航的各类陌生UI界面，引导您完成实现任务所需执行的步骤，最终完成任务。**操作方法**构件默认为启用。要禁用该构件，请从用户名下的下拉列表中选择**用户首选项**，然后取消选中 **How-To 设置**选项卡中的**启用 How-To** 复选框。要打开“操作方法”构件，请选择**帮助 (Help)** > **操作方法 (How-Tos)**。

注释 通常情况下，逐步指导对所有UI页面可用，并且不区分用户角色。但是，根据用户权限的不同，某些菜单项将不会显示在 防火墙管理中心 界面上。因此，逐步指导将不会在此类页面上执行。

防火墙管理中心 上提供了以下逐步指导：

有关 防火墙管理中心 中支持的功能逐步指导的列表，请参阅Cisco Secure Firewall Management Center 支持的功能逐步指导。

可以使用以下文档路线图查找与其他文档：

浏览 Cisco Secure Firewall Threat Defense 文档。

Cisco.com 上的用户指南

在配置 Cisco Secure Firewall Management Center部署版本 6.0+ 时，以下文档可提供帮助。

注释 有些链接的文档不适用于 Cisco Secure Firewall Management Center部署。例如， Cisco Secure Firewall Threat Defense页面上的某些链接专用于 Cisco Secure Firewall 设备管理器管理的部署，并且硬件页面上的某些链接与 防火墙管理中心无关。为避免混淆，请特别注意文档标题。此外，有些文档涵盖多个产品，因此可能会出现在多个产品页面上。

Cisco Secure Firewall Management Center

- Cisco Secure Firewall Management Center硬件设备：

  http://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html

- Cisco Secure Firewall Management Center虚拟设备：
  - http://www.cisco.com/c/en/us/support/security/defense-center-virtual-appliance/tsd-products-support-series-home.html
  - http://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html

Cisco Secure Firewall Threat Defense，也称为 NGFW（下一代防火墙）设备

- Cisco Secure Firewall Threat Defense软件：

  http://www.cisco.com/c/en/us/support/security/firepower-ngfw/tsd-products-support-series-home.html

- Cisco Secure Firewall Threat Defense虚拟：

  http://www.cisco.com/c/en/us/support/security/firepower-ngfw-virtual/tsd-products-support-series-home.html

- Firepower 1000 系列：

  https://www.cisco.com/c/en/us/support/security/firepower-1000-series/tsd-products-support-series-home.html

- Cisco Secure Firewall 3100:

  https://www.cisco.com/c/en/us/support/security/secure-firewall-3100-series/series.html

- Firepower 4100 系列：

  https://www.cisco.com/c/en/us/support/security/firepower-4100-series/tsd-products-support-series-home.html

- Cisco Secure Firewall 4200：

  https://www.cisco.com/c/en/us/support/security/secure-firewall-4200-series/series.html

- Firepower 9300：

  https://www.cisco.com/c/en/us/support/security/firepower-9000-series/tsd-products-support-series-home.html

- ISA 3000：

  https://www.cisco.com/c/en/us/support/security/industrial-security-appliance-isa/tsd-products-support-series-home.html

文档中的许可声明

节开头的许可证声明指示必须将哪个经典或智能许可证分配到受管设备以启用该节所述的功能。

由于许可功能通常是累加的，因此许可证声明仅提供每项功能的最高要求许可证。

许可证声明中的“或”语句表明必须向受管设备分配特定许可证以启用该节所述的功能，但是附加许可证可以添加功能。例如，在文件策略中，某些文件规则操作要求向设备分配保护许可证，而其他操作则要求分配 恶意软件防御 许可证。

有关许可证的详细信息，请参阅关于许可证。

相关主题

关于许可证

文档中的受支持设备声明

章节或主题开头的“受支持设备”声明指示仅在指定的设备序列、系列或型号上才支持相应的功能。例如，许多功能仅在 Cisco Secure Firewall Threat Defense 设备上受支持。

有关此版本支持的平台的详细信息，请参阅版本说明。

文档中的访问声明

本文档中每个程序开头的“访问”声明表明执行此程序所需的预定义用户角色。所列的任何角色都可以执行此程序。

自定义角色的用户可以拥有不同于预定角色的权限。预定角色用于指示某个程序的访问要求时，具有相似权限的自定义角色也能访问。某些具有自定义角色的用户可以使用略有不同的菜单路径到达配置页面。例如，具有仅有入侵策略权限的自定义角色的用户通过入侵策略而非通过访问控制策略的标准路径来访问网络分析策略。

Firepower 系统 IP 地址约定

您可以使用 IPv4 无类域间路由选择 (CIDR) 表示法和类似的 IPv6 前缀长度表示法定义 Firepower 系统中很多位置的地址块。

使用 CIDR 或前缀长度表示法指定 IP 地址块时，Firepower 系统**只**使用掩码或前缀长度指定的那部分网络 IP 地址。例如，如果键入 10.1.2.3/8，则 Firepower 系统使用 10.0.0.0/8。

换句话说，虽然思科建议您在使用 CIDR 或前缀长度表示法时采用使用位边界上网络 IP 地址的标准方法，但是 Firepower 系统并不要求必须这么做。

其他资源

除了我们提供的大量文档外，防火墙社区也是内容丰富的参考资料库。在这里，您可以找到思科硬件的三维模型、硬件配置选择器、产品资料、配置示例、故障排除技术笔记、培训视频、实验和 Cisco Live 大会、社交媒体公众号、思科博客，以及技术出版团队发布的所有文档。

在社区网站或视频分享网站上发帖的某些个人（包括版主在内）在思科系统公司工作。这些网站上发表的观点以及任何相关评论均为原作者的个人观点，与思科无关。此处内容仅用于提供信息，不作为思科或其他各方的认可或声明。

注释 防火墙社区 上的一些视频、技术说明和参考材料指向的是旧版 防火墙管理中心。您的 防火墙管理中心 版本与视频或技术说明中引用的版本可能在用户界面上有不同之处，从而导致过程不尽相同。

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。