Dynamic Attributes Connector

以下主题讨论如何配置和使用Dynamic Attributes Connector。

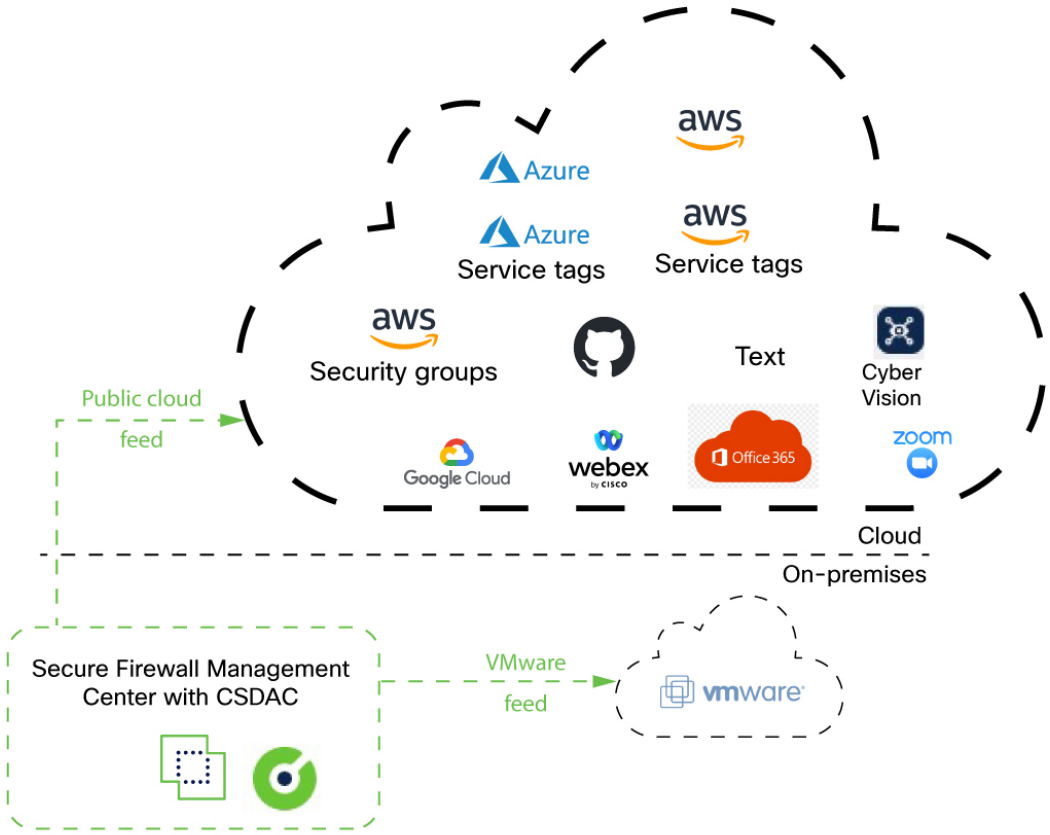
关于 dynamic attributes connector

dynamic attributes connector使您的访问控制策略和 DNS 策略能够实时适应公有云和私有云工作负载以及业务关键型软件即服务 (SaaS) 应用的变化。它通过保持规则最新（无需繁琐的手动更新和策略部署）来简化策略管理。客户需要根据非网络结构（例如虚拟机名称或安全组）定义策略规则，以便即使 IP 地址或 VLAN 发生更改，防火墙策略也能保持不变。

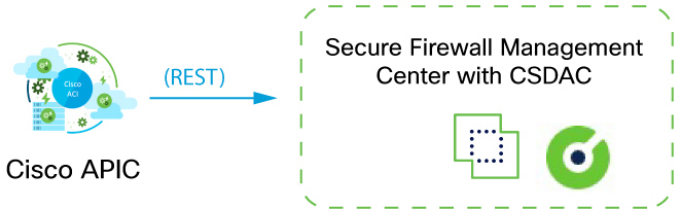
运作方式

本主题讨论 dynamic attributes connector 的架构。

下图显示了系统的总体运行情况。



Cisco APIC integration with the Secure Firewall Management Center



- 系统支持某些公共云提供商。

  本主题讨论受支持的 连接器 （即与这些提供程序的连接）。

- dynamic attributes connector 随 Secure Firewall Management Center 一起提供。

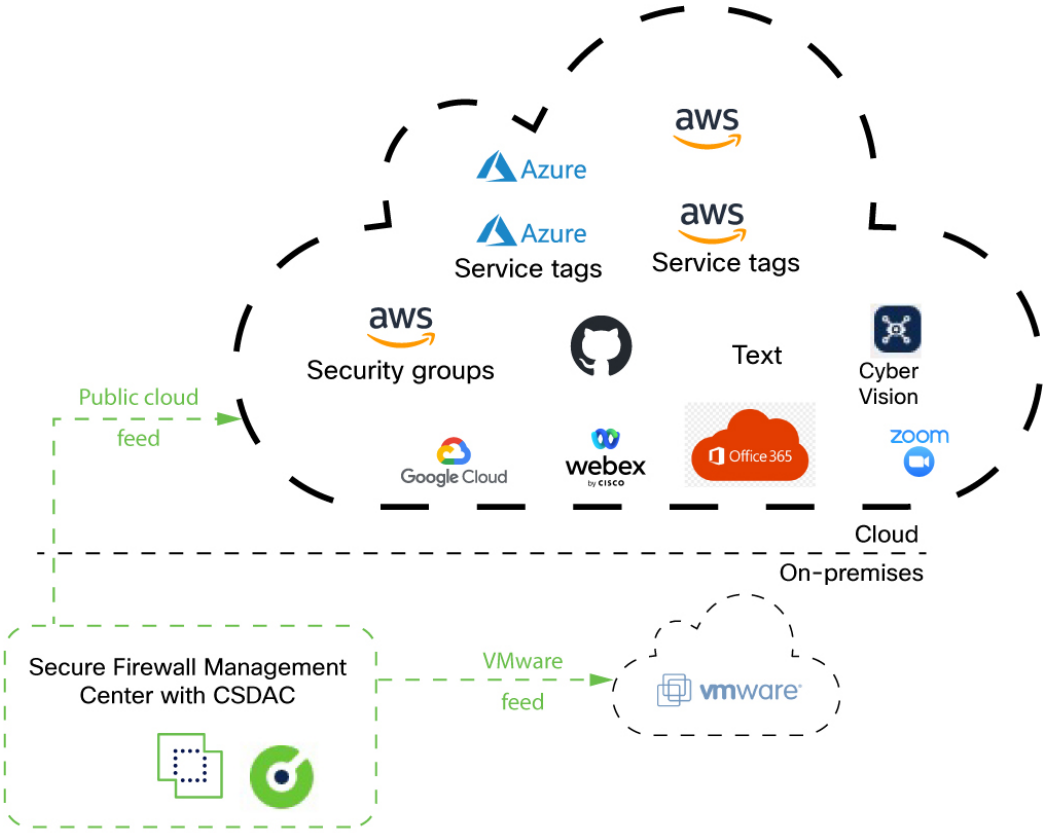
相关主题

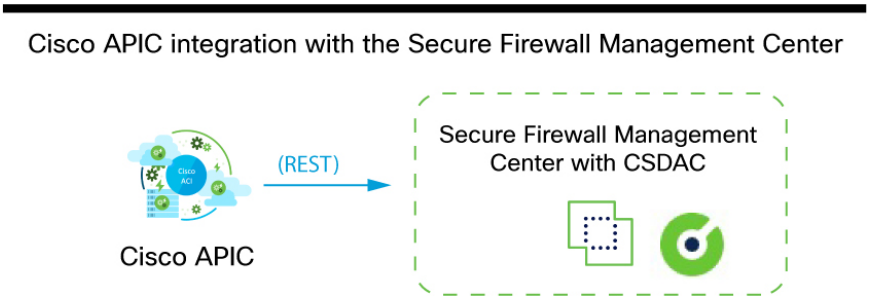
- 启用 dynamic attributes connector
- 关于控制面板， 第 9 页

网络下载模式

dynamic attributes connector一直在网络下载模式下运行，我们需要从互联网下载其工作所需的映像。如果您有更严格的安全要求，可以考虑气隙模式。

架构概述：





网络下载模式支持：

表 *1:* 按 ***dynamic attributes connector*** 版本和 平台列出的受支持连接器列表

CSDAC 版本	**AWS**	**AWS** 安全组	**AWS** 服务标记	**Azure**	**Azure** 服务标签	思科 **APIC**	**Cisco Cyber Vision**	思科多集群 **Defense**	通用文本	**GitHub**	**Google Cloud**	**Microsoft Office 365**	**Tenable**	**vCenter**	**Webex**	**Zoom**
版本 1.1（本地）	支持	否	否	支持	支持	否	否	否	否	否	否	支持	否	支持	否	否
版本 2.0（本地）	支持	否	否	支持	支持	否	否	否	否	否	支持	支持	否	支持	否	否
版本 2.2（本地）	支持	否	否	支持	支持	否	否	否	否	支持	支持	支持	否	支持	否	否
版本 2.3（本地）	支持	否	否	支持	支持	否	否	否	否	支持	支持	支持	否	支持	支持	支持
版本 3.0（本地）	支持	支持	支持	支持	支持	否	支持	否	支持	支持	支持	支持	否	支持	支持	支持
版本 3.1（本地）	支持	支持	支持	支持	支持	支持	支持	支持	支持	支持	支持	支持	否	支持	支持	支持
云交付 (Security Cloud Control)	支持	否	否	支持	支持	否	否	支持	否	支持	支持	支持	支持	否	否	否
Secure Firewall Management Center 7.4.1	支持	否	否	支持	支持	否	否	否	支持	支持	支持	支持	否	支持	支持	支持
Secure Firewall Management Center 7.6	支持	支持	支持	支持	支持	否	支持	否	支持	支持	支持	支持	否	支持	支持	支持
Secure Firewall Management Center 7.7	支持	支持	支持	支持	支持	否	支持	否	支持	支持	支持	支持	否	支持	支持	支持
Secure Firewall Management Center 10.0.0	支持	支持	支持	支持	支持	支持	支持	否	支持	支持	支持	支持	否	支持	支持	支持

dynamic attributes connector 的历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
DNS规则对动态对象和安全组标记的支持。	10.0.0	10.0.0	您可以在 DNS 策略中配置 DNS 规则以使用动态对象或安全组标记 (SGT)。如果您已经在访问控制规则中使用这些类型的对象，现在可以将其使用扩展到您的 DNS 策略。 我们在添加/编辑 DNS 规则对话框中添加了“动态属性”选项卡。
动态防火墙	10.0.0	10.0.0	以前，Secure Firewall Management CenterSecure Firewall Management Center 仅从配置的身份源（如 Microsoft Active Directory、被动身份代理、思科身份服务引擎 (Cisco ISE) 等）收集有关用户的信息。此信息通常包括用户名、组和 IP 地址。 借助 动态防火墙，您可以将来自思科 身份情报 的用户风险评分添加到身份源提供的信息中，以便根据始终最新的用户终端安全评估和风险设置策略。我们支持您将用户身份与智能配对，并在报告和访问控制策略中使用该信息。 **新增/修改的屏幕：** • 请点击 **集成** > **动态属性连接器**。然后点击身份源名称旁的  ，点击**创建动态防火墙**。
思科 APIC 连接器	10.0.0	10.0.0	dynamic attributes connector 使您能够将 思科 APIC 动态终端组 (EPG) 和终端安全组 (ESG) 数据从 思科 APIC 租户发送到 。 **新增/更新的屏幕：** • **集成** > **动态属性连接器** > **连接器** > **新建连接器**
新连接器	7.6	20241127	AWS 安全组、AWS 服务标签和 Cisco Cyber Vision 这些连接器可以像 Security Cloud Control 一样发送本地 Secure Firewall Management Center 动态对象。 要从本地 dynamic attributes connector 接收动态对象，需要使用 3.0 版本的本地动态属性连接器。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
Dynamic Attributes Connector	7.4.0	7.4.0	引入了此功能。 Dynamic Attributes Connector 现在包含在 Secure Firewall Management Center中。您可以在访问控制规则中使用 dynamic attributes connector 从基于云的平台（例如 Microsoft Azure）获取 IP 地址，而无需部署到托管设备。 详细信息： • 此产品随附的 dynamic attributes connector： 关于 dynamic attributes connector，第 1 页 • 独立 dynamic attributes connector： 《*Cisco Secure Dynamic Attributes Connector* 配置指南》 新的/修改后的屏幕： **集成 > 动态属性连接器**

Dynamic Attributes Connector 的系统要求

Dynamic Attributes Connector 具有以下内存要求：

FMCv：RAM 大小	Secure Firewall Management Center 硬件型号	最大数量（连接器 + Azure AD 领域）
至少 32 GB	Firepower 1000、Firepower 1600、vFMC	10
至少 64 GB	Firepower 2500、Firepower 2600、vFMC 300	20
至少 128 GB	Firepower 4500、Firepower 4600	30

上述限制适用于虚拟机和物理机。

系统会阻止您超出这些限制，以避免部署问题。

启用 dynamic attributes connector

此任务讨论如何在 Secure Firewall Management Center启用 dynamic attributes connector 。 dynamic attributes connector是一种集成，它使得来自云网络产品的对象能够用于Secure Firewall Management Center访问控制和 DNS 规则。

过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center 。

步骤 2 请点击 **集成** > **动态属性连接器**。

步骤 3 滑动到**已启用 (Enabled)**。

步骤 4 启用 dynamic attributes connector 时，系统会显示消息。

如果出现错误，请重试。如果错误仍然存在，请联系思科 TAC。

下一步做什么

请参阅创建连接器 ， 第 16 页。

相关主题

关于 动态防火墙 ， 第 63 页
如何配置 动态防火墙 ， 第 63 页

为 Docker 容器配置网络和子网

Dynamic Attributes Connector 使用 Docker 容器检索 Secure Firewall Management Center中的连接器数据。为避免与网络中使用的 Secure Firewall Management Center 管理接口和其他 IP 地址冲突，您可以选择使用本节中讨论的 命令来更改 Docker IP 地址和范围。

关于 Docker 网络

dynamic attributes connector 使用 Docker 守护程序需要以下网络：

- Docker 后台守护程序在内部使用的`docker0` 。
- 一系列名为 `veth`*`number`*的 IPv6 网络。

  这些是 dynamic attributes connector使用的内部网桥网络。
- dynamic attributes connector 连接器使用的 Docker 网桥网络，名为 `br-`*`number`*。

在启用 dynamic attributes connector 之前，只有一个名为 `Docker0` 的 Docker 接口，设置为 172.18.0.1/16（对于 Cisco Secure Firewall Management Center Virtual；本地管理器使用不同的 IP 地址范围）。示例部分的表格提供了详细信息。

更改 Docker 网络和子网

首先启用 dynamic attributes connector，如 启用 dynamic attributes connector中所述。

要更改 Docker 网络和子网，请以具有 `root` 权限的用户身份运行 `/usr/local/sf/bin/change_docker_subnet.sh -b` *`CIDR-network`*`-s` *`address-pool-size`* ，其中：

- `-b CIDR-network` 以 CIDR 表示法设置网络基址池。
- `-s address-pool-size` 设置网络基址的网络掩码。如果网络范围与现有网络范围重叠，可以使用此选项限制基址范围内的地址数量；特别是，我们建议 Secure Firewall Management Center 型号的某些 `-s` 值，以确保不会超过计算机中的可用 RAM。（Docker 容器由 dynamic attributes connector 连接器使用，这些限制显示在 Dynamic Attributes Connector 的系统要求，第 6 页中。）

重要事项 分配给 Docker 的网络必须在内部网络范围内，并且 不得 与 Secure Firewall Management Center 或内部网络中的其他设备使用的网络冲突。

示例

下表显示示例。

Secure Firewall Management Center 型号	推荐 **-s** 值	示例 **-b** 值	**Dynamic Attributes Connector** 使用的容器地址
Firepower 1000、Firepower 1600、vFMC	27（子网掩码 255.255.255.224）	172.19.0.0/16	30 个 IP 地址 `docker0`: 172.19.0.1 网桥网络 `br-编号` 网关 `172.19.0.33`，子网 为 `172.19.0.32/27` 在 `172.19.0.38/27`、`172.19.0.39/27`等网络中创建的连接器
Firepower 2500、Firepower 2600、vFMC 300	26（子网掩码 255.255.255.192）	192.168.0.0/16	62 个 IP 地址 `docker0`: 192.168.1.1 网桥网络 `br-编号` 网关 `192.168.1.65`，子网为 `192.168.1.64/26` 在 `192.168.1.71/26`、`192.168.1.72/26`等网络中创建的连接器
Firepower 4500、Firepower 4600	25（子网掩码 255.255.255.128）	192.168.0.0/16	126 个 IP 地址 `docker0`: 192.168.1.1 网桥网络 `br-编号` 网关 `192.168.1.129`，子网为 `192.168.1.128/25` 在 `192.168.1.136/25`、 `192.168.1.135/25` 等网络中创建的连接器

作为参考，完整的命令如下：

```
sudo /usr/local/sf/bin/change_docker_subnet.sh -b 172.19.0.0/16 -s 27
sudo /usr/local/sf/bin/change_docker_subnet.sh -b 192.168.0.0/16 -s 26
sudo /usr/local/sf/bin/change_docker_subnet.sh -b 192.168.0.0/16 -s 25
```

检验网络

要验证网络设置，请输入 `sudo docker network inspect muster-net`。命令结果以 JSON 格式显示。

故障排除

以下是使用此命令可能遇到的常见错误的一些解决方案。

错误： `拉取子网值不能大于大小`

解决方案：更改 `-s` 的值，使其小于 CIDR 网络值。

例如，

错误： `sudo /usr/local/sf/bin/change_docker_subnet.sh -b 172.19.0.0/16 -s 8`

正确： `sudo /usr/local/sf/bin/change_docker_subnet.sh -b 172.19.0.0/16 -s 20`

错误：运行命令后，Docker 网络错误。

解决方案：重新启动 Docker 后台守护程序： `sudo pmtool restartbyid docker`

错误： `无法连接到位于 unix:///var/run/docker.sock 的 Docker 后台守护程序。Docker 守护程序是否正在运行？`

解决方案：重新启动 Docker： `pmtool restartbyid docker`

错误：输入不能为空

`-s` 需要此参数。

错误： `提取大小 - 32 - 不能大于 32 或小于 0`

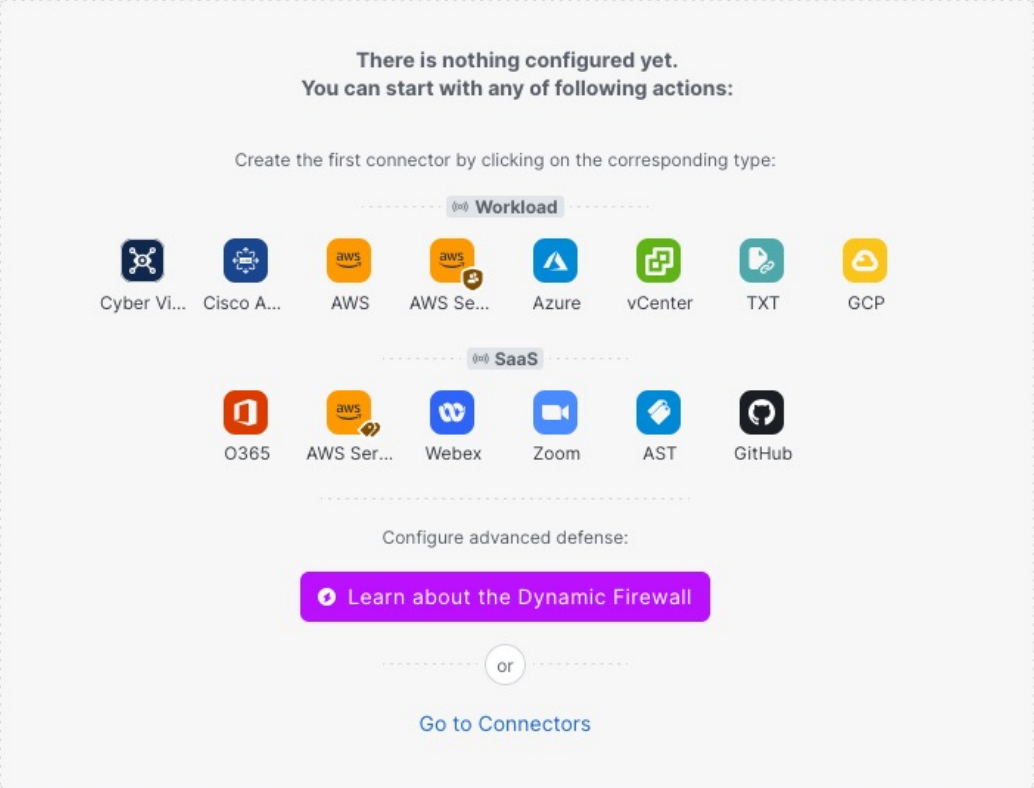
解决方案：更改 `-s` 的值，使其大于 0 且小于 32。

关于控制面板

要访问 dynamic attributes connector 控制面板，请登录 Cisco Secure Firewall 管理器并点击页面顶部的**集成 > 动态属性连接器**。

如果 dynamic attributes connector 未启用，请移动滑块将其启用。此过程需要几分钟时间才能完成。

dynamic attributes connector 控制面板页面会显示连接器、适配器和过滤器的状态。以下是未配置系统的控制面板示例：



您可以通过控制面板来执行的操作包括：

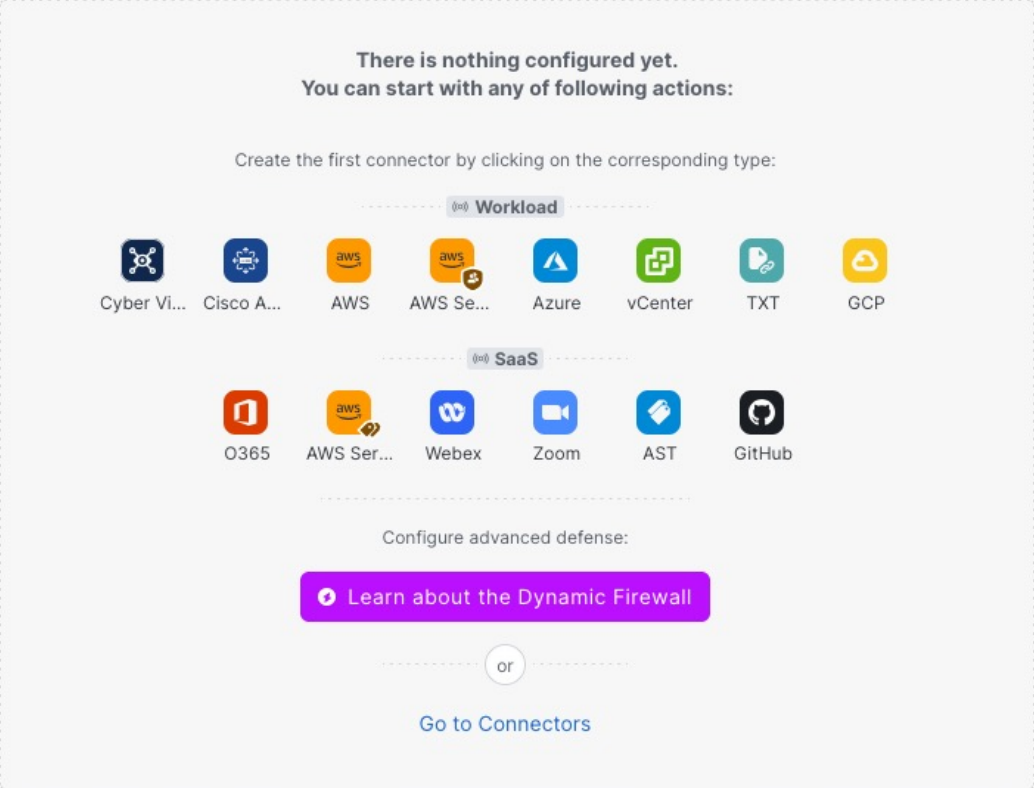
- 添加、编辑和删除连接器和动态属性过滤器。
- 了解连接器和动态属性过滤器之间的关系。
- 查看警告和错误。

相关主题

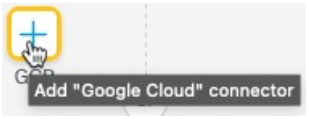
- 未配置系统的控制面板， 第 10 页
- 已配置系统的控制面板， 第 11 页
- 添加、编辑或删除连接器， 第 13 页
- 添加、编辑或删除动态属性过滤器， 第 14 页

未配置系统的控制面板

未配置系统的 dynamic attributes connector 控制面板页面示例：



控制面板最初显示您可以为系统配置的所有类型的连接器。您可以执行以下任何操作：

- 将鼠标指针悬停在连接器上，然后点击 

新建一个。
- 点击**转到连接器 (Go to Connectors)** 以添加、编辑或删除连接器（适用于同时创建、编辑或删除多个连接器）。

  有关详细信息，请参阅创建连接器，第 16 页。

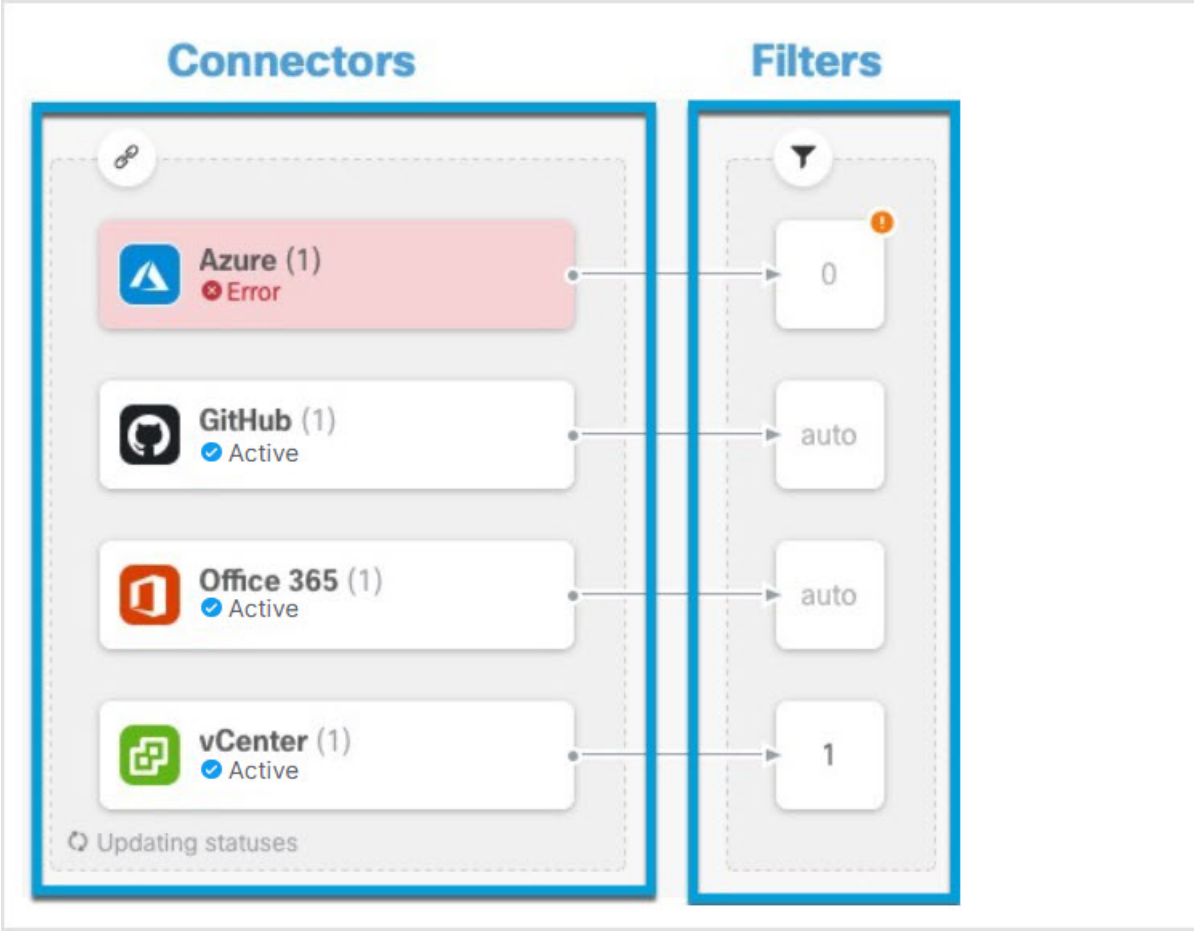
相关主题

- 已配置系统的控制面板，第 11 页
- 添加、编辑或删除连接器，第 13 页
- 添加、编辑或删除动态属性过滤器，第 14 页

已配置系统的控制面板

已配置系统的 dynamic attributes connector 控制面板页面示例：

点击图中的某个区域以了解详细信息，或点击该图后面的链接之一。



1 创建连接器， 第 16 页
2 创建动态属性过滤器

控制面板显示以下内容（从左到右）：

“连接器”(Connectors) 列	“过滤器”(Filters) 列
连接器列表，其中包含指示每种类型的配置数量的编号。连接器会收集可以发送到 Cisco Secure Firewall 管理器的动态属性。动态属性过滤器会指定要发送的数据。 点击 以查看有关所有已配置连接器的详细信息。您还可以点击连接器的名称来添加、编辑或删除连接器；或者查看有关它们的详细信息。有关详细信息，请参阅添加、编辑或删除连接器， 第 13 页。	与每个连接器关联的动态属性过滤器列表，其中带有一个数字，表示每个过滤器与连接器关联的数量。 点击 以查看有关所有已配置过滤器的详细信息。您还可以点击过滤器的名称来添加、编辑或删除过滤器；或者查看有关它们的详细信息。有关详细信息，请参阅添加、编辑或删除动态属性过滤器， 第 14 页。

注释 某些连接器（例如 Outlook 365 和 Azure 服务标记）会自动提取可用的动态对象，而无需使用动态属性过滤器。这些连接器在 列中显示为**自动 (Auto)**。

控制面板会指明对象是否可用。控制面板页面会每 15 秒刷新一次，但您可以随时点击页面顶部的**刷新** （ ） 来立即刷新。如果问题仍然存在，请检查网络连接。

相关主题

- 添加、编辑或删除连接器 ， 第 13 页
- 添加、编辑或删除动态属性过滤器 ， 第 14 页

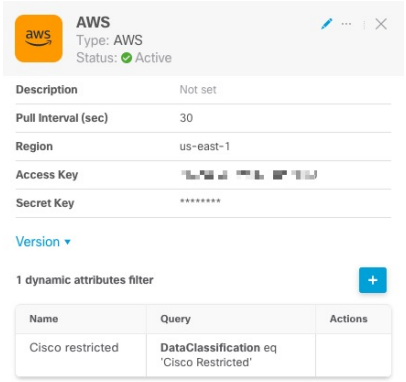
添加、编辑或删除连接器

通过控制面板，您可以查看或编辑连接器。您可以点击连接器的名称以查看该连接器的所有实例，

也可以点击 以查看以下其他选项：

- **转到连接器**可同时查看所有连接器；您可以在此处添加、编辑和删除连接器。
- **添加连接器 (Add Connector)** > **类型**以添加指定类型的连接器。

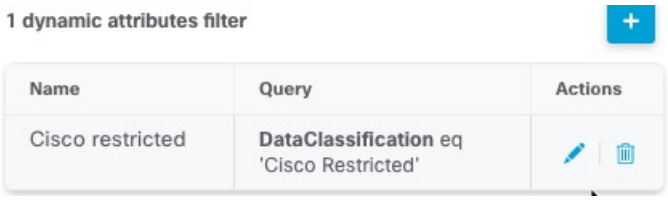
点击连接器列 ( ) 中的任意连接器可显示更多相关信息；示例如下：



您有以下选择：

- 点击 编辑图标 （ ） 以编辑此连接器。
- 点击 更多图标 （ ） 以查看其他选项。
- 点击 关闭面板。
- 点击 **版本**以显示版本。如果思科 TAC 需要，您可以选择将版本复制到剪贴板。

通过面板底部的表格，您可以添加动态属性过滤器；或编辑或 dynamic attributes connector 删除连接器。示例如下：



点击 添加图标 （ ） 以便为此连接器添加动态属性过滤器。有关详细信息，请参阅创建动态属性过滤器。

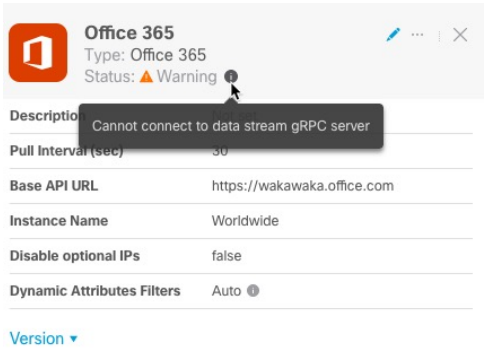
将鼠标指针悬停在“操作”(Actions) 列上，以编辑或删除指示的连接器。

查看错误信息

要查看连接器的错误信息，请执行以下操作：

1. 在控制面板上，点击显示错误的连接器的名称。
2. 在右侧窗格中，点击 **信息** （ ）。

   示例如下。



3. 要解决此问题，请按照创建 Office 365 连接器 ，第 44 页中所述编辑连接器设置。
4. 如果您无法解决问题，请点击**版本 (Version)** 并将版本复制到文本文件。
5. 向思科 TAC 提供所有这些信息。https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

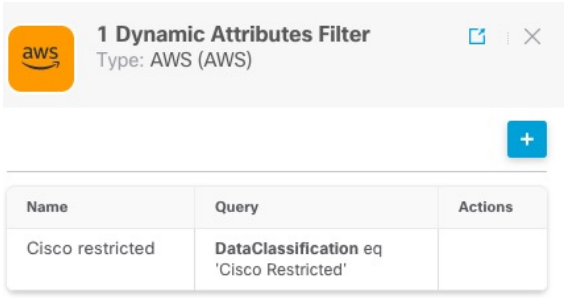
添加、编辑或删除动态属性过滤器

控制面板让您能够添加、编辑或删除动态属性过滤器。您可以点击过滤器的名称以查看该过滤器的所有实例，也可以点击 以查看下列附加选项：

- **转至动态属性过滤器** 以查看所有已配置的动态属性过滤器。您可以从这里添加、编辑或删除动态属性过滤器。
- **添加动态属性过滤器**以添加过滤器。

有关添加动态属性过滤器的详细信息，请参阅创建动态属性过滤器。

如下所示：



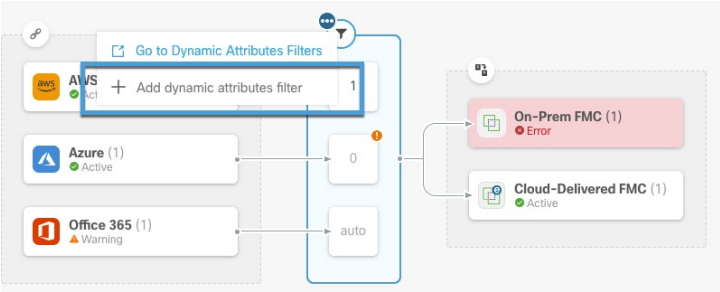
注释 某些连接器（例如 Outlook 365 和 Azure 服务标记）会自动提取可用的动态对象，而无需使用动态属性过滤器。这些连接器在 列中显示为**自动 (Auto)**。

您有以下选择：

- 点击过滤器实例可查看与连接器关联的动态属性过滤器的摘要信息。
- 点击 添加图标 （ ） 以添加新的动态属性过滤器。

  有关详细信息，请参阅创建动态属性过滤器。
- 在表示指明的连接器没有关联的动态属性过滤器的过滤器列 ( ) 中点击 。如果没有关联的过滤器，连接器将无法向 防火墙管理中心 发送任何内容。

  解决此问题的一种方法是点击过滤器列中的 ，然后点击**添加动态属性过滤器 (Add Dynamic Attributes Filter)**。示例如下。



- 点击 以添加、编辑或删除过滤器。

- 点击 × 关闭面板。

创建连接器

连接器是云服务的接口。连接器从云服务检索网络信息，以便网络信息可用于 Secure Firewall Management Center上的策略。

我们支持以下内容：

*表 2: 按 **dynamic attributes connector** 版本和 平台列出的受支持连接器列表*

CSDAC 版本	AWS	AWS 安全组	AWS 服务标记	Azure	Azure 服务标签	思科 APIC	Cisco Cyber Vision	思科多集群 Defense	通用文本	GitHub	Google Cloud	Microsoft Office 365	Tenable	vCenter	Webex	Zoom
版本 1.1（本地）	支持	否	否	支持	支持	否	否	否	否	否	否	支持	否	支持	否	否
版本 2.0（本地）	支持	否	否	支持	支持	否	否	否	否	否	支持	支持	否	支持	否	否
版本 2.2（本地）	支持	否	否	支持	支持	否	否	否	否	支持	支持	支持	否	支持	否	否
版本 2.3（本地）	支持	否	否	支持	支持	否	否	否	否	支持	支持	支持	否	支持	支持	支持
版本 3.0（本地）	支持	支持	支持	支持	支持	否	支持	否	支持	支持	支持	支持	否	支持	支持	支持
版本 3.1（本地）	支持	支持	支持	支持	支持	支持	支持	支持	支持	支持	支持	支持	否	支持	支持	支持
云交付 (Security Cloud Control)	支持	否	否	支持	支持	否	否	支持	否	支持	支持	支持	支持	否	否	否
Secure Firewall Management Center 7.4.1	支持	否	否	支持	支持	否	否	否	支持	支持	支持	支持	否	支持	支持	支持
Secure Firewall Management Center 7.6	支持	支持	支持	支持	支持	否	支持	否	支持	支持	支持	支持	否	支持	支持	支持
Secure Firewall Management Center 7.7	支持	支持	支持	支持	支持	否	支持	否	支持	支持	支持	支持	否	支持	支持	支持
Secure Firewall Management Center 10.0.0	支持	支持	支持	支持	支持	支持	支持	否	支持	支持	支持	支持	否	支持	支持	支持

Amazon Web Services 连接器 — 关于用户权限和导入的数据

dynamic attributes connector 会将动态属性从 AWS 导入 Secure Firewall Management Center，以便用于策略。

动态属性已导入

我们从 AWS 导入以下动态属性：

- 标签，可用于组织 AWS EC2 资源的用户定义的键值对。

  有关更多信息，请参阅 AWS 文档中的 标记 EC2 资源

- AWS 中虚拟机的 *IP* 地址。

所需的最低权限

dynamic attributes connector 要求用户至少具有允许 `ec2:DescribeTags`、`ec2:DescribeVpcs` 和 `ec2:DescribeInstances` 以便能够导入动态属性的策略。

为 dynamic attributes connector 创建具有最小权限的 AWS 用户

此任务讨论如何设置具有最低权限的服务帐户，以向 Secure Firewall Management Center 发送动态属性。有关这些属性的列表，请参阅 Amazon Web Services 连接器 — 关于用户权限和导入的数据，第 17 页。

开始之前

您必须已设置 Amazon Web 服务 (AWS) 帐户。有关执行此操作的更多信息，请参阅 AWS 文档中的此文章。

过程

步骤 1 以具有网络管理员角色的用户身份登录 AWS 控制台。

步骤 2 在控制面板中，点击**安全、身份和合规性 (Security, Identity & Compliance)** > **IAM**。

步骤 3 点击**访问管理 (Access Management)** > **用户 (Users)**。

步骤 4 点击**添加用户 (Add Users)**。

步骤 5 在**用户名 (User Name)** 字段中，输入用于标识用户的名称。

步骤 6 点击**访问密钥 - 编程访问 (Access Key - Programmatic Access)**。

步骤 7 在“设置权限”(Set permissions) 页面中，点击**下一步 (Next)** 而不授予用户任何访问权限；稍后执行此操作。可以稍后授予用户访问权限。

步骤 8 如果需要，向用户添加标签。

步骤 9 点击**创建用户**。

步骤 10 点击 **Download.csv**，将用户的密钥下载到计算机。

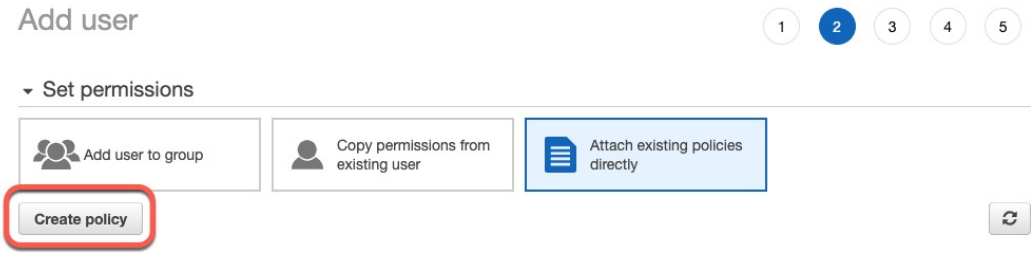
注释
这是您检索用户密钥的唯一机会。

步骤 11 点击**关闭 (Close)**。

步骤 12 在身份和访问管理 (IAM) 页面的左侧列中，点击**访问管理 (Access Management)** > **策略 (Policies)**。

步骤 13 点击**创建策略 (Create Policy)**。

步骤 14 在“创建策略”(Create Policy) 页面中，点击 **JSON**。



步骤 15 在字段中输入以下策略：

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeTags",
    "ec2:DescribeInstances",
    "ec2:DescribeVpcs"
   ],
   "Resource": "*"
  }
 ]
}
```

步骤 16 点击**下一步 (Next)**。

步骤 17 点击**审核 (Review)**。

步骤 18 在“查看策略”(Review Policy) 页面中输入请求的信息，然后点击**创建策略 (Create Policy)**。

步骤 19 在“策略”(Policies) 页面上，在搜索字段中输入全部或部分策略名称，然后按 Enter 键。

步骤 20 点击您刚刚创建的策略。

步骤 21 点击**操作 (Actions)** > **附加 (Attach)**。

步骤 22 如有必要，请在搜索字段中输入全部或部分用户名，然后按 Enter 键。

步骤 23 点击**附加策略 (Attach Policy)**。

下一步做什么

创建 AWS 连接器， 第 19 页。

创建 AWS 连接器

此任务讨论如何配置将数据从 AWS 发送到 Secure Firewall Management Center 以用于访策略的连接器。

开始之前

创建至少具有为 dynamic attributes connector 创建具有最小权限的 AWS 用户，第 17 页中所述权限的用户。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标（  ），然后点击连接器名称。
- 编辑或删除连接器：点击**更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
提取间隔	（默认为 30 秒。）从 AWS 检索 IP 映射的间隔。
地区	（必需。）输入您的 AWS 区域代码。
访问密钥	（必需。）输入访问密钥。
加密密钥	（必需。）输入加密密钥。

步骤 5 点击**保存**。

步骤 6 确保“状态”(Status) 列中显示**确定**。

Amazon Web 服务安全组连接器 - 关于用户权限

dynamic attributes connector 会将动态属性从 AWS 导入 Secure Firewall Management Center，以便用于策略。

所需的最低权限

dynamic attributes connector 要求用户至少具有允许 `ec2:DescribeTags`、`ec2:DescribeVpcs` 和 `ec2:DescribeInstances` 以便能够导入动态属性的策略。

为 dynamic attributes connector 创建具有最小权限的 AWS 用户

此任务讨论如何设置具有最低权限的服务帐户，以向 Secure Firewall Management Center 发送动态属性。有关这些属性的列表，请参阅 Amazon Web Services 连接器 — 关于用户权限和导入的数据，第 17 页。

开始之前

您必须已设置 Amazon Web 服务 (AWS) 帐户。有关执行此操作的更多信息，请参阅 AWS 文档中的此文章。

过程

步骤 1 以具有网络管理员角色的用户身份登录 AWS 控制台。

步骤 2 在控制面板中，点击**安全、身份和合规性 (Security, Identity & Compliance)** > **IAM**。

步骤 3 点击**访问管理 (Access Management)** > **用户 (Users)**。

步骤 4 点击**添加用户 (Add Users)**。

步骤 5 在**用户名 (User Name)** 字段中，输入用于标识用户的名称。

步骤 6 点击**访问密钥 - 编程访问 (Access Key - Programmatic Access)**。

步骤 7 在“设置权限”(Set permissions) 页面中，点击**下一步 (Next)** 而不授予用户任何访问权限；稍后执行此操作。可以稍后授予用户访问权限。

步骤 8 如果需要，向用户添加标签。

步骤 9 点击**创建用户**。

步骤 10 点击 **Download.csv**，将用户的密钥下载到计算机。

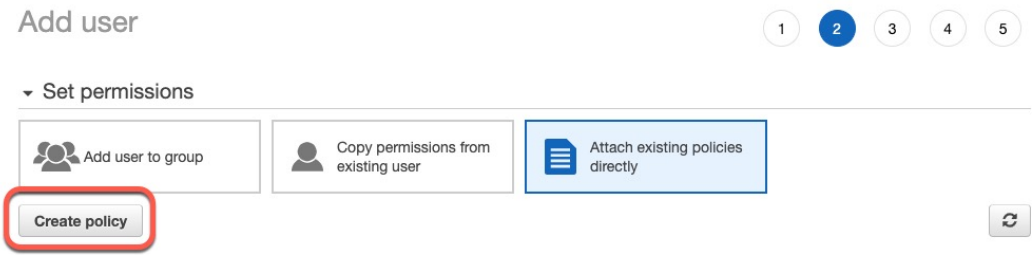
注释
这是您检索用户密钥的唯一机会。

步骤 11 点击**关闭 (Close)**。

步骤 12 在身份和访问管理 (IAM) 页面的左侧列中，点击**访问管理 (Access Management)** > **策略 (Policies)**。

步骤 13 点击**创建策略 (Create Policy)**。

步骤 14 在“创建策略”(Create Policy) 页面中，点击 **JSON**。



步骤 15 在字段中输入以下策略：

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeTags",
    "ec2:DescribeInstances",
    "ec2:DescribeVpcs"
   ],
   "Resource": "*"
  }
 ]
}
```

步骤 16 点击**下一步 (Next)**。

步骤 17 点击**审核 (Review)**。

步骤 18 在“查看策略”(Review Policy) 页面中输入请求的信息，然后点击**创建策略 (Create Policy)**。

步骤 19 在“策略”(Policies) 页面上，在搜索字段中输入全部或部分策略名称，然后按 Enter 键。

步骤 20 点击您刚刚创建的策略。

步骤 21 点击**操作 (Actions)** > **附加 (Attach)**。

步骤 22 如有必要，请在搜索字段中输入全部或部分用户名，然后按 Enter 键。

步骤 23 点击**附加策略 (Attach Policy)**。

下一步做什么

创建 AWS 连接器，第 19 页。

创建 AWS 安全组连接器

本任务讨论如何配置将 AWS 安全组数据发送到 Secure Firewall Management Center 以在策略中使用的连接器。

开始之前

执行以下所有操作：

- 按照 AWS 文档站点上的 使用安全组 中的说明创建 AWS 安全组。

- 创建至少具有为 dynamic attributes connector 创建具有最小权限的 AWS 用户，第 17 页中所述权限的用户。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （  ），然后点击连接器名称。
- 编辑或删除连接器：点击**更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
提取间隔	（默认为 30 秒。）从 AWS 检索 IP 映射的间隔。 最小**拉取间隔时间 (Pull Interval)** 值为 1 秒。您可以将最大值设置为任何想要的值。我们建议不要将最小值设得太低，因为这会产生大量流量，而且在适用情况下，可能会导致您为流量付费。
地区	（必需。）输入您的 AWS 区域代码。
AWS 访问密钥	（必需。）输入访问密钥。
AWS 加密密钥	（必需。）输入加密密钥。

步骤 5 点击**保存**。

步骤 6 确保“状态”(Status) 列中显示**确定**。

创建 AWS 服务标签连接器

本主题讨论了如何为 Amazon Web 服务 (AWS) 标签创建到 Secure Firewall Management Center 的连接器，以供在策略中使用。

有关详细信息，请参阅 AWS 文档网站上的以下资源：

- 什么是标签？
- AWS IP 地址范围
- 标记 AWS 资源
- AWS 上的标记指南
- AWS 服务点

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （  ），然后点击连接器名称。
- 编辑或删除连接器：点击**更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
URL	（必需。）除非建议，否则请勿更改URL。

步骤 5 点击**保存**。

步骤 6 确保“状态”(Status) 列中显示**确定**。

Azure 连接器 - 关于用户权限和导入的数据

dynamic attributes connector 会将动态属性从 Azure 导入 Secure Firewall Management Center，以便用于策略。

动态属性已导入

我们从 Azure 导入以下动态属性：

- 标签，与资源、资源组和订用关联的键值对。

有关详细信息，请参阅 Microsoft 文档中的本页面。

- Azure 中虚拟机的 *IP* 地址。

所需的最低权限

dynamic attributes connector 要求至少具有**读者 (Reader)** 权限的用户才能导入动态属性。

创建对 dynamic attributes connector 具有最小权限的 Azure 用户

此任务讨论如何设置具有最低权限的服务帐户，以向 Secure Firewall Management Center 发送动态属性。有关这些属性的列表，请参阅 Azure 连接器 - 关于用户权限和导入的数据，第 23 页。

开始之前

您必须已经拥有 Microsoft Azure 帐户。要进行设置，请参阅 Azure 文档站点上的本页面。

过程

步骤 1 以订用所有者的身份登录到 Azure 门户 。

步骤 2 点击 **Azure Active Directory**。

步骤 3 查找要设置的应用的 Azure Active Directory 实例。

步骤 4 点击**添加 (Add)** > **应用注册 (App registration)**。

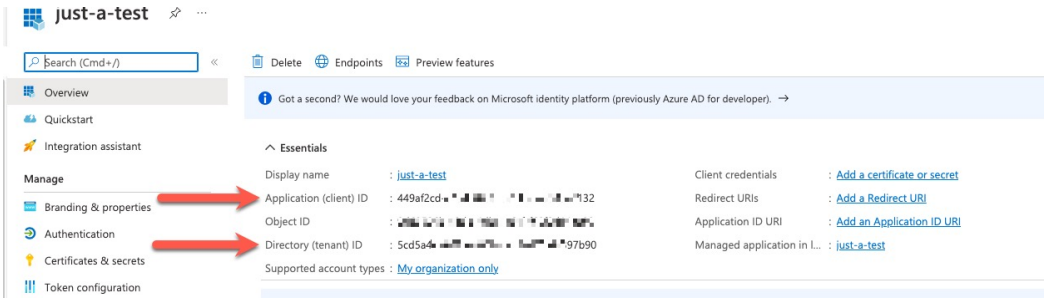
步骤 5 在 **名称 (Name)** 字段中，输入用于标识此应用的名称。

步骤 6 在此页面上输入贵组织所要求的其他信息。

步骤 7 点击**注册 (Register)**。

步骤 8 在下一页上，写下或复制客户端 ID（也称为应用 *ID*）和租户 ID（也称为目录 *ID*）。

示例如下。

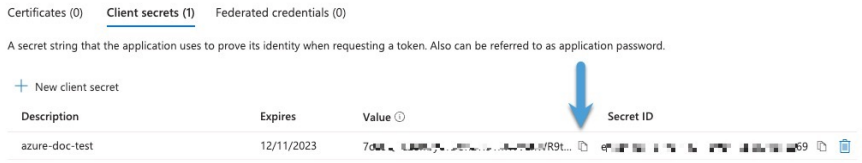


步骤 9 点击客户端凭证旁边的 **添加证书或密钥**。

步骤 10 点击**新建客户端密钥 (New Client Secret)**。

步骤 11 输入请求的信息，然后点击**添加 (Add)**。

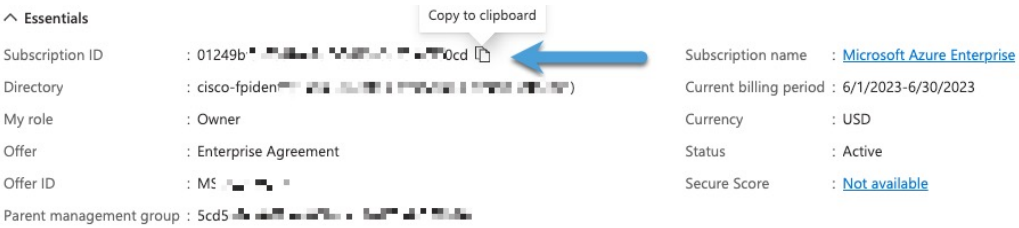
步骤 12 将 **值** 字段的值复制到剪贴板。此值是客户端密钥， 而不是 **密钥** ***ID***。



步骤 13 返回到 Azure 门户主页面，然后点击**订用 (Subscriptions)**。

步骤 14 点击您的订用的名称。

步骤 15 将订用 ID 复制到剪贴板。



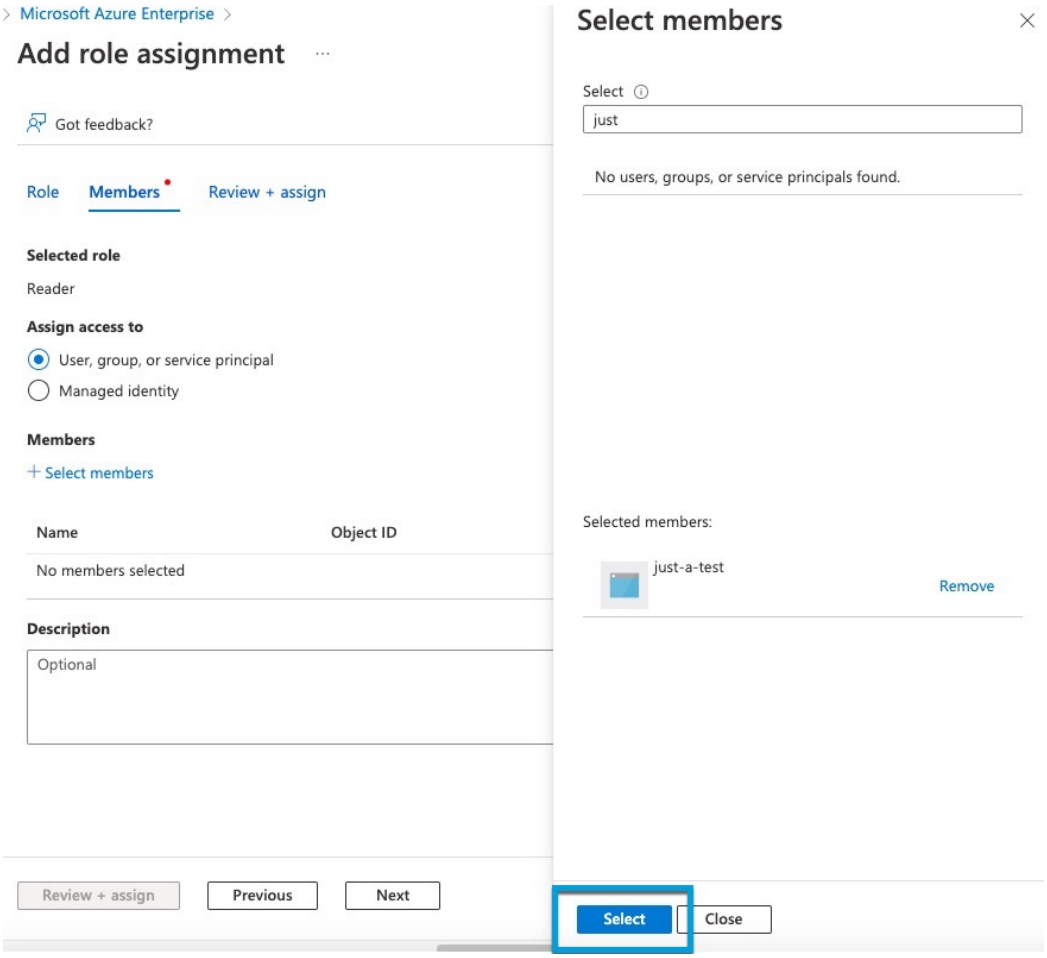
步骤 16 点击**访问控制 (IAM) (Access Control [IAM])**。

步骤 17 点击**添加 (Add)** > **添加角色分配 (Add role assignment)**。

步骤 18 点击**读者 (Reader)**，然后点击**下一步 (Next)**。

步骤 19 点击**选择成员 (Select Members)**。

步骤 20 在页面右侧，点击您注册的应用的名称，然后点击**选择 (Select)**。



步骤 21 点击查看 + 分配 **(Review + Assign)**，然后按照提示完成操作。

下一步做什么

请参阅创建 Azure 连接器， 第 26 页。

创建 Azure 连接器

此任务讨论如何创建从 Azure 向 Secure Firewall Management Center 发送数据的连接器，以用于策略中。

开始之前

创建至少具有 创建对 dynamic attributes connector 具有最小权限的 Azure 用户， 第 24 页 中所述权限的 Azure 用户。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （  ），然后点击连接器名称。
- 编辑或删除连接器：点击**更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
提取间隔	（默认为 30 秒。）从 Azure 检索 IP 映射的间隔。 最小**拉取间隔时间 (Pull Interval)** 值为 1 秒。您可以将最大值设置为任何想要的值。我们建议不要将最小值设得太低，因为这会产生大量流量，而且在适用情况下，可能会导致您为流量付费。
订用 ID	（必需。）输入 Azure 订用 ID。
租户 ID	（必需。）输入租户 ID。
客户端 ID	（必需。）输入您的客户端 ID。
客户端密钥	（必需。）输入您的客户端密钥。

步骤 5 点击**保存**。

步骤 6 确保“状态”(Status) 列中显示**确定**。

创建 Azure 服务标签连接器

本主题讨论了如何为 Azure 服务标签创建到 Secure Firewall Management Center 的连接器，以供在策略中使用。Microsoft 会每周更新与这些标记的 IP 地址关联。

有关详细信息，请参阅 Microsoft TechNet 上的虚拟网络服务标签。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （  ），然后点击连接器名称。
- 编辑或删除连接器：点击**更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
提取间隔	（默认为 30 秒。）从 Azure 检索 IP 映射的间隔。 最小**拉取间隔时间 (Pull Interval)** 值为 1 秒。您可以将最大值设置为任何想要的值。我们建议不要将最小值设得太低，因为这会产生大量流量，而且在适用情况下，可能会导致您为流量付费。
订用 ID	（必需。）输入 Azure 订用 ID。
租户 ID	（必需。）输入租户 ID。
客户端 ID	（必需。）输入您的客户端 ID。
客户端密钥	（必需。）输入您的客户端密钥。

步骤 5 点击**保存**。

步骤 6 确保“状态”(Status) 列中显示**确定**。

思科 APIC 连接器

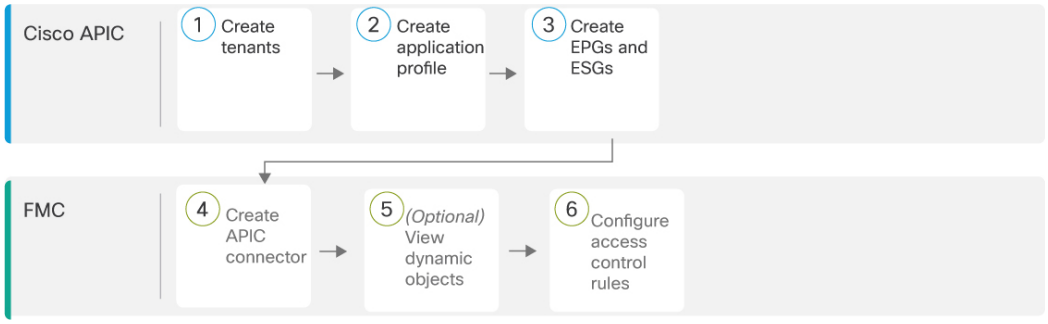
以下主题讨论如何配置 思科 APIC 与 Secure Firewall Management Center 的集成。

相关主题

与 思科 APIC 集成的系统要求， 第 30 页
获取集成所需的信息， 第 30 页
创建连接器思科 APIC， 第 34 页

如何在访问控制规则或 DNS 规则中使用 Secure Firewall Management Center 中 思科 APIC 的动态对象，第 29 页
手动获取证书颁发机构 (CA) 链，第 35 页

如何在访问控制规则或 DNS 规则中使用 Secure Firewall Management Center 中 思科 APIC 的动态对象



1 基本用户租户配置
2 基本用户租户配置
3 EPG
4 创建连接器思科 APIC，第 34 页
5 在 Secure Firewall Management Center 中查看动态对象，第 59 页
6 使用动态属性过滤器来创建访问控制规则或 DNS 规则

表 *3:* 使用网络对象组配置 ***Secure Firewall Management Center*** 访问控制规则或 ***DNS*** 规则

1	思科 APIC	租户允许 思科 APIC 管理员设置基于域的访问控制。 请参阅基本用户租户配置
2	思科 APIC	应用配置文件是其他对象（例如终端组 (EPG)）的容器。 请参阅基本用户租户配置
3	思科 APIC	EPG 是网络对象的容器，是设备连接到网络的方式。ESG 是包含物理或虚拟网络终端集合的逻辑实体。 请参阅 EPG 和 ESG
	Secure Firewall Management Center	如果您尚未这样做，请启用 dynamic attributes connector。
4	Secure Firewall Management Center	创建从 思科 APIC 检索 EPG 和 ESG 的 思科 APIC 连接器，并使其可用于 Secure Firewall Management Center 访问控制策略或 DNS 策略。 请参阅 创建连接器思科 APIC，第 34 页。
5	Secure Firewall Management Center	（可选。）查看从 思科 APIC 获取的动态对象。 请参阅在 Secure Firewall Management Center 中查看动态对象，第 59 页。

6	Secure Firewall Management Center	要在访问控制策略 或 DNS 策略中使用动态对象，您必须将它们作为动态对象添加到这些规则中。 请参阅使用动态属性过滤器来创建访问控制规则或 DNS 规则。

相关主题

与 思科 APIC 集成的系统要求 ， 第 30 页
获取集成所需的信息 ， 第 30 页
创建连接器思科 APIC ， 第 34 页
如何在访问控制规则或 DNS 规则中使用 Secure Firewall Management Center 中 思科 APIC 的动态对象 ， 第 29 页
手动获取证书颁发机构 (CA) 链 ， 第 35 页
思科 APIC 连接器 ， 第 28 页

与 思科 APIC 集成的系统要求

您的系统必须满足以下要求：

- Secure Firewall Management Center 版本：10.0.0 及更高版本。

  需要 Essentials 或更高级别的许可证；支持高可用性。

- Firewall Threat Defense 版本：7.2 及更高版本。
- 思科 APIC 版本：3.0(1k) 或更高版本。
- 如果您使用 ACI 终端更新应用程序，其版本必须为 2.6。

相关主题

与 思科 APIC 集成的系统要求 ， 第 30 页
获取集成所需的信息 ， 第 30 页
创建连接器思科 APIC ， 第 34 页
如何在访问控制规则或 DNS 规则中使用 Secure Firewall Management Center 中 思科 APIC 的动态对象 ， 第 29 页
手动获取证书颁发机构 (CA) 链 ， 第 35 页

获取集成所需的信息

本部分讨论以下内容：

- 配置集成所需的信息
- 动态对象名称中使用的信息

思科 ACI 终端更新应用 站点前缀和更新间隔

仅当您当前使用思科 ACI 终端更新应用时，此信息才适用于您；否则，您可以跳过。

要查找 思科 ACI 终端更新应用 站点前缀和更新间隔，请执行以下操作：

1. 以具有管理员权限的用户身份登录 思科 APIC。

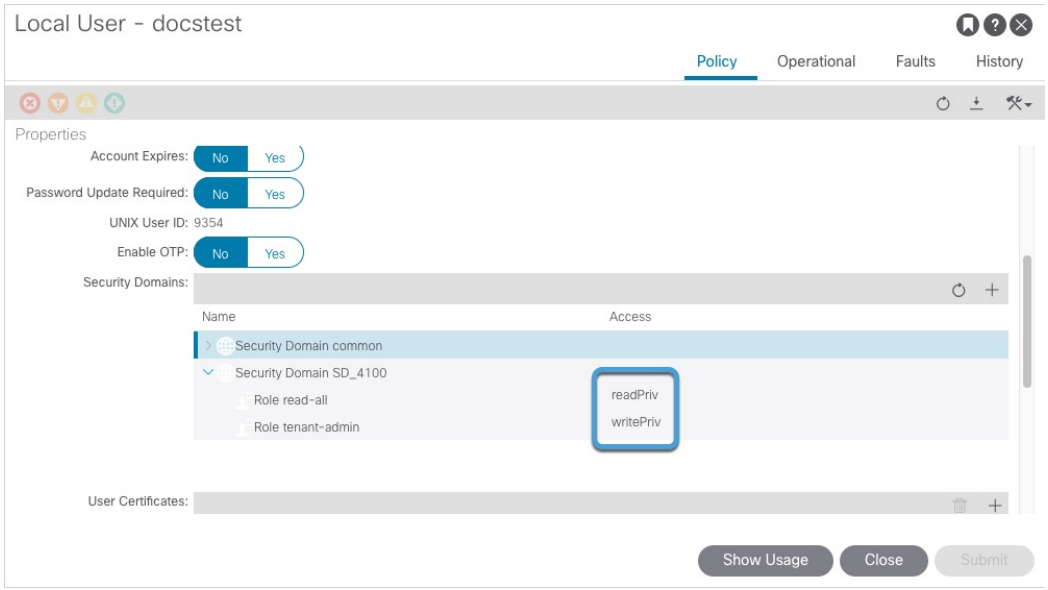
   有关详细信息，请参阅 *APIC* 角色和权限表。

2. 点击**应用 (Apps)**。
3. 在“ACI 终端更新应用”(ACI Endpoint Update app)，点击**打开 (Open)**。
4. 请点击 **编辑** ()。
5. 记下**更新间隔（以秒为单位）Update Interval [In seconds])** 和**站点前缀 (Site Prefix)** 的值。

配置集成所需：找到具有适当访问权限的用户

要查找包含 安全域至少具有 `readPriv` 访问权限的 `read-all` 角色和具有 `writePriv` 访问权限的 `tenant-admin` 角色 的用户，请执行以下操作：

1. 登录 思科 APIC。
2. 点击**管理员 (Admin)**。
3. 在左侧窗格中，点击**用户 (Users)**。
4. 在右侧窗格中，双击用户的名称。
5. 滚动到“安全域”(Security Domains)。
6. 对于相关安全域，请确保用户具有 安全域至少具有 `readPriv` 访问权限的 `read-all` 角色和具有 `writePriv` 访问权限的 `tenant-admin` 角色，如下图所示。



思科 APIC 租户名称

此集成创建的动态对象的名称中会使用思科 APIC租户名称。查找方法如下：

1. 登录 思科 APIC。
2. 点击**租户 (Tenants)**。
3. 记下包含要发送到 的对象的租户名称。

思科 APIC 应用配置文件名称

此集成创建的动态对象的名称中会使用思科 APIC应用配置文件名称。查找方法如下：

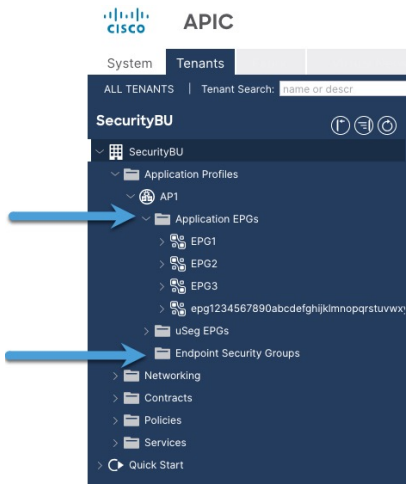
1. 登录 思科 APIC。
2. 点击**租户 (Tenants)**。
3. 双击您的租户的名称。
4. 展开您的租户。
5. 展开**应用配置文件 (Application Profiles)**。
6. 记下包含要与 ASA 集成的 EPG 和 ESG 的应用配置文件的名称。

EPG 名称

此集成创建的动态对象的名称中会使用思科 APIC EPG 名称。查找方法如下：

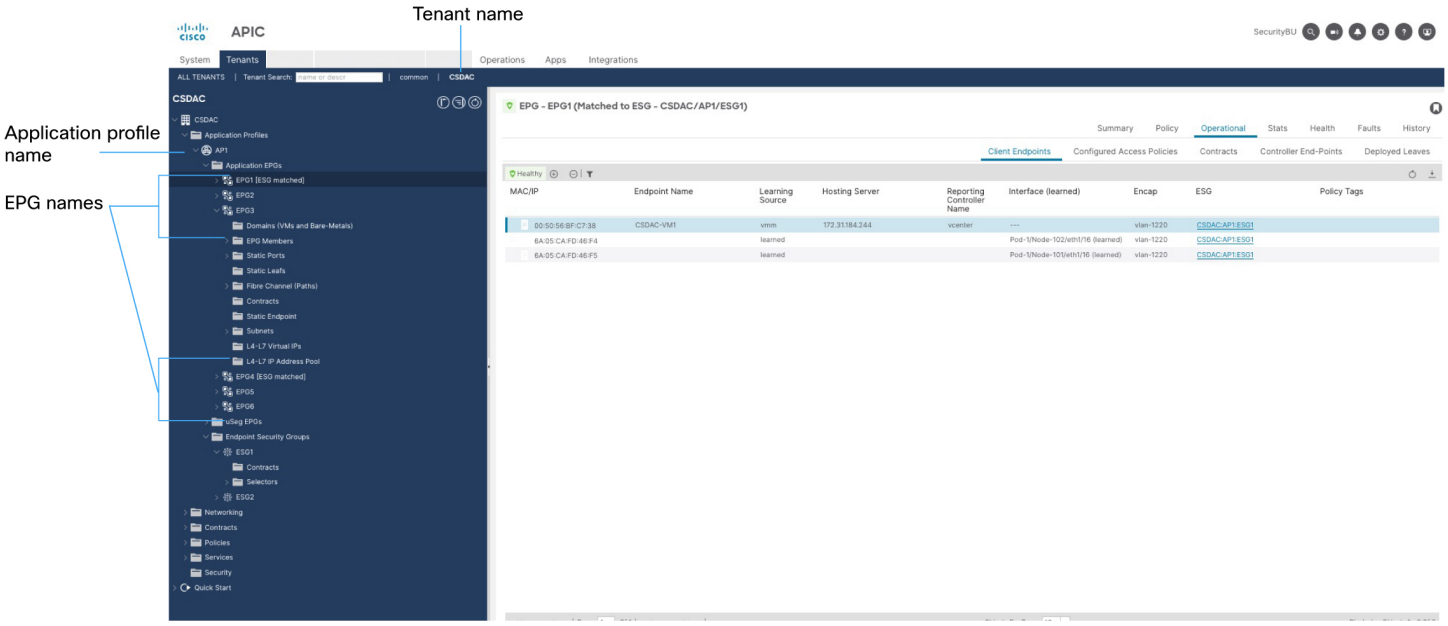
1. 登录 思科 APIC。
2. 点击**租户 (Tenants)**。
3. 双击您的租户的名称。
4. 展开您的租户。
5. 展开**应用配置文件 (Application Profiles)**。
6. 展开应用配置文件的名称。
7. 展开**应用 EPG**。
8. 记下有网络对象组要发送到 ASA 的EPG 或 ESG 的名称。

   下图显示了一个示例。



示例

下图显示了 思科 APIC 中的值。



相关主题

与 思科 APIC 集成的系统要求， 第 30 页
获取集成所需的信息， 第 30 页
创建连接器思科 APIC， 第 34 页
如何在访问控制规则或 DNS 规则中使用 Secure Firewall Management Center 中 思科 APIC 的动态对象， 第 29 页
手动获取证书颁发机构 (CA) 链， 第 35 页

创建连接器思科 APIC

本主题讨论了如何创建 思科 APIC 连接器，以便从 思科 APIC 上已配置的终端组 (EPG) 获取网络对象组。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （  ），然后点击连接器名称。
- 编辑或删除连接器：点击**更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
提取间隔	（默认值为 60 秒。）从 思科 APIC 检索 IP 映射的间隔。 建议将此值设置为 15 秒。
IP 或主机名	输入 思科 APIC 服务器的全称域名或 IP 地址，以便从 EPG 和 ESG 中检索网络对象组。 不要输入方案（如 **https://**），也不要包含尾部斜杠。
添加另一个集群 IP	（可选。）输入 思科 APIC 集群中其他服务器的 IP 地址。
用户名	输入至少包含 安全域至少具有 `readPriv` 访问权限的 `read-all` 角色和具有 `writePriv` 访问权限的 `tenant-admin` 角色 的 思科 APIC 用户的名称。 用户拥有权限的所有租户的对象都可以推送到 。
密码	输入用户的密码。

值	说明
服务器证书	（如果使用完全限定域名，则建议使用。） 您有以下选择： • 粘贴您找到的证书授权 (CA) 链，如手动获取证书颁发机构 (CA) 链，第 35 页中所述。 • 点击**获取证书** > **获取**以自动获取证书，或者，如果无法获取证书，请按照手动获取证书颁发机构 (CA) 链，第 35 页中所述手动获取证书。 • 点击 **获取证书** > **从文件浏览** 以上传您之前下载的证书链。

步骤 5 点击**测试 (Test)** 并确保测试成功后再保存连接器。

步骤 6 点击**保存**。

步骤 7 确保“状态”(Status) 列中显示**确定**。

相关主题

与 思科 APIC 集成的系统要求，第 30 页
获取集成所需的信息，第 30 页
创建连接器思科 APIC，第 34 页
如何在访问控制规则或 DNS 规则中使用 Secure Firewall Management Center 中 思科 APIC 的动态对象，第 29 页
手动获取证书颁发机构 (CA) 链，第 35 页

手动获取证书颁发机构 (CA) 链

在事件中无法自动获取证书颁发机构链，使用以下浏览器特定程序之一获取用于安全连接到vCenter、防火墙管理中心。

证书链是根证书和所有从属证书。

您可以选择使用以下程序之一连接到以下设备：

- vCenter 或 NSX
- 防火墙管理中心
- 思科 APIC

获取证书链 - Mac（Chrome 和 Firefox）

使用此程序在 Mac OS 上使用 Chrome 和 Firefox 浏览器来获取证书链。

1. 打开终端窗口。
2. 输入以下命令。

```
security verify-cert -P url[:port]
```

其中 *url* 是 vCenter、 防火墙管理中心 的 URL（包括方案）。例如：

```
security verify-cert -P https://myvcenter.example.com
```

如果使用 NAT 或 PAT 访问 vCenter、 防火墙管理中心，可以按如下方式添加端口：

```
security verify-cert -P https://myvcenter.example.com:12345
```

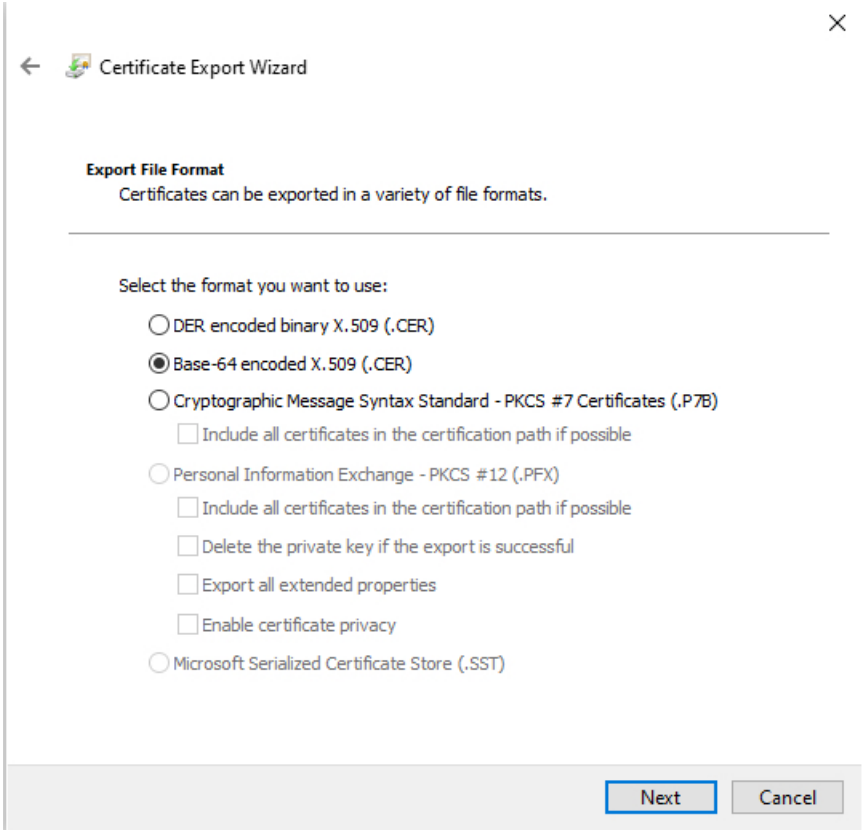
3. 将整个证书链保存到纯文本文件中。
   - 包括所有 `-----BEGIN CERTIFICATE-----` 和 `-----END CERTIFICATE-----` 分隔符。
   - 排除任何无关的文本（例如，证书的名称和尖括号 (< and >) 中包含的任何文本以及尖括号本身。
4. 对 vCenter 防火墙管理中心 重复这些任务。

获取证书链 - Windows Chrome

使用此程序在 Windows 上使用 Chrome 浏览器来获取证书链。

1. 使用 Chrome 登录 vCenter、 防火墙管理中心。
2. 在浏览器地址栏中点击主机名左侧的锁图标。
3. 点击**证书 (Certificate)**。
4. 点击**认证路径 (Certification Path)** 选项卡。
5. 点击证书链中顶部的（即第一个）证书。
6. 点击**查看证书 (View Certificates)**。
7. 点击**详细信息 (Details)** 选项卡。
8. 点击**复制到文件 (Copy to File)**。
9. 按照提示创建包含整个证书链的 CER 格式证书文件。

   当系统提示您选择导出文件格式时，点击 **Base 64-Encoded X.509 (.CER)**，如下图所示。



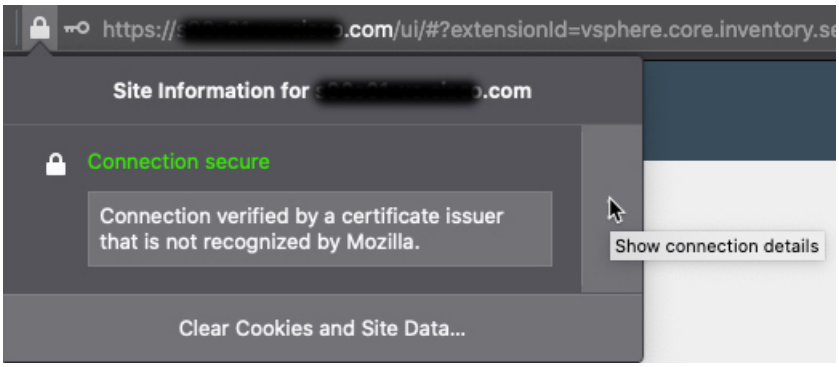
10. 按照提示完成导出。
11. 在文本编辑器中打开证书。
12. 对证书链中的所有证书重复此过程。

    您必须先按顺序将每个证书粘贴到文本编辑器中。
13. 对 vCenter、 防火墙管理中心 重复这些任务。

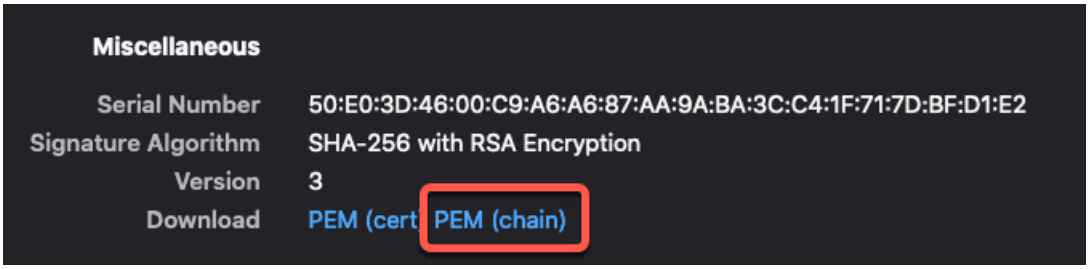
获取证书链 - Windows Firefox

使用以下程序为 Windows 或 Mac OS 上的 Firefox 浏览器来获取证书链。

1. 使用 Firefox 登录 vCenter、 防火墙管理中心。
2. 点击主机名左侧的锁图标。
3. 点击右箭头（**显示连接详细信息**）。下图显示了一个示例。



4. 点击更多信息 **(More Information)**。
5. 点击查看证书 **(View Certificates)**。
6. 如果生成的对话框包含选项卡页面，请点击与顶层 CA 对应的选项卡页面。
7. 滚动到“其他”(Miscellaneous) 部分。
8. 点击下载行中的 **PEM**（链）**(PEM [chain])**。下图显示了一个示例。



9. 保存文件。
10. 对 vCenter、 防火墙管理中心 重复这些任务。

相关主题

与 思科 APIC 集成的系统要求， 第 30 页
获取集成所需的信息， 第 30 页
创建连接器思科 APIC， 第 34 页
如何在访问控制规则或 DNS 规则中使用 Secure Firewall Management Center 中 思科 APIC 的动态对象， 第 29 页
手动获取证书颁发机构 (CA) 链， 第 35 页
思科 APIC 连接器， 第 28 页

创建 Cisco Cyber Vision 连接器

此任务讨论如何将数据从 Cisco Cyber Vision 发送到 Secure Firewall Management Center 。

开始之前

必须可从运行 dynamic attributes connector 的计算机访问 Cisco Cyber Vision。您必须知道其 IP 地址、端口和 API 密钥。

要在 Cyber Vision 管理控制台中查找 API 密钥，请点击**管理 (Admin)** > **API** > **令牌 (Token)**，然后点击**显示 (Show)** 以显示令牌，并点击  以将令牌复制到剪贴板。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （  ），然后点击连接器名称。
- 编辑或删除连接器：点击**更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
Cyber Vision 前缀	输入一个字母数字字符串，以便在将对象发送到 Secure Firewall Management Center 时标识来自此 Cyber Vision IP 地址的动态对象。 如果您有一个 Cyber Vision IP 地址，则可以输入任何值，例如 **1**。
提取间隔	（默认值为 60 秒。）从 Cyber Vision 获取数据映射的时间间隔。 最小**拉取间隔时间 (Pull Interval)** 值为 1 秒。您可以将最大值设置为任何想要的值。我们建议不要将最小值设得太低，因为这会产生大量流量，而且在适用情况下，可能会导致您为流量付费。
主机	（必需。）输入 Cyber Vision 的完全限定主机名或 IP 地址。
端口	（必需。）输入 Cyber Vision 侦听端口。
令牌	（必需。）输入 API 令牌。

步骤 5 点击**测试 (Test)** 并确保测试成功后再保存连接器。

步骤 6 点击**保存**。

步骤 7 确保“状态”(Status) 列中显示**确定**。

创建通用文本连接器

此任务讨论如何创建手动维护的 IP 地址临时列表，并按您选择的时间间隔（默认情况下为 30 秒）进行检索。您可以随时更新地址列表。

开始之前

创建包含 IP 地址的文本文件，并将其放在可从 Secure Firewall Management Center 访问的 Web 服务器上。IP 地址可以包含 CIDR 表示法。文本文件每行只能有一个 IP 地址。

例如，访问控制规则中的“允许列表”可能有一个 IP 地址列表，访问控制规则中的“阻止列表”可能有另一个 IP 地址列表。

每个文本文件最多可以指定 10,000 个 IP 地址。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （  ），然后点击连接器名称。
- 编辑或删除连接器：点击**更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息：

项目	说明
名称	输入名称以唯一标识此连接器。
说明	（可选。）输入说明。
提取间隔	在提取间隔 (Pull Interval) 字段中，更改动态属性连接器从 text 文件检索 IP 地址的频率（以秒为单位）。默认值为 30 秒。 最小**拉取间隔时间 (Pull Interval)** 值为 1 秒。您可以将最大值设置为任何想要的值。我们建议不要将最小值设得太低，因为这会产生大量流量，而且在适用情况下，可能会导致您为流量付费。
URL	输入要从中检索 IP 地址的 URL。
添加其他 URL	（可选。）点击链接可向现有列表中添加更多 URL。
用户名	（可选。）如果文本文件所在的服务器使用身份验证，请在此字段中输入用户名。 基本身份验证

项目	说明
密码	（可选。）输入用户的密码。
证书	（可选。）如果安全连接到 Web 服务器需要证书链，您有以下选择： • 点击 **获取证书** > **获取** 以自动获取证书，或者，如果无法获取证书，请按照 手动获取证书颁发机构 (CA) 链，第 35 页中所述手动获取证书。 • 点击 **获取证书** > **从文件浏览** 以上传您之前下载的证书链。

步骤 5 点击**测试 (Test)** 并确保测试成功后再保存连接器。

步骤 6 点击**保存**。

步骤 7 确保“状态”(Status) 列中显示**确定**。

创建 GitHub 连接器

此部分讨论如何创建将数据发送到 Secure Firewall Management Center 以用于策略的 GitHub 连接器。与这些标签关联的 IP 地址由 GitHub 进行维护。您不必创建动态属性过滤器。

有关详细信息，请参阅关于 GitHub 的 IP 地址。

注释 请勿更改 URL，否则将无法检索任何 IP 地址。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （  ），然后点击连接器名称。
- 编辑或删除连接器：点击**更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入**名称**和可选说明。

步骤 5 （可选。）在**提取间隔 (Pull Interval)** 字段中，更改动态属性连接器从 GitHub 检索 IP 地址的频率（以秒为单位）。默认值为 21,600 秒（6 小时）。

步骤 6 点击**保存**。

步骤 7 确保“状态”(Status) 列中显示**确定**。

Google 云连接器 - 关于用户权限和导入的数据

dynamic attributes connector 会将动态属性从 Google Cloud 导入 Secure Firewall Management Center，以便用于策略。

动态属性已导入

我们会从 Google 云导入以下动态属性：

- 标签，可用于组织 Google 云资源的键值对。

  有关详细信息，请参阅 Google 云文档中的创建和管理标签。

- 网络标记，与组织、文件夹或项目关联的键值对。

  有关详细信息，请参阅 Google 云文档中的创建和管理标签。

- Google 云中虚拟机的 *IP* 地址。

所需的最低权限

dynamic attributes connector 要求至少具有**基本** > **查看者**权限的用户才能导入动态属性。

创建对 dynamic attributes connector 具有最小权限的 Google 云用户

此任务讨论如何设置具有最低权限的服务帐户，以向 Secure Firewall Management Center 发送动态属性。有关这些属性的列表，请参阅 Google 云连接器 - 关于用户权限和导入的数据，第 42 页。

开始之前

您必须已设置 Google 云帐户。有关执行此操作的详细信息，请参阅 Google 云文档中的设置环境。

过程

步骤 1 以所有者角色的用户身份登录您的 Google 云帐户。

步骤 2 点击**IAM 和管理 (IAM & Admin)** > **服务帐户 (Service Accounts)** > **创建服务帐户 (Create Service Account)**。

步骤 3 输入以下信息：

- **服务帐户名称**：用于标识此帐户的名称；例如，**CSDAC**。
- **服务帐户 ID**：应在您输入服务帐户名称后填写唯一值。
- **服务帐户说明**：输入可选说明。

有关服务帐户的详细信息，请参阅 Google 云文档中的了解服务帐户。

步骤 4 点击**创建并继续 (Create and Continue)**。

步骤 5 按照屏幕上的提示操作，直到显示“授予用户对此服务帐户的访问权限”部分。

步骤 6 授予用户**基本** > **查看者**角色。

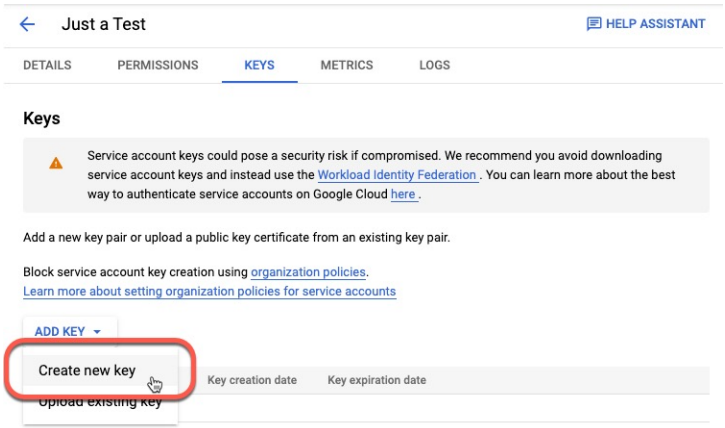
步骤 7 点击**完成**。

系统将显示服务帐户列表。

步骤 8 点击您所创建的服务帐户一行末尾的 **更多** (⋮)。

步骤 9 点击**管理密钥 (Manage Keys)**。

步骤 10 点击**添加密钥 (Add Key)** > **创建新密钥 (Create New Key)**。



步骤 11 点击 **JSON**。

步骤 12 点击**创建 (Create)**。

JSON 密钥将下载到您的计算机。

步骤 13 配置 GCP 连接器时，请将密钥放在手边。

下一步做什么

请参阅创建 Google Cloud 连接器，第 43 页。

创建 Google Cloud 连接器

开始之前

准备好 Google 云 JSON 格式的服务帐户数据；它是设置连接器所必需的。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （ ），然后点击连接器名称。
- 编辑或删除连接器：点击**更多** （ ），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
提取间隔	（默认为 30 秒。）从 AWS 检索 IP 映射的间隔。 最小**拉取间隔时间 (Pull Interval)** 值为 1 秒。您可以将最大值设置为任何想要的值。我们建议不要将最小值设得太低，因为这会产生大量流量，而且在适用情况下，可能会导致您为流量付费。
GCP 区域	（必需。）输入您的 Google 云所在的 GCP 区域。有关详细信息，请参阅 Google 云文档中的区域和地区。
服务帐户	粘贴 Google 云服务帐户的 JSON 代码。

步骤 5 点击**保存**。

步骤 6 确保“状态”(Status) 列中显示**确定**。

创建 Office 365 连接器

此任务讨论如何为 Office 365 标记创建连接器，从而将数据发送到 Secure Firewall Management Center 以便用于策略。Microsoft 会每周更新与这些标记的 IP 地址关联。您不必创建动态属性过滤器即可使用数据。

有关详细信息，请参阅 docs.microsoft.com 上的 Office 365 URL 和 IP 地址范围。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （ ），然后点击连接器名称。
- 编辑或删除连接器：点击**更多** （ ），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
提取间隔	（默认为 30 秒。）从 Azure 检索 IP 映射的间隔。 最小**拉取间隔时间 (Pull Interval)** 值为 1 秒。您可以将最大值设置为任何想要的值。我们建议不要将最小值设得太低，因为这会产生大量流量，而且在适用情况下，可能会导致您为流量付费。
基本 API URL	（必需。）输入要从中检索 Office 365 信息的 URL（如果其与默认值不同）。有关详细信息，请参阅 Microsoft 文档站点上的 Office 365 IP 地址和 URL Web 服务。
实例名称	（必需。）从列表中，点击实例名称。有关详细信息，请参阅 Microsoft 文档站点上的 Office 365 IP 地址和 URL Web 服务。
禁用可选 IP	（必需。）输入 **true** 或 **false**。

步骤 5 点击**保存**。

步骤 6 确保“状态”(Status) 列中显示**确定**。

vCenter 连接器 - 关于用户权限和导入的数据

Dynamic Attributes Connector 会将动态属性从 vCenter 导入 Secure Firewall Management Center，以便用于访问控制策略。

动态属性已导入

我们会从 vCenter 导入以下动态属性：

- 操作系统
- *MAC* 地址
- *IP* 地址
- *NSX* 标记

所需的最低权限

Dynamic Attributes Connector 要求至少具有**只读**权限的用户才能导入动态属性。

创建对 dynamic attributes connector 具有最小权限的 vCenter 用户

此任务讨论如何设置具有最低权限的服务帐户，以向 Secure Firewall Management Center 发送动态属性。有关这些属性的列表，请参阅 vCenter 连接器 - 关于用户权限和导入的数据，第 45 页。

开始之前

您必须已设置 vCenter 服务器帐户。有关执行此操作的详细信息，请参阅 vCenter 文档中的关于 vCenter 服务器安装和设置。

过程

步骤 1 以管理员身份登录 vCenter。

步骤 2 点击**菜单 (Menu)** > **管理 (Administration)**。

步骤 3 在左侧窗格中，点击**单点登录 (Single Sign On)** > **用户和组 (Users and Groups)**。

步骤 4 从**域 (Domain)** 列表中，点击域的名称以添加用户。

步骤 5 点击**添加用户**。

步骤 6 输入请求的信息，然后点击**添加 (Add)**。

步骤 7 在左侧窗格中，点击**访问控制 (Access Control)** > **全局权限 (Global Permissions)**。

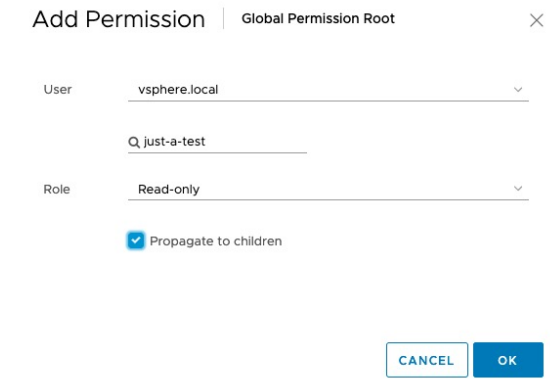
步骤 8 点击**添加** (+)。

步骤 9 在**用户**字段中，点击您在其中创建用户的 vCenter 域的名称。

步骤 10 在搜索字段中，输入用户名的一部分。

步骤 11 从**角色 (Role)** 列表中，点击**只读 (Read-only)**。

步骤 12 选择 **传播到子项** 复选框。



步骤 13 点击**确定**。

下一步做什么

请参阅创建 vCenter 连接器，第 47 页。

创建 vCenter 连接器

此任务讨论如何为 VMware vCenter 创建连接器，从而将数据发送到 Secure Firewall Management Center 以用于策略。

开始之前

如果使用不受信任的证书与 vCenter 通信，请参阅手动获取证书颁发机构 (CA) 链，第 35 页。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

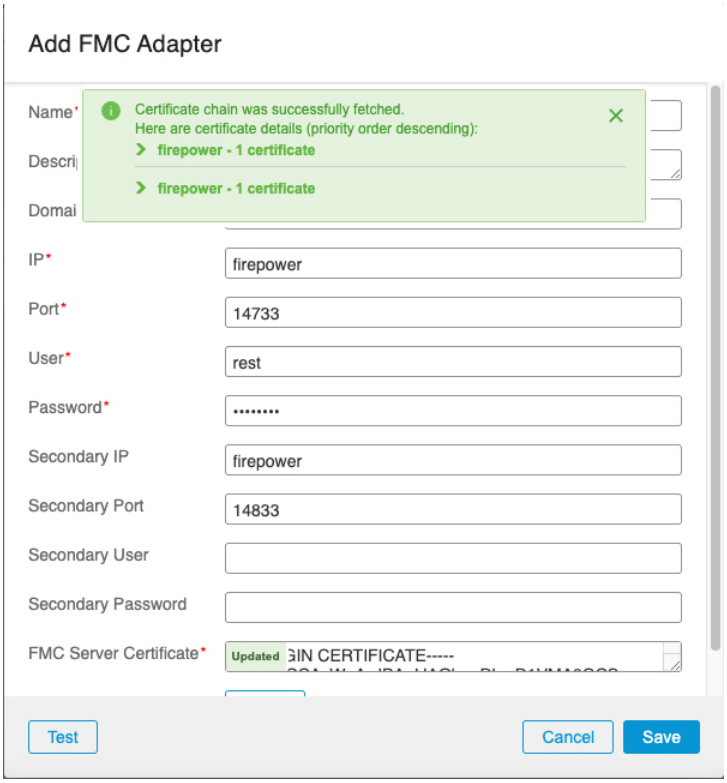
- 添加新连接器：点击添加图标（  ），然后点击连接器名称。
- 编辑或删除连接器：点击**更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	输入可选的说明。
提取间隔	（默认为 30 秒。）从 vCenter 检索 IP 映射的间隔。 最小**拉取间隔时间 (Pull Interval)** 值为 1 秒。您可以将最大值设置为任何想要的值。我们建议不要将最小值设得太低，因为这会产生大量流量，而且在适用情况下，可能会导致您为流量付费。
主机	（必需。）输入以下任意命令： • vCenter 的完全限定主机名 • vCenter 的 IP 地址 • （可选。）A 端口 请勿输入方案（例如 **`https://`**）或末尾斜杠。 例如，**`myvcenter.example.com`** 或 **`192.0.2.100:9090`**
用户	（必需。）输入至少具有只读角色的用户的用户名。用户名区分大小写。

值	说明
密码	（必需。）输入用户的密码。
NSX IP	如果使用 vCenter 网络安全可视化 (NSX)，请输入其 IP 地址。
NSX 用户	输入至少具有审核员角色的 NSX 用户的用户名。
NSX 类型	输入 **NSX-T**。
NSX 密码	输入 NSX 用户的密码。
vCenter 证书	您有以下选择： • 粘贴您找到的证书授权 (CA) 链，如 手动获取证书颁发机构 (CA) 链，第 35 页中所述。 • 点击**获取 (Fetch)** 以自动获取证书，或者，如果无法获取证书，请按照手动获取证书颁发机构 (CA) 链，第 35 页中所述手动获取证书。 • 点击 **获取证书** > **获取** 以自动获取证书，或者，如果无法获取证书，请按照 手动获取证书颁发机构 (CA) 链，第 35 页中所述手动获取证书。 • 点击 **获取证书** > **从文件浏览** 以上传您之前下载的证书链。

以下是成功获取证书链的示例：



展开对话框顶部的证书 CA 链会显示类似于以下内容的证书。

如果无法通过这种方式获取证书，您可以手动获取证书链，如 手动获取证书颁发机构 (CA) 链，第 35 页中所述。

步骤 5 点击**保存**。

创建 Webex 连接器

此部分讨论如何创建将数据发送到 Secure Firewall Management Center 以用于策略的 Webex 连接器。与这些标签关联的 IP 地址由 Webex 进行维护。您不必创建动态属性过滤器。

有关详细信息，请参阅 Webex Calling 的端口参考。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标（  ），然后点击连接器名称。
- 编辑或删除连接器：点击**更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
提取间隔	（默认为 30 秒。）从 Webex 检索 IP 映射的间隔。 最小**拉取间隔时间 (Pull Interval)** 值为 1 秒。您可以将最大值设置为任何想要的值。我们建议不要将最小值设得太低，因为这会产生大量流量，而且在适用情况下，可能会导致您为流量付费。
运营商预留 IP	（必需。）（必需。）滑动至已启用以检索任何保留的 IP 地址。

步骤 5 点击**测试 (Test)** 并确保测试成功后再保存连接器。

步骤 6 点击**保存**。

步骤 7 确保“状态”(Status) 列中显示**确定**。

创建 Zoom 连接器

此部分讨论如何创建将数据发送到 Secure Firewall Management Center 以用于策略的 Zoom 连接器。与这些标签关联的 IP 地址由 Zoom 进行维护。您不必创建动态属性过滤器。

有关详细信息，请参阅 Zoom 网络防火墙或代理服务器设置。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （  ），然后点击连接器名称。
- 编辑或删除连接器：点击**更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
提取间隔	（默认为 30 秒。）从 Zoom 检索 IP 映射的间隔。 最小**拉取间隔时间 (Pull Interval)** 值为 1 秒。您可以将最大值设置为任何想要的值。我们建议不要将最小值设得太低，因为这会产生大量流量，而且在适用情况下，可能会导致您为流量付费。
运营商预留 IP	（必需。）滑动至已启用以检索任何保留的 IP 地址。

步骤 5 点击**测试 (Test)** 并确保测试成功后再保存连接器。

步骤 6 点击**保存**。

步骤 7 确保“状态”(Status) 列中显示**确定**。

创建动态属性过滤器

使用 Dynamic Attributes Connector 定义的动态属性过滤器会在 Secure Firewall Management Center 中显示为可在访问控制策略中使用的动态对象。例如，您可以将财务部门对 AWS 服务器的访问权限限制为 Microsoft Active Directory 中定义的财务组成员。

注释 您不能为 通用文本、Office 365Azure Service Tags、Webex 或 Zoom 创建动态属性过滤器。这些类型的云对象会提供自己的 IP 地址。

有关访问控制规则或DNS规则的详细信息，请参阅使用动态属性过滤器来创建访问控制规则或 DNS 规则。

开始之前

创建连接器，第 16 页

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **动态属性筛选器**。

步骤 3 执行以下任一操作：

- 添加新过滤器：点击 **添加** ( )。
- 编辑或删除过滤器：点击 **更多**（ ），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

项目	说明
名称	用于在策略和 Secure Firewall Management Center 对象管理器（**外部属性** > **动态对象**）中标识动态过滤器（作为动态对象）的唯一名称。
连接器	在列表中点击要使用的连接器的名称。
查询	请点击 添加 。

步骤 5 要添加或编辑查询，请输入以下信息。

项目	说明
密钥	点击列表中的一个键。密钥会从连接器获取。

项目	说明
操作	点击以下选项之一： • **等于 (Equals)** 会将密钥与值完全匹配。 • **包含 (Contains)** 会将键与值匹配（如果值的任何部分匹配）。
值	点击**任意 (Any)** 或**全部 (All)**，然后点击列表中的一个或多个值。点击**添加其他值 (Add another value)** 以便向查询中添加值。

步骤 6 点击**显示预览 (Show Preview)** 以便显示查询返回的网络或 IP 地址的列表。

步骤 7 完成后，点击**保存**。

步骤 8 （可选。）验证 Secure Firewall Management Center 中的动态对象。

a) 至少要以具有网络管理员角色的用户身份登录 Secure Firewall Management Center 。

b) 请点击 **对象 (Objects)** > **外部属性 (External Attributes)** > **动态对象 (Dynamic Object)**。

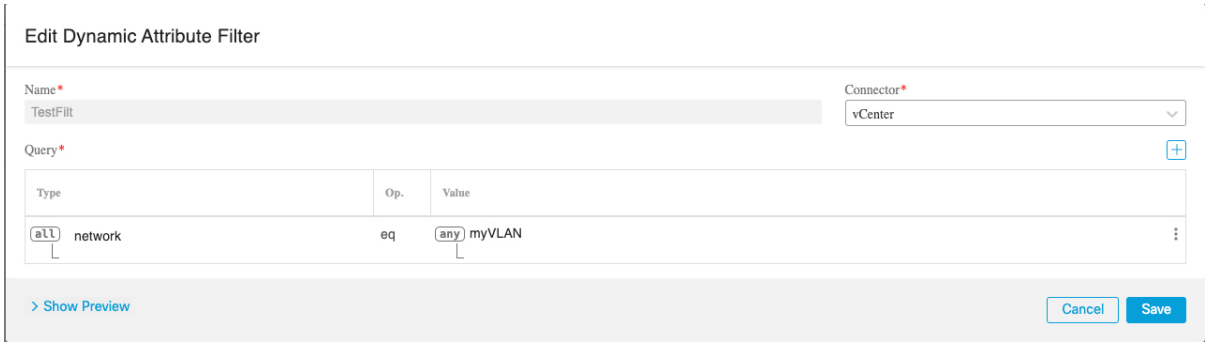
您创建的动态属性查询应显示为动态对象。

动态属性过滤器示例

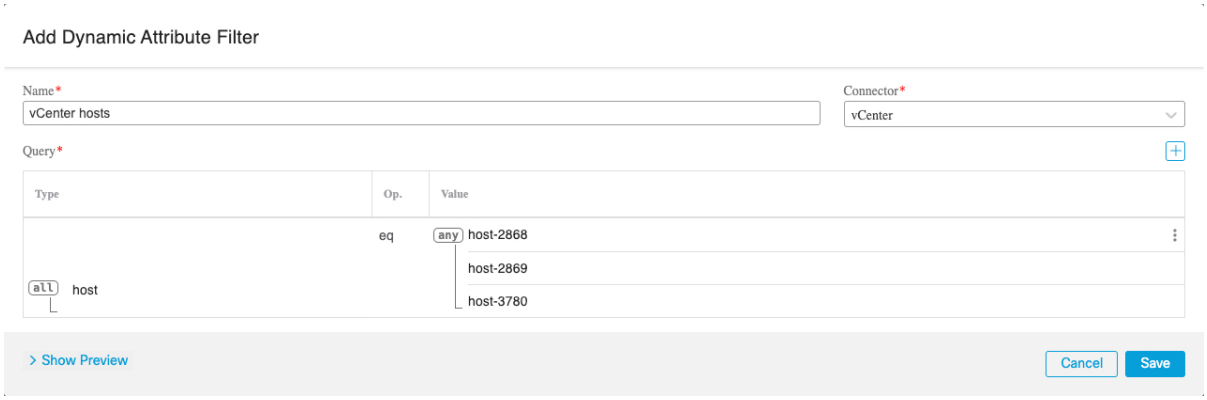
本主题提供了设置动态属性过滤器的一些示例。

示例：vCenter

以下示例显示了一个条件：VLAN。

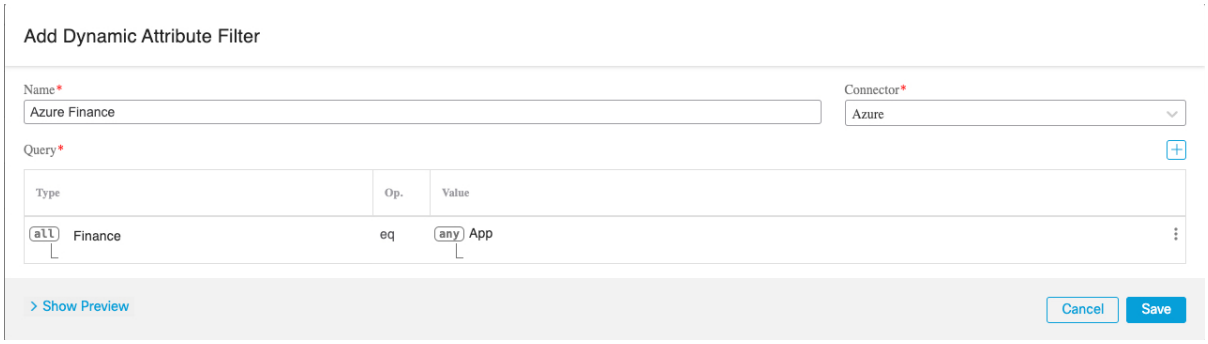


以下示例显示了使用 OR 连接的三个条件：查询匹配三个主机中的任何一个。



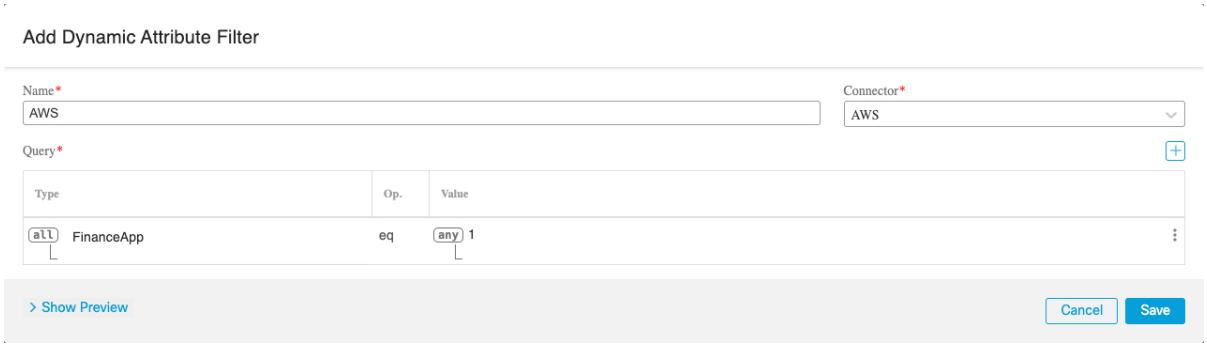
示例：Azure

以下示例显示了一个条件：标记为财务应用的服务器。



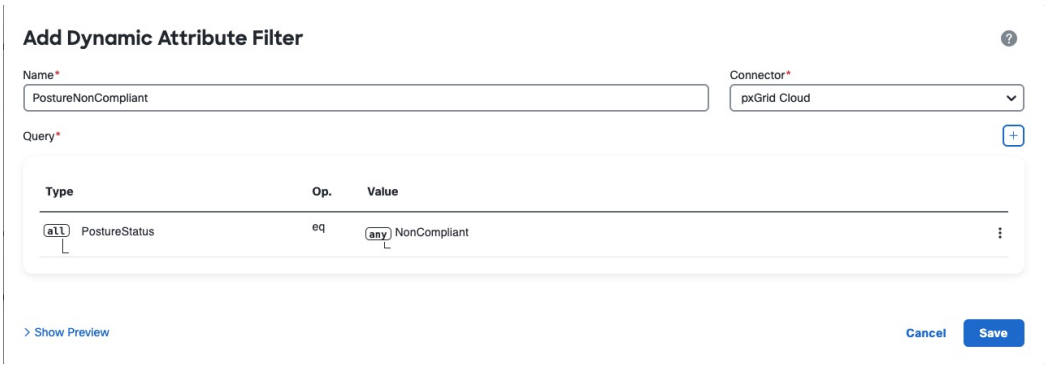
示例：AWS

以下示例显示了一个条件：值为 1 的 FinanceApp。



示例：pxGrid 云

以下示例显示一个条件：PostureStatus 为 NonCompliant。



手动获取证书颁发机构 (CA) 链

在事件中无法自动获取证书颁发机构链，使用以下浏览器特定程序之一获取用于安全连接到vCenter、防火墙管理中心。

证书链是根证书和所有从属证书。

您可以选择使用以下程序之一连接到以下设备：

- vCenter 或 NSX
- 防火墙管理中心
- 思科 APIC

获取证书链 - Mac（Chrome 和 Firefox）

使用此程序在 Mac OS 上使用 Chrome 和 Firefox 浏览器来获取证书链。

1. 打开终端窗口。
2. 输入以下命令。

   ```
   security verify-cert -P url[:port]
   ```

   其中 *url* 是 vCenter、 防火墙管理中心 的 URL（包括方案）。例如：

   ```
   security verify-cert -P https://myvcenter.example.com
   ```

   如果使用 NAT 或 PAT 访问 vCenter、 防火墙管理中心，可以按如下方式添加端口：

   ```
   security verify-cert -P https://myvcenter.example.com:12345
   ```

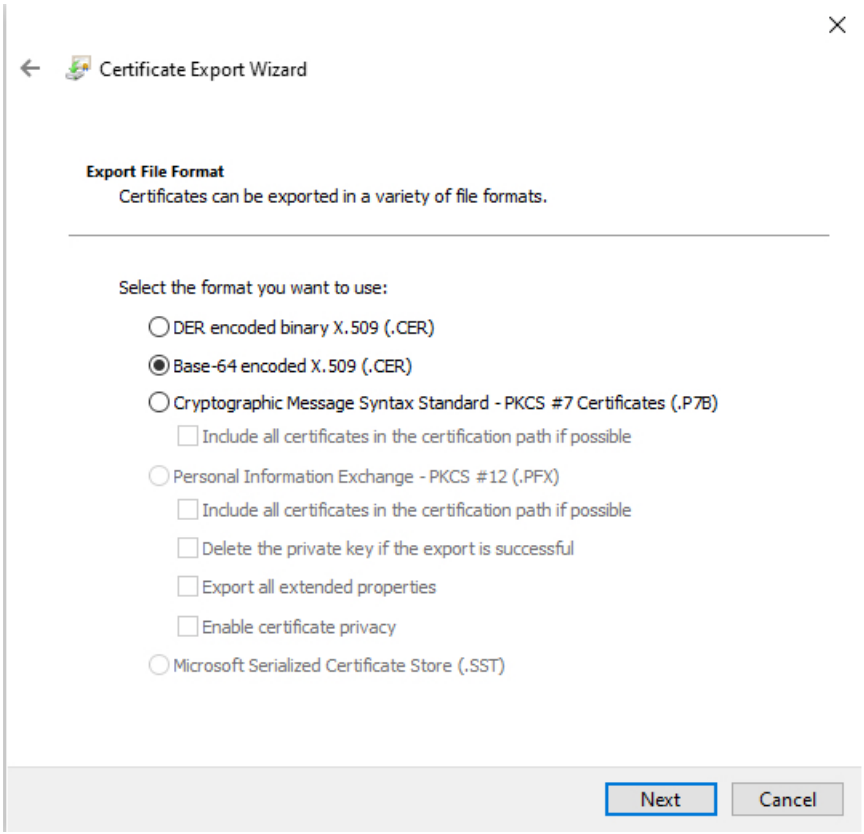
3. 将整个证书链保存到纯文本文件中。
   - 包括所有 `-----BEGIN CERTIFICATE-----` 和 `-----END CERTIFICATE-----` 分隔符。
   - 排除任何无关的文本（例如，证书的名称和尖括号 (< and >) 中包含的任何文本以及尖括号本身。
4. 对 vCenter 防火墙管理中心 重复这些任务。

获取证书链 - Windows Chrome

使用此程序在 Windows 上使用 Chrome 浏览器来获取证书链。

1. 使用 Chrome 登录 vCenter、 防火墙管理中心。
2. 在浏览器地址栏中点击主机名左侧的锁图标。
3. 点击**证书 (Certificate)**。
4. 点击**认证路径 (Certification Path)** 选项卡。
5. 点击证书链中顶部的（即第一个）证书。
6. 点击**查看证书 (View Certificates)**。
7. 点击**详细信息 (Details)** 选项卡。
8. 点击**复制到文件 (Copy to File)**。
9. 按照提示创建包含整个证书链的 CER 格式证书文件。

   当系统提示您选择导出文件格式时，点击 **Base 64-Encoded X.509 (.CER)**，如下图所示。



10. 按照提示完成导出。
11. 在文本编辑器中打开证书。

12. 对证书链中的所有证书重复此过程。

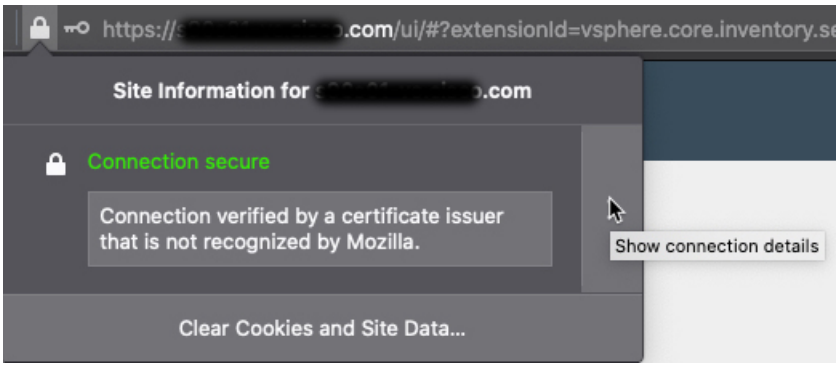
    您必须先按顺序将每个证书粘贴到文本编辑器中。

13. 对 vCenter、 防火墙管理中心 重复这些任务。

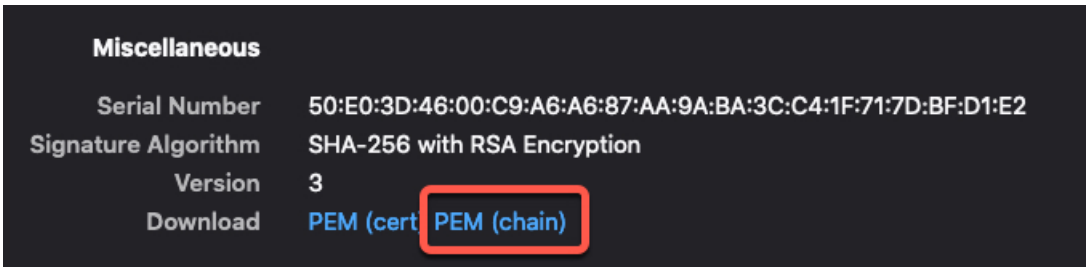
获取证书链 - Windows Firefox

使用以下程序为 Windows 或 Mac OS 上的 Firefox 浏览器来获取证书链。

1. 使用 Firefox 登录 vCenter、 防火墙管理中心。
2. 点击主机名左侧的锁图标。
3. 点击右箭头（**显示连接详细信息**）。下图显示了一个示例。



4. 点击**更多信息 (More Information)**。
5. 点击**查看证书 (View Certificates)**。
6. 如果生成的对话框包含选项卡页面，请点击与顶层 CA 对应的选项卡页面。
7. 滚动到“其他”(Miscellaneous) 部分。
8. 点击下载行中的 **PEM（链）(PEM [chain])**。下图显示了一个示例。



9. 保存文件。
10. 对 vCenter、 防火墙管理中心 重复这些任务。

相关主题

与 思科 APIC 集成的系统要求 ， 第 30 页

获取集成所需的信息，第 30 页
创建连接器思科 APIC，第 34 页
如何在访问控制规则或 DNS 规则中使用 Secure Firewall Management Center 中 思科 APIC 的动态对象，第 29 页
手动获取证书颁发机构 (CA) 链，第 35 页
思科 APIC 连接器，第 28 页

在访问控制策略或 DNS 策略中使用动态对象

通过 dynamic attributes connector，您可以在访问控制规则或 DNS 策略中配置动态属性过滤器（在 Secure Firewall Management Center 中可视为动态对象）。

关于访问控制规则或 DNS 规则中的动态对象

在创建连接器并在连接器上保存动态属性过滤器之后，动态对象会自动从 dynamic attributes connector 推送到 Cisco Secure Firewall 管理器。

您可以在访问控制规则的或DNS规则的**动态属性**选项卡页面使用这些动态对象。您可以将动态对象添加为源或目标属性；例如，在访问控制阻止规则中，您可以将财务动态对象添加为目标属性，以阻止通过匹配规则中其他条件的对象访问财务服务器。

注释 您不能为 通用文本、Office 365Azure Service Tags、Webex 或 Zoom 创建动态属性过滤器。这些类型的云对象会提供自己的 IP 地址。

创建动态属性过滤器

使用 Dynamic Attributes Connector 定义的动态属性过滤器会在 Secure Firewall Management Center 中显示为可在访问控制策略中使用的动态对象。例如，您可以将财务部门对 AWS 服务器的访问权限限制为 Microsoft Active Directory 中定义的财务组成员。

注释 您不能为 通用文本、Office 365Azure Service Tags、Webex 或 Zoom 创建动态属性过滤器。这些类型的云对象会提供自己的 IP 地址。

有关访问控制规则或DNS规则的详细信息，请参阅使用动态属性过滤器来创建访问控制规则或 DNS 规则。

开始之前

创建连接器，第 16 页

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **动态属性筛选器**。

步骤 3 执行以下任一操作：

- 添加新过滤器：点击 **添加** ( )。
- 编辑或删除过滤器：点击 **更多**（ ），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

项目	说明
名称	用于在策略和 Secure Firewall Management Center 对象管理器（**外部属性** > **动态对象**）中标识动态过滤器（作为动态对象）的唯一名称。
连接器	在列表中点击要使用的连接器的名称。
查询	请点击 添加 。

步骤 5 要添加或编辑查询，请输入以下信息。

项目	说明
密钥	点击列表中的一个键。密钥会从连接器获取。
操作	点击以下选项之一： • **等于 (Equals)** 会将密钥与值完全匹配。 • **包含 (Contains)** 会将键与值匹配（如果值的任何部分匹配）。
值	点击**任意 (Any)** 或**全部 (All)**，然后点击列表中的一个或多个值。点击**添加其他值 (Add another value)** 以便向查询中添加值。

步骤 6 点击**显示预览 (Show Preview)** 以便显示查询返回的网络或 IP 地址的列表。

步骤 7 完成后，点击**保存**。

步骤 8 （可选。）验证 Secure Firewall Management Center 中的动态对象。

a) 至少要以具有网络管理员角色的用户身份登录 Secure Firewall Management Center 。

b) 请点击 **对象 (Objects)** > **外部属性 (External Attributes)** > **动态对象 (Dynamic Object)**。

您创建的动态属性查询应显示为动态对象。

动态属性规则条件

动态属性包括：

- （源或目标。）动态对象（例如来自 dynamic attributes connector）

  dynamic attributes connector 让您能够从云提供商收集数据（例如网络和 IP 地址）并将其发送到 Secure Firewall Management Center 以便将它们用于访问控制规则中。

  有关dynamic attributes connector的详细信息，请参阅《关于 dynamic attributes connector，第 1 页》。

- （仅源。）安全组标记 (SGT) 对象，包含手动定义或通过 ISE 定义的标记。有关更多信息，请参阅《源和目标安全组标记 (SGT) 匹配》和《安全组标记》。
- （仅源。）位置 IP 对象 由Cisco ISE定义
- （仅源。）设备类型对象，由（也称为终端配置文件）Cisco ISE定义。

动态属性可用作访问控制规则中的源条件和目标条件。使用以下准则：

- 不同类型的对象通过 AND 连接在一起
- 将相似类型的对象一起进行 ORd 运算

例如，如果选择源目标条件 SGT 1、SGT 2 和设备类型 1；如果在 SGT 1 或 SGT 2 上检测到设备类型 1，则规则匹配。例如，如果同时选择安全组标记和列出 IP 地址的动态对象，如果带有 标记的流量源自（或发往）其中一个 IP 地址，则该规则匹配。

在 Secure Firewall Management Center 中查看动态对象

（可选。）以下任务讨论如何在 **对象 (Objects)** > **外部属性 (External Attributes)** > **动态对象 (Dynamic Object)** 中查看 思科 APIC 网络对象。

开始之前

完成之前所有 思科 APIC 与 Secure Firewall Management Center 集成相关的任务。

过程

步骤 1 登录至 Secure Firewall Management Center

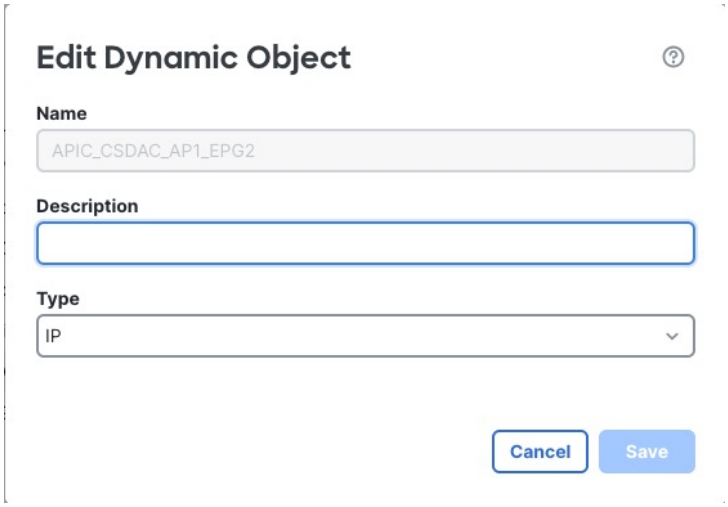
步骤 2 展开 **对象 (Objects)** > **外部属性 (External Attributes)** > **动态对象 (Dynamic Object)**。

动态对象有其自己的命名约定；例如，AWS 动态对象的名称类似于 `aws_AMAZON`。

通过与 思科 APIC 集成而创建的动态对象，其名称符合以下模式：

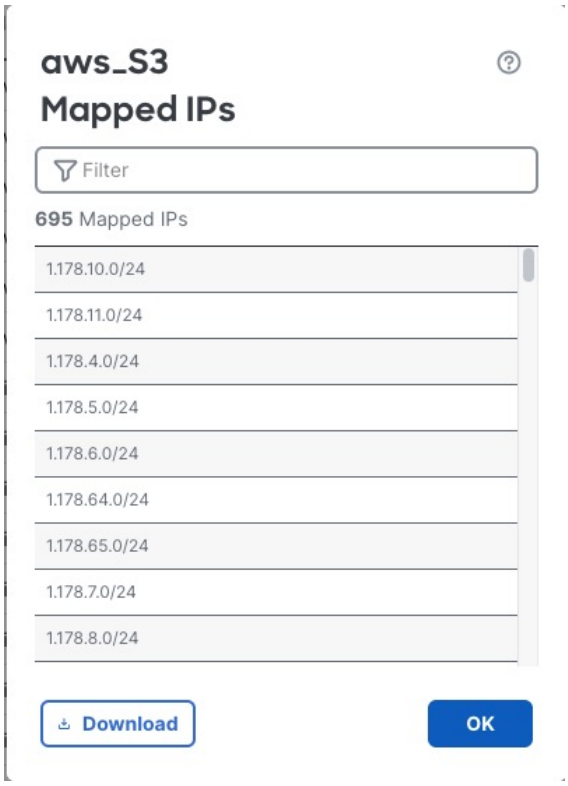
```
APIC-site-name_tenant-name_application-profile-name_EPG-or-ESG-name
```

示例：



步骤 3 要查看与每个动态对象关联的 IP 地址，请点击行末的 (IP)。

示例：



下一步做什么

请参阅使用动态属性过滤器来创建访问控制规则或 DNS 规则。

使用动态属性过滤器来创建访问控制规则或 DNS 规则

本主题讨论如何使用动态对象（这些动态对象以您之前创建的动态属性过滤器来命名）创建访问控制规则。

要向 DNS 策略添加动态属性过滤器，请参阅创建基本 DNS 策略。

要将动态属性过滤器添加到 DNS 策略，请参阅创建基本 DNS 策略。

开始之前

按照创建动态属性过滤器中所述，创建动态属性筛选器。

注释 您不能为 通用文本、Office 365Azure Service Tags、Webex 或 Zoom 创建动态属性过滤器。这些类型的云对象会提供自己的 IP 地址。

过程

步骤 1 登录至 Secure Firewall Management Center

步骤 2 请点击 **策略** > **安全策略** > **访问控制**。

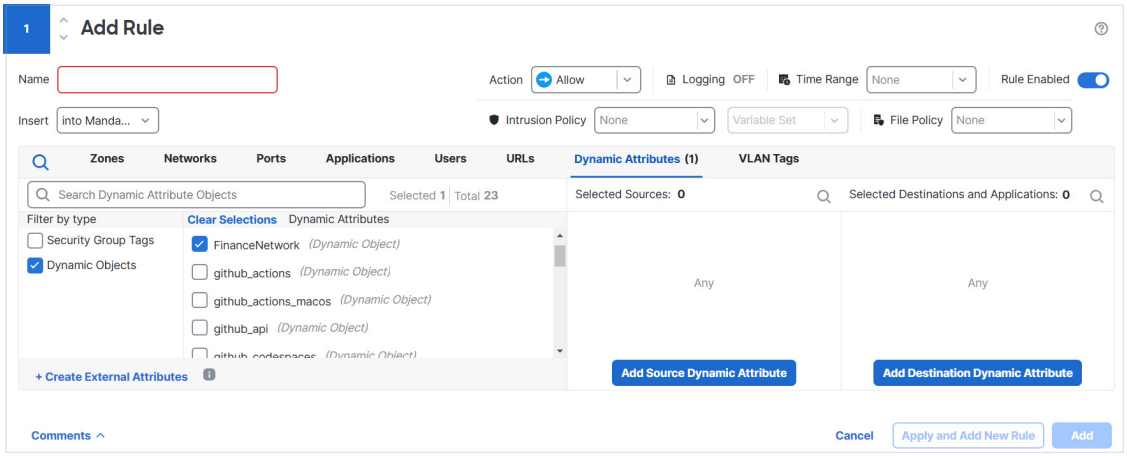
步骤 3 点击访问控制策略旁边的 **编辑**（ ）。

步骤 4 点击**添加规则 (Add Rule)**。

步骤 5 点击**动态属性 (Dynamic Attributes)** 选项卡。

步骤 6 在“可用属性”(Available Attributes) 部分中，点击列表中的**动态对象 (Dynamic Objects)**。

下图显示了一个示例。



本示例显示一个名为 APIC 动态属性的动态对象，它对应于 dynamic attributes connector 中创建的动态属性筛选器。

步骤 7 将所需对象添加到源或目标属性。

步骤 8 如果需要，向规则中添加其他条件。

下一步做什么

请参阅动态属性规则条件，第 59 页。

在 DNS 策略中使用动态对象

动态属性连接器使您能够在 DNS 规则中配置动态筛选器（在 Secure Firewall Management Center 中视为动态对象）。有关 DNS 策略的信息，请参阅 安全情报 DNS 策略。

在连接器上创建连接器并保存动态属性筛选器后，动态对象会自动从动态属性连接器推送到 Secure Firewall Management Center。

可以在 DNS 规则的“动态属性”选项卡页面上使用这些动态对象，类似于使用安全组标记 (SGT) 的方式。可以将动态对象添加为源或目标属性，但终端设备类型对象除外，它们仅作为源。

过程

步骤 1 点击 **策略** > **安全策略** > **DNS** 并创建或编辑 DNS 策略。

步骤 2 添加或编辑规则。

步骤 3 点击**动态属性 (Dynamic Attributes)** 选项卡。

步骤 4 在**动态属性**列表中，选择要使用的对象，然后将它们添加到相应的源列表或目标列表。最初，会列出所有安全组和动态对象，但可以取消选中“安全组”选项以仅查看动态对象。

步骤 5 在 **DNS** 选项卡上，选择与目标 DNS 请求匹配的相应列表或源。

步骤 6 根据需要向规则添加其他条件并设置操作。

步骤 7 点击**保存**。

动态防火墙

这些主题介绍如何将用户身份数据（包括 Microsoft AD 和 ISE）与 身份情报 提供的用户信任数据相集成，以增强您在网络中检测基于身份的漏洞的能力。

相关主题

关于 动态防火墙，第 63 页
如何配置 动态防火墙，第 63 页

关于 动态防火墙

以前，Secure Firewall Management Center 仅从配置的身份源（如 Microsoft Active Directory、被动身份代理、思科身份服务引擎 (Cisco ISE) 等）收集有关用户的信息。此信息通常包括用户名、组和 IP 地址。

借助 动态防火墙，您可以将来自思科 身份情报 的用户风险评分添加到身份源提供的信息中，以便根据始终最新的用户终端安全评估和风险设置策略。我们支持您将用户身份与智能配对，并在报告和访问控制策略中使用该信息。

要使用 动态防火墙，您必须：

- 拥有一个 身份情报 租户

  请参阅具有 Cisco Identity Intelligence 的 Duo Identity Security。

- 启用 Dynamic Attributes Connector
- 设置身份源：
  - 思科身份服务引擎 (Cisco ISE)
  - pxGrid 云

    pxGrid 云 在同一源中结合身份和终端安全评估

    详细信息：什么是 pxGrid?

  除了提供身份验证信息外，Cisco ISE 和 pxGrid 云 还可以提供以下信息（如果需要）：
  - 基于 TCP 的 SGT 交换协议 (SXP) 绑定和目录会话信息。有关详细信息，请参阅《思科身份识别服务引擎管理员指南》。
  - 终端安全评估和移动设备管理合规性。有关详细信息，请参阅合规。
- 设置身份领域：
  - 创建 LDAP 领域或 Active Directory 领域和领域目录
  - 为被动身份验证创建Microsoft Azure AD (SAML)领域

身份源提供身份验证信息（登录、注销）以及终端安全评估。如果需要，身份源还可以提供 SXP 绑定和会话目录信息。

身份领域提供用户、组和 IP 地址信息。

相关主题

关于 动态防火墙 ， 第 63 页
如何配置 动态防火墙 ， 第 63 页

如何配置 动态防火墙

本主题有助于您了解关于 动态防火墙 ， 第 63 页中讨论的配置 动态防火墙 相关概念和选项

process_summary

动态防火墙 将身份源（如 Cisco ISE）与思科身份智能集成，以向 Secure Firewall Management Center 提供用户信任信息。

1. 配置思科身份智能以收集用户信任信息。
2. 配置受支持的 Secure Firewall Management Center 身份源。
3. 配置支持的身份领域。
4. 启用dynamic attributes connector。
5. 配置动态防火墙。

process_workflow

以下过程概述了如何配置 动态防火墙。

1. 作为具有所有者角色的 Duo 用户，配置思科 身份情报 租户。

   您可以按照调配思科身份智能租户中的说明，从 Duo Advantage 调配租户。

2. 在思科 身份情报 中，创建 API 集成，并使用相关信息来设置 动态防火墙。

   我们使用思科 身份情报 在您的网络中查找用户和设备风险信息。

   有关思科 身份情报 的详细信息，请参阅《操作指南》。

   有关此任务的详细信息，请参阅获取所需的 身份情报 信息，第 66 页。

3. （仅限 Microsoft Azure AD 领域。）在 身份情报 中，创建 Microsoft Entra ID 集成。

   有关详细信息，请参阅《Microsoft Entra ID (Azure AD) 数据集成》。

4. 创建身份源。（如果您已有身份源，请继续执行下一步。）

   您可以通过以下任何一种方式执行此操作：

   - 配置动态防火墙对话框会显示**配置**链接，用于开始设置您的身份源。
   - 请点击 **集成** > **身份** > **身份源**。

   有关创建身份源的详细信息，请参阅：

   - 配置思科身份服务引擎 (Cisco ISE)身份源的方法
   - 如何配置 pxGrid 云身份源（Cisco ISE 3.3 或更早版本）
   - 如何配置 pxGrid 云身份源（Cisco ISE 3.4 或更高版本）

5. 创建身份领域。

   我们支持以下领域：

   - 创建 LDAP 领域或 Active Directory 领域和领域目录

     仅支持 Microsoft AD；不支持 LDAP 领域。

- 为被动身份验证创建Microsoft Azure AD (SAML)领域

6. 启用dynamic attributes connector。

   使用 动态防火墙 需借助 dynamic attributes connector。它使您的身份源能够与 身份情报 集成，从而提供有关用户活动的增强洞察。

   请参阅启用 dynamic attributes connector。

7. 创建 动态防火墙 实例。（如果您已有 动态防火墙 实例，请继续执行下一步。）

   点击 **集成** > **动态属性连接器**，然后点击**配置动态防火墙**。

   请参阅创建 动态防火墙 实例， 第 68 页。

8. 将您的身份源与思科 身份情报 相关联。

   请参阅将身份源与 身份情报 相关联， 第 69 页。

9. 查看系统定义的过滤器。

   我们为以下内容创建动态属性过滤器：

   - 不可信设备
   - 可信设备
   - 不可信用户
   - 可疑用户

   您可以按照创建动态属性过滤器， 第 77 页中的说明编辑或替换这些动态属性过滤器。

10. 查看系统定义的访问控制规则。

    我们会创建一个名为“动态防火墙策略”（或类似名称）的访问控制策略，其中包含以下规则：

    - 阻止不可信用户从任何源网络访问任何目标网络。
    - 监控可疑用户从任何源网络访问任何目标网络。
    - 阻止不可信设备从任何源网络访问任何目标网络。

    您可以按照查看和编辑系统创建的访问控制策略， 第 76 页中的说明编辑或删除访问控制策略和规则。

相关主题

关于 动态防火墙， 第 63 页
如何配置 动态防火墙， 第 63 页

启用 dynamic attributes connector

此任务讨论如何在 Secure Firewall Management Center启用 dynamic attributes connector 。 dynamic attributes connector是一种集成，它使得来自云网络产品的对象能够用于Secure Firewall Management Center访问控制和 DNS 规则。

过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center 。

步骤 2 请点击 **集成** > **动态属性连接器**。

步骤 3 滑动到**已启用 (Enabled)**。

步骤 4 启用 dynamic attributes connector 时，系统会显示消息。

如果出现错误，请重试。如果错误仍然存在，请联系思科 TAC。

下一步做什么

请参阅创建连接器，第 16 页。

相关主题

关于 动态防火墙，第 63 页
如何配置 动态防火墙，第 63 页

获取所需的 身份情报 信息

此任务讨论如何创建 API 客户端，该客户端提供在动态防火墙中设置身份情报所需的所有信息。

如果您已有 API 客户端，并且知道以下所有值，则可以跳过此过程并继续执行创建 动态防火墙 实例，第 68 页：

- **客户 ID**
- **API URL**
- **令牌 URL**
- **客户端密钥**

开始之前

与 动态防火墙 集成要求您在 身份情报 中创建 *API* 客户端集成。

您必须了解的关于 API 客户端集成的值包括客户端密钥，该密钥仅在创建 API 客户端时显示。因此，您可能需要先创建 API 集成。

有关创建 API 客户端集成的详细信息，请参阅公共 API。

过程

步骤 1 登录到您的 身份情报 租户。

步骤 2 点击 （**集成**）。

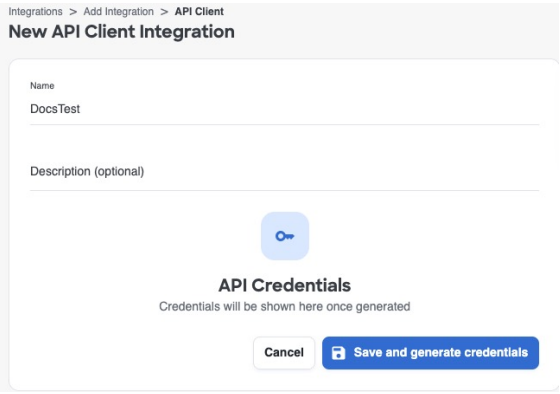
步骤 3 点击**添加集成**。

步骤 4 在下一页上，在“API 客户端”下，点击**添加 API 客户端**。

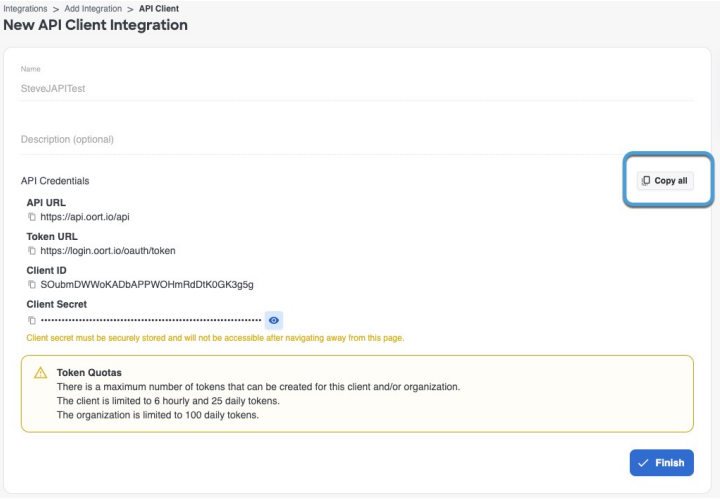
步骤 5 输入**名称**和可选的**说明**。

步骤 6 点击**保存并生成凭证**。

下图显示了一个示例。



步骤 7 在下一页上，如以下图所示，点击**全部复制**。



步骤 8 保存凭证以供稍后使用。

步骤 9 点击**完成 (Finish)**。

下一步做什么

请参阅创建 动态防火墙 实例 ， 第 68 页。

相关主题

关于 动态防火墙 ， 第 63 页
如何配置 动态防火墙 ， 第 63 页

为 动态防火墙 创建身份源和领域

在配置 动态防火墙 之前，您必须配置受支持的身份领域和身份源。

配置身份领域

支持以下身份领域：

- 创建 LDAP 领域或 Active Directory 领域和领域目录

  仅支持 Microsoft AD；不支持 LDAP 领域。

- 为被动身份验证创建Microsoft Azure AD (SAML)领域

配置身份源

支持以下身份源：

- 本地 Cisco ISE：配置思科身份服务引擎 (Cisco ISE)身份源的方法
- 单个或多个 Cisco ISE 集群：
  - 如何配置 pxGrid 云身份源（Cisco ISE 3.4 或更高版本）
  - 如何配置 pxGrid 云身份源（Cisco ISE 3.3 或更早版本）

相关主题

关于 动态防火墙 ， 第 63 页
如何配置 动态防火墙 ， 第 63 页

创建 动态防火墙 实例

此任务讨论如何创建 动态防火墙 的新实例，该实例是身份源与 身份情报 之间的关联。

开始之前

执行以下所有操作：

- 启用 dynamic attributes connector，如启用 dynamic attributes connector中所述。
- 创建身份源：
  - 配置思科身份服务引擎 (Cisco ISE)身份源的方法。
  - 创建一个 pxGrid 云身份源。

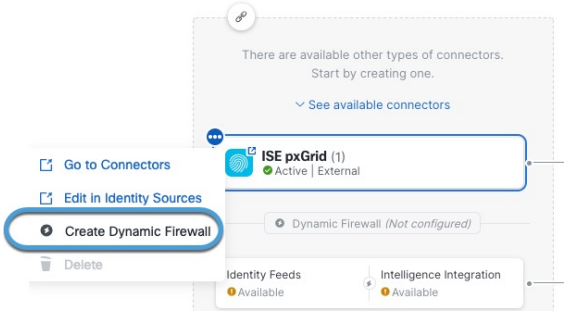
过程

步骤 1 如果尚未执行此操作，请登录 Secure Firewall Management Center。

步骤 2 点击**集成** > **动态属性连接器**。

步骤 3 点击身份源名称旁边的 ，通过它可以添加 动态防火墙。

下图显示了一个示例。



注释

如果未看到身份源，请先创建一个身份源，然后再继续：

- 配置思科身份服务引擎 (Cisco ISE)身份源的方法
- 如何配置 pxGrid 云身份源（Cisco ISE 3.3 或更早版本）
- 如何配置 pxGrid 云身份源（Cisco ISE 3.4 或更高版本）

步骤 4 点击**创建动态防火墙**。

步骤 5 继续将身份源与 身份情报 相关联 ， 第 69 页。

相关主题

关于 动态防火墙 ， 第 63 页
如何配置 动态防火墙 ， 第 63 页

将身份源与 身份情报 相关联

此任务讨论如何将身份源与 身份情报 相关联， 会向 Secure Firewall Management Center 提供用户和设备信任评分。

有关详细信息，请参阅用户信任级别。

开始之前

开始之前，请确保您：

- 了解关于 动态防火墙 ， 第 63 页中讨论的身份领域、身份源和 身份情报 如何协同工作。

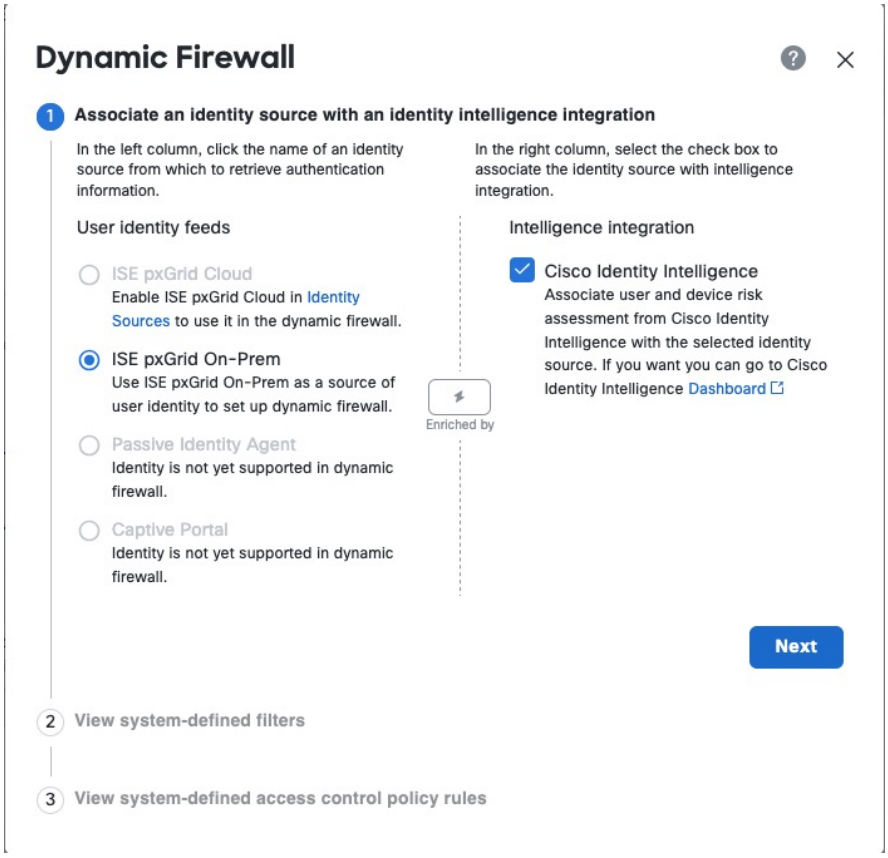
- 完成创建 动态防火墙 实例， 第 68 页中讨论的任务。

过程

步骤 1 首先创建 动态防火墙 实例， 第 68 页。

步骤 2 在下一页的左列中，点击您的身份源。然后，从右列选中**思科身份智能**复选框，以添加用户智能（包括用户和设备风险）。

下图显示了一个示例。



步骤 3 点击**下一步 (Next)**。

步骤 4 继续执行配置 身份情报， 第 71 页。

相关主题

关于 动态防火墙， 第 63 页

如何配置 动态防火墙， 第 63 页

配置 身份情报

此任务讨论如何将身份源与 身份情报 相关联，后者会向 Secure Firewall Management Center 提供用户和设备风险评分。

开始之前

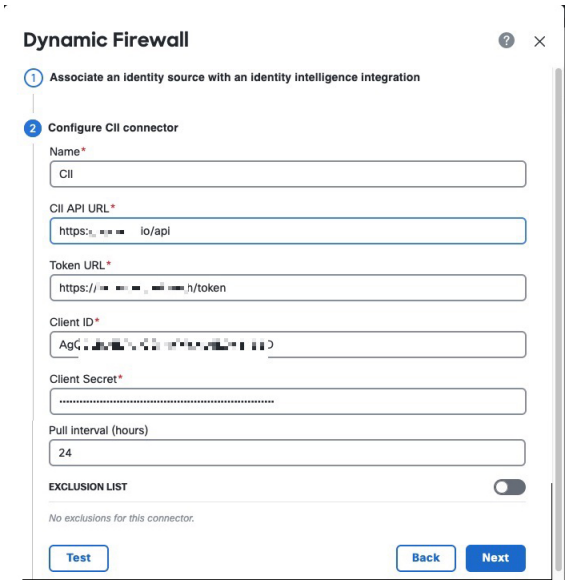
完成 将身份源与 身份情报 相关联， 第 69 页中讨论的任务。

过程

步骤 1 完成 将身份源与 身份情报 相关联， 第 69 页中讨论的任务。

步骤 2 如果您选中了**思科身份智能**复选框，请输入您找到的 身份情报 相关信息，如获取所需的 身份情报 信息， 第 66 页中所述。

下图显示了一个示例。



步骤 3 （可选。）要让 身份情报 将特定用户组视为可信用户，请将**排除列表**滑动至**滑块已启用** ( )。

按 **username@domain.com** 格式每行输入一个用户名。此列表中的用户会被 身份情报 视为可信用户。

步骤 4 点击**测试**。

仅当测试成功时，才继续执行下一步。

如果显示任何错误，请检查所有 身份情报 值并重试。

步骤 5 点击**下一步 (Next)**。

步骤 6 继续执行查看系统定义的过滤器，第 72 页。

相关主题

关于 动态防火墙，第 63 页
如何配置 动态防火墙，第 63 页

查看系统定义的过滤器

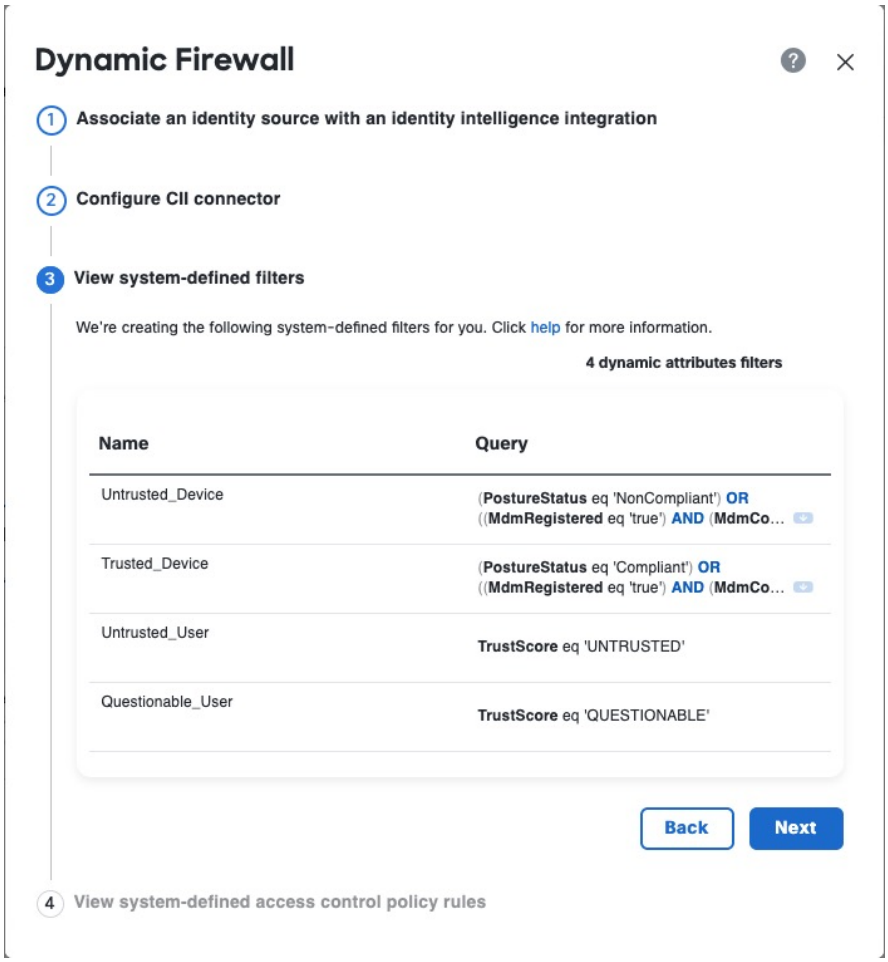
此任务讨论如何将身份源与思科 身份情报 相关联，后者会向 Secure Firewall Management Center 提供用户和设备风险评分。

开始之前

请参阅配置 身份情报，第 71 页。

过程

步骤 1 系统显示一组系统定义的动态属性过滤器，如下图所示。



步骤 2 查看系统创建的过滤器。点击任意行上的 即可展开过滤器，以便查看过滤器及其详细信息。

步骤 3 点击**下一步 (Next)**。

步骤 4 继续执行查看系统定义的访问控制规则，第 73 页。

相关主题

关于 动态防火墙，第 63 页
如何配置 动态防火墙，第 63 页

查看系统定义的访问控制规则

本任务讨论由 动态防火墙 创建的访问控制规则。

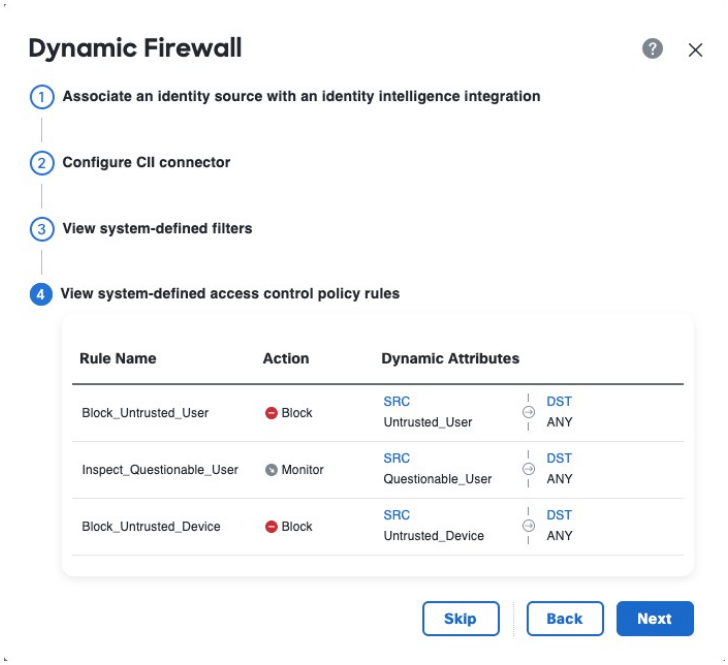
开始之前

请参阅查看系统定义的过滤器，第 72 页。

过程

步骤 1 查看系统创建的访问控制规则。

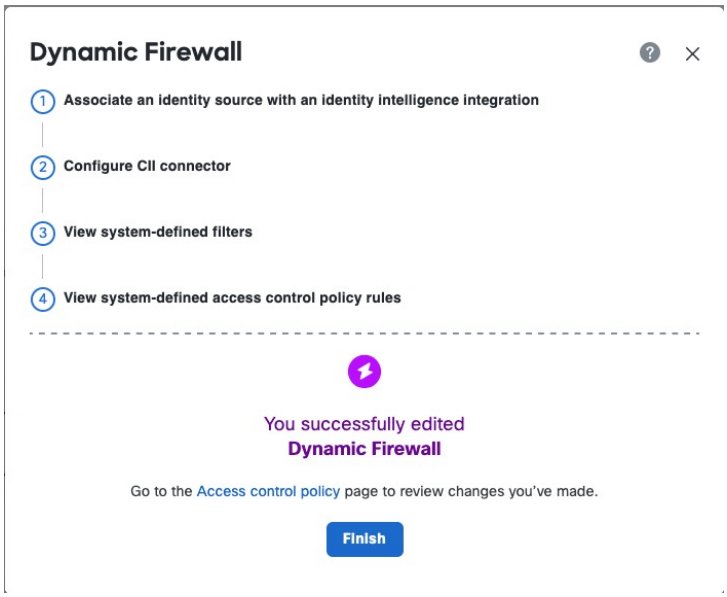
下图显示了一个示例。



步骤 2 选择以下选项之一：

- 点击**跳过**以跳过创建这些访问控制规则。您可以随时创建自己的规则。
- 点击**下一步**，创建一个名为“动态防火墙策略”的访问控制策略，其中包含上图所示的规则。
- 点击**返回**可返回到系统创建的过滤器。

步骤 3 点击**下一步**后，如果成功创建了访问控制规则，将显示以下页面：



相关主题

关于 动态防火墙， 第 63 页
如何配置 动态防火墙， 第 63 页

编辑用户排除列表

（可选。）您可以指示 身份情报 将特定用户视为可信用户。

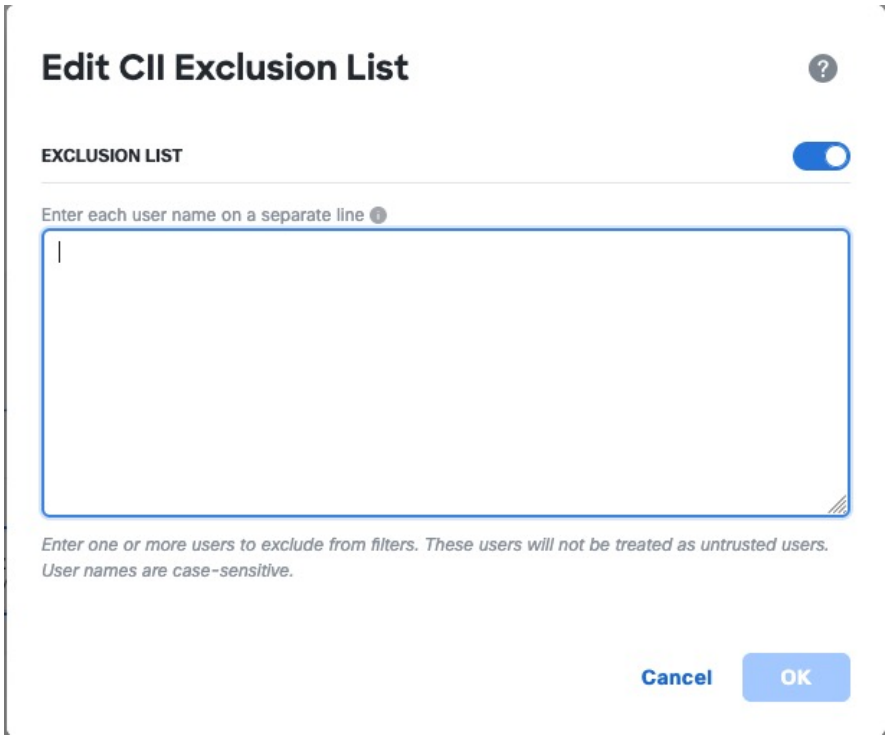
开始之前

按照创建 动态防火墙 实例， 第 68 页中所述配置 动态防火墙。

过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center。
步骤 2 请点击 **集成** > **动态属性连接器**。
步骤 3 点击身份源名称旁边的 。
步骤 4 点击**编辑 CII 排除列表**。

系统将显示以下对话框。



步骤 5 在提供的字段中，按 `username@domain.com` 格式在一行中输入一个用户名，按 Enter 键，然后输入另一个用户名。

每个用户名都会被 身份情报 视为可信用户。

相关主题

关于 动态防火墙，第 63 页
如何配置 动态防火墙，第 63 页

查看和编辑系统创建的访问控制策略

本主题讨论如何编辑系统创建的访问控制规则和策略。最初，该策略未与任何设备关联，但如果要使用它，可添加设备、更改规则、重新排序规则或删除规则。

开始之前

完成查看系统定义的访问控制规则，第 73 页中所述的任务。

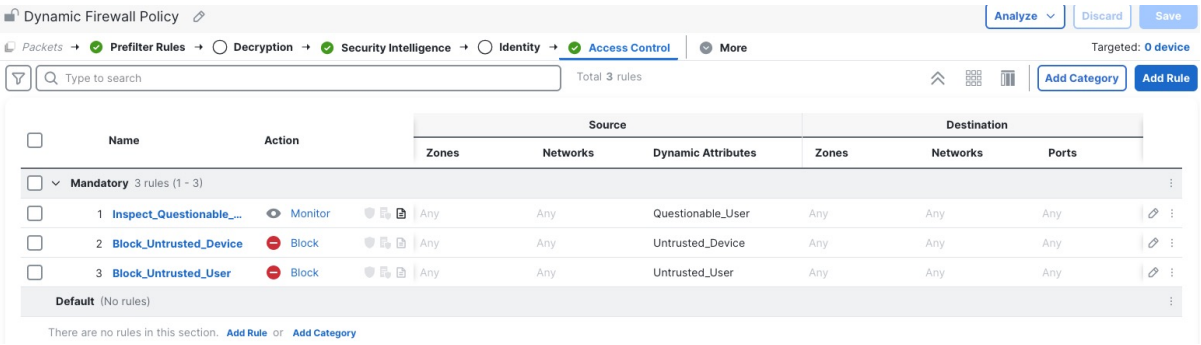
过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center。

步骤 2 请点击 **策略** > **安全策略** > **访问控制**。

步骤 3 点击名为“动态防火墙策略”（或类似名称）的策略旁边的 **编辑** ()。

下图显示了一个示例访问控制策略。



请注意，在此访问控制策略中，只有设置为监控可疑用户的规则会记录日志。要调整日志记录设置，请参阅访问控制策略的日志记录设置。

步骤 4 执行以下任一操作：

- 将访问控制策略定位到设备：将设备分配给访问控制策略。
- 编辑策略，包括添加日志记录：管理访问控制策略。
- 编辑访问控制规则：管理访问控制规则。
- 设置高级策略选项：为访问控制策略配置高级设置。
- 将其他策略与该访问控制策略关联： 将其他策略与访问控制相关联。

相关主题

关于 动态防火墙 ， 第 63 页
如何配置 动态防火墙 ， 第 63 页

创建动态属性过滤器

使用 Dynamic Attributes Connector 定义的动态属性过滤器会在 Secure Firewall Management Center 中显示为可在访问控制策略中使用的动态对象。例如，您可以将财务部门对 AWS 服务器的访问权限限制为 Microsoft Active Directory 中定义的财务组成员。

有关访问控制规则的详细信息，请参阅使用动态属性过滤器来创建访问控制规则或 DNS 规则。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新过滤器：点击 **添加** ()。
- 编辑或删除过滤器：点击 **更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

项目	说明
名称	用于在访问控制策略和 Secure Firewall Management Center 对象管理器（**外部属性 (External Attributes)** > **动态对象 (Dynamic Object)**）中标识动态过滤器（作为动态对象）的唯一名称。
连接器	在列表中点击要使用的连接器的名称。
查询	请点击 添加  。

步骤 5 要添加查询，请输入以下信息。

项目	说明
密钥	点击列表中的一个键。密钥会从连接器获取。
操作	点击以下选项之一： • **等于 (Equals)** 会将密钥与值完全匹配。 • **包含 (Contains)** 会将键与值匹配（如果值的任何部分匹配）。
值	点击**任意 (Any)** 或**全部 (All)**，然后点击列表中的一个或多个值。点击**添加其他值 (Add another value)** 以便向查询中添加值。

步骤 6 点击**显示预览 (Show Preview)** 以便显示查询返回的网络或 IP 地址的列表。

步骤 7 完成后，点击**保存**。

步骤 8 （可选。）验证 Secure Firewall Management Center 中的动态对象。

a) 至少要以具有网络管理员角色的用户身份登录 Secure Firewall Management Center 。

b) 请点击 **对象 (Objects)** > **外部属性 (External Attributes)** > **动态对象 (Dynamic Object)**。
您创建的动态属性查询应显示为动态对象。

相关主题

关于 动态防火墙 ， 第 63 页
如何配置 动态防火墙 ， 第 63 页

禁用 dynamic attributes connector

如果您不想再从云源收集动态对象，可以禁用 Dynamic Attributes Connector 中的 Secure Firewall Management Center ，如以下任务中所述。

过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center 。

步骤 2 请点击 **集成** > **动态属性连接器**。

步骤 3 滑动到 **已禁用**。

使用 Secure Firewall Management Center 进行故障排除

此任务讨论如何为 Secure Firewall Management Center生成故障排除文件。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 > **运行状况** > **监控器故障排除** 。

步骤 3 在左侧窗格中，点击 **防火墙管理中心**。

步骤 4 点击顶部的 **系统和故障排除详细信息**。

步骤 5 点击 **Generate Troubleshooting Files**。

步骤 6 将文件提供给思科 TAC 或您的 Beta 版协调员。

手动获取证书颁发机构 (CA) 链

在事件中无法自动获取证书颁发机构链，使用以下浏览器特定程序之一获取用于安全连接到vCenter、防火墙管理中心。

证书链是根证书和所有从属证书。

您可以选择使用以下程序之一连接到以下设备：

- vCenter 或 NSX
- 防火墙管理中心

- 思科 APIC

获取证书链 - Mac（Chrome 和 Firefox）

使用此程序在 Mac OS 上使用 Chrome 和 Firefox 浏览器来获取证书链。

1. 打开终端窗口。
2. 输入以下命令。

   ```
   security verify-cert -P url[:port]
   ```

   其中 *url* 是 vCenter、 防火墙管理中心 的 URL（包括方案）。例如：

   ```
   security verify-cert -P https://myvcenter.example.com
   ```

   如果使用 NAT 或 PAT 访问 vCenter、 防火墙管理中心，可以按如下方式添加端口：

   ```
   security verify-cert -P https://myvcenter.example.com:12345
   ```

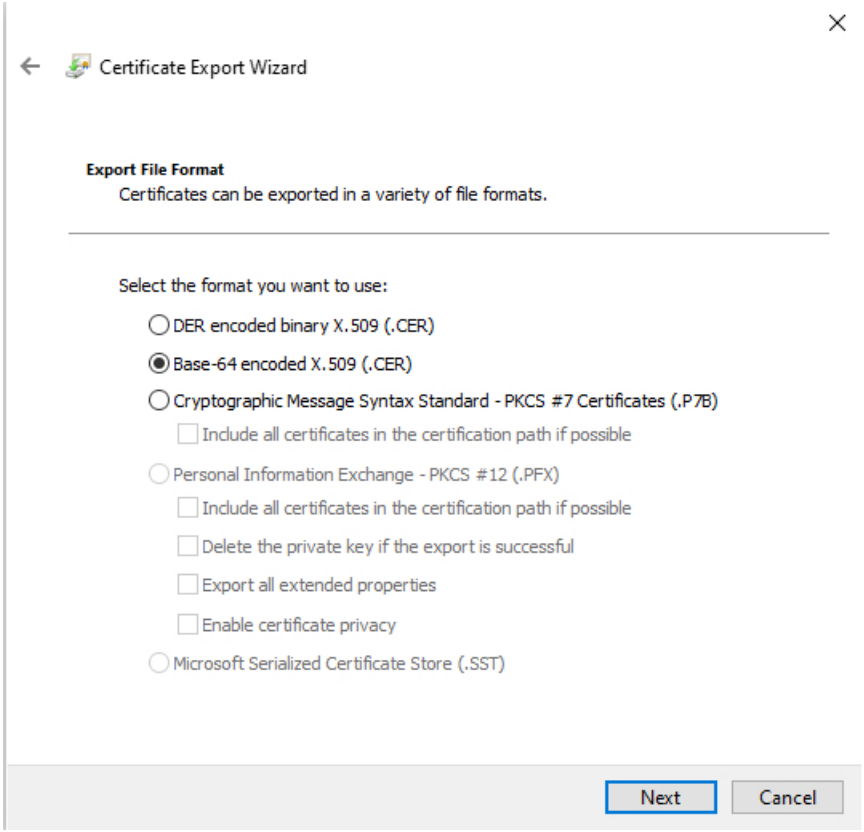
3. 将整个证书链保存到纯文本文件中。
   - 包括所有 `-----BEGIN CERTIFICATE-----` 和 `-----END CERTIFICATE-----` 分隔符。
   - 排除任何无关的文本（例如，证书的名称和尖括号 (< and >) 中包含的任何文本以及尖括号本身。
4. 对 vCenter 防火墙管理中心 重复这些任务。

获取证书链 - Windows Chrome

使用此程序在 Windows 上使用 Chrome 浏览器来获取证书链。

1. 使用 Chrome 登录 vCenter、 防火墙管理中心。
2. 在浏览器地址栏中点击主机名左侧的锁图标。
3. 点击**证书 (Certificate)**。
4. 点击**认证路径 (Certification Path)** 选项卡。
5. 点击证书链中顶部的（即第一个）证书。
6. 点击**查看证书 (View Certificates)**。
7. 点击**详细信息 (Details)** 选项卡。
8. 点击**复制到文件 (Copy to File)**。
9. 按照提示创建包含整个证书链的 CER 格式证书文件。

   当系统提示您选择导出文件格式时，点击 **Base 64-Encoded X.509 (.CER)**，如下图所示。



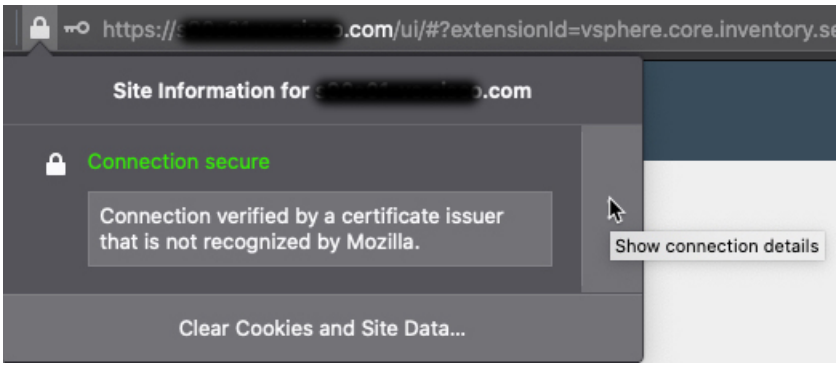
10. 按照提示完成导出。
11. 在文本编辑器中打开证书。
12. 对证书链中的所有证书重复此过程。

    您必须先按顺序将每个证书粘贴到文本编辑器中。
13. 对 vCenter、 防火墙管理中心 重复这些任务。

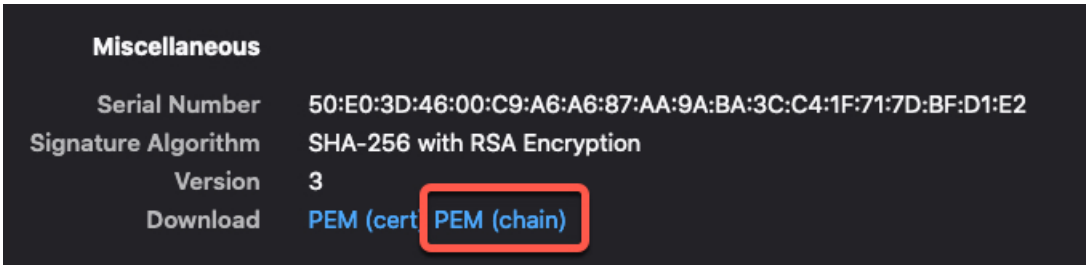
获取证书链 - Windows Firefox

使用以下程序为 Windows 或 Mac OS 上的 Firefox 浏览器来获取证书链。

1. 使用 Firefox 登录 vCenter、 防火墙管理中心。
2. 点击主机名左侧的锁图标。
3. 点击右箭头（**显示连接详细信息**）。下图显示了一个示例。



4. 点击**更多信息 (More Information)**。
5. 点击**查看证书 (View Certificates)**。
6. 如果生成的对话框包含选项卡页面，请点击与顶层 CA 对应的选项卡页面。
7. 滚动到“其他”(Miscellaneous) 部分。
8. 点击下载行中的 **PEM（链）(PEM [chain])**。下图显示了一个示例。



9. 保存文件。
10. 对 vCenter、 防火墙管理中心 重复这些任务。

相关主题

与 思科 APIC 集成的系统要求 ， 第 30 页
获取集成所需的信息 ， 第 30 页
创建连接器思科 APIC ， 第 34 页
如何在访问控制规则或 DNS 规则中使用 Secure Firewall Management Center 中 思科 APIC 的动态对象 ， 第 29 页
手动获取证书颁发机构 (CA) 链 ， 第 35 页
思科 APIC 连接器 ， 第 28 页

安全要求

为了保护dynamic attributes connector，应将其安装在受保护的内部网络中。虽然dynamic attributes connector被配置为仅提供必要的服务和端口，但您必须确保该防御中心不会受到攻击。

如果 dynamic attributes connector 和 Secure Firewall Management Center 位于同一个网络，您可以将 Secure Firewall Management Center 连接到与 dynamic attributes connector 相同的受保护内部网络。

无论如何部署设备，内部系统通信将始终加密。但是，您仍需采取措施，确保设备之间的通信不会出现中断、阻塞或受到篡改；例如，遭受分布式拒绝服务 (DDoS) 或中间人攻击。

互联网接入要求

默认情况下，dynamic attributes connector 会被配置为使用端口 443/tcp (HTTPS) 上的 HTTPS 通过互联网与 Firepower 系统通信。如果您不希望 dynamic attributes connector 直接访问互联网，则可以配置代理服务器。

以下信息会告知您 dynamic attributes connector 用来与 Secure Firewall Management Center 和外部服务器通信的 URL。

表 *4: Dynamic Attributes Connector* 访问要求

URL	原因
https://*fmc-ip***/api/fmc_platform/v1/auth/generatetoken**	身份验证
https://*fmc-ip***/api/fmc_config/v1/domain/***domain-id***/object/dynamicobjects**	GET 和 POST 动态对象
https://*fmc-ip***/api/fmc_config/ v1/domain/***domain-id***/object/dynamicobjects/***object-id***/mappings?action=add**	添加映射
https://*fmc-ip***/api/fmc_config/v1/domain/***domain-id* **/object/dynamicobjects/***object-id***/mappings?action=remove**	删除映射

表 *5: Dynamic Attributes Connector vCenter* 访问要求

URL	原因
https://*vcenter-ip***/rest/com/vmware/cis/session**	身份验证
https://*vcenter-ip***/rest/vcenter/vm**	获取 VM 信息
https://*nsx-ip***/api/v1/fabric/virtual-machines/***vm-id***	获取与虚拟机关联的 NSX-T 标记

从 DockerHub 迁移到 Amazon ECR

Dynamic Attributes Connector 的 Docker 映像正在从 Docker Hub 迁移到 Amazon Elastic Container Registry (Amazon ECR)。

要使用新的字段包，必须允许通过防火墙或代理访问以下所有 URL：

- https://public.ecr.aws
- https://csdac-cosign.s3.us-west-1.amazonaws.com
- https://d2glxqk2uabbnd.cloudfront.net
- https://d5l0dvt14r5h8.cloudfront.net

有关 Amazon CloudFront URL 的更多信息，请参阅 EKS Anywhere 文档。

Dynamic Attributes Connector Azure 访问要求

dynamic attributes connector 会调用内置 SDK 方法获取实例信息。这些方法会在内部调用 https://login.microsoft.com（用于身份验证）和 https://management.azure.com（用于获取实例信息）。

dynamic attributes connector 的历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
DNS规则对动态对象和安全组标记的支持。	10.0.0	10.0.0	您可以在 DNS 策略中配置 DNS 规则以使用动态对象或安全组标记 (SGT)。如果您已经在访问控制规则中使用这些类型的对象，现在可以将其使用扩展到您的 DNS 策略。 我们在添加/编辑 DNS 规则对话框中添加了“动态属性”选项卡。
动态防火墙	10.0.0	10.0.0	以前，Secure Firewall Management CenterSecure Firewall Management Center 仅从配置的身份源（如 Microsoft Active Directory、被动身份代理、思科身份服务引擎 (Cisco ISE) 等）收集有关用户的信息。此信息通常包括用户名、组和 IP 地址。 借助 动态防火墙，您可以将来自思科 身份情报 的用户风险评分添加到身份源提供的信息中，以便根据始终最新的用户终端安全评估和风险设置策略。我们支持您将用户身份与智能配对，并在报告和访问控制策略中使用该信息。 **新增/修改的屏幕：** • 请点击 **集成** > **动态属性连接器**。然后点击身份源名称旁的  ，点击**创建动态防火墙**。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
思科 APIC 连接器	10.0.0	10.0.0	dynamic attributes connector 使您能够将 思科 APIC 动态终端组 (EPG) 和终端安全组 (ESG) 数据从 思科 APIC 租户发送到 。 **新增/更新的屏幕：** • **集成** > **动态属性连接器** > **连接器** > **新建连接器**
新连接器	7.6	20241127	AWS 安全组、AWS 服务标签和 Cisco Cyber Vision 这些连接器可以像 Security Cloud Control 一样发送本地 Secure Firewall Management Center 动态对象。 要从本地 dynamic attributes connector 接收动态对象，需要使用 3.0 版本的本地动态属性连接器。
Dynamic Attributes Connector	7.4.0	7.4.0	引入了此功能。 Dynamic Attributes Connector 现在包含在 Secure Firewall Management Center中。您可以在访问控制规则中使用 dynamic attributes connector 从基于云的平台（例如 Microsoft Azure）获取 IP 地址，而无需部署到托管设备。 详细信息： • 此产品随附的 dynamic attributes connector： 关于 dynamic attributes connector，第 1 页 • 独立 dynamic attributes connector： *《Cisco Secure Dynamic Attributes Connector 配置指南》* 新的/修改后的屏幕： **集成** > **动态属性连接器**

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。

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。

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。