对象管理

本章介绍如何管理可重用对象。

对象简介

为了提高灵活性和 Web 界面的易用性，Firepower 系统会使用命名对象，命名对象是将名称与值相关联的可重用配置。当您要使用该值时，可使用命名对象来替代。系统支持在 Web 界面中的不同位置使用这些对象，包括许多策略和规则、事件搜索、报告、控制面板等等。系统提供许多代表常用配置的预定义对象。

使用对象管理器创建和管理对象。许多使用对象的配置也允许您根据需要即时创建对象。您也可以使用对象管理器进行以下操作：

- 查看使用网络、端口、VLAN 或 URL 对象的策略、设置和其他对象；请参阅查看对象及其使用情况，第 8 页。
- 将对象分组，以用一个配置引用多个对象；请参阅对象组，第 10 页。
- 覆盖所选设备或所选域（在多域部署中）的对象值；请参阅对象覆盖，第 11 页。

编辑在活动策略中使用的对象后，必须重新部署更改的配置，才能使更改生效。您无法删除活动策略正在使用的对象。

注释 当且仅当某个对象用于分配到某个受管设备的策略中时，该对象才会在受管设备上予以配置。如果从分配到给定设备的所有策略中删除某个对象，则该对象也会从下一次部署的设备配置中被删除，对其进行的后续更改不会在设备配置中反映出来。

对象类型

下表列出了您可以在 Firepower 系统中创建的对象，并指示是否可以对每个对象类型进行分组或配置以允许覆盖。

对象类型	是否可分组？	是否允许覆盖？
网络	是	是
端口	是	是
接口： • 安全区 • 接口组	否	否

对象类型	是否可分组？	是否允许覆盖？
隧道区域	否	否
应用过滤器	否	否
VLAN 标记	是	是
外部属性：安全组标记 (SGT) 和动态对象	否	否
URL	是	是
地理定位	否	否
时间范围	否	否
变量集	否	否
安全情报：网络、DNS 和 URL 列表和源	否	否
Sinkhole	否	否
文件列表	否	否
密码套件列表	否	否
可分辨名称	是	否
公钥基础设施 (PKI)： • 内部和受信任 CA • 内部和外部证书	是	否
密钥链	否	是
DNS 服务器组	否	否
SLA 监控器	否	否
前缀列表：IPv4 和 IPv6	否	是
路由映射	否	是
访问列表：标准和扩展	否	是
AS 路径	否	是
社区列表	否	是
策略列表	否	是
FlexConfig：文本和 FlexConfig 对象	否	是

对象和多租户

在多域部署中，您可以在全局域和后代域中创建对象，只能在全局域中创建的安全组标记 (SGT) 对象除外。系统会显示在当前域中创建的对象，您可以对其进行编辑。它还会显示在祖先域中创建的对象，但您无法对其进行编辑，除了安全区域和接口组。

注释 因为安全区域和接口组与在分叶级别配置的设备接口绑定，后代域中的管理员可以查看并编辑在祖先域中创建的区域和组。子域用户可以在祖先区域和组中添加和删除接口，但无法删除或重命名区域/组。

对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

对于支持分组的对象，可以将当前域中的对象与从祖先域中继承的对象分到一组。

对象覆盖允许您定义某些类型对象的设备特定或域特定值，包括网络、端口、VLAN 标记和 URL。在多域部署中，可以为祖先域中的对象定义默认值，但允许后代域中的管理员为该对象添加覆盖值。

对象管理器

可以使用对象管理器创建和管理对象和对象组。

对象管理器每页显示 20 个对象或对象组。如果有超过 20 个任何类型的对象或对象组，请使用位于页面底部的导航链接查看其他页面。您还可以转到特定页或点击 **刷新** （ ） 来刷新视图。

默认情况下，页面会按名称的字母顺序列示对象和对象组。您可以按名称或值对页面上的对象进行过滤。

正在导入对象

对象可以通过逗号分隔值文件导入。一次最多可以导入1000个对象。逗号分隔值文件的内容应依照特定的格式。每种对象类型的格式不同。只能导入几种类型的对象。请参阅下表以了解支持的对象类型以及相应的规则。

对象类型	规则

单个对象	• 列标题必须以大写字母表示。
	• 文件必须包含以下列标题：
	  • 名称
	  • DN
	• 要导入条目，必须同时输入 NAME 和 DN 列条目。
	• 您可以将单个对象直接导入到现有的可分辨名称对象组中。

网络对象	• 列标题必须以大写字母表示。
	• 文件必须包含以下列标题：
	  • 名称
	  • DESCRIPTION
	  • TYPE
	  • 值
	  • 查询
	• 必须提供 NAME 和 VALUE 列条目才能导入主机、范围或网络对象类型的条目。
	• 对于 FQDN 对象，TYPE 列条目必须提及“fqdn”，而 LOOKUP 列条目必须指定为“ipv4”、“ipv6”或“ipv4_ipv6”。
	• 如果 FQDN 对象的 LOOKUP 列条目中未提供内容，则要使用 ipv4_ipv6 字段值来保存该对象。

对象类型	规则

Port	• 列标题必须以大写字母表示。
	• 文件必须包含以下列标题：
	  • 名称
	  • PROTOCOL
	  • PORT
	  • ICMPCODE
	  • ICMPTYPE
	• NAME 列条目为必填。
	• 对于“tcp”和“udp”协议类型，PORT 列条目为必填。
	• 对于“icmp”和“icmp6”协议类型，ICMPCODE 和 ICMPTYPE 列条目为必填。

URL	• 列标题必须以大写字母表示。
	• 文件必须包含以下列标题：
	  • 名称
	  • DESCRIPTION
	  • URL
	• 必须提供 NAME 和 URL 列条目才能导入条目。

VLAN 标签	• 列标题必须以大写字母表示。
	• 文件必须包含以下列标题：
	  • 名称
	  • DESCRIPTION
	  • 标签
	• 必须提供 NAME 和 TAG 列条目才能导入条目。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从左侧窗格中选择以下对象类型之一：

- **可分辨名称 (Distinguished Name)** > **单个对象 (Individual Objects)** >
- **网络对象**
- **端口**
- **URL**
- **VLAN 标签**

步骤 3 从**添加 [对象类型] (Add [Object Type])** 下拉列表中选择**导入对象 (Import Object)**。

注释 如果您在上一步中选择了**单个对象 (Individual Objects)**，请点击**导入 (Import)**。

步骤 4 点击**浏览 (Browse)**。

步骤 5 在系统上找到并选择以逗号分隔的文件。

步骤 6 点击 **Open**。

注释 导入**可分辨名称**对象时，可以选中**将导入的可分辨名称对象添加到下面的对象组 (Add imported Distinguished Name objects to the below object group)** 复选框，然后从下拉框中选择组名称，以将对象直接导入现有的可分辨名称对象组。

步骤 7 点击**导入 (Import)**。

编辑对象

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从列表中选择对象类型；请参阅对象简介，第 2 页。

步骤 3 点击要编辑的对象旁边的 **编辑**（）。

如果显示**视图**（），则表明对象属于祖先域且已配置为不允许覆盖，或者您没有修改对象的权限。

步骤 4 根据需要修改对象设置。

步骤 5 如果编辑的是变量集，请管理变量集中的变量；请参阅管理变量，第 98 页。

步骤 6 对于可以配置为允许覆盖的对象：

- 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 13 页。只可以为属于当前域的对象更改此设置。
- 如果要将覆盖值添加到此对象，请展开“覆盖”(Override) 部分并点击**添加 (Add)**；请参阅添加对象覆盖，第 13 页。

步骤 7 点击**保存 (Save)**。

步骤 8 如果编辑的是变量集，并且该变量集正在被一个访问控制策略使用，请点击**是 (Yes)** 以确认要保存更改。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

查看对象及其使用情况

您可以在“对象管理”(Object Management) 页面上查看对象的使用详细信息。管理中心 为许多对象类型提供此功能。但是，某些对象类型不受支持。

注释 在多域部署中，您可以查看任何其他域中的对象。但是，要查看后代域中的对象使用情况，请切换至该域。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 选择以下支持的对象类型之一：

- 访问列表 > 扩展
- 访问列表 > 标准
- AS 路径
- 社区列表
- 接口
- 网络
- 策略列表
- Port
- 前缀列表 > IPv4 前缀列表
- 前缀列表 > IPv6 前缀列表

- 路由映射
- SLA 监控器
- URL
- VLAN 标签

步骤 3 点击对象旁边的 **查找使用情况** （  ） 图标。

“对象使用情况”(Object Usage) 窗口会显示使用对象的所有策略、对象和其他设置的列表。点击列出的任何项目，了解有关对象使用情况的详细信息。对于会用到对象的策略和一些其他设置，您可以点击相应的链接以访问相应的 UI 页面。

过滤对象或对象组

在多域部署中，系统会显示在当前域和祖先域中创建的对象，您可以对其进行过滤。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 在**过滤 (Filter)** 字段中输入过滤器条件。

页面会在您键入内容时进行更新，以显示匹配的项目。

您可以使用以下通配符：

- 星号 (*) 匹配零或重复出现的一个字符。
- 脱字符 (^) 匹配字符串开头的内容。
- 美元符号 ($) 匹配字符串结尾的内容。

步骤 3 选中**显示未使用的对象 (Show Unused Object)** 复选框，以查看系统中任何位置未使用的对象和对象组。

注释

- 如果对象是未使用的对象组的一部分，则该对象会被视为已使用。但是，如果选中**显示未使用的对象 (Show Unused Object)** 复选框，则会显示未使用的对象组。
- **显示未使用的对象 (Show Unused Object)** 复选框仅适用于网络、端口、URL 和 VLAN 标记对象类型。

对象组

将对象分组使得可以引用带有单个配置的多个对象。系统允许在 Web 界面中互用对象和对象组。例如，在任何要使用端口对象的地方，也可以使用端口对象组。

可以将网络、端口、VLAN 标记、URL 和 PKI 对象分组。网络对象组可以嵌套，即您可以将一个网络对象组添加到另一个网络对象组中，最高可达 10 个级别。

相同类型的对象和对象组不能具有相同的名称。在多域部署中，对象组的名称在域层次结构中必须是唯一的。请注意，系统可能会识别出与您在当前域中无法查看的对象组名称的冲突。

编辑策略中使用的对象组（例如，访问控制策略中使用的网络对象组）时，您必须重新部署已更改的配置以使更改生效。

删除组不会删除组中的对象，只会删除对象之间的相关性。此外，您也无法删除活动策略中正在使用的组。例如，无法删除用于已保存访问控制策略中的 VLAN 条件的 VLAN 标记组。

对可重用对象进行分组

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

可以将当前域中的对象与从祖先域中继承的对象分到一组。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 如果要分组的对象类型为**网络 (Network)**、**端口 (Port)**、**URL** 或 **VLAN 标记 (VLAN Tag)**：

a) 从对象类型列表中选择对象类型。

b) 从**添加（对象类型）(Add [Object Type])** 下拉列表中选择**添加组 (Add Group)**。

步骤 3 如果要分组的对象类型为**可分辨名称 (Distinguished Name)**：

a) 展开**可分辨名称 (Distinguished Name)** 节点。

b) 选择**对象组 (Object Groups)**。

c) 点击**添加可分辨名称 (Add Distinguished Name)**。

步骤 4 如果要分组的对象类型为 **PKI**：

a) 展开 **PKI** 节点。

b) 选择以下其中一个选项：

- **内部 CA 证书 (Internal CA Groups)**
- **受信任 CA 证书 (Trusted CA Groups)**
- **内部证书组 (Internal Cert Groups)**
- **外部证书组 (External Cert Groups)**

c) 点击**添加[对象类型]组 (Add [Object Type] Group)**。

步骤 5 在**名称 (Name)** 中输入唯一的名称。

步骤 6 从列表中选择一个或多个对象，然后点击**添加 (Add)**。

您还可以：

- 使用过滤器字段 (**搜索**（）) 可搜索要包括的现有对象，在您键入时，该字段会更新以显示匹配项目。点击搜索字段上方的 **重新加载**（），或点击搜索字段中的 **清除**（） 以清除搜索字符串。
- 如果现有对象不符合您的需要，可点击 **添加**（） 快速创建对象。

步骤 7 或者对于**网络 (Network)**、**端口 (Port)**、**URL** 和 **VLAN 标记 (VLAN Tag)** 组：

- 输入**说明 (Description)**。
- 选中**允许覆盖 (Allow Override)** 复选框，允许对此对象组进行覆盖；请参阅允许对象覆盖，第 13 页。

步骤 8 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象组，请部署配置更改；请参阅部署配置更改。

对象覆盖

通过对象覆盖，您可以为对象定义一个备选值，系统将为您指定的设备使用该值。

您可以创建其定义适用于大多数设备的对象，然后使用覆盖为需要不同定义的几个设备指定对象的修改。您还可以创建需要为所有设备覆盖的对象，但其使用使您能够为所有设备创建单个策略。对象覆盖允许您创建较小的一组在设备间使用的共享策略，而不会失去在各个设备需要时修改策略的能力。

例如，您可能想要拒绝 ICMP 流量传送到公司的不同部门，每个部门连接到不同的网络。可以通过定义带有特定规则（包括一个称为“部门网络”的网络对象）的访问控制策略来实现。通过允许覆盖此对象，即可在每个相关设备上创建覆盖，指定该设备所连接的实际网络。

在多域部署中，可以为祖先域中的对象定义默认值，并允许后代域中的管理员为该对象添加覆盖值。例如，托管安全服务提供商 (MSSP) 可以使用单一 管理中心来管理多个客户的网络安全。MSSP 的管理员可以在全局域中定义在所有客户的部署中使用的对象。每个客户的管理员可以登录后代域，为其组织覆盖该对象。这些本地管理员无法查看或影响 MSSP 的其他客户的覆盖值。

您可以将对象覆盖的目标对准特定域。在这种情况下，除非已在设备级覆盖该值，否则系统会将对象覆盖值用于目标域中的所有设备。

在对象管理器中，可以选择可覆盖的对象并为该对象定义设备级或域级覆盖列表。

只能使用具有以下对象类型的对象覆盖：

- 网络
- 端口
- VLAN 标记
- URL
- SLA 监控器
- 前缀列表
- 路由映射
- 访问列表
- AS 路径
- 社区列表
- 策略列表
- PKI 注册
- 密钥链

如果可以覆盖对象，则系统会在对象管理器中为该对象类型显示**覆盖 (Override)** 列。此列的可能值包括：

- 绿色勾选标记 - 表示可为对象创建覆盖且尚未添加任何覆盖
- 红色 X - 表示无法为对象创建覆盖
- 数字 - 表示已添加到该对象的覆盖计数（例如，“2”表示已添加两个覆盖）

管理对象覆盖

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中进行选择；请参阅对象简介，第 2 页。

步骤 3 点击要编辑的对象旁边的 **编辑**（）。

如果显示**视图**（），则表明对象属于祖先域且已配置为不允许覆盖，或者您没有修改对象的权限。

步骤 4 管理对象覆盖：

- 添加 - 添加对象覆盖；请参阅添加对象覆盖，第 13 页。
- 允许 - 允许对象覆盖；请参阅允许对象覆盖，第 13 页。
- 删除 - 在对象编辑器中，点击要删除的覆盖旁边的 **删除**（）。

- 编辑 - 编辑对象覆盖；请参阅编辑对象覆盖 ， 第 14 页。

允许对象覆盖

过程

步骤 1 在对象编辑器中，选中**允许覆盖**复选框。

步骤 2 点击**保存 (Save)**。

下一步做什么

添加对象覆盖值；请参阅添加对象覆盖 ， 第 13 页。

添加对象覆盖

开始之前

允许对象覆盖；请参阅允许对象覆盖 ， 第 13 页。

过程

步骤 1 在对象编辑器中，展开**覆盖**部分。

步骤 2 点击**添加 (Add)**。

步骤 3 在**目标 (Targets)** 中，选择**可用设备和域 (Available Devices and Domains)** 列表中的域或设备，然后点击**添加 (Add)**。

步骤 4 在“覆盖”(Override) 选项卡中，输入**名称**。

步骤 5 输入**说明**（可选）。

步骤 6 输入覆盖值。

示例：

对于网络对象，请输入网络值。

步骤 7 点击**添加 (Add)**。

步骤 8 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

编辑对象覆盖

可以修改说明和现有覆盖的值，但不可以修改现有目标列表。相反，您必须添加一个具有新目标的新覆盖，该覆盖将代替现有覆盖。

过程

步骤 1 在对象编辑器中，展开**覆盖 (Override)** 部分。

步骤 2 点击要修改的覆盖旁边的 **编辑**（）。

步骤 3 或者，修改**说明 (Description)**。

步骤 4 修改覆盖值。

步骤 5 点击**保存 (Save)** 保存覆盖。

步骤 6 点击**保存 (Save)** 保存对象。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

AAA 服务器

添加可重用的 AAA 服务器对象。

添加 RADIUS 服务器组

Radius 服务器组对象包含一个或多个对 RADIUS 服务器的引用。这些服务器用于对通过远程接入 VPN 连接登录的用户进行身份验证。

您可以将此对象与 威胁防御 设备一起使用。

开始之前

注释 不能覆盖 Radius 服务器组对象。

过程

步骤 1 选择 **对象** > **对象管理** > **AAA 服务器** > **Radius 服务器组**。

将列出所有当前配置的 Radius 服务器组对象。使用过滤器缩小列表的范围。

步骤 2 选择并编辑列出的 Radius 服务器组对象，或者添加一个新的对象。

参阅RADIUS 服务器选项，第 16 页和RADIUS 服务器组选项，第 15 页以配置此对象。

步骤 3 点击**保存**

RADIUS 服务器组选项

导航路径

对象 > **对象管理** > **AAA 服务器** > **RADIUS 服务器组**。选择并编辑已配置的 RADIUS 服务器组对象，或添加一个新的相应对象。

字段

- **名称**和**说明** - 输入名称，并可选择性地输入说明，以标识此 RADIUS 服务器组对象。
- **组记帐模式** - 将记帐消息发送到组中的 RADIUS 服务器的方法。选择**单个**，记帐消息会发送到组中的单个服务器，这是默认设置。或者，选择 **多个**，记帐消息将同时发送到组中的所有服务器。
- **重试间隔** - 两次尝试与 RADIUS 服务器联系之间的间隔。值范围为 1 秒至 10 秒。
- **领域**（可选）- 指定或选择此 RADIUS 服务器组与之关联的 Active Directory (AD) 领域。然后，在身份策略中选择此领域，以便在确定流量的 VPN 身份验证身份源时访问关联的 RADIUS 服务器组。此领域有效地提供了从身份策略到此 Radius 服务器组的桥接。如果没有与此 RADIUS 服务器组关联的领域，则无法访问 RADIUS 服务器组以确定身份策略中流量的 VPN 身份验证身份源。

注释 如果使用具有用户身份和 RADIUS 作为身份源的远程访问 VPN，则此字段为必填。

- **仅启用授权** - 如果此 RADIUS 服务器组未用于身份验证，但正在用于授权或记帐，请选中此字段以为 RADIUS 服务器组启用仅授权模式。

  在仅授权模式下，无需在 Access-Request 中包含 RADIUS 服务器密码。因此，为各个 RADIUS 服务器配置的密码将被忽略。

- **启用临时帐户更新**和**间隔** - 启用生成 RADIUS 临时记帐更新消息的功能，以便将新分配的 IP 地址通知 RADIUS 服务器。在“间隔”字段中设置定期记帐更新之间的间隔长度（以小时为单位）。有效范围是 1 至 120，默认值为 24。
- **启用动态授权**和**端口** - 为此 RADIUS 服务器组启用 RADIUS 动态授权或授权更改 (CoA) 服务。在**端口**字段中指定用于 RADIUS CoA 请求的侦听端口。有效范围是 1024 至 65535，默认值为 1700。定义后，相应的 RADIUS 服务器组将注册用于 CoA 通知，并侦听相应端口以获取来自思科身份服务引擎 (ISE) 的 CoA 策略更新。

- **RADIUS 服务器** - 请参阅RADIUS 服务器选项，第 16 页。

相关主题

添加 RADIUS 服务器组，第 14 页

RADIUS 服务器选项

导航路径

对象 > **对象管理** > **AAA 服务器** > **Radius 服务器组**。选择并编辑某一已列出的 RADIUS 服务器组对象，或者添加一个新的 RADIUS 服务器组对象。然后在“RADIUS 服务器组”对话框中，选择并编辑某一已列出的 RADIUS 服务器，或者添加一个新的 RADIUS 服务器。

字段

- **IP 地址/主机名** - 标识将要向其发送身份验证请求的 RADIUS 服务器的主机名或 IP 地址的网络对象。只能选择一项，以向“RADIUS 服务器组”列表中添加其他服务器、添加其他 RADIUS 服务器。

注释 设备现在支持 IPv6 IP 地址用于 RADIUS 身份验证。

- **身份验证端口** - 在其上执行 RADIUS 身份验证和授权的端口。默认值为 1812。
- **密钥**和**确认密钥** - 用于在受管设备（客户端）与 RADIUS 服务器之间加密数据的共享密钥。

  该密钥是一个区分大小写的字母数字字符串，最多 127 个字符。允许使用特殊字符。

  在此字段中定义的密钥必须与 RADIUS 服务器上的密钥相匹配。在“确认”字段中再次数据该密钥。
- **记帐端口** - 在其上执行 RADIUS 记帐的端口。默认值为 1813。
- **超时** - 身份验证的会话超时。

注释 RADIUS 双因素身份验证的超时值必须为 60 秒或以上。默认超时值为 10 秒。

- **连接方式** - 使用路由查找或特定接口建立从设备到 RADIUS 服务器的连接。
  - 点击**路由 (Routing)** 单选按钮以使用路由表。
  - 点击**特定接口 (Specific Interface)** 单选按钮，然后从下拉列表中选择一个安全区/接口组或诊断 接口（默认）。。
- **重定向 ACL** - 从列表中选择重定向 ACL 或添加新 ACL。

注释 此为在设备中定义的用于决定重定向流量的ACL名称。此处的重定向ACL名称必须与 ISE 服务器中的 *redirect-acl* 名称相同。在配置 ACL 对象时，请确保对ISE和DNS服务器选择“阻止”操作，并对其余服务器选择“允许”操作。

相关主题

添加 RADIUS 服务器组，第 14 页
RADIUS 服务器组选项，第 15 页

添加单点登录服务器

开始之前

从 SAML 身份提供程序获取以下信息：

- 身份提供程序实体 ID URL
- 登录 URL
- 注销 URL
- 身份提供者证书，并使用 管理中心 Web 界面（**设备 (Devices)** > **证书 (Certificates)**）在 威胁防御 中注册证书

有关详细信息，请参阅配置 SAML 单点登录身份验证。

过程

步骤 1 依次选择 **对象** > **对象管理** > **AAA服务器** > **单点登录服务器**。

步骤 2 点击 **添加单点登录服务器** 并提供以下详细信息：

- **名称**-SAML 单点登录服务器对象的名称。
- **身份提供程序实体 ID (Identity Provider Entity ID)** - 在 SAML IdP 中定义的用于唯一标识服务提供商的 URL。

  用于提供元数据 XML 的页面的 URL，元数据 XML 说明了 SAML 颁发者将如何响应请求。
- **SSO URL**-用于登录到 SAML 身份提供程序服务器的 URL。
- **注销 URL**-用于注销 SAML 身份提供程序服务器的 URL。
- **基本 URL (Base URL)** - 在身份提供程序身份验证完成后，将用户重定向回 威胁防御 的 URL。这是为 威胁防御 远程访问 VPN 配置的访问接口的 URL。

- **身份提供程序证书 (Identity Provider Certificate)** - 注册到 威胁防御 以验证由 IdP 签名的消息的 IdP 的证书。

  从列表中选择一个标识提供程序证书，或点击添加以创建新的证书注册对象。

  有关详细信息，请参阅管理 威胁防御 证书。

  您必须在 威胁防御上将所有 Microsoft Azure 注册应用 CA 证书注册为信任点。Microsoft Azure SAML 身份提供程序在 威胁防御上为初始应用配置。所有连接配置文件映射到配置的 MS Azure SAML 身份提供程序。对于每个 MS Azure 应用（默认设置除外），您可以在远程访问 VPN 的连接配置文件配置中选择所需的信任点（CA 证书）。

  有关详细信息，请参阅配置远程访问 VPN 的 AAA 设置。

- **服务提供商证书 (Service Provider Certificate)** - 威胁防御 证书，用于签署请求并与 IdP 建立信任圈。

  如果您尚未注册内部 威胁防御 证书，请点击 **+** 添加并注册证书。有关详细信息，请参阅管理 威胁防御 证书。

- **请求签名**-选择用于对 SAML 单点登录请求签名的加密算法。

  签名从最弱到最强列出：SHA1，SHA256，SHA384，SHA512。选择“无”可禁用加密。

- **请求超时 (Request Timeout)** - 指定用户完成单点登录请求的 SAML 断言有效期。SAML IdP 有两个超时： *NotBefore* 和 *NotOnOrAfter*。威胁防御 会验证其当前时间是否在（下限）*NotBefore* 和（上限）*NotBefore* 加上 *timeout* 和 *NotOnOrAfter* 中的较小者的时间范围内。因此，如果设置的超时长于 IdP 的 *NotOnOrAfter* 超时，则忽略指定的超时，并选择 *NotOnOrAfter* 超时。如果指定超时和 *NotBefore* 超时的总和小于 *NotOnOrAfter* 时间，则 威胁防御 超时会覆盖超时。

  超时范围是 1-7200 秒，默认是 300 秒。

- **启用仅在内部网络上可访问的 IdP (Enable IdP only accessible on Internal Network)** - 如果 SAML IdP 位于内部网络上，请选择此选项。威胁防御 会充当网关，并使用匿名 webvpn 会话在用户和 IdP 之间建立通信。

- **请求 IdP 在登陆重新进行身份验证**-选择此选项以在每次登录时对用户进行身份验证，即使之前的 IdP 会话有效。

- **允许覆盖**-选中此复选框以允许对此单点登录服务器对象进行覆盖。

步骤 3 点击**保存 (Save)**。

相关主题

配置远程访问 VPN 的 AAA 设置

访问列表

访问列表对象（也称为访问控制列表[ACL]），选择服务将应用到的流量。您可在配置特定功能（例如路由映射，对 威胁防御 设备）时使用这些对象。对于识别为 ACL 所允许的流量，系统会提供服务，而“阻止”流量则会从服务中排除。从服务中排除流量未必意味着完全丢弃该流量。

您可以配置以下类型的 ACL：

- 扩展 - 根据源地址/端口和目标地址/端口识别流量。支持 IPv4 和 IPv6 地址（可以在给定规则中混用）。
- 标准 - 仅根据目标地址识别流量。仅支持 IPv4。

ACL 由一个或多个访问控制条目 (ACE) 或规则组成。ACE 的顺序非常重要。当评估 ACL 以确定数据包是否与“允许的”ACE 匹配时，该数据包会按照条目的列出顺序针对每个 ACE 进行测试。找到匹配项后，不再检查更多 ACE。例如，如果要“允许”10.100.10.1，但是“阻止”10.100.10.0/24 的其余地址，则允许条目必须在阻止条目之前。一般来说，将更具体的规则置于 ACL 的顶部。

与“允许”条目不匹配的数据包被视为受阻止。

以下主题介绍如何配置 ACL 对象。

配置扩展 ACL 对象

当要根据源和目标地址、协议和端口、应用组匹配流量时或者如果流量为IPv6，可使用扩展ACL对象。

过程

步骤 1 依次选择**对象 (Objects)** > **对象管理 (Object Management)** 并从目录中选择**访问控制列表 (Access Control Lists)** > **扩展 (Extended)**。

步骤 2 执行以下操作之一：

- 点击**添加扩展 ACL (Add Extended ACL)** 以创建新对象。
- 点击 **编辑**（ ） 以编辑现有对象。

步骤 3 在“扩展 ACL 对象”(Extended ACL Object) 对话框中，输入对象的名称（不允许使用空格），并配置访问控制条目：

a) 执行以下操作之一：

- 点击**添加 (Add)** 以创建新条目。
- 点击 **编辑**（ ） 以编辑现有条目。

右键点击菜单还包括用于剪切、复制和粘贴条目或者删除这些条目的选项。

b) 选择**操作 (Action)**，是允许（匹配）还是阻止（不匹配）流量标准。

注释 **日志记录 (Logging)**、**日志级别 (Log Level)** 以及**日志间隔 (Log Interval)** 选项仅用于访问规则（附加到接口或全局应用的 ACL）。由于 ACL 对象不用于访问规则，请将这些值保留其默认值。

c) 使用以下任一方法在**网络 (Network)** 选项卡上配置源和目标地址：

- 从“可用”(Available) 列表中选择所需的网络对象或组，然后点击**添加到源 (Add to Source)** 或**添加到目标 (Add to Destination)**。您可以通过点击列表上方的 + 按钮创建新对象。您可以混合使用 IPv4 和 IPv6 地址。
- 在源或目标列表下面的编辑框中输入地址并点击**添加 (Add)**。您可以指定单个主机地址（如 10.100.10.5 或 2001:DB8::0DB8:800:200C:417A）或子网（10.100.10.0/24 或 10.100.10.0 255.255.255.0 格式，或 2001:DB8:0:CD30::/60 这种 IPv6 格式）。

d) 点击**端口 (Port)** 选项卡并使用以下任一方法配置服务。

- 从可用列表中选择所需的端口对象，然后点击 **添加到源** 或 **添加到目标**。您可以通过点击列表上方的 + 按钮创建新对象。对象可以指定 TCP/UDP 端口、ICMP/ICMPv6 消息类型或其他协议（包括“任意”[any]）。但是，通常留空的源端口只接受 TCP/UDP。您无法选择端口组。

  对于TCP/UDP，请注意，如果同时指定了源和目标字段，则必须在两者中使用相同的协议。例如，您不能指定 UDP 源端口和 TCP 目标端口。

- 在源或目标列表下面的编辑框中输入或选择端口或协议并点击**添加 (Add)**。

注释 要获取适用于所有 IP 流量的条目，请选择指定“所有”协议的目标端口对象。

e) 点击 **应用** 选项卡，然后选择要为直接互联网访问策略分组的应用。

重要事项

- 不能为集群设备配置应用。因此，此选项卡不适用于集群设备。
- 仅对策略型路由中的应用使用扩展 ACL。请勿在其他策略中使用它，因为其行为未知且不受支持。

注释

- **可用应用** 列表显示一组固定的预定义应用。此列表是访问控制策略上可用的应用的子集，因为只有第一个数据包（FQDN 终端解析为 IP 地址和端口）可以检测到这些应用。应用定义通过 VDB 更新进行更新，并在后续部署期间推送到 威胁防御 。
- 不支持用户定义的自定义应用或应用组。
- 目前， 管理中心 既不支持用户定义的自定义应用或应用组，也不允许您修改预定义的应用列表。
- 您可以使用应用过滤器下提供的 **应用过滤器** 优化此列表。

f) 选择所需的应用，然后点击 **添加到规则**。

注释
- 请勿在扩展 ACL 对象中配置目标网络和应用。
- 每个访问控制条目中的所选应用（Nertwork 服务对象）组成一个网络服务组 (NSG)，此组部署在 威胁防御上。NSG 用于直接互联网访问，根据与所选应用组的匹配对流量进行分类。

g) 点击**添加 (Add)** 以将条目添加到对象。
h) 如有必要，请点击并拖动条目，以按照规则顺序将其上移或下移到所需位置。

重复该过程以创建或编辑对象中的其他条目。

步骤 4 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 13 页。

步骤 5 点击**保存 (Save)**。

配置标准 ACL 对象

当要仅根据目标 IPv4 地址匹配流量时，请使用标准 ACL 对象。否则，请使用扩展 ACL。

过程

步骤 1 依次选择**对象 (Object)** > **对象管理 (Object Management)** 并从目录中选择**访问控制列表 (Access Control Lists)** > **标准 (Standard)**。

步骤 2 执行以下操作之一：
- 点击**添加标准 ACL (Add Standard ACL)** 以创建新对象。
- 点击 **编辑**（ ） 以编辑现有对象。

步骤 3 在“标准 ACL 对象”(Standard ACL Object) 对话框中，输入对象的名称（不允许使用空格），并配置访问控制条目：

a) 执行以下操作之一：
- 点击**添加 (Add)** 以创建新条目。
- 点击 **编辑**（ ） 以编辑现有条目。

右键点击菜单还包括用于剪切、复制和粘贴条目或者删除这些条目的选项。

b) 对于每个访问控制条目，请配置以下属性：
- **操作 (Action)** - 是允许（匹配）还是阻止（不匹配）流量标准。
- **网络 (Network)** - 添加用于识别流量目标的 IPv4 网络对象或组。

c) 点击**添加 (Add)** 以将条目添加到对象。
d) 如有必要，请点击并拖动条目，以按照规则顺序将其上移或下移到所需位置。

重复该过程以创建或编辑对象中的其他条目。

步骤 4 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 13 页。

步骤 5 点击**保存 (Save)**。

地址池

您可以为 IPv4 和 IPv6 配置 IP 地址池，该地址池可用于 具有 集群 的诊断接口，或 用于 VPN 远程访问配置文件。

过程

步骤 1 选择**对象** > **对象管理** > **地址池** > **IPv4 池**。

步骤 2 点击**添加 IPv4 池**并配置以下字段：

- **名称** - 输入地址池的名称。最多可包含 64 个字符
- **说明** - 为该池添加可选说明。
- **IP 地址** - 输入池中可用地址的范围。在开始地址和结束地址之间使用虚线十进制符号和破折号，例如：10.10.147.100-10.10.147.177。
- **掩码** - 标识此 IP 地址池所属的子网。
- **允许覆盖** - 选中此复选框可启用对象覆盖。点击展开箭头可显示**覆盖**表。您可以通过点击**添加**来添加新的覆盖。有关详细信息，请参阅对象覆盖，第 11 页。

步骤 3 点击**保存**。

步骤 4 点击**添加 IPv6 池**并配置以下字段：

- **名称** - 输入地址池的名称。最多可包含 64 个字符
- **说明** - 为该池添加可选说明。
- **IPv6 地址** - 输入配置的池中可用的第一个 IP 地址和前缀长度（以位为单位）。例如：2001:DB8::1/64。
- **地址数量** - 标识地址池中从开始 IP 地址开始的 IPv6 地址的数量。
- **允许覆盖** - 选中此复选框可启用覆盖。点击展开箭头可显示**覆盖**表。您可以通过点击**添加**来添加新的覆盖。有关详细信息，请参阅对象覆盖，第 11 页。

步骤 5 点击**保存 (Save)**。

应用过滤器

借助系统提供的应用过滤器，您可以根据应用的基本特征（类型、风险、业务关联性、类别和标记）组织应用，从而执行应用控制。您可以在对象管理器中，以系统提供的过滤器的组合为基础或以应用的自定义组合为基础，创建并管理可重复使用的用户定义的应用过滤器。有关详细信息，请参阅应用规则条件。

AS 路径

AS 路径是用于设置 BGP 的必需属性。它是 AS 编号序列，通过其可以访问网络。AS-PATH 是形成供数据包传播的定向路由的源和目标路由器之间的中间 AS 编号序列。相邻自治系统 (ASes) 使用 BGP 交换和更新有关如何到达不同的 AS 前缀的消息。在每个路由器制定有关目标的最佳路由的新本地决策后，它会将该路由或路径信息以及随附的距离指标和路径属性发送到其每个对等体。由于此信息通过网络传播，因此路径沿线的每个路由器会将其唯一 AS 编号预置到 BGP 消息中的 ASes 列表。此列表是路由的AS-PATH。AS-PATH 以及 AS 前缀通过网络为单向传输路由提供特定处理。使用“配置 AS 路径”(Configure AS Path) 页面创建、复制和编辑自治系统 (AS) 路径策略对象。您可以创建 AS 路径对象以在配置路由映射、策略映射、BGP 邻居过滤时使用。AS 路径过滤器使您能够通过使用正则表达式来过滤路由更新消息。

您可以将此对象与 威胁防御 设备一起使用。

过程

步骤 1 依次选择**对象 (Objects)** > **对象管理 (Object Management)** 并从目录中选择 **AS 路径 (AS Path)**。

步骤 2 点击**添加 AS 路径 (Add AS Path)**。

步骤 3 在**名称 (Name)** 字段中输入 AS 路径对象的名称。有效值介于 1 与 500 之间。

步骤 4 点击**新建 AS 路径对象 (New AS Path Object)** 窗口上的**添加 (Add)**。

a) 从**操作 (Action)** 下拉列表中选择“允许”(Allow) 或“阻止”(Block) 选项以指示重新分发访问。

b) 在**正则表达式 (Regular Expression)** 字段中指定用于定义 AS 路径过滤器的正则表达式。

c) 点击**添加 (Add)**。

步骤 5 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖 ， 第 13 页。

步骤 6 点击**保存 (Save)**。

密码套件列表

密码套件列表是由多个密码套件组成的对象。每个预定义密码套件值代表用于协商 SSL 或 TLS 加密会话的一个密码套件。您可以在 SSL 规则中使用密码套件和密码套件列表根据协商 SSL 会话的客户

端和服务器是否使用该加密套件来控制加密流量。如果将密码套件列表添加到 SSL 规则，使用该列表中的任何密码套件协商的 SSL 会话都匹配该规则。

注释 虽然密码套件和密码套件列表在 Web 界面中可使用的位置相同，但不能添加、修改或删除密码套件。

创建密码套件列表

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择**密码套件列表 (Cipher Suite List)**。

步骤 3 点击 **Add Cipher Suites**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 从**可用密码 (Available Ciphers)** 列表中选择一个或多个密码套件。

步骤 6 点击 **Add**。

步骤 7 或者，点击**所选密码 (Selected Ciphers)** 列表中要删除的任何密码套件旁边的 **删除**（ ）。

步骤 8 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

社区列表

社区是可选的过渡BGP属性。社区是指一组共享某个通用属性的目标。它用于路由标记。BGP社区属性是可分配给特定前缀并通告到其他邻居的数值。社区可用于标记共享通用属性的一组前缀。上游提供商可以使用这些标记应用通用路由策略，例如过滤或分配特定本地首选项或者修改其他属性。使用“配置社区列表”页面创建、复制和编辑社区列表策略对象。您可以创建社区列表对象以在配置路由映射或策略映射时使用。您可以使用社区列表创建要在路由映射的匹配子句中使用的社区组。社区列表是匹配语句的有序列表。目标根据规则进行匹配，直至找到匹配项为止。

您可以将此对象与 威胁防御 设备一起使用。

过程

步骤 1 依次选择**对象** > **对象管理**并从目录中选择**社区列表**。

步骤 2 点击**添加社区列表**。

步骤 3 在**名称**字段中，指定社区列表对象的名称。

步骤 4 点击**新建社区列表对象**窗口上的**添加**。

步骤 5 选择**标准**单选按钮以指示社区规则类型。

标准社区列表用于指定已知的社区和社区编号。

注释 不能在同一社区列表对象中同时具有使用“标准”和使用“扩展”社区规则类型的条目。

a) 从**操作**下拉列表中选择“允许”或“阻止”选项以指示重新分发访问。
b) 在**社区**字段中，指定社区号。有效值可以从 1 到 4294967295 或者从 0:1 到 65534:65535。
c) 选择相应的**路由类型**。

- **互联网** - 选择指定互联网已知社区。系统向所有对等体（内部和外部）通告具有此社区的路由。
- **无通告** - 选择指定不通告已知社区。系统不向任何对等体（内部或外部）通告具有此社区的路由。
- **无导出** - 选择指定不导出已知社区。系统仅向同一自治系统中的对等体或仅向联盟内的其他子自治系统通告具有此社区的路由。不会向外部对等体通告这些路由。

步骤 6 选择**扩展**单选按钮以指示社区规则类型。

扩展的社区列表通过正则表达式用于过滤社区。正则表达式用于指定要与社区属性匹配的模式。

a) 从**操作**下拉列表中选择“允许”或“阻止”选项以指示重新分发访问。
b) 在**表达式**字段中指定正则表达式。

步骤 7 点击**添加 (Add)**。

步骤 8 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖 ，第 13 页。

步骤 9 点击**保存 (Save)**。

扩展社区

扩展社区是一组更大的共享某个通用属性的目的。BGP 扩展社区列表具有可用于标记共享通用属性的一组前缀的属性。这些标记用在路由映射的 match 子句中，用于过滤路由以实现虚拟路由器之间的路由泄漏。您还可以使用扩展社区列表定义策略列表对象以进行过滤。扩展社区列表是匹配语句的有序列表。路由会根据规则进行匹配，直到找到具有指定路由目标（标准）或正则表达式（扩展）的匹配项。使用“扩展社区”页面创建和编辑扩展社区列表策略对象。

注释 扩展社区列表仅适用于配置路由的导入或导出。

您可以将此对象与 威胁防御 设备一起使用。

过程

步骤 1 依次选择**对象** > **对象管理**，并在目录中选择**社区列表** > **扩展社区**。

步骤 2 点击**添加扩展社区列表**。

步骤 3 在**名称**字段中，指定扩展社区列表对象的名称。名称的长度不能超过 80 个字符。

步骤 4 选择扩展社区规则类型：

- 点击**标准**单选按钮，指定一个或多个路由目标。
- 点击**扩展**单选按钮，指定正则表达式。

注释 在同一个扩展社区列表对象中不能同时具有使用“标准”和“扩展”扩展社区规则类型的条目。

步骤 5 点击**添加 (Add)**。

步骤 6 如果已选择**标准**作为扩展社区规则类型，请指定以下内容：

a) 在**序列号**字段中，输入希望规则执行的顺序。

序列号在列表中必须唯一。

b) 在**操作**下拉列表中，如果要允许具有此处指定的匹配路由目标的路由，请选择**允许**； 如果要拒绝具有在此处指定的匹配路由目标的路由，请选择**阻止**。

c) 在**路由目标**字段中，指定路由目标。

- 您可以在单个条目中添加单个路由目标或一组以逗号分隔的路由目标。例如 *1:2,1:4,1:6*。
- 有效值可以是 1:1 到 65534:65535。
- 一个条目中最多可以包含 8 个路由目标。
- 不能跨多个条目设置多余的路由目标。例如，假设要使用 *1:200,100:100,1:300* 路由目标配置 *seq1*，并使用 *1:300,100:100,1:200* 路由目标配置 *seq2*。这会导致设置多余的路由目标，且无法部署。

步骤 7 如果已选择**扩展**作为扩展社区规则类型，请指定以下内容：

a) 在**序列号**字段中，输入希望规则执行的顺序。

序列号在列表中必须唯一。

b) 在**操作**下拉列表中，如果要允许具有此处指定的匹配正则表达式的路由，请选择**允许**； 如果要拒绝具有此处指定的匹配正则表达式的路由，请选择**阻止**。

c) 在**表达式**字段中指定正则表达式。

- 可以在单个条目中添加单个路由目标或一组以空格分隔的路由目标。例如，*^((16)|(18)):(.)$*。
- 最多可以向一个条目中添加 16 个正则表达式。

- 不能跨多个条目设置多余的正则表达式。例如，假设要使用 *^((16) | (18)):(.)$ ^4_[0-9]*$* 路由目标配置 *seq1*，并使用 *^4_[0-9]*$ ^((16) | (18)):(.)$* 路由目标配置 *seq2*。这会导致设置多余的正则表达式，且无法部署。

有关 BGP 正则表达式的详细信息，请参阅此处。

步骤 8 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 13 页。

步骤 9 点击**保存**。

可以在路由映射对象或策略列表对象的 match 子句中引用扩展社区列表：

- 在路由映射对象中，扩展社区列表的名称显示在**添加路由映射条目** > **Match 子句** > **BGP** > **社区列表** > **添加扩展社区列表**对话框中。有关在路由映射中配置 BGP 设置的详细信息，请参阅路由映射，第 66 页。
- 在策略列表对象中，扩展社区列表的名称显示在**添加策略列表** > **社区规则** > **添加扩展社区列表**对话框中。有关在策略列表中配置 BGP 设置的详细信息，请参阅策略列表，第 62 页。

可分辨名称

每个可分辨名称对象代表的公共密钥的使用者或颁发者的可分辨名称。您可在 TLS/SSL 规则中使用可分辨名称对象和对象组根据协商 TLS/SSL 会话的客户端和服务器是否使用将该可分辨名称作为使用者或颁发者的服务器证书来控制加密流量。

（可分辨名称组是现有可分辨名称对象的命名集合。）

可分辨名称可以包含国家/地区代码、公用名、组织和组织单位，但通常只会包含一个公用名。例如，`https://www.cisco.com` 的证书中的公用名为 `cisco.com`。（但情况并非总是这么简单；可分辨名称 (DN) 规则条件 显示了如何查找常用名称。）证书可以包含多个可在规则条件中用作 DN 的使用者可选名称 (SAN)。有关 SAN 的详细信息，请参阅 RFC 5280 第 4.2.1.6 节。

引用通用名称的可分辨名称对象的格式为 `CN=name`。如果添加不带 `CN=` 的 DN 规则条件，系统会在名称前面加上 `CN=`，再保存对象。

如 可分辨名称 (DN) 规则条件 中进一步所述，系统尽可能使用服务器名称指示 (SNI) (Server Name Indication [SNI]) 来匹配 TLS/SSL 规则中的 DN。

还可以添加带有下表中列出的每个属性（用逗号隔开）的一个可分辨名称。

表 *1:* 可分辨名称属性

属性	说明	允许的值
选	国家/地区代码	两个字母字符
CN	公用名称	最多 64 个字母数字、斜杠 (/)、连字符 (-)、引号 (")、星号 (*) 字符或空格

属性	说明	允许的值
O	组织	最多 64 个字母数字、斜杠 (/)、连字符 (-)、引号 (")、星号 (*) 字符或空格
OU	组织单位	最多 64 个字母数字、斜杠 (/)、连字符 (-)、引号 (")、星号 (*) 字符或空格

有关 DN 规则条件的重要说明

- 系统首次检测新服务器的加密会话时，DN 数据不可用于 ClientHello 处理，因为这可能会导致首个会话不解密。

  如果服务器请求 TLS 1.3，则 TLS 服务器身份发现的设置可以确保在做出 SSL 策略 决策之前知道服务器证书，从而提供帮助。有关详细信息，请参阅访问控制策略高级设置。

- 如果还选择了**解密 - 已知密钥 (Derypt - Known Key)** 操作，则无法配置可分辨名称条件。由于该操作要求选择服务器证书来解密流量，因此证书已经与流量相匹配。

通配符示例

可以定义一个或多个星号 (*) 作为属性中的通配符。在通用名称属性中，您可以为每个域名标签定义一个或多个星号。通配符仅在该标签中匹配，但您可以使用通配符定义多个标签。请参阅下表中的示例。

表 *2:* 公用名属性通配符示例

属性	匹配	不匹配
CN=*ample.com	example.com	mail.example.com example.text.com ampleexam.com
CN=exam*.com	example.com	mail.example.com example.text.com ampleexam.com
CN=*xamp*.com	example.com	mail.example.com example.text.com ampleexam.com
CN=*.example.com	mail.example.com	www.myhost.example.com example.com example.text.com ampleexam.com

注释 DN 对象 `CN=amp.cisco.com` 与 `CN=auth.amp.cisco.com` 不匹配，因此我们建议要在这些情况下使用通配符。

有关详细信息和示例，请参阅可分辨名称 (DN) 规则条件。

相关主题

可分辨名称 (DN) 规则条件

创建可分辨名称对象

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 展开**可分辨名称 (Distinguished Name)** 节点，然后选择**单个对象 (Individual Objects)**。

步骤 3 点击 **Add Distinguished Name**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 在 **DN** 字段中，输入可分辨名称或公用名的值。您有以下选择：

- 如果添加可分辨名称，则可包括可分辨名称，第 27 页中列出的每个属性（以逗号隔开）。
- 如果添加公用名，则可包括多个标签和通配符。

步骤 6 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

DNS 服务器组

域名系统 (DNS) 服务器会将完全限定域名 (FQDN)（例如 www.example.com）解析为 IP 地址。

创建 DNS 服务器组对象

过程

步骤 1 选择**对象 (Object)** > **对象管理 (Object Management)**。

步骤 2 点击网络对象列表中的 **DNS 服务器组**。

步骤 3 点击**添加 DNS 服务器组**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 或者，输入用于附加到非完全限定主机名的**默认域**。

此设置仅用于默认服务器组。

步骤 6 默认的**超时**和**重试次数**值已预填。如有必要，可更改这些值。

- 重试次数 - 系统接收不到响应时，重试 DNS 服务器列表的次数，介于 0 和 10 次之间。默认值为 2。
- 超时 (Timeout) - 尝试下一个 DNS 服务器之前要等待的秒数，介于 1 和 30 秒之间。默认值为 2 秒。每次系统重试服务器列表，此超时将加倍。

步骤 7 输入将属于此组的 **DNS 服务器**，可为 IPv4 或 IPv6 格式的逗号分隔条目。

一个组最多可包含 6 个 DNS 服务器。

步骤 8 点击**保存 (Save)**。

下一步做什么

在 DNS 服务器组中配置的 DNS 服务器应当分配到 DNS 平台设置中的接口对象。有关详细信息，请参阅配置 DNS。

外部属性

动态对象

动态对象是可以使用 IP 或使用 Cisco Secure Dynamic Attributes Connector 来创建的对象，作为一种集成，它允许在 管理中心 访问控制规则中使用来自云网络产品的对象。

有关 dynamic attributes connector 的详细信息，请参阅本指南后面的信息。

动态对象和网络对象之间的差异如下：

- 使用 dynamic attributes connector 创建的动态对象会在创建后立即被推送到 管理中心，并且还会定期更新。
- API 创建的动态对象：
  - 是 IP 地址，有或没有或无类域间路由 (CIDR)，可以在访问控制规则中使用，与网络对象很相似。
  - 不支持完全限定域名或地址范围。
  - 必须使用 API 进行更新。

相关主题

添加或编辑动态对象 ，第 31 页

添加或编辑动态对象

此过程讨论如何添加或编辑动态对象， 动态对象是一组使用 API 的 IP 地址，可以在访问控制规则中使用或不使用无类域间路由 (*CIDR*)，就像网络对象一样。

注释 如果使用 Cisco Secure Dynamic Attributes Connector ，则无需执行此过程，因为它会自动为您创建动态对象。

开始之前

有关使用对象服务 API 为 IP 对象填充地址的信息，请参阅《*Firepower* 管理中心 *REST API* 快速入门指南》。动态对象不需要部署。

过程

步骤 1 点击 **对象** > **对象管理**。

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

步骤 3 点击**添加动态对象 (Add Dynamic Object)** 或 **编辑**（ ）。

步骤 4 输入对象的**名称**和可选的**说明**。

步骤 5 在**类型 (Type)** 列表中，点击 **IP**。

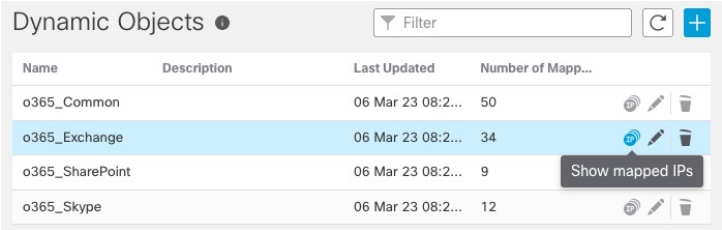
下一步做什么

如有必要，请使用 API 来更新动态对象。不需要部署。

动态对象映射

如果使用 API 或使用 dynamic attributes connector 配置动态对象，则连接器会定期向 管理中心 发送与动态属性过滤器匹配的 IP。

要查看或下载这些 IP 地址的当前列表，请点击**显示映射 ID (Show Mapped IDs)**，如下图所示。



IP 地址随时间动态添加，因此您应考虑定期执行此操作，尤其是在访问控制规则未按预期运行的情况下。

相关主题

- 动态对象 ， 第 30 页

安全组标记

安全组标记 (SGT) 对象指定单个 (SGT) 值。您可以使用规则中的 SGT 对象来控制具有**并非**由思科 ISE 分配的 SGT 属性的流量。您不能分组或覆盖 SGT 对象。

相关主题

从自定义 SGT 自动过渡到 ISE SGT
自定义 SGT 条件
ISE SGT 与自定义 SGT 规则条件

创建安全组标记对象

您只能在全局域中创建这些对象。要在经典设备上使用对象，您必须拥有控制许可证。对于智能许可设备，任何许可证均可。

开始之前

- 禁用 ISE/ISE-PIC 连接。如果使用 ISE/ISE-PIC 作为身份源，则不能创建自定义 SGT 对象。

过程

步骤 1 请点击 **对象** > **对象管理**。

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

步骤 3 点击**添加安全组标记 (Add Security Group Tag)**。

步骤 4 输入 **Name**。

步骤 5 输入**说明 (Description)**（可选）。

步骤 6 在**标记 (Tag)** 字段中，输入单个 SGT。

步骤 7 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

文件列表

如果使用恶意软件防护，而 AMP 云错误地识别某个文件的处置情况，则您可以将该文件添加到文件列表，以便将来能够更好地检测该文件。这些文件使用 SHA-256 散列值进行指定。每个文件列表最多可以包含 10000 个唯一的 SHA-256 值。

文件列表有两种预定义类别：

干净的列表

如果将某个文件添加到此列表，则系统视为 AMP 云为其分配了干净处置情况。

自定义检测列表

如果将某个文件添加到此列表，则系统视为 AMP 云为其分配了恶意软件处置情况。

在多域部署中，将为每个域呈现一个干净的列表和自定义检测列表。在低层域中，您可以查看但无法修改祖先列表。

由于您手动指定这些列表中包含的文件的阻止行为，系统不会在 AMP 云中查询这些文件的处置情况。您必须配置文件策略中的规则（通过**恶意软件云查找 [Malware Cloud Lookup]** 或**阻止恶意软件 [Block Malware]** 操作）和匹配的文件类型才能计算文件的 SHA 值。

⚠

注意 请**勿**在干净的列表中包含恶意软件。干净的列表会覆盖 AMP 云和自定义检测列表。

文件列表的源文件

可通过上传包含 SHA-256 值和描述的列表的逗号分隔值 (CSV) 源文件将多个 SHA-256 值添加到文件列表。管理中心验证内容并使用有效的 SHA-256 值填充文件列表。

源文件必须为具有 .csv 文件扩展名的简单文本文件。所有标题必须以井号 (#) 开头；标题将被视为注释，不会上传。每个条目都应包含一个 SHA-256 值，后跟说明并以 `LF` 或 `CR+LF` 换行字符结尾。系统将会忽略条目中的任何其他信息。

请注意以下提示：

- 从文件列表删除源文件也会从该文件列表删除所有相关的 SHA-256 散列值。

- 如果成功上传源文件导致文件列表包含超过 10000 个不同的 SHA-256 值，则不能将多个文件上传到该文件列表。
- 上传时，系统会截去描述中超过256个字符的字符，仅保留前256个字符。如果描述包括逗号，必须使用转义字符 (\,)。如果未包含描述，将会改为使用源文件名。
- 所有非重复的SHA-256值都将被添加到文件列表。如果文件列表包含SHA-256值，并且上传了包括该值的源文件，新上传的值不会修改现有SHA-256值。查看与SHA-256值相关的捕获的文件、文件事件或恶意软件事件时，所有威胁名称或描述都来源于单个 SHA-256 值。
- 系统不会在源文件中上传无效的 SHA-256 值。
- 如果多个上传的源文件包括相同 SHA-256 值的条目，系统将使用最新的值。
- 如果源文件包括相同 SHA-256 值的多个条目，系统将使用最后一个。
- 不能在对象管理器中直接编辑源文件。要进行更改，必须首先直接修改源文件，删除系统中的副本，然后上传修改后的源文件。
- 与源文件相关的条目数是指不同的SHA-256值的数量。如果从文件列表删除某个源文件，文件列表包含的 SHA-256 条目总数将会减少等于该源文件中有效条目的数量。

将单个 SHA-256 值添加到文件列表

您必须有此程序的 恶意软件 许可证。

可以提交文件的 SHA-256 值以将其添加到文件列表。不能添加重复的 SHA-256 值。

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

开始之前

- 在事件视图中右键点击某个文件或恶意软件事件，在情景菜单中选择**显示全文 (Show Full Text)**，然后复制完整的 SHA-256 值以粘贴到列表中。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择**文件列表 (File List)**。

步骤 3 点击要添加文件的干净列表或自定义检测列表旁边的 **编辑**（ ）。

如果显示**视图**（ ），则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 4 从**添加方式 (Add by)** 下拉列表中选择 `Enter SHA Value`。

步骤 5 在 **Description** 字段中输入源文件的描述。

步骤 6 在 **SHA-256** 字段中输入或粘贴文件的完整值。系统不支持匹配部分值。

步骤 7 点击**添加 (Add)**。

步骤 8 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

注释 在部署配置更改后，系统不再查询 AMP 云以查找列表中的文件。

将单个文件上传到文件列表

您必须有此程序的 恶意软件 许可证。

如果要将文件副本添加到文件列表，则可将文件上传到 Cisco Secure Firewall Management Center进行分析；系统会计算文件的 SHA-256 值并将文件添加到列表。系统不对用于 SHA-256 计算的文件大小强制实施任何限制。

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择**文件列表 (File List)**。

步骤 3 点击要添加文件的干净列表或自定义检测列表旁边的 **编辑**（）。

如果显示**视图**（），则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 4 从**添加方式 (Add by)** 下拉菜单中，选择**计算 SHA (Calculate SHA)**。

步骤 5 或者，在**说明 (Description)** 字段中输入文件的说明。如果不输入说明，在上传时文件名将被用作说明。

步骤 6 点击**浏览 (Browse)**，然后选择要上传的文件。

步骤 7 点击**计算并添加 SHA (Calculate and Add SHA)**。

步骤 8 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

注释 在部署配置更改后，系统不再查询 AMP 云以查找列表中的文件。

将源文件上传到文件列表

您必须有此程序的 恶意软件 许可证。

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 点击 **File List**。

步骤 3 点击要从源文件向其添加值的文件列表旁边的 **编辑**（）。

如果显示**视图**（），则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 4 从**添加方式 (Add by)** 下拉菜单中，选择 `List of SHAs`。

步骤 5 或者，在**说明 (Description)** 字段中输入源文件的说明。如果不输入说明，系统将会使用文件名。

步骤 6 点击**浏览 (Browse)** 浏览到源文件，然后点击**上传并添加列表 (Upload and Add List)**。

步骤 7 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

注释 在部署策略后，系统不再查询 AMP 云以查找列表中的文件。

编辑文件列表中的 SHA-256 值

您必须有此程序的 恶意软件 许可证。

可以编辑或删除文件列表中的各个 SHA-256 值。请注意，不能在对象管理器中直接编辑源文件。要进行更改，必须首先直接修改源文件，删除系统中的副本，然后上传修改后的源文件。

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 点击 **File List**。

步骤 3 点击要修改文件的干净列表或自定义检测列表旁边的 **编辑**（）。

如果显示**视图**（），则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 4 您可以执行以下操作：

- 点击要更改的 SHA-256 值旁边的 **编辑**（），并根据需要修改 **SHA-256** 或**说明 (Description)** 值。
- 点击要删除的 SHA-256 值旁边的 **删除**（）。

步骤 5 点击**保存 (Save)** 以更新列表中的文件条目。

步骤 6 点击**保存 (Save)** 以保存文件列表。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

注释 在部署配置更改后，系统不再查询 AMP 云以查找列表中的文件。

从文件列表下载源文件

您必须有此程序的 恶意软件 许可证。

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择**文件列表 (File List)**。

步骤 3 点击要下载源文件的干净列表或自定义检测列表旁边的 **编辑**（）。

如果显示**视图**（），则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 4 点击要下载的源文件旁边的 **视图**（）。

步骤 5 点击**下载 SHA 列表 (Download SHA List)** 并按照提示保存源文件。

步骤 6 点击 **Close**。

FlexConfig

可以使用 FlexConfig 策略中的 FlexConfig 策略对象为 威胁防御设备上您不能使用 Cisco Secure Firewall Management Center另行配置的功能提供自定义配置。有关 FlexConfig 策略的更多信息，请参阅 FlexConfig 策略概述。

可为 FlexConfig 配置以下类型的对象。

文本对象

文本对象定义了在 FlexConfig 对象中用作变量的自由形式的文本字符串。这些对象可以具有单个值，或是多个值的列表。

有几种预定义文本对象可以用于预定义 FlexConfig 对象。如果使用相关联的 FlexConfig 对象，则只需编辑文本对象的内容，即可自定义 FlexConfig 对象配置给定设备的方式。在编辑预定义对象时，为您配置的每台设备创建设备覆盖，而不是直接更改这些对象的默认值，通常是更好的选择。这有助于避免如果另一个用户希望将同一 FlexConfig 对象用于一组不同的设备可能导致的意外后果。

有关配置文本对象的信息，请参阅配置 FlexConfig 文本对象。

FlexConfig 对象

FlexConfig 对象包括设备配置命令、变量和脚本语言指令。在配置部署过程中，将处理这些指令，以创建一系列带有自定义参数的配置命令，用于配置目标设备上的特定功能。

这些指令要么是在系统配置常规 管理中心策略和设置中定义的功能之前（预置）进行配置，要么是在此之后（附加）进行配置。必须将任何取决于 Cisco Secure Firewall Management Center配置的对象（例如网络对象）的 FlexConfig 附加到配置部署，否则在所需 FlexConfig 参考所需对象之前，不会配置这些对象。

有关配置 FlexConfig 对象的更多信息，请参阅配置 FlexConfig 对象。

地理定位

配置的每个地理定位对象代表系统识别为受监控网络上流量的源或目标的一个或多个国家/地区或大洲。可在系统 Web 界面中的不同位置使用地理定位对象，包括访问控制策略、SSL 策略和事件搜索。例如，可编写阻止流向或来自某些国家/地区的流量的访问控制规则。

要确保使用最新信息来过滤网络流量，思科强烈建议您定期更新地理位置数据库 (GeoDB)。

创建地理位置对象

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择**地理位置 (Geolocation)**。

步骤 3 点击 **Add Geolocation**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 选中要包括到地理定位对象中的国家/地区和大洲的相应复选框。选中大洲会选中该大洲的所有国家/地区，以及 GeoDB 更新将来可能添加到该大洲下的所有国家/地区。取消选中大洲下的任意国家/地区会取消选中该大洲。您可以选择国家/地区和大洲的任意组合。

步骤 6 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

接口

每个接口可以被分配给安全区域和/或接口组。然后，根据区域或组应用您的安全策略。例如，您可以将“内部”接口分配到“内部”区域，而将“外部”接口分配到“外部”区域。例如，可以配置访问控制策略，允许流量从内部传到外部，但不允许从外部传入内部。某些策略仅支持安全区域，而其他策略则支持区域和组。

有关接口对象的详细信息，请参阅安全区域和接口组。

要添加接口对象，请参阅创建安全区域和接口组对象。

密钥链

为了增强设备的数据安全和防护，引入了用于对持续时间为 180 天以内的 IGP 对等体进行身份验证的轮换密钥。轮换密钥可阻止任何恶意用户猜测用于路由协议身份验证的密钥，从而保护网络，避免通告错误的路由和重定向流量。频繁更改密钥可降低密钥最终被猜到的风险。在配置提供密钥链的路由协议的身份验证时，请为密钥链中的密钥配置重叠的生存期。这有助于防止由于缺少活动密钥而丢失受密钥保护的通信。轮换密钥仅适用于 OSPFv2 协议。如果密钥生存期到期且未找到活动密钥，则 OSPF 会使用最后一个有效密钥来维持对等体之间的邻接关系。

注释 身份验证仅使用 MD5 加密算法。

密钥生存期

为了维持稳定的通信，每个设备会将密钥链身份验证密钥存储起来，并对某个功能同时使用多个密钥。密钥链管理基于密钥的发送和接受生存期，提供了一种安全机制来处理密钥滚动。设备使用密钥生存期来确定密钥链中的哪些密钥处于活动状态。

密钥链中的每个密钥具有两个生存期：

- 接受生存期 - 设备在与另一设备进行密钥交换期间接受密钥的时间间隔。
- 发送生存期 - 设备在与另一设备进行密钥交换期间发送密钥的时间间隔。

在密钥发送生存期内，设备会将路由更新数据包与密钥一起发送。当发送的密钥不在设备上密钥的接受生存期内时，设备将不会接受来自其他设备的通信。

如果未配置生存期，则相当于配置没有时间线的 MD5 身份验证密钥。

密钥选择

- 当密钥链含有多个有效密钥时，OSPF 会选择生存期最长的密钥。
- 首选具有无限生存期的密钥。
- 如果密钥生存期相同，则首选密钥 ID 较高的密钥。

创建密钥链对象

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择**密钥链**。

步骤 3 点击**添加密钥链**。

步骤 4 在“添加密钥链对象”对话框的**名称**字段中输入密钥链的名称。

该名称必须以下划线或字母开头，后跟字母数字字符或特殊字符（-、_、+、.）。

步骤 5 要向密钥链添加密钥，请点击**添加**。

步骤 6 在**密钥 ID** 字段中指定密钥标识符。

密钥 ID 值可介于 0 到 255 之间。仅在表明无效密钥时使用值 0。

步骤 7 **算法**字段和**密码加密类型**字段分别显示支持的算法和加密类型，即 MD5 和明文。

步骤 8 在**加密密钥字符串**字段中输入密码，然后在**确认加密密钥字符串**字段中重新输入该密码。

- 密码的最大长度可为 80 个字符。
- 密码不能为单个数字或以数字加空格开头。例如，“0 pass”或“1”为无效密码。

步骤 9 要设置设备与其他设备进行密钥交换期间接受/发送密钥的时间间隔，请在**接受生存期**和**发送生存期**字段中提供生存期值：

注释 “日期时间”值默认为 UTC 时区。

结束时间可为持续时间，即接受/发送生存期结束时的绝对时间或永不到期。默认结束时间为日期时间。

以下为开始值和结束值的验证规则：

- 在指定了结束生存期时，开始生存期不可为空值。
- 接受或发送生存期的开始生存期必须早于相应的结束生存期。

步骤 10 点击**添加**。

重复步骤 5 到 10 以创建密钥。为具有重叠生存期的密钥链创建至少两个密钥。这有助于防止由于缺少活动密钥而丢失受密钥保护的通信。

步骤 11 管理对象的覆盖：

- 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 13 页。
- 如果要将覆盖值添加到此对象，请展开“覆盖”(Override) 部分并点击**添加 (Add)**；请参阅添加对象覆盖，第 13 页。

步骤 12 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

网络

网络对象表示一个或多个 IP 地址。您可以在多个位置使用网络对象和组合，包括访问控制策略、网络变量、身份规则、网络发现规则、事件搜索、报告、身份识别等等。

当配置需要网络对象的选项时，系统会自动过滤列表，以仅显示对于该选项有效的那些对象。例如，某些选项需要主机对象，而其他选项则需要子网。

网络对象可以是以下类型之一：

主机

单个 IP 地址。

IPv4 示例：

209.165.200.225

IPv6 示例：

2001:DB8::0DB8:800:200C:417A 或 2001:DB8:0:0:0DB8:800:200C:417A

范围

IP 地址范围。

IPv4 示例：

209.165.200.225-209.165.200.250

IPv6 示例：

2001:db8:0:cd30::1-2001:db8:0:cd30::1000

网络

地址块，也称为子网。

IPv4 示例：

209.165.200.224/27

IPv6 示例：

2001:DB8:0:CD30::/60

注释 “安全智能”会忽略使用 /0 掩码的 IP 地址块。

FQDN

单个完全限定域名 (FQDN)。您可以将 FQDN 解析限制为仅 IPv4 地址，仅 IPv6 地址或 IPv4 和 IPv6 地址。FQDN 必须以数字或字母开头和结尾。FQDN 中仅允许使用字母、数字和短划线作为内部字符。

例如：

```
www.example.com
```

注释 您可在访问控制规则和预过滤规则中使用 FQDN 对象， 或手动 NAT 规则，仅限 。规则匹配通过 DNS 查找获取的 FQDN IP 地址。要使用 FQDN 网络对象，请确保已分别在 DNS 服务器组，第 29 页和配置 DNS中配置 DNS 服务器设置和 DNS 平台设置。

您不能在身份规则中使用 FDQN 网络对象。

组

一组网络对象或其他网络对象组。您可以通过将一个网络对象组添加到另一个网络对象组创建嵌套组。最多可以嵌套 10 个级别的组。

网络通配符掩码

您可以从“对象管理”(Object Management) 页面创建和管理通配符掩码对象。

您可以创建具有扩展子网 IP 地址的网络对象。现有网络对象已扩展为支持网络和网络通配符对象。使用通配符掩码的网络对象在网络对象列表页面的**类型 (Type)** 列中列为**网络通配符**。

通配符掩码是不连续的位掩码的 IP 地址。可以使用连续掩码为通配符网络对象创建标准网络对象和不连续的掩码。

IP 地址示例	网络通配符？	对象类型
192.0.0.0/8	不支持	网络
10.10.0.0/255.255.0.0	不支持	网络
10.10.0.10/255.255.0.255	是	网络通配符
72.0.240.10/255.255.240.255	是	网络通配符

注释 只有在配置以下策略时才允许使用网络通配符对象以及包含网络通配符对象的对象组：

- 预过滤器策略
- 访问控制策略
- NAT 策略

准则和限制

- 要创建网络通配符对象，请在 FMC UI 中依次选择**对象 (Objects)** > **对象管理 (Object Management)** > **网络 (Network)** 并点击**添加网络 (Add Network)**，然后点击**添加对象 (Add Object)**。选择**网络 (Network)** 选项并输入扩展子网掩码形式的值。示例：10.0.10.10/255.255.0.255。
- 支持对象覆盖、组对象支持、组对象覆盖、通配符文本和通配符对象导入。
- 仅 IPv4 地址支持网络通配符对象。
- FMC 和 FTD 7.1 及更高版本可支持网络通配符对象。
- 仅 Snort-3 支持网络通配符对象。

创建网络对象

威胁防御功能历史记录：

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择**网络 (Network)**。

步骤 3 从**添加网络 (Add Network)** 下拉菜单中选择**添加对象 (Add Object)**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 输入**说明 (Description)**（可选）。

步骤 6 在**网络**字段中，选择所需选项，然后输入适当的值；请参阅网络，第 41 页。

步骤 7 （仅限 FQDN 对象）从**查找**下拉菜单中选择 DNS 解析以确定是否要将 IPv4 地址、IPv6 地址，或这两个地址与 FQDN 关联。

步骤 8 管理对象的覆盖：

- 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 13 页。
- 如果要将覆盖值添加到此对象，请展开“覆盖”(Override) 部分并点击**添加 (Add)**；请参阅添加对象覆盖，第 13 页。

步骤 9 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

导入网络对象

有关导入网络对象的详细信息，请参阅正在导入对象，第 4 页。

PKI

用于 SSL 应用的 PKI 对象

PKI 对象代表支持您的部署所需的公钥证书和配对的私钥。内部和可信 CA 对象包括证书颁发机构 (CA) 证书；内部 CA 对象还包括与证书配对的私钥。内部和外部证书对象包括服务器证书；内部证书对象还包括与证书配对的私钥。

如果使用可信证书颁发机构对象和内部证书对象来配置与 ISE/ISE-PIC 的连接，则可使用 ISE/ISE-PIC 作为身份源。

如果使用内部证书对象来配置强制网络门户，在连接到用户的 Web 浏览器时，系统可验证强制网络门户设备的身份。

如果使用可信证书颁发机构对象来配置领域，则可配置与 LDAP 或 AD 服务器的安全连接。

如果在 SSL 规则中使用 PKI 对象，可以匹配使用以下证书加密的流量：

- 外部证书对象中的证书
- 由受信任 CA 对象中的 CA 签名的证书或在 CA 的信任链中的证书

如果在 SSL 规则中使用 PKI 对象，可以解密：

- 传出流量（通过对带有内部 CA 对象的服务器证书进行重签）
- 传入流量（使用内部证书对象中的已知私钥）

可以手动输入证书和密钥信息，上传包含这些信息的文件，在某些情况下，还可以生成新的 CA 证书和私有密钥。

在对象管理器中查看 PKI 对象列表时，系统会将证书的使用者可分辨名称显示为对象值。将指针悬停在该值上可查看证书使用者的完整可分辨名称。要查看其他证书的详细信息，请编辑 PKI 对象。

注释 管理中心和受管设备在保存存储在内部 CA 对象和内部证书对象中的所有私钥之前，会使用随机生成的密钥对它们进行加密。如果上传受密码保护的私钥，设备会使用用户提供的密码对该密钥解密，然后用随机生成的密钥对其加密，再进行保存。

用于证书注册的 PKI 对象

证书注册对象包含创建证书签名请求 (CSR) 以及从指定的证书颁发机构 (CA) 获取身份证书所需的 CA 服务器信息和注册参数。这些活动发生在您的私有密钥基础设施 (PKI) 中。

证书注册对象还可能包括证书撤销信息。有关 PKI、数字证书和证书注册的详细信息，请参阅PKI 基础设施和数字证书。

内部证书颁发机构对象

配置的每个内部证书颁发机构 (CA) 对象代表组织控制的 CA 的 CA 公共密钥证书。此类对象由对象名称、CA 证书和配对私钥组成。您可以在 SSL 规则中使用内部 CA 对象和组通过使用内部 CA 对服务器证书进行重新签名来解密传出加密流量。

注释 如果在**解密 - 重新签名 (Decrypt - Resign)** SSL 规则中引用内部 CA 对象，且该规则与加密会话相匹配，在协商 SSL 握手时，用户的浏览器可能会警告证书不可信。要避免此问题，请将内部 CA 对象证书添加到受信任根证书的客户端或域列表。

可以通过以下方式创建内部 CA 对象：

- 导入现有基于 RSA 或基于椭圆曲线的 CA 证书和私有密钥
- 生成新的基于 RSA 的自签 CA 证书和私有密钥

- 生成未签名的基于 RSA 的 CA 证书和私有密钥。使用内部 CA 对象之前，必须向另一个 CA 提交证书签名请求 (CSR) 以对证书进行签名。

创建包含签名证书的内部 CA 对象后，可以下载 CA 证书和私钥。系统使用用户提供的密码对下载的证书和私钥进行加密。

无论是系统生成还是用户创建的内部 CA 对象名称，您都只能修改其名称，但不能修改其他对象属性。

不能删除正在使用的内部 CA 对象。此外，在编辑用于 SSL 策略的内部 CA 对象后，相关联的访问控制策略已过时。必须重新部署访问控制策略才能使更改生效。

CA 证书和私钥导入

可以通过导入 X.509 v3 RSA 证书和私有密钥来配置内部 CA 对象。可以上传采用下列其中一种受支持格式编码的文件：

- 可分辨编码规则 (DER)
- 隐私增强电子邮件 (PEM)

如果私有密钥文件受密码保护，您可以提供解密密码。如果证书和密钥采用 PEM 格式编码，还可以复制并粘贴信息。

如果要上传文件，文件中必须包含正确的证书或密钥信息，并且可以相互配对。系统在保存对象前将验证配对。

注释 如果配置具有 **Decrypt - Resign** 操作的规则，除了任何配置的规则条件之外，该规则还根据引用的内部 CA 证书的加密算法类型匹配流量。例如，必须上传一个基于椭圆曲线的 CA 证书，以解密用基于椭圆曲线的算法进行加密的出站流量。

导入 CA 证书和私钥

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 展开 **PKI** 节点，然后选择**内部 CA (Internal CAs)**。

步骤 3 点击**导入 CA**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 在 **Certificate Data** 字段上方，点击 **Browse** 上传 DER 或 PEM 编码的 X.509 v3 CA 证书文件。

步骤 6 在 **Key** 字段上方，点击 **Browse** 上传 DER、PEM 编码的配对私有密钥文件。

步骤 7 如果上传的文件受密码保护，请选中**已加密，密码为：(Encrypted, and the password is:)** 复选框并输入密码。

步骤 8 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

生成新的 CA 证书和私钥

可以通过提供识别信息生成基于 RSA 的自签 CA 证书和私有密钥来配置内部 CA 对象。

生成的 CA 证书有效期为十年。有效期起始日期为生成一周之前。

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 展开 **PKI** 节点，然后选择**内部 CA (Internal CAs)**。

步骤 3 点击**生成 CA (Generate CA)**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 输入标识属性。

步骤 6 点击 **Generate self-signed CA**。

新签名证书

可以通过从 CA 获取签名证书来配置内部 CA 对象。这包括两个步骤：

- 提供识别信息以配置内部 CA 对象。这会生成未签名证书和配对私钥，并创建向您指定的 CA 发出的证书签名请求 (CSR)。
- 在 CA 颁发签名证书后，请上传证书到内部 CA 对象，用以替换未签名证书。

仅当内部 CA 对象包含签名证书时，才能在 SSL 规则中引用该对象。

创建未签名的 CA 证书和 CSR

过程

步骤 1 选择对象 > 对象管理。

步骤 2 展开 **PKI** 节点，然后选择内部 **CA (Internal CAs)**。

步骤 3 点击生成 **CA (Generate CA)**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 输入标识属性。

步骤 6 点击 **Generate CSR**（生成 **CSR**）。

步骤 7 复制 CSR 以将其提交到 CA。

步骤 8 点击 **OK**。

下一步做什么

- 必须上传由 CA 颁发的签名证书，如 中所述 上传为响应 CSR 而颁发的签名证书，第 48 页

上传为响应 CSR 而颁发的签名证书

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

上传之后，签名证书可在 SSL 规则中引用。

过程

步骤 1 选择对象 > 对象管理。

步骤 2 展开 **PKI** 节点，然后选择内部 **CA (Internal CAs)**。

步骤 3 点击包含等待 CSR 的未签名证书的 CA 对象旁边的 编辑（）。

步骤 4 点击 **Install Certificate**。

步骤 5 点击浏览 **(Browse)** 上传 DER 或 PEM 编码的 X.509 v3 CA 证书文件。

步骤 6 如果上传的文件受密码保护，请选中已加密，密码为：**(Encrypted, and the password is:)** 复选框并输入密码。

步骤 7 点击保存 **(Save)** 以将签名证书上传到 CA 对象。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

CA 证书和私钥下载

可以通过下载包含内部 CA 对象中的证书和密钥信息的文件来备份或传输 CA 证书和配对私钥。

⚠

注意　系统始终将下载的密钥信息存储在安全的位置。

系统在保存密钥信息之前，会使用随机生成的密钥对存储在内部 CA 对象中的私钥进行加密。如果从内部 CA 下载证书和私钥，系统在创建包含证书和私钥信息的文件之前，会首先对这些信息进行解密。然后，您必须提供系统用于加密下载文件的密码。

⚠

注意　作为系统备份一部分下载的私钥将被解密，然后存储在未加密的备份文件中。

下载 CA 证书和私钥

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

可以同时为当前域和祖先域下载 CA 证书。

过程

步骤 1　选择**对象** > **对象管理**。

步骤 2　展开 **PKI** 节点，然后选择**内部 CA (Internal CAs)**。

步骤 3　在要下载其证书和私钥的内部 CA 对象旁边，点击 **编辑**（✎）。

在多域部署中，点击 **视图**（👁），为祖先域中的对象下载证书和私钥。

步骤 4　点击**下载**。

步骤 5　在**密码 (Password)** 和**确认密码 (Confirm Password)** 字段中输入加密密码。

步骤 6　点击**确定 (OK)**。

受信任证书颁发机构对象

配置的每个受信任证书颁发机构 (CA) 对象代表属于受信任 CA 的 CA 公钥证书。此类对象由对象名称和 CA 公共密钥证书组成。您可以在以下位置使用外部 CA 对象和组：

- SSL 策略，用于控制使用由受信任 CA 或信任链中的任何 CA 签名的证书加密的流量。

- 领域配置，用于建立与 LDAP 或 AD 服务器的安全连接。
- 您的 ISE/ISE-PIC 连接。为 **pxGrid 服务器 CA (pxGrid Server CA)** 和 **MNT 服务器 CA (MNT Server CA)** 对象选择受信任证书颁发机构对象。

创建受信任 CA 对象后，可以修改名称和添加证书撤销列表 (CRL)，但不能更改其他对象属性。可添加到对象的CRL数量没有限制。要修改已上传到对象的CRL，必须删除该对象并重新创建对象。

注释 在 ISE/ISE-PIC 集成配置中使用对象时，将 CRL 添加到该对象没有任何作用。

不能删除正在使用的可信 CA 对象。此外，在编辑正在使用的受信任 CA 对象后，关联的访问控制策略会过期。必须重新部署访问控制策略才能使更改生效。

受信任的 CA 对象

您可以通过上传 X.509 v3 CA 证书来配置外部 CA 对象。可以上传采用下列其中一种受支持格式编码的文件：

- 可分辨编码规则 (DER)
- 隐私增强电子邮件 (PEM)

如果文件受密码保护，必须提供解密密码。如果证书采用PEM格式编码，还可以复制并粘贴信息。

仅当文件包含适当的证书信息时，才可以上传 CA 证书；系统在保存对象之前会对证书进行验证。

添加受信任 CA 对象

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 展开 **PKI** 节点，然后选择**受信任 CA (Trusted CAs)**。

步骤 3 点击 **Add Trusted CAs**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 点击**浏览 (Browse)** 上传 DER 或 PEM 编码的 X.509 v3 CA 证书文件。

步骤 6 如果文件受密码保护，请选中**已加密，密码为：(Encrypted, and the password is:)** 复选框并输入密码。

步骤 7 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

受信任 CA 对象中的证书撤销列表

您可以将 CRL 上传到受信任 CA 对象。如果在 SSL 策略中引用受信任 CA 对象，则可以根据颁发会话加密证书的 CA 随后是否会撤销证书来控制加密流量。可以上传采用下列其中一种受支持格式编码的文件：

- 可分辨编码规则 (DER)
- 隐私增强电子邮件 (PEM)

添加CRL后，可以查看已撤销证书的列表。要修改已上传到对象的CRL，必须删除该对象并重新创建对象。

只能上传包含适当 CRL 的文件。可添加到受信任 CA 对象的 CRL 数量没有限制。但是，每次上传 CRL 之后，必须先保存对象再添加另一个 CRL。

注释 在 ISE/ISE-PIC 集成配置中使用对象时，将 CRL 添加到该对象没有任何作用。

向受信任 CA 对象添加证书撤销列表

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

注释 在 ISE/ISE-PIC 集成配置中使用对象时，将 CRL 添加到该对象没有任何作用。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 展开 **PKI** 节点，然后选择**受信任 CA (Trusted CAs)**。

步骤 3 点击可信 CA 对象旁边的 **编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击**添加 CRL (Add CRL)** 上传 DER 或 PEM 编码的 CRL 文件。

步骤 5 点击**确定 (OK)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

外部证书对象

您配置的每个外部证书对象都表示一个不属于贵组织的服务器公钥证书。该对象由对象名称和证书组成。可以在 SSL 规则中使用外部证书对象和对象组来控制使用服务器证书加密的流量。例如，您可以上传您信任的自签服务器证书，但不能使用可信 CA 证书进行验证。

您可以通过上传 X.509 v3 服务器证书来配置外部证书对象。可以上传采用下列其中一种受支持格式的文件：

- 可分辨编码规则 (DER)
- 隐私增强电子邮件 (PEM)

仅当文件包含适当的服务器证书信息时，才可以上传文件；系统在保存对象之前会对文件进行验证。如果证书采用 PEM 格式编码，还可以复制并粘贴信息。

添加外部证书对象

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 展开 **PKI** 节点，然后选择**外部证书 (External Certs)**。

步骤 3 点击 **Add External Cert**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 在 **Certificate Data** 字段上方，点击 **Browse** 上传 DER 或 PEM 编码的 X.509 v3 服务器证书文件。

步骤 6 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

内部证书对象

您配置的每个内部证书对象都代表一个属于您组织的服务器公共密钥证书。此类对象由对象名称、公共密钥证书和配对私钥组成。您可以在以下位置使用内部证书对象和组：

- SSL 规则，用于通过已知私钥解密传入到您的组织其中一台服务器的流量。
- 您的 ISE/ISE-PIC 连接。为 **MC 服务器证书 (MC Server Certificate)** 字段选择内部证书对象。
- 强制网络门户配置，用于在连接到用户的 Web 浏览器时对强制网络门户设备的身份进行身份验证。为**服务器证书 (Server Certificate)** 字段选择内部证书对象。

可以通过上传基于 X.509 v3 RSA 或基于椭圆曲线的服务器证书和配对的私有密钥来配置内部证书对象。可以上传采用下列其中一种受支持格式的文件：

- 可分辨编码规则 (DER)
- 隐私增强电子邮件 (PEM)

如果文件受密码保护，必须提供解密密码。如果证书和密钥采用 PEM 格式编码，还可以复制并粘贴信息。

如果要上传文件，文件中必须包含正确的证书或密钥信息，并且可以相互配对。系统在保存对象前将验证配对。

创建内部证书对象后，可以修改名称，但不能修改其他对象属性。

不能删除正在使用的内部证书对象。此外，在编辑正在使用的内部证书对象后，关联的访问控制策略会过期。必须重新部署访问控制策略才能使更改生效。

添加内部证书对象

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 展开 **PKI** 节点，然后选择**内部证书 (Internal Certs)**。

步骤 3 点击 **Add Internal Cert**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 在 **Certificate Data** 字段上方，点击 **Browse** 上传 DER 或 PEM 编码的 X.509 v3 服务器证书文件。

步骤 6 在 **Key** 字段上方，点击 **Browse** 上传 DER、PEM 编码的配对私有密钥文件。

步骤 7 如果上传的私有密钥文件受密码保护，请选中**已加密，密码为：**复选框并输入密码。

步骤 8 点击**保存 (Save)**。

证书注册对象

通过信任点，您可以管理并跟踪 CA 和证书。信任点表示 CA 或身份对。信任点包括 CA 的身份、CA 特定配置参数，以及与一个注册的身份证书的关联。

证书注册对象包含创建证书签名请求 (CSR) 以及从指定的证书颁发机构 (CA) 获取身份证书所需的 CA 服务器信息和注册参数。这些活动发生在您的私有密钥基础设施 (PKI) 中。

证书注册对象还可能包括证书撤销信息。有关 PKI、数字证书和证书注册的详细信息，请参阅PKI 基础设施和数字证书。

如何使用 证书注册对象

证书注册对象用于将受管设备注册到PKI基础设施中，并通过执行以下操作在支持VPN连接的设备上创建信任点（CA 对象）：

1. 在证书注册对象中定义用于CA身份验证和注册的参数。指定共享参数，并使用覆盖功能为不同的设备指定唯一的对象设置。
2. 在需要身份证书的每个受管设备上关联并安装此对象。在设备上，它将成为信任点。

   当证书注册对象与某个设备关联并安装至该设备后，证书注册过程会立即开始。对于自签名、SCEP， EST， 和 PKCS12 文件注册类型，此过程将自动执行，这意味着不需要任何额外的管理员操作。手动证书注册需要额外的管理员操作。
3. 在您的 VPN 配置中指定创建的信任点。

管理证书注册对象

要管理证书注册对象，请转至**对象 > 对象管理**，然后从导航窗格中选择 **PKI > 证书注册**。系统将显示以下信息：

- 现有证书注册对象会在**名称**列中列出。

  使用搜索字段（放大镜）过滤列表。
- 每个对象的注册类型显示在**类型**列中。可以使用以下注册方法：
  - **自签名** - 受管设备将生成其自己的自签名根证书。
  - **EST**-设备使用安全传输注册从 CA 获取身份证书。
  - **SCEP** -（默认）简单证书注册协议由设备使用以从 CA 获取身份证书。
  - **手动** - 注册过程由管理员手动执行。
  - **PKCS12 文件** - 在支持 VPN 连接的 Firepower 威胁防御受管设备上导入 PKCS12 文件。PKCS#12、PFX 或 P12 文件将服务器证书、任何中间证书和私钥保存在一个加密文件中。输入**口令**值进行解密。
- **覆盖 (Override)** 列指示对象是允许覆盖（绿色复选标记）还是不允许覆盖（红色的 X）。如果显示一个数字，则它是现有的覆盖数。

  使用“覆盖”选项自定义作为VPN配置一部分的每个设备的对象设置。覆盖将使每个设备的信任点详细信息都是唯一的。通常，在VPN配置中，为每个设备覆盖“公用名”或“使用者”。

  有关覆盖任意类型对象的详细信息和操作步骤，请参阅对象覆盖， 第 11 页。

- 点击编辑图标（铅笔）可**编辑**之前创建的证书注册对象。只有在注册对象未与任何受管设备关联时，才能进行编辑。请参阅有关编辑证书注册对象的添加说明。您可以对失败的注册对象进行编辑。
- 点击删除图标（垃圾桶）可**删除**之前创建的证书注册对象。如果证书注册对象已与任意受管设备关联，则无法将其删除。

按 **(+) 添加证书注册**打开**添加证书注册**对话框并配置证书注册对象，请参阅添加证书注册对象，第 55 页。然后在每个受管的前端设备上安装证书。

相关主题

使用自签注册安装证书
使用 EST 注册安装证书
使用 SCEP 注册安装证书
使用手动注册安装证书
使用 PKCS12 文件安装证书

添加证书注册对象

您可以将这些对象与 威胁防御 设备一起使用。您必须具有管理员或网络管理员权限才能执行此任务。

过程

步骤 1 打开**添加证书注册**对话框：

- 直接从对象管理打开：在**对象 > 对象管理**屏幕中，从导航窗格中选择 **PKI > 证书注册**，然后按**添加证书注册**。
- 在配置受管设备时：在**设备 > 证书** 屏幕中，选择 **添加 > 添加新证书**，然后为 **证书注册**字段点击 **(+)**。

步骤 2 输入此注册对象的**名称 (Name)** 和**说明 (Description)**（后者为可选项）。

注册完成后，此名称将成为信任点在其关联的受管设备上的名称。

步骤 3 打开 **CA 信息 (CA Information)** 选项卡并选择**注册类型 (Enrollment Type)**。

- **自签名证书** - 作为 CA 的受管设备将生成其自己的自签名根证书。此窗格中不需要其他信息。

  注释 注册自签名证书时，必须在证书参数中指定公用名称 (CN)。

- **EST**-在安全传输协议上注册。指定EST信息。请参阅证书注册对象 EST选项，第 56 页。
- **SCEP** - （默认）简单证书注册协议。指定 SCEP 信息。请参阅证书注册对象 SCEP 选项，第 57 页。
- **手动**
  - **仅 CA**-选中此复选框可仅从所选 CA 创建 CA 证书。不会为此证书创建身份证书。

如果不选中此复选框，则CA证书不是强制性的。您可以在没有CA证书的情况下生成CSR并获取身份证书。

- **CA证书**-在框中粘贴CA证书信息。您也可以通过从其他设备复制CA证书来获取该证书。

  如果选择不使用 CA 证书生成 CSR，则可以将此框留空。

- **PKCS12 文件** - 在支持 VPN 连接的 威胁防御受管设备上导入 PKCS12 文件。PKCS#12 或 PFX 文件将服务器证书、中间证书和私钥保存在一个加密文件中。 输入 **口令** 解密值。
- **跳过 CA 证书基本限制中的 CA 标志检查**-如果要跳过检查信任证书中的基本限制扩展和 CA 标志，请选中此复选框。
- **验证使用**-选择在 VPN 连接期间验证证书的选项
  - **IPsec 客户端** - 验证 IPsec 站点间 VPN 连接的客户端证书。
  - **SSL 客户端**-在远程访问 VPN 连接尝试期间验证 SSL 客户端证书。
  - **SSL 服务器**-选择以验证 SSL 服务器证书，例如作为 Cisco Umbrella 服务器证书。

步骤 4 （可选） 打开**证书参数 (Certificate Parameters)** 选项卡并指定证书内容。请参阅证书注册对象 证书参数，第 58 页。

此类信息会置于证书中，从路由器接收证书的任何一方均可访问这些信息。

步骤 5 （可选） 打开**密钥 (Key)** 选项并指定密钥信息。请参阅证书注册对象 密钥选项，第 59 页。

步骤 6 （可选） 点击**撤销**选项卡并指定撤销选项：请参阅证书注册对象 撤销选项，第 61 页。

步骤 7 如有需要，**允许覆盖 (Allow Overrides)** 此对象。有关对象覆盖的完整说明，请参阅对象覆盖，第 11 页。

下一步做什么

关联注册对象并将其安装到某设备上，以在该设备上创建一个信任点。

相关主题

使用自签注册安装证书
使用 EST 注册安装证书
使用 SCEP 注册安装证书
使用手动注册安装证书
使用 PKCS12 文件安装证书

证书注册对象 EST选项

Cisco Secure Firewall Management Center 导航路径

对象 > **对象管理**，然后从导航窗格中选择 **PKI** > **Cert 注册**。点击 **(+) 添加 Cert 注册** 来打开 **添加 Cert 注册** 对话框，然后选择 **CA 信息** 选项卡。

字段

注册类型-设置为 **EST**。

注释

- EST 注册类型不支持 EdDSA 密钥。
- 不支持 EST 在证书过期时自动注册设备的功能。

注册 **URL (Enrollment URL)** - 设备应尝试注册到的 CA 服务器的 URL。

使用 **https://CA_name:port** 形式的 HTTPS URL，其中 *CA_name* 是 CA 服务器的主机 DNS 名称或 IP 地址。 端口 号为必填项。

用户名-用于访问 CA 服务器的用户名。

密码/确认密码-访问 CA 服务器的密码。

指纹-当使用 EST 检索 CA 证书时，您可以为 CA 服务器输入指纹。使用指纹验证 CA 服务器证书的真实性有助于防止未经授权的第三方使用虚假证书替代真证书。输入十六进制格式的 CA 服务器**指纹 (Fingerprint)**。如果您输入的值与证书的指纹不匹配，则证书将被拒绝。通过直接联系服务器获取 CA 的指纹。

源接口-与 CA 服务器交互的接口。默认情况下，显示诊断接口。要将数据接口配置为源接口，请选择相应的安全区域或接口组对象。

忽略 **EST** 服务器证书验证-默认情况下，EST 服务器证书验证已完成。如果要忽略 FTD 验证 EST 服务器证书，请选中此复选框。

证书注册对象 SCEP 选项

Cisco Secure Firewall Management Center 导航路径

对象 (Objects) > 对象管理 (Object Management)，然后从导航窗格中选择 **PKI > PKI 注册 (PKI Enrollment)**。按 **(+) 添加 PKI 注册 ([+] Add PKI Enrollment)** 打开**添加 PKI 注册 (Add PKI Enrollment)** 对话框，然后选择 **CA 信息 (CA Information)** 选项卡。

字段

注册类型 **(Enrollment Type)** - 设置为 **SCEP**。

注册 **URL (Enrollment URL)** - 设备应尝试注册到的 CA 服务器的 URL。

使用 **`http://CA_name:port`** 形式的 HTTP URL，其中 CA_name 是 CA 服务器的主机 DNS 名称或 IP 地址。端口 号为必填项。

注释 如果使用主机名/FQDN 引用 SCEP 服务器，请使用 FlexConfig 对象配置 DNS 服务器。

如果 CA 中的 CA cgi-bin 脚本位置不是默认位置 (/cgi-bin/pkiclient.exe)，则您也必须将非标准脚本位置包含在 http://CA_name:port/script_location 形式的 URL 中，其中 script_location 是 CA 脚本的完整路径。

质询密码/确认密码 (Challenge Password/Confirm Password) - CA 服务器验证设备身份时所使用的密码。您可以通过直接连接 CA 服务器或通过在网络浏览器中输入以下地址获取密码：**`http://URLHostName/certsrv/mscep/mscep.dll`**。从 CA 服务器获取的密码在获取后 60 分钟内有效。因此，创建密码后请务必尽快部署。

重试时间段 (Retry Period) - 各证书请求尝试之间的时间间隔（以分钟为单位）。值可以是 1 到 60 分钟。默认值为 1 分钟。

重试计数 (Retry Count) - 若首次请求后未发出证书，应进行重试的次数。值可以是 1 到 100。默认值为 10。

CA 证书源 (CA Certificate Source) - 指定获取 CA 证书的方式。

- **使用 SCEP 检索**（默认选项，也是唯一受支持的选项）- 使用简单证书注册流程 (SCEP) 从 CA 服务器检索证书。使用 SCEP 在设备和 CA 服务器之间建立连接。在开始注册过程之前，请确保存在从设备到 CA 服务器的路由。

指纹 - 当使用 SCEP 检索 CA 证书时，您可以为 CA 服务器输入指纹。使用指纹验证 CA 服务器证书的真实性有助于防止未经授权的第三方使用虚假证书替代真证书。输入十六进制格式的 CA 服务器**指纹 (Fingerprint)**。如果您输入的值与证书的指纹不匹配，则证书将被拒绝。通过直接连接 CA 服务器或通过在网络浏览器中输入以下地址获取 CA 的指纹：**`http://<URLHostName>/certsrv/mscep/mscep.dll`**。

证书注册对象 证书参数

在发送到 CA 服务器的证书请求中指定其他信息。此类信息会置于证书中，从路由器接收证书的任何一方均可查看这些信息。

Cisco Secure Firewall Management Center 导航路径

对象 (Objects) > 对象管理 (Object Management)，然后从导航窗格中选择 **PKI > PKI 注册 (PKI Enrollment)**。按 **(+) 添加 PKI 注册 ([+] Add PKI Enrollment)** 打开**添加 PKI 注册 (Add PKI Enrollment)** 对话框，然后选择**证书参数 (Certificate Parameters)** 选项卡。

字段

使用标准 LDAP X.500 格式输入所有信息。

- **包含 FQDN (Include FQDN)** - 是否将设备的完全限定域名 (FQDN) 包含在证书请求中。选项如下：
  - **将设备主机名用作 FQDN**
  - **请不要在证书中使用 FQDN**
  - **自定义 FQDN (Custom FQDN)** - 选择此选项，然后在显示的**自定义 FQDN (Custom FQDN)** 字段中指定 FQDN。

- **包含设备的 IP 地址 (Include Device's IP Address)** - 将接口的 IP 地址包含在证书请求中。
- **公用名 (CN)(Common Name [CN])** - 要包含在证书中的 X.500 公用名。

注释 注册自签名证书时，必须在证书参数中指定公用名称 (CN)。

- **组织单位 (OU)** - 要包含在证书中的组织单位名称（例如部门名称）。
- **组织 (O) (Organization [O])** - 要包含在证书中的组织或公司名称。
- **位置 (L) (Locality [L])** - 要包含在证书中的位置。
- **州/省 (ST) (State [ST])** - 要包含在证书中的州或省。
- **国家/地区代码 (C) (County Code [C])** - 要包含在证书中的国家/地区。这些代码符合 ISO 3166 国家/地区缩写规范，例如“US”表示美国。
- **邮件 (E) (Email [E])** - 要包含在证书中的邮件地址。
- **包含设备的序列号 (Include Device’s Serial Number)** - 是否将设备的序列号包含在证书中。CA 使用序列号对证书进行验证，或者之后将证书与特定设备相关联。如有疑问，请含序列号，因为这对调试用途非常有用。

证书注册对象 密钥选项

Cisco Secure Firewall Management Center 导航路径

对象 > 对象管理，然后从导航窗格中选择 **PKI > Cert 注册**。按 **(+) 添加 Cert 注册** 打开 **添加 Cert 注册** 对话框，然后选择 **密钥** 选项卡。

字段

- **密钥类型**-RSA、ECDSA、EdDSA。

注释
- 对于 EST 注册类型，请勿选择 EdDSA 密钥，因为它不受支持。
- EdDSA 仅在站点间 VPN 拓扑中受支持。
- EdDSA 不支持作为远程访问 VPN 的身份证书。

- **密钥名称**-如果要与证书关联的密钥对已存在，则此字段指定该密钥对的名称。如果密钥对不存在，则此字段指定要分配给将在注册期间生成的密钥对的名称。如果您不指定名称，系统将使用完全限定域名 (FQDN) 密钥对。

- **密钥大小 (Key Size)** - 如果密钥对不存在，可定义所需的密钥大小（模数，以位为单位）。建议大小为2048位。模数越大，密钥越安全。但是，生成模数较大的密钥需要更长的时间（模数大于 512 位时需要一分钟或更长时间），而且交换时的处理时间也更长。

重要事项

- 在 管理中心 和 威胁防御 7.0 及更高版本上，您无法使用 RSA 加密算法注册使用 RSA 密钥大小小于 2048 位的密钥和密钥。但是，您可以使用 使用弱加密的 PKI 证书注册 ，以允许使用具有 RSA 加密算法和较小密钥大小的 SHA-1 的证书。
- 对于 威胁防御 7.0，您无法生成大小小于 2048 位的 RSA 密钥，即使启用了弱加密选项也是如此。

- **高级设置** -如果不希望在 IPsec 远程客户端证书的密钥使用和扩展密钥使用扩展中验证值，请选择 **忽略 IPsec 密钥使用** 。您可以抑制对 IPsec 客户端证书的密钥用法检查。默认情况下不启用此选项。

注释 对于站点间 VPN 连接，如果使用 Windows 证书颁发机构（CA），则默认应用策略扩展名为 **IP 安全 IKE 中间**。如果使用此默认设置，则必须为所选对象选择 **忽略 IPsec 密钥使用** 选项。否则，终端无法完成站点间 VPN 连接。

使用弱加密的 PKI 证书注册

SHA-1 散列签名算法和 RSA 密钥大小（小于 2048 位用于认证）在 管理中心 和 威胁防御7.0 及更高版本上不受支持。可以用过RSA密钥（大小小于 2048 位）来注册证书。

要在管理 威胁防御运行低于 7.0 版本的 管理中心 7.0 上覆盖这些限制，您可以在 威胁防御上使用启用弱加密选项。我们不建议允许使用弱加密密钥，因为此类密钥不如具有更大密钥大小的密钥安全。

注释 威胁防御 7.0 或更高版本不支持生成大小小于 2048 位的RSA密钥，即使您允许使用弱加密。

要在设备上启用弱加密，请导航至 **设备 > 证书** 页面。点击针对 威胁防御 设备提供的**启用弱加密**（🔒）按钮。当弱加密选项启用时，按钮更改为 🔓。默认情况下，弱加密选项已禁用。

注释 当由于弱密码使用导致证书注册失败时， 管理中心 会显示警告消息，提示您启用弱加密选项。同样，当您启用启用弱加密按钮时， 管理中心 会在设备上启用弱加密配置之前显示警告消息。

将早期版本升级到 威胁防御 7.0

当您升级到威胁防御 7.0 时，现有证书配置会保留。但是，如果这些证书的 RSA 密钥小于 2048 位，并使用 SHA-1 加密算法，则无法用于建立 VPN 连接。您必须获取 RSA 密钥大小大于 2048 位的证书，或者为 VPN 连接启用允许弱加密选项。

证书注册对象 撤销选项

通过选择和配置相关方法指定是否检查证书的撤销状态。撤销检查默认处于关闭状态，不选中任何一种方法（CRL 或 OCSP）。

Cisco Secure Firewall Management Center 导航路径

对象 (Objects) > 对象管理 (Object Management)，然后从导航窗格中选择 **PKI > PKI 注册 (PKI Enrollment)**。按 **(+) 添加 PKI 注册 ([+] Add PKI Enrollment)** 打开**添加 PKI 注册 (Add PKI Enrollment)** 对话框，然后选择**撤销 (Revocation)** 选项卡。

字段

- **启用证书撤销列表 (Enable Certificate Revocation Lists)** - 选中可启用 CRL 检查。
  - **使用来自证书的 CRL 分发点 (Use CRL distribution point from the certificate)** - 选中可获取来自证书的撤销列表分发 URL。
  - **使用已配置的静态 URL (Use static URL configured)** - 选中可添加静态的预定义的撤销列表分发 URL。然后添加 URL。

    CRL 服务器 URL (CRL Server URL) - 可从中下载 CRL 的 LDAP 服务器的 URL。

    URL 必须以 **`ldap://`**、**`http://`** 或 **`https://`** 开头。在 URL 中包含端口号。

- **启用在线证书状态协议 (Enable Online Certificate Status Protocol) (OCSP)** - 选中可启用 OCSP 检查。

  OCSP 服务器 URL (OCSP Server URL) - 需要进行 OCSP 检查时，用以检查撤销的 OCSP 服务器的 URL。

  URL 必须以 **`http://`** 或 **`https://`** 开头。

- **如果撤销信息无法访问，请考虑证书是否有效 (Consider the certificate valid if revocation information can not be reached)** - 默认处于选中状态。如果您不想允许此操作，请取消选中此字段。

注释 **如果撤销信息无法访问，请考虑证书是否有效 (Consider the certificate valid if revocation information cannot be reached)** 复选框对运行版本 6.5+ 的 威胁防御 设备没有影响。

策略列表

使用“配置策略列表”页面创建、复制和编辑策略列表策略对象。您可以创建策略列表对象以在配置路由映射时使用。当在路径映射中引用策略列表时，将评估并处理此策略列表中的所有匹配语句。通过一个路由映射可以配置两个或更多策略列表。策略列表也可以与任何其他预先存在的匹配共存，并设置在同一路径映射内部、策略列表外部配置的语句。当多个策略列表在路由映射条目中执行匹配时，所有策略列表仅在传入属性上进行匹配。

您可以将此对象与 威胁防御 设备一起使用。

过程

步骤 1 依次选择**对象** > **对象管理**并从目录中选择**策略列表**。

步骤 2 点击**添加策略列表**。

步骤 3 在**名称**字段中输入策略列表对象的名称。对象名称不区分大小写。

步骤 4 从**操作**下拉列表中选择是允许还是阻止匹配条件的访问。

步骤 5 点击**接口**选项卡以分发使其下一跳脱离其中一个指定接口的路由。

在**区域/接口**列表中，添加包含设备可通过其与管理站通信的接口的区域。对于不在区域中的接口，您可以在**所选区域/接口**列表下方的字段中键入接口名称，然后点击**添加**。仅在设备包含所选接口或区域时，系统才会在设备上配置主机。

步骤 6 点击**地址**选项卡以重新分发任何具有标准访问列表或前缀列表允许的目标地址的路由。

选择是否使用**访问列表**或**前缀列表**进行匹配，然后输入或选择要用于匹配的标准访问列表对象或前缀列表对象。

步骤 7 点击**下一跳**选项卡，重新分发具有指定访问列表或前缀列表传递的下一跳路由器地址的任何路由。

选择是否使用**访问列表**或**前缀列表**进行匹配，然后输入或选择要用于匹配的标准访问列表对象或前缀列表对象。

步骤 8 点击**路由源**选项卡，重新分发在访问列表或前缀列表指定的地址由路由器和接入服务器通告的路由。

选择是否使用**访问列表**或**前缀列表**进行匹配，然后输入或选择要用于匹配的标准访问列表对象或前缀列表对象。

步骤 9 点击 **AS 路径**选项卡以匹配 BGP 自治系统路径。如果指定多条 AS 路径，则路由可以匹配任一 AS 路径。

步骤 10 点击**社区规则**选项卡，以支持将BGP社区或扩展社区分别与指定的社区列表对象或扩展社区列表对象相匹配。如果指定多个规则，系统会根据规则验证路由，直到满足某个匹配允许或拒绝条件为止。

a) 要为规则指定社区列表，请点击**选定社区列表**字段中的给定**编辑**（✎）。社区列表显示在**可用社区列表**下。选择所需列表，点击**添加**，然后点击**确定**。

要使 BGP 社区与指定社区完全匹配，请选中**完全匹配指定社区**复选框。

b) 要添加扩展社区列表，请点击**选定扩展社区列表**字段中的给定**编辑**（）。扩展社区列表显示在**可用扩展社区列表**下。选择所需列表，点击**添加**，然后点击**确定**。

注释 扩展社区列表仅适用于配置路由的导入或导出。

步骤 11 点击**指标与标记**选项卡以匹配路由的指标和安全组标记。

a) 在**指标**字段中输入用于匹配的指标值。可以输入多个以逗号分隔的值。通过此设置可匹配具有指定指标的任何路由。指标值范围可以在 0 到 4294967295 之间。

b) 在**标记**字段中输入用于匹配的标记值。可以输入多个以逗号分隔的值。通过此设置可匹配任何具有指定安全组标记的路由。标记值范围在 0 到 4294967295 之间。

步骤 12 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 13 页。

步骤 13 点击**保存 (Save)**。

端口

端口对象以略有不同的方式代表不同协议：

TCP 和 UDP

代表传输层协议（协议号括在括号内，加上一个可选的关联端口或端口范围）的端口对象。例如：`TCP(6)/22`。

ICMP 和 ICMPv6 (IPv6-ICMP)

代表互联网层协议再加上可选类型和代码的端口对象。例如：`ICMP(1):3:3`。

您可以按类型和代码（如果适用）来限制 ICMP 或 IPV6-ICMP 端口对象。有关 ICMP 类型和代码的详细信息，请参阅：

- http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
- http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml

其他

可以代表不使用端口的其他协议的端口对象。

系统为已知端口提供默认端口对象。您无法修改或删除这些默认对象。除默认对象以外，还可以创建自定义端口对象。

可在系统 Web 界面中的不同位置使用端口对象和对象组，包括访问控制策略、身份规则、网络发现规则、端口变量和事件搜索。例如，如果您的组织使用的自定义客户端使用特定范围的端口并导致系统生成过多误导事件，可以配置网络发现策略来排除对这些端口的监控。

使用端口对象时，请遵循以下准则：

- 不能为访问控制规则中的源端口条件添加除 TCP 或 UDP 以外的任何协议。此外，在规则中设置源端口条件和目标端口条件时，不能混用传输协议。

- 如果要将不受支持的协议添加到用于源端口条件的端口对象组，则在部署配置时使用该协议的规则不会在受管设备上生效。
- 如果创建同时包含 TCP 和 UDP 端口的端口对象，然后将其添加为规则的源端口条件，则不能添加目标端口，反之亦然。

创建端口对象

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择**端口 (Port)**。

步骤 3 从**添加端口 (Add Port)** 下拉列表中选择**添加对象 (Add Object)**。

步骤 4 输入 **Name**。

步骤 5 选择**协议 (Protocol)**。

步骤 6 根据选择的协议，按**端口 (Port)** 进行限制，或者选择 ICMP **类型 (Type)** 和**代码 (Code)**。

可输入 `1` 到 `65535` 之间的端口。使用连字符指定端口范围。如果选择与**所有 (All)** 协议匹配，则必须使用**其他 (Other)** 下拉列表按端口限制对象。

步骤 7 管理对象的覆盖：

- 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 13 页。
- 如果要将覆盖值添加到此对象，请展开“覆盖”(Override) 部分并点击**添加 (Add)**；请参阅添加对象覆盖，第 13 页。

步骤 8 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

导入端口对象

有关导入端口对象的详细信息，请参阅正在导入对象，第 4 页。

前缀列表

您可以为 IPv4 和 IPv6 创建前缀列表对象以在配置路由映射、策略映射、OSPF 过滤或 BGP 邻居过滤时使用。

配置 IPv6 前缀列表

使用“配置 IPv6 前缀列表”(Configure IPv6 Prefix list) 页面创建、复制和编辑前缀列表对象。您可以创建前缀列表对象以在配置路由映射、策略映射、OSPF 过滤或 BGP 邻居过滤时使用。

您可以将此对象与 威胁防御 设备一起使用。

过程

步骤 1 依次选择**对象 (Object)** > **对象管理 (Object Management)** 并从目录中选择**前缀列表 (Prefix Lists)** > **IPv6 前缀列表 (IPv6 Prefix List)**。

步骤 2 点击**添加前缀列表 (Add Prefix List)**。

步骤 3 在**新建前缀列表对象 (New Prefix List Object)** 窗口上的**名称 (Name)** 字段中输入前缀列表对象的名称。

步骤 4 点击**新建前缀列表对象 (New Prefix List Object)** 窗口上的**添加 (Add)**。

步骤 5 从**操作 (Action)** 下拉列表中选择相应的操作（“允许”[Allow] 或“阻止”[Block]），以指示重新分发访问。

步骤 6 在**序列号 (Sequence No.)** 字段中输入用于指示新前缀列表条目在已为此对象配置的前缀列表条目列表中将具有的位置的唯一编号。如果保留为空白，则序列号将默认为比当前使用中的最大序列号大 5。

步骤 7 在 **IP 地址 (IP address)** 字段中指定 IP 地址/掩码长度格式的 IPv6 地址。掩码长度必须是介于 1 和 128 之间的有效值。

步骤 8 在**最小前缀长度 (Minimum Prefix Length)** 中输入最小前缀长度。该值必须大于掩码长度并小于或等于“最大前缀长度”(Maximum Prefix Length)（如果指定）。

步骤 9 在**最大前缀长度 (Maximum Prefix Length)** 字段中输入最大前缀长度。该值必须大于或等于“最小前缀长度”(Minimum Prefix Length)（如果存在），或者大于掩码长度（如果未指定“最小前缀长度”[Minimum Prefix Length]）。

步骤 10 点击**添加 (Add)**。

步骤 11 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖 ， 第 13 页。

步骤 12 点击**保存 (Save)**。

配置 IPv4 前缀列表

使用“配置 IPv4 前缀列表”(Configure IPv4 Prefix list) 页面创建、复制和编辑前缀列表对象。您可以创建前缀列表对象以在配置路由映射、策略映射、OSPF 过滤或 BGP 邻居过滤时使用。

您可以将此对象与 威胁防御 设备一起使用。

过程

步骤 1 依次选择**对象 (Object)** > **对象管理 (Object Management)** 并从目录中选择**前缀列表 (Prefix Lists)** > **IPv4 前缀列表 (IPv4 Prefix List)**。

步骤 2 点击**添加前缀列表 (Add Prefix List)**。

步骤 3 在**新建前缀列表对象 (New Prefix List Object)** 窗口上的**名称 (Name)** 字段中输入前缀列表对象的名称。

步骤 4 点击 **Add**。

步骤 5 从**操作 (Action)** 下拉列表中选择相应的操作（“允许”[Allow] 或“阻止”[Block]），以指示重新分发访问。

步骤 6 在**序列号 (Sequence No.)** 字段中输入用于指示新前缀列表条目在已为此对象配置的前缀列表条目列表中将具有的位置的唯一编号。如果保留为空白，则序列号将默认为比当前使用中的最大序列号大 5。

步骤 7 在 **IP 地址 (IP address)** 字段中指定 IP 地址/掩码长度格式的 IPv4 地址。掩码长度必须是介于 1 和 32 之间的有效值。

步骤 8 在**最小前缀长度 (Minimum Prefix Length)** 中输入最小前缀长度。该值必须大于掩码长度并小于或等于“最大前缀长度”(Maximum Prefix Length)（如果指定）。

步骤 9 在**最大前缀长度 (Maximum Prefix Length)** 字段中输入最大前缀长度。该值必须大于或等于“最小前缀长度”(Minimum Prefix Length)（如果存在），或者大于掩码长度（如果未指定“最小前缀长度”[Minimum Prefix Length]）。

步骤 10 点击**添加 (Add)**。

步骤 11 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 13 页。

步骤 12 点击**保存 (Save)**。

路由映射

在将路由重新分发到任何路由过程中时，将会使用路由映射。在为路由进程生成默认路由时也会使用路由映射。路由映射定义了允许将来自指定路由协议的哪些路由重新分发到目标路由进程。配置路由映射，以创建路由映射对象的新路由映射条目或编辑现有路由映射条目。

您可以将此对象与 威胁防御 设备一起使用。

开始之前

路由映射可以使用其中一个或多个对象；不必添加所有对象。根据需要创建并使用其中任何对象，以配置路由映射。

- 添加 ACL。
- 添加前缀列表。
- 添加 AS 路径。

- 添加社区列表。
- 添加扩展社区列表。

注释 扩展社区列表仅适用于配置路由的导入或导出。

- 添加策略列表。

过程

步骤 1 依次选择**对象** > **对象管理**并从目录中选择**路由映射**。

步骤 2 点击**添加路由映射**。

步骤 3 点击**新建路由映射对象**窗口上的**添加**。

步骤 4 在**序列号**字段中，输入 0 到 65535 之间的数字，该数字指示新路由映射条目在已为此路由映射对象配置的路由映射条目列表中的位置。

注释 建议至少以 10 为间隔对子句进行编号，以便将来想要插入子句时保留编号空间。

步骤 5 从**重新分发**下拉列表中选择相应的操作，即“允许”或“阻止”，以指示重新分发访问。

步骤 6 点击**匹配子句**选项卡以根据在目录中选择的以下条件来匹配（路由/流量）：

- **安全区域** - 根据（入口/出口）接口匹配流量。可以选择区域并添加这些区域，或者键入接口名称并添加这些接口。
- **IPv4** - 根据以下条件匹配 IPv4（路由/流量）；选择该选项卡可定义条件。
  1. 点击**地址**选项卡以根据路由地址来匹配路由。对于 IPv4 地址，请从下拉列表中选择要使用访问列表还是前缀列表进行匹配，然后输入或选择要用于匹配的ACL对象或前缀列表对象。
  2. 点击**下一跳**选项卡以根据路由的下一跳地址来匹配路由。对于 IPv4 地址，请从下拉列表中选择要使用访问列表还是前缀列表进行匹配，然后输入或选择要用于匹配的 ACL 对象或前缀列表对象。
  3. 点击**路由源**选项卡以根据路由的通告源地址来匹配路由。对于 IPv4 地址，请从下拉列表中选择要使用访问列表还是前缀列表进行匹配，然后输入或选择要用于匹配的 ACL 对象或前缀列表对象。
- **IPv6** - 根据路由的路由地址、下一跳地址或通告源地址来匹配 IPv6（路由/流量）。
- **BGP** - 根据以下条件来匹配 BGP（路由/流量）；选择该选项卡可定义条件。
  1. 点击 **AS 路径**选项卡以支持将 BGP 自治系统路径访问列表与指定的路径访问列表相匹配。如果指定多个路径访问列表，则路由可以匹配任一路径访问列表。
  2. 点击**社区列表**选项卡以支持将 BGP 社区或扩展社区分别与指定的社区列表对象或扩展社区列表对象相匹配。

- 要为规则指定社区列表，请点击**选定社区列表**字段中的给定**编辑**（）。社区列表显示在**可用社区列表**下。选择所需列表，点击**添加**，然后点击**确定**。有关如何创建社区列表对象的信息，请参阅社区列表，第 24 页
- 要添加扩展社区列表，请点击**选定扩展社区列表**字段中的给定**编辑**（）。扩展社区列表显示在**可用扩展社区列表**下。选择所需列表，点击**添加**，然后点击**确定**。有关如何创建扩展社区列表对象的信息，请参阅扩展社区，第 25 页。

要使 BGP 社区与指定社区列表对象完全匹配，请选中**完全匹配指定社区**复选框。此选项不适用于扩展社区列表。

注释 如果指定多个规则，系统会根据规则验证路由，直到满足某个匹配允许或拒绝条件为止。出站路由映射中将不会通告与至少一个匹配社区不匹配的路由。

3. 点击**策略列表**选项卡以配置路由映射来评估和处理 BGP 策略。当多个策略列表在路由映射条目中执行匹配时，所有策略列表仅在传入属性上进行匹配。

- **其他** - 根据以下条件来匹配路由或流量。

1. 在**指标路由值**字段中输入要用于匹配的指标值，以支持匹配路由的指标。可以输入多个以逗号分隔的值。通过此设置可匹配具有指定指标的任何路由。指标值范围可以在0到4294967295之间。
2. 在**标签值**字段中输入要用于匹配的标签值。可以输入多个以逗号分隔的值。通过此设置可匹配任何具有指定安全组标记的路由。标记值范围在 0 到 4294967295 之间。
3. 选中相应的**路由类型**选项以启用路由类型匹配。有效路由类型为 External1、External2、Internal、Local、NSSA-External1 和 NSSA-External2。可以从列表中选择多个路由类型。

步骤 7 点击**设置子句**选项卡以根据在目录中选择的以下条件来设置路由/流量：

- **指标值** - 设置“带宽”、所有值或无任何值。

1. 在**带宽**字段中以千位/秒为单位输入指标值或带宽。有效值是范围从 0 到 4294967295 的整数值。
2. 从**指标类型**下拉列表中选择指定目标路由协议的指标类型。有效值为：internal、type-1 或 type-2。

- **BGP 子句** - 根据以下条件设置 BGP 路由；选择该选项卡可定义条件。

1. 点击 **AS 路径**选项卡以修改 BGP 路由的自治系统路径。
    1. 在**预置 AS 路径**字段中输入 AS 路径编号，以将任意自治系统路径字符串预置到 BGP 路由。通常本地 AS 编号预置多次，从而增加自治系统路径长度。如果指定多个 AS 路径编号，则路径可以预置任一 AS 编号。
    2. 在**将最后一个 AS 预置到 AS 路径**字段中输入 AS 路径编号，来为 AS 路径预置最后一个 AS 编号。为 AS 编号输入 1 到 10 之间的值。

3. 选中**将路由标签转换为 AS 路径**复选框以将路由的标签转换为自治系统路径。

2. 点击**社区列表**选项卡以设置社区属性：

   在**特定社区**下：

   1. 点击**无** 单选按钮以从用于传递路由映射的前缀中删除社区属性。
   2. 点击**特定社区**单选按钮以输入社区编号（如果适用）。有效值范围为 1 至 4294967295。
   3. 选中**添加到现有社区**以将社区添加到已经现有的社区。
   4. 选中 **Internet**、**无通告**或**无导出**复选框以使用已知社区之一。

   在**特定扩展社区**下的**路由目标**字段中，输入 *ASN:nn* 格式的路由目标编号：

   - 您可以输入在 1:1 到 65534:65535 范围内的值。

     您可以在单个条目中添加单个路由目标或一组以逗号分隔的路由目标。例如*1:2,1:4,1:6*。
   - 一个条目中最多可以包含 8 个路由目标。
   - 路由映射中不能包含多余的路由目标条目。

3. 点击**其他**选项卡以设置其他属性。

   1. 选中**设置自动标签**复选框以自动计算标签值。
   2. 在**设置本地首选项**字段中输入自治系统路径的首选项值。输入 0 到 4294967295 之间的值。
   3. 在**设置权重**字段中输入路由表的 BGP 权重。输入 0 到 65535 之间的值。
   4. 选择指定 BGP 源代码。有效值为**本地 IGP** 和**不完整**。
   5. 在“IPv4 设置”部分中，指定数据包输出到的下一跳的下一跳 IPv4 地址。它不需要是相邻路由器。如果指定多个 IPv4 地址，则数据包可以在任一 IP 地址输出。

      选择在**前缀列表**下拉列表中指定 IPv4 前缀列表。
   6. 在“IPv6 设置”部分中，指定数据包输出到的下一跳的下一跳 IPv6 地址。它不需要是相邻路由器。如果指定多个 IPv6 地址，则数据包可以在任一 IP 地址输出。

      选择在**前缀列表**下拉列表中指定 IPv6 前缀列表。

步骤 8 点击**添加 (Add)**。

步骤 9 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖 ，第 13 页。

步骤 10 点击**保存 (Save)**。

安全情报

安全情报功能需要 威胁许可证（适用于 威胁防御 设备）或保护许可证（所有其他设备类型）。

安全情报 列表 和 源 是 IP 地址，域名和 URL 的集合，可用于快速过滤与列表或源上的条目匹配的流量。

- 列表是一个可手动管理的静态集合。
- 源是按一定间隔通过 HTTP 或 HTTPS 更新的动态集合。

安全情报列表/源分组为：

- DNS （域名）
- 网络 （IP 地址）
- URL

系统-提供的源

Cisco 提供以下源作为安全情报对象：

- 安全情报源定期更新来自以下方面的最新威胁情报：Talos
  - Cisco-DNS-and-URL-Intelligence-Feed（在 DNS 列表和源下）
  - Cisco 智能馈送（对于 IP 地址，在网络列表和馈送下）

  虽然无法删除系统提供的源，但可以更改其更新频率（或禁用更新）。
- Cisco-TID-Feed（在网络列表和源下）

  此源不在访问控制策略的“安全情报”选项卡中使用。

  相反，您必须启用并配置 Cisco Secure Firewall 威胁智能导向器 以使用此源，它是 TID 可观察对象数据的集合。

  可以使用此对象来设置将此类数据发布到 TID 元素的频率。

预定义列表：全局阻止列表和全局不阻止列表

系统随附域（DNS）、IP 地址（网络）和 URL 的预定义全局阻止列表和不阻止列表。

这些列表在您填充之前为空。要构建这些列表，请参阅 全局和域安全情报列表，第 71 页。

默认情况下，访问控制和 DNS 策略使用这些名单作为安全情报的一部分。

自定义源

您可以使用第三方源，或者，利用自定义内部源，您可以在具有多个Cisco Secure Firewall Management Center设备的大型部署中轻松维护企业级阻止列表。

请参阅自定义安全情报源，第 77 页。

自定义列表

自定义列表可扩充和微调源和全局列表。

请参阅自定义安全情报列表，第 79 页。

自定义安全情报列表和源使用的地方

- IP 地址和地址块 - 用于访问控制策略的阻止列表和不阻止列表，作为安全情报的一部分。
- 域名 - 用于 DNS 策略的阻止列表和不阻止列表，作为安全情报的一部分。
- URL - 用于访问控制策略的阻止列表和不阻止列表，作为安全情报的一部分。此外，您还可以在访问控制和 QoS 规则中使用 URL 列表，这些规则的分析和处理阶段发生在安全情报之后。

如何修改安全情报对象

要添加或删除阻止列表、不阻止列表、源或 Sinkhole 对象中的条目，请执行以下操作：

对象类型	编辑功能	编辑后是否需要重新部署？
自定义阻止和不阻止列表	使用对象管理器上传新列表和替代列表。	不支持
默认（但自定义填充）阻止列表和不阻止列表：全局、后代和特定域	使用上下文菜单来添加条目或使用对象管理器删除条目。	不支持
系统提供的情报源	使用对象管理器禁用或更改更新频率。	否
自定源	使用对象管理器进行全面修改。	否
Sinkhole	使用对象管理器进行全面修改。	是

全局和域安全情报列表

Firepower管理中心随附空的全局阻止和不阻止列表，您可以随时向网络中的事件立即添加URL，域和 IP 地址。这些列表允许您使用安全情报始终阻止特定连接，或通过安全情报免除特定连接的阻止，从而允许您已配置的其他威胁检测进程对其进行评估。

例如，如果注意到入侵事件中的一组可路由IP地址涉及漏洞攻击尝试，可以立即阻止这些IP地址。虽然更改可能需要几分钟时间才能完成传播，但您无需重新部署。

默认情况下，访问控制和DNS策略使用这些适用于所有安全区域的全局列表。您可以为每个策略选择不使用这些列表。

注释 这些选项仅适用于安全情报。安全情报无法阻止已使用快速路径的流量。同样，安全情报也不会自动将受信任或快速路径匹配流量列入不阻止列表。有关详细信息，请参阅关于安全情报。

在多域部署中，可以选择要通过向域列表和全局列表添加项目来实施列入阻止列表或从安全情报阻止中排除操作的 Firepower 系统域；请参阅 安全情报列表和多租户，第 72 页。

安全情报列表和多租户

在多域部署中，全局域拥有全局阻止列表和不阻止列表。只有全局管理员才可以在全局列表中添加或删除项目。因此，子域用户可以将网络、域名和 URL 列入阻止列表和不阻止列表，多租户则添加：

- 域列表 - 内容只适用于特定子域的阻止列表和不阻止列表。全局列表是全局域的域列表。
- 后代域列表 - 汇聚当前域的后代的域列表的阻止列表和不阻止列表。

域列表

除了能够访问（但不能编辑）全局列表之外，每个子域都具有自己的命名列表，命名列表的内容只应用于该子域。例如，名为 Company A 的子域拥有：

- 域阻止列表-公司 A 和域不阻止列表-公司 A
- DNS 域阻止列表-公司 A，DNS 的域不阻止列表-公司 A
- URL 域阻止列表-公司 A，URL 的域不阻止列表-公司 A

当前或以上域中的任何管理员都可以填充这些列表。您可以用情景菜单将当前及所有后代域中的项目列入阻止列表和不阻止列表。但只有关联域中的管理员可以删除域列表中的项目。

例如，全局管理员可以选择将全局域和公司 A 的域中的相同 IP 地址列入阻止列表，但不能在公司 B 的域中将其列入阻止列表。此操作会将 IP 地址添加到：

- 全局阻止列表（只有全局管理员可以将其删除）
- 域阻止列表 - 公司 A（只有公司 A 管理员可以将其删除）

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

后代域列表

后代域列表是汇聚当前域的后代的域列表的不阻止列表和阻止列表。分叶域没有后代域列表。

后代域列表很有用，因为较高级别的域管理员可以执行通用安全情报设置，但仍允许子域用户将其自己部署中的项目列入阻止列表和不阻止列表。

例如，全局域具有以下后代域列表：

- 后代阻止列表 - 全局、后代不阻止列表 - 全局

- 后代 DNS 阻止列表 - 全局、后代 DNS 不阻止列表 - 全局
- 后代 URL 阻止列表 - 全局、后代 URL 不阻止列表 - 全局

注释 后代域列表不显示在对象管理器中，因为它们是象征性汇聚，不是手动填写列表。它们显示在您可以使用它们的位置：访问控制策略和 DNS 策略。

将条目添加到全局安全情报列表

查看事件和控制面板时，您可以通过将这些事件中显示的 IP 地址、域和 URL 添加到预定义的阻止列表，立即阻止这些流量。

同样，如果安全情报阻止了您希望在安全情报阻止之后由威胁检测进程评估的流量，则可以将事件中的 IP 地址、域和 URL 添加到预定义的“不阻止”列表。

在威胁检测的安全情报阶段，将根据这些列表中的条目评估流量。

有关这些列表的详细信息，请参阅 全局和域安全情报列表，第 71 页。

开始之前

由于将条目添加到安全情报列表会影响访问控制，因此必须具有以下其中一种角色：

- 管理员
- 角色的组合：网络管理员或访问管理员，加上安全分析师和安全审批人
- 同时具有“修改访问控制策略”(Modify Access Control Policy) 和“将配置部署到设备”(Deploy Configuration to Devices) 权限的自定义角色

如果适用，请验证这些列表是否用于您期望使用它们的策略中。

过程

步骤 1 导航至包含要始终使用安全情报阻止或免于安全情报阻止的 IP 地址、域或 URL 的事件。

步骤 2 右键点击 IP 地址、域或 URL，然后选择相应的选项：

项目类型	上下文菜单选项
IP 地址	将 IP 添加到阻止列表 将 IP 添加到不阻止列表 这些选项将 IP 地址添加到相应的网络列表。
URL	将 URL 添加到 URL 的全局阻止列表 将 URL 添加到 URL 的全局不阻止列表

项目类型	上下文菜单选项
URL 字段中的 URL 域	将域添加到 URL 的全局阻止列表 将域添加到 URL 的全局不阻止列表
DNS 查询字段中的域	将域添加到 DNS 的全局阻止列表 将域添加到 DNS 的全局不阻止列表

下一步做什么

您无需重新部署即可使这些更改生效。

如果要从列表中删除项目，请参阅从全局安全情报列表中删除条目，第 74 页。

从全局安全情报列表中删除条目

注释

- 在多域部署中，这些列表的名称可能不是“全局”。有关详细信息，请参阅安全情报列表和多租户，第 72 页。
- 要向这些列表中添加条目，请参阅将条目添加到全局安全情报列表，第 73 页。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 请点击**安全情报 (Security Intelligence)**。

步骤 3 点击适当的选项：

- **网络列表和源** （对于 IP 地址）
- **DNS 列表和源** （用于域名）
- **URL 列表和源**

步骤 4 点击“全局阻止”(Global Block) 或“全局不阻止”(Global Do-Not-Block) 列表旁边的铅笔。

步骤 5 点击要删除的条目旁边的垃圾桶按钮。

安全情报的列表和源更新

列表和源更新会将现有列表或源文件替换为新文件的内容。现有文件和新文件的内容不会合并。

如果系统下载损坏的源或具有无法识别的条目的源，则系统会继续使用旧源数据（除非是第一次下载）。但是，如果系统可以识别即便源中的一个条目，也会使用其可识别的条目。

默认情况下，各个源每两小时更新一次管理中心，您可以修改频率。管理中心收到的任何更新都会立即传递到托管设备。此外，托管设备每 30 分钟轮询一次 FMC 以了解更改。您无法修改此频率。

在多域部署中，系统提供的源属于全局域，并且只能由该域中的管理员进行修改。您可以修改属于您的域的自定义源的更新频率。

要修改源更新间隔，请参阅更改安全情报源的更新频率，第 75 页。

更改安全情报源的更新频率

您可以指定 Firepower 管理中心更新安全情报源的间隔。

有关源更新的详细信息，请参阅安全情报的列表和源更新，第 74 页。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 展开**安全情报 (Security Intelligence)** 节点，然后选择要更改其频率的源类型。

系统提供的 URL 源与 **DNS 列表和源**下的域源合并。

步骤 3 在要更新的源旁边，点击 **编辑**（）。

如果显示**视图**（），则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 4 编辑 **Update Frequency**。

步骤 5 点击**保存 (Save)**。

自定义安全情报列表和源

自定义列表和源：要求

列表和源格式

每个列表或源必须是不大于 500 MB 的简单文本文件。列表文件必须包括 .txt 扩展名。每行包括一个条目或注释：一个 IP 地址、一个 URL、一个域名。

提示 可包含的条目数受该文件的最大大小限制。例如，没有注释、平均 URL 长度为 100 个字符（包括 Punycode 或百分比 Unicode 表示和换行符）的 URL 列表可包含 524 万个以上条目。

在 DNS 列表条目中，您可以为域标签指定星号 (*) 通配符。所有标签都与通配符匹配。例如，条目 `www.example.*` 与 `www.example.com` 和 `www.example.co` 均匹配。

如果在源文件中添加注释行，则其必须以井号(#)字符开头。如果上传具有注释的源文件，则系统会在上传期间删除注释。您下载的源文件包含不带注释的所有条目。

源要求

配置源时，可使用 URL 指定位置；但 URL 不能使用 Punycode 编码。

对于 30 分钟或更短的源更新间隔，必须指定 MD5 URL。这可以防止频繁下载未更改的源。如果源服务器未提供 MD5 URL，则必须使用至少 30 分钟的下载间隔。

如果您使用 MD5 校验和，校验和必须存储在仅带有该校验和的简单文本文件中。不支持注释。

URL 列表和源：URL 语法和匹配条件

安全智能URL列表和源（包括全局阻止列表和不阻止列表中的自定义列表和源和条目）可以包括以下内容，它们具有所述的匹配行为：

- 主机名

  例如，**www.example.com**。

- URL

  example.com 匹配 **example.com** 和所有子域，包括 **www.example.com**、**eu.example.com**、**example.com/abc** 和 **www.example.com/def** -- 但不包括 **example.co.uk** 或 **examplexyz.com** 或 **example.com.malicious-site.com**

  您也可以包括整个 URL 路径，例如 **https://www.cisco.com/c/en/us/products/security/firewalls/index.html**

- URL 末尾的斜杠，用于指定精确匹配项

  example.com/ 仅匹配 **example.com**；它不匹配 **www.example.com** 或任何其他 URL。

- 表示 URL 中任何域的通配符 (*)

  星号可以表示由点分隔的完整域字符串，但不能表示部分域字符串，也不能表示URL中第一个斜杠后面的任何部分。

  有效示例：

  - ***.example.com**
  - **www.*.com**
  - **example.***

    （例如，这将匹配 **example.com** 和 **example.org** 和 **example.de**，但不匹配 **example.co.uk**）

  - ***.example.***
  - **example.*/**

  无效示例：

- **example*.com**
- **example.com/***

- IP 地址 (IPv4)

  对于 IPv6 地址，或者要使用范围或 CIDR 表示法，请使用安全智能网络对象。

  您可以包含一个或多个表示八位组的通配符，例如 10.10.10.* 或 10.10.*.*。

另请参阅自定义安全情报列表，第 79 页。

自定义安全情报源

自定义或第三方安全情报源允许您使用互联网上其他定期更新且信誉良好的不阻止列表和阻止列表来扩充系统提供的情报源。也可以设置内部源；如果要使用一个源列表来更新部署中的多个 Cisco Secure Firewall Management Center 设备，这将会很有用。

注释 您不能通过在安全情报源中使用 /0 网络掩码，将地址块列入阻止列表或不阻止列表。如果要监控或阻止策略所针对的所有流量，请分别使用包含**监控 (Monitor)** 或**阻止 (Block)** 规则操作的访问控制规则，并对**源网络 (Source Networks)** 和**目标网络 (Destination Networks)** 使用默认值 any。

您也可以将系统配置为使用MD5校验和来确定是否下载更新的源。如果校验和自上次系统下载源以来没有更改，则系统无需重新下载该源。您可能希望将MD5校验和用于内部源，尤其是那些很大的内部源。

注释 在下载自定义源时，系统不执行对等 SSL 证书验证，系统也不支持使用证书捆绑包或自签证书来验证远程对等设备。

如果要对系统从互联网更新源的时间进行严格控制，可以禁用该源的自动更新。但是，自动更新可确保获取最新的相关数据。

手动更新安全情报源会更新所有源，包括情报源。

请参阅 自定义列表和源：要求，第 75 页完成要求

创建安全情报源

您必须拥有 威胁 许可证（适用于 威胁防御 设备）或保护许可证（所有其他设备类型）。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 展开**安全情报 (Security Intelligence)** 节点，然后选择要添加的源类型。

步骤 3 点击适合您在上方所选源类型的选项：

- 添加网络列表和源（对于 IP 地址）
- 添加 **DNS** 列表和源 **(Add DNS Lists and Feeds)**
- 添加 **URL** 列表和源 **(Add URL Lists and Feeds)**

步骤 4 为源输入**名称 (Name)**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 从**类型 (Type)** 下拉列表中选择**源 (Feed)**。

步骤 6 输入**源 URL (Feed URL)**。

步骤 7 输入 **MD5 URL**。

这用于确定自上次更新以来源内容是否已更改，因此系统不会下载未更改的源。

小于 30 分钟的更新间隔需要 MD5 URL。

如果源服务器未提供 MD5 URL，则必须选择至少 30 分钟的间隔。

步骤 8 选择**更新频率 (Update Frequency)**。

步骤 9 点击**保存 (Save)**。

除非已禁用源更新，否则系统会尝试下载并验证源。

手动更新安全情报源

您必须拥有 威胁 许可证（适用于 威胁防御 设备）或保护许可证（所有其他设备类型）。

开始之前

必须至少将一个设备添加到管理中心。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 展开**安全情报 (Security Intelligence)** 节点，然后选择源类型。

步骤 3 点击**更新源 (Update Feeds)**，然后确认。

步骤 4 点击 **OK**。

Cisco Secure Firewall Management Center下载和验证源更新后，会将任何更改通知其受管设备。您的部署开始使用更新的源过滤流量。

自定义安全情报列表

安全情报列表是手动上传到系统的IP地址和地址块、URL或域名的简单静态列表。如果要扩充和微调单个Cisco Secure Firewall Management Center的受管设备的源或其中一个全局列表，自定义列表很有用。

例如，如果信誉良好的源错误地阻止对重要资源的访问，但整体来说对组织有用，您即可创建仅包含分类不当的 IP 地址的自定义不阻止列表，而不是从访问控制策略的阻止列表中删除 IP 地址源对象。

注释 您不能通过在安全情报列表中使用 `/0` 网络掩码，将地址块列入阻止列表或不阻止列表。如果要监控或阻止策略所针对的所有流量，请分别使用包含**监控 (Monitor)** 或**阻止 (Block)** 规则操作的访问控制规则，并对**源网络 (Source Networks)** 和**目标网络 (Destination Networks)** 使用默认值 `any`。

有关列表条目格式，请注意以下事项：

- 地址块的网络掩码可以是 `0` 到 `32` 之间或 `0` 到 `128` 之间的整数（分别适用于 IPv4 和 IPv6）。
- 域名中的 Unicode 必须使用 Punycode 格式进行编码，并且不区分大小写。
- 域名中的字符不区分大小写。
- URL 中的 Unicode 应使用百分比编码格式进行编码。
- URL 子目录中的字符区分大小写。
- 以井号 (`#`) 开头的列表条目被视为注释。
- 请参阅 自定义列表和源：要求，第 75 页中的其他格式要求。

有关匹配的列表条目，请注意以下事项：

- 如果在 URL 或 DNS 列表中存在较高级别的域，则系统与子级别域匹配。例如，如果将 `example.com` 添加到 DNS 列表，则系统与 `www.example.com` 和 `test.example.com` 均匹配。
- 系统不对 DNS 或 URL 列表条目执行 DNS 查找（正向或反向）。例如，如果向 URL 列表中添加 `http://192.168.0.2`，并且其解析为 `http://www.example.com`，则系统仅与 `http://192.168.0.2` 匹配，而与 `http://www.example.com` 不匹配。

将新的安全情报列表上传到 Cisco Secure Firewall Management Center

要修改安全情报列表，必须更改源文件并上传新副本。不能使用 Web 界面来修改文件内容。如果您无法访问源文件，可以从系统下载副本。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 展开**安全情报 (Security Intelligence)** 节点，然后选择列表类型。

步骤 3 点击适合您在上方所选列表的选项：

- **添加网络列表和源**（对于 IP 地址）
- **添加 DNS 列表和源 (Add DNS Lists and Feeds)**
- **添加 URL 列表和源 (Add URL Lists and Feeds)**

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 从**类型 (Type)** 下拉列表中，选择**列表 (List)**。

步骤 6 点击 **Browse** 浏览至列表 `.txt` 文件，然后点击 **Upload**。

步骤 7 点击**保存 (Save)**。

下一步做什么

您无需重新部署这些更改即可生效。如果要从列表中删除条目，请参阅从全局安全情报列表中删除条目，第 74 页。

更新安全情报列表

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 展开**安全情报 (Security Intelligence)** 节点，然后选择列表类型。

步骤 3 在要更新的列表旁边，点击 **编辑**（ ）。

如果显示**视图**（ ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 如果需要对要编辑的列表保留副本，请点击**下载**，然后按照浏览器的提示将该列表另存为文本文件。

步骤 5 根据需要对列表进行更改。

步骤 6 在“安全情报”弹出窗口中，点击**浏览**以浏览到修改后的列表，然后点击**上传**。

步骤 7 点击**保存 (Save)**。

下一步做什么

您无需重新部署这些更改即可生效。如果要从列表中删除条目，请参阅从全局安全情报列表中删除条目，第 74 页。

Sinkhole

Sinkhole 对象代表为 Sinkhole 中所有域名提供非可路由地址的 DNS 服务器或没有解析到服务器的 IP 地址。您可以在 DNS 策略规则中引用 Sinkhole 对象，以将匹配流量重定向到 Sinkhole。您必须为对象同时分配 IPv4 地址和 IPv6 地址。

创建 Sinkhole 对象

您必须拥有 威胁 许可证（适用于 威胁防御 设备）或保护许可证（所有其他设备类型）。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择 **Sinkhole**。

步骤 3 点击**添加 Sinkhole (Add Sinkhole)**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 输入 Sinkhole 的 **IPv4 地址 (IPv4 Address)**和 **IPv6 地址 (IPv6 Address)**。

步骤 6 您有以下选择：

- 如果要将流量重定向到 Sinkhole 服务器，请选择**记录与 Sinkhole 的连接 (Log Connections to Sinkhole)**。
- 如果要将流量重定向到非解析 IP 地址，请选择**阻止并记录与 Sinkhole 的连接 (Block and Log Connections to Sinkhole)**。

步骤 7 如果要将危害表现 (IoC) 类型分配给 Sinkhole，请从**类型 (Type)** 下拉列表中选择一种类型。

步骤 8 点击**保存 (Save)**。

SLA 监控器

每个互联网协议服务级别协议 (SLA) 监控器定义受监控地址的连接策略，并跟踪地址路由的可用性。通过发送 ICMP 回应请求并等待响应，定期检查路由的可用性。如果请求超时，路由将从路由表中删除并使用备份路由来替换。SLA 监控作业在部署后立即开始并持续运行，除非您从设备配置移除 SLA 监控器（即，监控器并未过期）。互联网协议服务级别协议 (SLA) 监控器对象用在 IPv4 静态路由策略的“路由跟踪”字段中。IPv6 路由无法选择通过路由跟踪使用 SLA 监控器。

您可以将这些对象与 威胁防御 设备一起使用。

过程

步骤 1 依次选择**对象 (Object)** > **对象管理 (Object Management)** 并从目录中选择 **SLA 监控器 (SLA Monitor)**。

步骤 2 点击**添加 SLA 监控器 (Add SLA Monitor)**。

步骤 3 在**名称 (Name)** 字段中输入对象的名称。

步骤 4 （可选）在**说明**字段中输入对象的说明。

步骤 5 在**频率 (Frequency)** 字段中输入 ICMP 回应请求传输的频率（以秒为单位）。有效值范围为 1 到 604800 秒（7 天）。默认值为 60 秒。

注释 频率不能小于超时值；您必须将频率转换为毫秒才可比较两个值。

步骤 6 在 **SLA 监控器 ID** 字段中输入 SLA 操作的 ID 编号。值范围为 1 到 2147483647。在一个设备上最多可以创建 2000 个 SLA 操作。每个 ID 编号在策略和设备配置中必须是唯一的。

步骤 7 在**阈值**字段中，输入在 ICMP 回应请求之后且在宣告上升阀值之前必须经过的时间（以毫秒为单位）。值的范围为 0 到 2147483647 毫秒。默认值为 5000 毫秒。阈值仅用于指示超过定义值的事件。可以使用这些事件来评估适合的超时值。它不是受监控地址可达性的直接指标。

注释 阈值不应超过超时值。

步骤 8 在**超时 (Timeout)** 字段中，输入 SLA 操作等待 ICMP 回应请求响应的时间量（以毫秒为单位）。值范围为 0 到 604800000 毫秒（7 天）。默认值为 5000 毫秒。如果在此字段中定义的时间内未从受监控地址收到响应，则从路由表中删除静态路由并用备份路由来替换。

注释 超时值不能超过频率值（将频率值转换为毫秒以比较两个数字）。

步骤 9 在**数据大小 (Data Size)** 字段中输入 ICMP 请求数据包负载的大小（以字节为单位）。值范围为 0 到 16384 字节。默认值为 28 字节，它会创建一个总计 64 字节的 ICMP 数据包。请勿将此值设置为高于协议或路径最大传输单位 (PMTU) 允许的最大值。为了实现可达性，可能需要增大默认数据大小，以检测源和目标之间的 PMTU 更改。低 PMTU 会影响会话性能，如果检测到此情况，则可能表示应使用辅助路径。

步骤 10 在 **ToS** 字段中输入在 ICMP 请求数据包的 IP 报头中定义的服务类型 (ToS) 的值。值范围为 0 到 255。默认值为 0。此字段包含延迟、优先级、可靠性等信息。可供网络上其他设备用于策略路由和承诺接入速率等功能。

步骤 11 在**数据包数量 (Number of Packets)** 字段中输入发送的数据包数量。值范围为 1 到 100。默认为 1 个数据包。

注释 如果担心丢包可能会错误地导致 Cisco Secure Firewall Threat Defense设备认为受监控的地址无法访问，则请增加默认数据包数量。

步骤 12 在**受监控的地址 (Monitored Address)** 字段中，输入由 SLA 操作监控其可用性的 IP 地址。

步骤 13 **可用区域**列表同时显示区域和接口组。在**区域/接口**列表中，添加包含设备可通过其与管理站通信的接口的区域或接口组。要指定单个接口，则需要为该接口创建区域或接口组；请参阅创建安全区域和接口组对象。仅在设备包含所选接口或区域时，系统才会在设备上配置主机。

步骤 14 点击**保存 (Save)**。

时间范围

使用时间范围对象定义用于确定规则应用时间的时间段。

注释 从 管理中心 7.0 开始，Snort 3 也支持基于时间的 ACL。

创建时间范围对象

如果希望策略仅在指定的时间范围内应用，请创建一个时间范围对象，然后在策略中指定该对象。请注意，此对象仅适用于 威胁防御 设备。

只能在本主题底部列出的策略类型中指定时间范围对象。

注释 时区表示设备的本地时间，仅用于在支持时间范围的策略中应用时间范围。时区不会更改设备的配置时间。要验证配置，请在 威胁防御 CLI 中，使用 **show time-range timezone** 和 **show time** 命令（请参阅 Cisco Secure Firewall Threat Defense 命令参考 指南）。此外，机箱的时区会覆盖管理中心时区。

开始之前

根据与处理流量的设备关联的时区应用时间范围。默认情况下为 UTC。要更改与设备关联的时区，请转至 **设备 > 平台设置**。

过程

步骤 1 选择**对象 > 对象管理**。

步骤 2 从对象类型列表中，选择**时间范围**。

步骤 3 点击**添加时间范围 (Add Time Range)**。

步骤 4 输入值。

请遵守以下准则：

- 如果您在输入的对象名称周围看到一个红色的错误框，则将光标移到**名称**字段上可查看命名限制。
- 所有时间均为 UTC，除非您在 **设备 > 平台设置**中为设备指定时区。
- 使用 24 小时制时钟输入时间。例如，输入 13:30 表示 13:30。
- 要指定一个连续的范围，例如典型的周末时间（星期五下午 5 点到星期一上午 8 点，包括晚上和夜晚），请选择“范围类型”**范围**。

- 要指定多天的一部分，例如星期一到星期五的上午 8 点到下午 5 点（不包括每日的晚上、夜晚和凌晨），请选择“范围类型”**每日间隔**。
- 您可以在单个对象中最多指定 28 个时间段。
- 要为一天或不同天的不同时间制定多个不连续时间，请创建多个重复间隔。例如，要在标准工作时间以外的所有时间应用策略，请创建一个具有以下两个重复间隔的单个时间范围对象：
  - 星期一到星期五的下午 5 点到上午 8 点的每日间隔，以及
  - 星期五下午 5 点到星期一上午 8 点的范围重复间隔。

步骤 5 点击**保存 (Save)**。

下一步做什么

配置以下任意时间范围：

- 访问控制规则
- 预过滤器规则
- 隧道规则
- VPN 组策略

在 VPN 组策略对象中，使用 **访问时间** 字段指定时间范围对象。有关详细信息，请参阅配置组策略对象，第 107 页和组策略高级选项，第 113 页。

时区

要为托管设备指定本地时区，请创建时区对象，并在分配给设备的设备平台设置策略中指定该对象。

该设备本地时间仅用于在支持时间范围的策略（例如访问控制、预过滤器和VPN组策略）中应用规则中的时间范围。如果不为设备分配时区，在这些策略中应用时间范围时，将默认使用 UTC。系统中的任何其他功能都不会使用时区对象中指定的时区。

只有 威胁防御 设备支持时区对象。

注释 从 管理中心 7.0 开始，Snort 3 也支持基于时间的 ACL。

隧道区域

隧道区域代表您为进行特殊分析而明确标记的特定类型的明文、传递隧道。虽然您可以将隧道区域用作某些配置中的接口限制，但它不是接口对象。

有关详细信息，请参阅隧道区域与预过滤。

URL

重要事项 有关在安全情报配置中使用此选项和类似选项的最佳实践，以及访问控制 和 QoS 策略中的 URL 规则，请参阅 手动 URL 过滤选项。

URL 对象定义单个 URL 或 IP 地址，而 URL 组对象可以定义多个 URL 或地址。您可在系统 Web 界面中的不同位置使用 URL 对象和对象组，包括访问控制策略和事件搜索。

在创建 URL 对象时，请记住以下要点：

- 如果不包含路径（即 URL 中无 / 字符），则匹配仅基于服务器主机名。如果主机名位于 :// 分隔符之后，或在主机名中的任何点之后，则认为该主机名匹配。例如，ign.com 匹配 ign.com 和 www.ign.com，但不匹配 verisign.com。
- 如果包含一个或多个 / 字符，则整个 URL 字符串将用于子字符串匹配，其中包括服务器名称、路径和任何查询参数。但是，我们建议您不要使用手动URL过滤阻止或允许个别网页或部分网站，因为这样可能会重组服务器并将页面移至新路径。子字符串匹配还可能导致意外匹配，其中 URL 对象中包含的字符串也与非预期服务器上的路径或查询参数中的字符串匹配。
- 系统忽略加密协议（HTTP 与 HTTPS）。换句话说，如果阻止网站，系统将阻止发往该网站的 HTTP 和 HTTPS 流量，除非您使用一个应用条件指定特定协议。在创建 URL 对象时，您不需要指定创建对象时的协议。例如，使用 example.com 而不是 http://example.com。
- 如果您计划使用 URL 对象匹配访问控制规则中的 HTTPS 流量，请使用加密流量时所使用的公钥中的使用者公用名创建该对象。此外，系统会忽略使用者公用名中的子域，因此，不包括子域信息。例如，使用 example.com 而不是 www.example.com。

  但请注意，证书中的使用者公用名可能与网站的域名完全无关。例如，youtube.com 证书中的使用者公用名是 *.google.com（当然，这可能会随时更改）。如果使用 SSL 解密策略解密 HTTPS 流量以便 URL 过滤规则可用于解密策略，则可能获得更一致的结果。

注释 如果由于证书信息不再可用，浏览器恢复 TLS 会话，则 URL 对象将不匹配 HTTPS 流量。因此，即使精心配置 URL 对象，也可能会得到不一致的 HTTPS 连接结果。

创建 URL 对象

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择 **URL**。

步骤 3 从**添加 URL (Add URL)** 下拉列表中选择**添加对象 (Add Object)**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 输入**说明 (Description)**（可选）。

步骤 6 输入 **URL** 或 IP 地址。

步骤 7 管理对象的覆盖：

- 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 13 页。
- 如果要将覆盖值添加到此对象，请展开“覆盖”(Override) 部分并点击**添加 (Add)**；请参阅添加对象覆盖，第 13 页。

步骤 8 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

变量集

变量代表通常在入侵规则中用来识别源 IP 地址、目标 IP 地址、源端口和目标端口的值。还可以在入侵策略中使用变量表示规则禁止、自适应配置文件和动态规则状态中的 IP 地址。

提示 无论入侵规则中使用的网络变量定义的主机如何，预处理器规则都可以触发事件。

可以使用变量集对变量进行管理、自定义和分组。可以使用系统提供的默认变量集，也可以创建您自己的自定义变量集。可以在任何变量集中修改预定义默认变量，以及添加和修改用户定义的变量。

系统提供的大多数共享对象规则和标准文本规则均使用预定义的默认变量来定义网络和端口号。例如，大部分规则使用变量 `$HOME_NET` 指定受保护网络，使用变量 `$EXTERNAL_NET` 指定未受保护（或外部）网络。此外，专用规则通常会使用其他预定义的变量。例如，检测针对网络服务器的漏洞攻击的规则使用 `$HTTP_SERVERS` 和 `$HTTP_PORTS` 变量。

当变量更准确地反映网络环境时，规则更加有效。至少应修改默认变量集中的的默认变量。通过确保变量（例如 $HOME_NET）正确地定义网络且 $HTTP_SERVERS 包括网络上的所有网络服务器，从而优化处理和监控所有相关系统的可疑活动。

要使用变量，请将变量集链接到与访问控制规则相关的入侵策略或访问控制策略的默认操作。默认情况下，默认设置集链接到访问控制策略使用的所有入侵策略。

将一个变量添加到任意变量集会将其添加到所有变量集；也就是说，每个变量集都是系统中当前配置的所有变量的集合。在任何变量集中，都可以添加用户定义的变量以及自定义任何变量的值。

最初，系统提供由预定义默认值组成的单个默认变量集。默认变量集中的每个变量最初设置为其默认值，对于预定义变量，该默认值是由Talos 情报小组 设置并在规则更新中提供的值。

虽然可以将预定义默认变量保留为所配置的默认值，但思科建议您修改预定义变量的子集。

可以仅使用默认变量集中的变量，但在许多情况下，执行以下操作可得到最大益处：添加一个或多个自定义变量集；在不同变量集中配置不同的变量值；甚至添加新变量。

使用多个变量集时务必谨记，默认变量集中任何变量的当前值决定所有其他变量集中该变量的默认值。

如果选择“对象管理器”(Object Management) 页面上的**变量集 (Variable Sets)**，则对象管理器会列出默认变量集以及您创建的任何自定义变量集。

在全新安装的系统上，默认变量集仅由思科预定义的默认变量组成。

每个变量集都包括系统提供的默认变量以及从任何变量集添加的所有自定义变量。请注意，可以编辑默认变量集，但不能重命名或删除默认变量集。

在多域部署中，系统会为每个子域生成默认变量集。

注意 导入访问控制策略或入侵策略会以导入的默认变量覆盖默认变量集中的现有默认变量。如果现有默认变量集包含不属于导入默认变量集的自定义变量，则会保留该唯一的变量。

相关主题

管理变量，第 98 页
管理变量集，第 97 页

入侵策略中的变量集

默认情况下，Firepower 系统会将默认变量集链接到访问控制策略中使用的所有入侵策略。部署使用入侵策略的访问控制策略时，入侵策略中已启用的入侵规则将使用已链接变量集中的变量值。

修改访问控制策略中的入侵策略所使用的自定义变量集时，系统会反映该策略的状态，在 Access Control 页面上将其状态显示为过时。必须重新部署该访问控制策略，才能使变量集的更改生效。修改默认变量集时，系统会将使用入侵策略的所有访问控制策略的状态显示为过时，因此，必须重新部署所有访问控制策略才能使更改生效。

变量

变量属于以下类别之一：

默认变量

Firepower 系统提供的变量。不能重命名或删除默认变量，也不能更改其默认值。但是，可以创建默认变量的自定义版本。

自定义变量

您创建的变量。这些变量可包括：

- 自定义的默认变量

  编辑默认变量的值时，系统会将该变量从“默认变量”(Default Variables) 区域转移到“自定义变量”(Customized Variables) 区域。由于默认变量集中的变量值决定自定义变量集中变量的默认值，因此，自定义默认变量集中的默认变量会修改所有其他变量集中该变量的默认值。

- 用户定义的变量

  您可以添加和删除自己的变量，在不同变量集中自定义这些变量的值，以及将自定义变量重置为默认值。重置用户定义的变量时，该变量保留在“自定义变量”(Customized Variables) 区域。

  用户定义的变量可以是以下类型之一：

  - 网络变量指定网络流量中的主机的 IP 地址。
  - 端口变量指定网络流量中的 TCP 或 UDP 端口，包括这两种端口类型的值 `any`。

例如，如果您创建自定义标准文本规则，您可能还希望添加自己的用户定义的变量，以便更准确地反映流量或作为快捷方式简化规则创建过程。或者，如果创建只检查“隔离区”(DMZ) 中流量的规则，可以创建名为 `$DMZ` 的变量，其值列出已暴露的服务器 IP 地址。这样，在所有为该区域编写的所有规则中都可以使用 `$DMZ` 变量。

高级变量

Firepower 系统在特定情况下提供的变量。这些变量的部署非常有限。

预定义默认变量

默认情况下，Firepower 系统提供一个由预定义默认变量组成的默认变量集。Talos 情报小组 使用规则更新来提供新的和已更新的入侵规则及其他入侵策略元素，包括默认变量。

由于系统提供的许多入侵规则使用预定义默认变量，因此应为这些变量设置适当的值。可以在任何或所有变量集中修改这些默认变量的值，具体取决于如何使用变量集识别网络流量。

⚠

注意 导入访问控制策略或入侵策略会以导入的默认变量覆盖默认变量集中的现有默认变量。如果现有默认变量集包含不属于导入默认变量集的自定义变量，则会保留该唯一的变量。

下表介绍系统提供的变量并指示通常会修改哪些变量。要获得为网络定制自定义变量方面的帮助，请联系专业服务或支持部门。

表 3: 系统提供的变量

变量名称	说明	是否修改？
$AIM_SERVERS	定义已知的 AOL Instant Messenger (AIM) 服务器，并用于基于聊天的规则和查找 AIM 漏洞攻击的规则。	不需要。
$DNS_SERVERS	定义域名服务 (DNS) 服务器。如果创建专门影响 DNS 服务器的规则，可以使用 $DNS_SERVERS 变量作为目标或源 IP 地址。	在当前规则集中不需要。
$EXTERNAL_NET	定义 Firepower 系统视为未受保护的网络，并在许多规则中用于定义外部网络。	需要；应该充分定义 $HOME_NET，然后避免将 $HOME_NET 作为 $EXTERNAL_NET 的值。
$FILE_DATA_PORTS	定义非加密端口，用于检测网络数据流中的文件的入侵规则。	不需要。
$FTP_PORTS	定义网络上 FTP 服务器的端口，用于 FTP 服务器漏洞攻击规则。	如果 FTP 服务器使用除默认端口以外的端口，需要修改（可以在 Web 界面中查看默认端口）。
$GTP_PORTS	定义数据包解码器用于提取 GTP（通用分组无线业务 [GPRS] 隧道协议）PDU 中的负载的数据信道端口。	不需要。
$HOME_NET	定义相关入侵策略监控的网络，用于许多定义内部网络的规则。	需要，以便包括内部网络的 IP 地址。
$HTTP_PORTS	定义网络上 Web 服务器的端口，用于 Web 服务器漏洞攻击规则。	如果网络服务器使用除默认端口以外的端口，需要修改（可以在 Web 界面中查看默认端口）。
$HTTP_SERVERS	定义网络上的 Web 服务器。用于 Web 服务器漏洞攻击规则。	如果运行 HTTP 服务器，需要修改。
$ORACLE_PORTS	定义网络上的 Oracle 数据库服务器端口，用于扫描针对 Oracle 数据库的攻击的规则。	如果运行 Oracle 服务器，需要修改。
$SHELLCODE_PORTS	定义希望系统对其扫描外壳代码漏洞的端口，用于检测使用外壳代码的漏洞的规则。	不需要。
$SIP_PORTS	定义网络上 SIP 服务器的端口，用于 SIP 服务器漏洞攻击规则。	不需要。
$SIP_SERVERS	定义网络上的 SIP 服务器，用于针对 SIP 的漏洞攻击的规则。	需要；如果运行 SIP 服务器，应该充分定义 $HOME_NET，然后包括 $HOME_NET 作为 $SIP_SERVERS 的值。

变量名称	说明	是否修改？
$SMTP_SERVERS	定义网络上的 SMTP 服务器，用于解决针对邮件服务器的漏洞的规则。	如果运行 SMTP 服务器，需要修改。
$SNMP_SERVERS	定义网络上的 SNMP 服务器，用于扫描针对 SNMP 服务器的攻击的规则。	如果运行 SNMP 服务器，需要修改。
$SNORT_BPF	识别传统高级变量，仅在 V5.3.0 之前的 Firepower 系统软件版本（后来升级到 V5.3.0 或更高版本）中的系统上存在该变量时，才会显示该变量。	不需要，只能查看或删除此变量。不能对其进行编辑，删除后也不能再恢复。
$SQL_SERVERS	定义网络上的数据库服务器，用于解决针对数据库的漏洞的规则。	如果运行 SQL 服务器，需要修改。
$SSH_PORTS	定义网络上 SSH 服务器的端口，用于 SSH 服务器漏洞攻击规则。	如果 SSH 服务器使用除默认端口以外的端口，需要修改（可以在 Web 界面中查看默认端口）。
$SSH_SERVERS	定义网络上的 SSH 服务器，用于解决针对 SSH 的漏洞的规则。	需要修改；如果运行 SSH 服务器，应该充分定义 $HOME_NET，然后包括 $HOME_NET 作为 $SSH_SERVERS 的值。
$TELNET_SERVERS	定义网络上的已知 Telnet 服务器，用于解决针对 Telnet 的漏洞的规则。	如果运行 Telnet 服务器，需要修改。
$USER_CONF	提供一个通用工具，让您能够配置无法通过网络界面使用的一个或多个功能。 存在冲突或重复的 $USER_CONF 配置会导致系统停止。	不需要，除非功能描述中有指示或在支持人员的指导下进行。

网络变量

网络变量代表可在已在入侵策略、入侵策略规则抑制、动态规则状态和自适应配置文件中启用的入侵规则中使用的 IP 地址。网络变量与网络对象和网络对象组的不同之处在于，网络变量特定于入侵策略和入侵规则，但可以使用网络对象和网络对象组在系统网络界面中的不同位置（包括访问控制策略、网络变量、入侵规则、网络发现规则、事件搜索和报告等）来代表 IP 地址。

可在以下配置中使用网络变量来指定网络上主机的 IP 地址：

- 入侵规则 - 通过入侵规则**源 IP (Source IPs)** 和**目标 IP (Destination IPs)** 报头字段，您可以将数据包检测限于源自或发往特定 IP 地址的数据包。
- 抑制 - 在特定 IP 地址或某个范围的 IP 地址触发入侵规则或预处理器时，通过源或目标入侵规则抑制中的**网络 (Network)** 字段，您可以抑制入侵事件通知。
- 动态规则状态 - 通过源或目标动态规则状态中的**网络 (Network)** 字段，您可以检测在给定时间段内出现入侵规则或预处理器规则的过多匹配项的情况。

- 自适应配置文件 - 启用自适应配置文件更新时，自适应配置文件**网络**字段识别您希望在其中改进被动部署中的数据包分段和 TCP 流的重组的主机。

在本节所述字段中使用变量时，链接至入侵策略的变量集决定使用该入侵策略的访问控制策略处理的网络流量中的变量值。

可以将以下网络配置的任意组合添加到变量：

- 从可用网络列表中选择的网络变量、网络对象和网络对象组的任意组合
- 从“新建变量”(New Variable) 或“编辑变量”(Edit Variable) 页面添加的单个网络对象（这些对象随后可添加到变量以及其他现有和将来的变量）
- 单个文字 IP 地址或地址块

  可以通过逐个添加来列出多个文字 IP 地址和地址块。可以单独列出 IPv4 和 IPv6 地址以及地址块，或者列出它们的任意组合。指定 IPv6 地址时，可使用 RFC 4291 中定义的任意寻址约定。

在任何变量中添加的包含网络的默认值是单词 `any`，它表示任意 IPv4 或 IPv6 地址。已排除网络的默认值为 `none`，它表示无网络。还可以使用文字值指定地址 `::`，以指示包含网络列表中的任何 IPv6 地址，或排除列表中没有 IPv6 地址。

将网络添加到排除列表会使指定的地址和地址块无效。也就是说，可以匹配除了被排除的 IP 地址或地址块以外的所有 IP 地址。

例如，排除文字地址 `192.168.1.1` 会指定除 192.168.1.1 以外的所有 IP 地址，排除 `2001:db8:ca2e::fa4c` 会指定除 2001:db8:ca2e::fa4c 以外的所有 IP 地址。

使用文字网络或可用网络可以排除任意的网络组合。例如，排除文字值 `192.168.1.1` 和 `192.168.1.5` 会包含除 192.168.1.1 或 192.168.1.5 以外的任何 IP 地址。也就是说，系统将此解释为“**既不是** 192.168.1.1 **也不是** 192.168.1.5”，这就会匹配除括号中列出的 IP 地址以外的所有 IP 地址。

添加或编辑网络变量时，请注意以下几点：

- 在逻辑上，不能排除值 `any`，如果排除该值，将表示无地址。例如，不能将具有值 `any` 的变量添加到排除网络列表。
- 网络变量为指定的入侵规则和入侵策略功能识别流量。请注意，无论入侵规则中使用的网络变量定义的主机如何，预处理器规则都可以触发事件。
- 已排除的值必须解析到已包括的值的子集。例如，不能包含地址块 192.168.5.0/24 并排除 192.168.6.0/24。

端口变量

端口变量代表可在入侵策略中启用的入侵规则的**源端口 (Source Port)** 和**目标端口 (Destination Port)** 报头字段中使用的 TCP 和 UDP 端口。端口变量与端口对象和端口变量特定于入侵规则的端口对象组不同。可以为除 TCP 和 UDP 以外的其他协议创建端口对象，还可以在系统 Web 界面中的不同位置使用端口对象，包括端口变量、访问控制策略、网络发现规则和事件搜索。

可以在入侵规则 **Source Port** 和 **Destination Port** 报头字段中使用端口变量来限制仅检查来自或发往特定 TCP 或 UDP 端口的数据包。

在这些字段中使用变量时，链接到与访问控制规则或策略相关的入侵策略的变量集决定部署访问控制策略的网络流量中这些变量的值。

可以将以下端口配置的任意组合添加到变量：

- 端口变量与您从可用端口列表中选择的端口对象的任何组合

  请注意，可用端口的列表不会显示端口对象组，因此您不能将这些端口对象组添加到变量。

- 从“新变量”(New Variable) 或“编辑变量”(Edit Variable) 页面添加的单个端口对象（这些对象随后可添加到变量以及其他现有和将来的变量）

  只有 TCP 和 UDP 端口（包括任一类型的值 `any`）是有效的变量值。如果您使用新的或编辑变量页面以添加不是有效变量值的有效端口对象，则该对象将被添加到系统，但不会显示在可用对象列表中。当您使用对象管理器来编辑变量中使用的端口对象时，只能将其值更改为有效的变量值。

- 单个文字端口值和端口范围

  您必须使用破折号 (-) 分隔端口范围。使用冒号 (:) 指示的端口范围支持向后兼容性，但您不能在您创建的端口变量中使用冒号。

  您可以通过在任何组合中单独添加每个文字端口值和范围，来列出多个文字端口值和范围。

在添加或编辑端口变量时，请注意以下要点：

- 在您添加的任何变量中，包括的端口的默认值为文字 `any`，它表示任何端口或端口范围。排除端口的默认值为 `none`，它表示无端口。

提示 要创建值为 `any` 的变量，请命名并保存该变量，而不要添加具体的值。

- 您不能在逻辑上排除值 `any`，如果排除，这将表示无端口。例如，您不能在将值为 `any` 的变量添加到已排除端口的列表时保存变量集。
- 将端口添加到已排除列表将使指定端口和端口范围无效。即您可以将任何端口与已排除的端口或端口范围进行匹配。
- 已排除的值必须解析到已包括的值的子集。例如，您不能包括端口范围 10-50 并排除端口 60。

高级变量

高级变量让您能够配置通常无法通过网络界面配置的功能。Firepower 系统当前只提供一个高级变量，即 USER_CONF 变量。

USER_CONF

USER_CONF 提供一个通用工具，让您能够配置无法以其他方式通过 Web 界面获得的一个或多个功能。

注意 请**勿**使用高级变量 USER_CONF 来配置入侵策略功能，除非功能描述或支持人员指示您这样做。存在冲突或重复的配置会导致系统停止。

编辑 USER_CONF 时，单行最多总共可输入 4096 个字符；达到该限制后，行会自动换行。可以包含任意数量的有效说明或行，直至达到变量的最大字符长度限制（8192 个字符）或物理限制（例如磁盘空间）。在命令指令中，可以在任何完整参数之后使用反斜线 (\) 续行符。

重置 USER_CONF 会将其清空。

变量重置

在变量集新建或编辑变量页面上，可以将变量重置为默认值。下表总结了重置变量的基本原则。

表 *4:* 变量重置值

要重置的变量类型	所属变量集类型	重置后的值
默认值	默认值	规则更新值
用户定义	默认值	`any`
默认变量或用户定义的变量	自定义	当前默认变量集值（已修改或未修改）

重置自定义变量集中的变量会将其重置为该变量在默认变量集中的当前值。

相反，重置或修改默认变量集中某个变量的值总是会更新所有自定义变量集中该变量的默认值。如果重置图标呈灰色显示，表示不能重置变量，这意味着该变量在该变量集中没有自定义值。除非自定义了自定义变量集中某个变量的值，否则对默认变量集中该变量的更改会更新与该变量集链接的任何入侵策略中使用的值。

注释 理想做法是修改默认变量集中的某个变量，以评估这些更改如何影响使用链接自定义变量集中的该变量的任何入侵策略，尤其是在尚未定制自定义变量集中的变量值时。

将指针悬停在变量集中的**重置图标** 上可查看重置值。当自定义值和重置值相同时，这表示以下其中一种情况属实：

- 您在自定义或默认变量集中，而且在其中添加了值为 `any` 的变量
- 您在自定义变量集中，在其中添加了具有显式值的变量，并且选择了使用配置值作为默认值

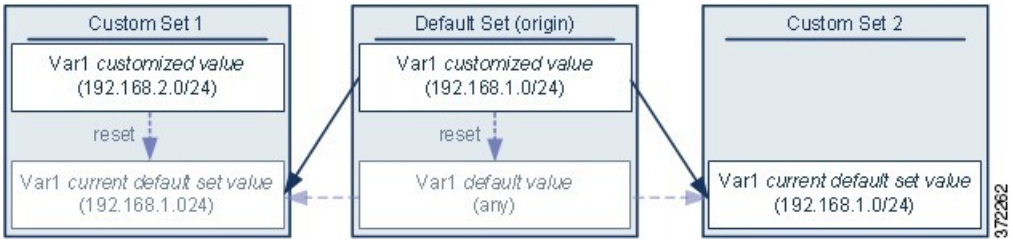
将变量添加到变量集

将变量添加到变量集会将其添加到所有其他变量集。添加自定义变量集中的变量时，必须选择是否使用配置值作为默认变量集中的定制值：

- **如果使用配置值**（例如 192.168.0.0/16），则该变量会被添加到使用配置值作为定制值、默认值为 any 的默认变量集中。由于默认变量集的当前值决定其他变量集的默认值，所以其他自定义变量集的初始默认值为配置值（在本例中为 192.168.0.0/16）。
- **如果不使用配置值**，则该变量将被添加到仅使用默认值 any 的默认变量集中，因此其他自定义变量集的初始默认值将为 any。

示例：将用户定义变量添加到默认变量集

下图说明了将用户定义的变量 Var1（其值为 192.168.1.0/24）添加到默认变量集时发生的变量集交互。



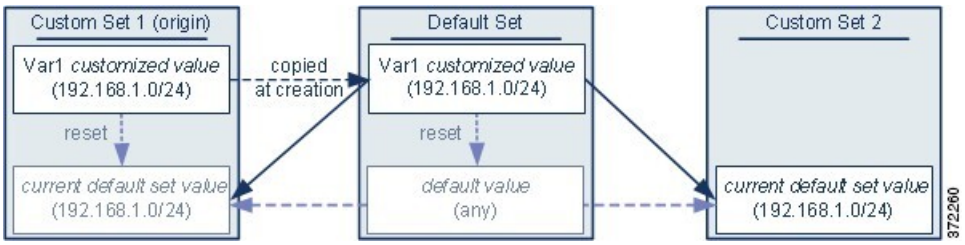
您可以在任何变量集中自定义 Var1 的值。在未自定义 Var1 的自定义变量集 2 中，此变量的值是 192.168.1.0/24。在自定义变量集 1 中，Var1 的自定义值 192.168.2.0/24 覆盖了默认值。重置默认变量集中某个用户定义的变量会将所有变量集中该变量的默认值重置为 any。

须注意的一点是，在本示例中，如果不更新自定义变量集 2 中的 Var1，进一步自定义或重置默认变量集中的 Var1 会导致更新自定义变量集 2 中 Var1 的默认值，从而影响与变量集相关联的所有入侵策略。

请注意，虽然在本示例中未显示，但用户定义的变量和默认变量的变量集交互是相同的，唯一不同的是重置默认变量集中的默认变量会在当前规则更新中将其值重置为由思科配置的值。

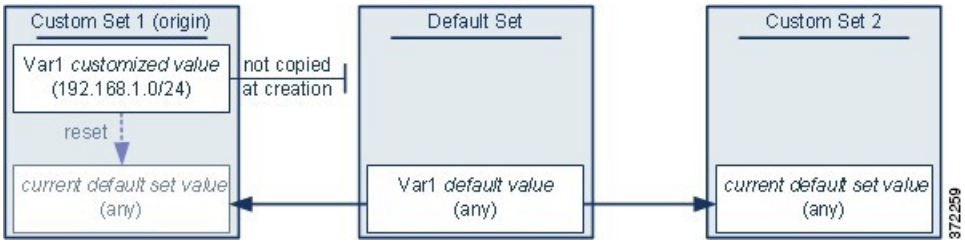
示例：将用户定义变量添加到自定义变量集

以下两个示例说明了将用户定义的变量添加到自定义变量集时变量集之间的交互。保存新变量时，系统会提示您选择是否将配置值用作其他变量集的默认值。在以下示例中，您选择**使用**配置值。



请注意，除了 Var1 来自自定义变量集 1 以外，本示例与以上将 Var1 添加到默认变量集的示例完全相同。将 Var1 的自定义值 192.168.1.0/24 添加到自定义变量集 1 会将该值复制到默认变量集，以作为默认值为 any 的自定义值。之后，Var1 值和交互就像之前将 Var1 添加到默认变量集一样。请记住，与前一个示例一样，进一步自定义或重置默认变量集中的 Var1 会导致更新自定义变量集 2 中 Var1 的默认值，从而影响与变量集相关联的所有入侵策略。

在下一个示例中，像前一个示例一样，将 Var1（其值为 192.168.1.0/24）添加到自定义变量集 1，但选择**不使用** Var1 的配置值作为其他变量集中的默认值。



此方法会将 Var1（其默认值为 any）添加到所有变量集。添加 Var1 后，可以在任何变量集中自定义它的值。此方法的优点是，通过最初不在默认变量集中自定义 Var1，可以降低这样的风险：在默认变量集中自定义此变量的值时，无意中更改了尚未自定义 Var1 的变量集（例如，自定义变量集 2）中的当前值。

嵌套变量

只要嵌套不是循环的，就可以嵌套变量。不支持嵌套的、否定的变量。

有效的嵌套变量

在此示例中，SMTP_SERVERS、HTTP_SERVERS 和 OTHER_SERVERS 是有效的嵌套变量。

变量	类型	包含的网络	排除的网络
SMTP_SERVERS	自定义默认值	10.1.1.1	-
HTTP_SERVERS	自定义默认值	10.1.1.2	-
OTHER_SERVERS	用户定义的变量	10.2.2.0/24	-
HOME_NET	自定义默认值	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

无效的嵌套变量

在本例中，HOME_NET 是一个无效的嵌套变量，因为 HOME_NET 的嵌套是循环的；即，OTHER_SERVERS 的定义包括 HOME_NET，因此您将在其自身中嵌套 HOME_NET。

变量	类型	包含的网络	排除的网络
SMTP_SERVERS	自定义默认值	10.1.1.1	-
HTTP_SERVERS	自定义默认值	10.1.1.2	-

变量	类型	包含的网络	排除的网络
OTHER_SERVERS	用户定义的变量	10.2.2.0/24 HOME_NET	-
HOME_NET	自定义默认值	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

不受支持的嵌套的、否定的变量

由于嵌套的、否定的变量不受支持，因此不能使用本例所示的变量 NONCORE_NET 来表示受保护网络之外的 IP 地址。

变量	类型	包含的网络	排除的网络
HOME_NET	自定义默认值	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	-
EXTERNAL_NET	自定义默认值	-	HOME_NET
DMZ_NET	用户定义的变量	10.4.0.0/16	-
NOT_DMZ_NET	用户定义的变量	-	DMZ_NET
NONCORE_NET	用户定义的变量	EXTERNAL_NET NOT_DMZ_NET	-

不受支持的嵌套的、否定的变量的替代方法

作为上述示例的替代方法，您可以通过创建变量 NONCORE_NET 来表示受保护网络之外的 IP 地址，如本例所示。

变量	类型	包含的网络	排除的网络
HOME_NET	自定义默认值	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	-
DMZ_NET	用户定义的变量	10.4.0.0/16	-
NONCORE_NET	用户定义的变量	-	HOME_NET DMZ_NET

管理变量集

要使用变量集，您必须拥有 威胁 许可证（适用于 威胁防御 设备）或保护许可证（所有其他设备类型）。

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择**变量集 (Variable Set)**。

步骤 3 管理变量集：

- 添加 - 如果要添加自定义变量集，请点击**添加变量集 (Add Variable Set)**；请参阅创建变量集，第 97 页。
- 删除 - 如果要删除自定义变量集，请点击变量集旁边的 **删除**（）），然后点击**是 (Yes)**。不能删除默认变量集或属于祖先域的变量集。

  注释 在删除的变量集中创建的变量不会被删除或以其他方式在其他集合中受影响。

- 编辑 - 如果要编辑变量集，请点击要修改的变量集旁边的 **编辑**（）；请参阅编辑对象，第 7 页。
- 过滤 - 如果要按名称过滤变量集，请开始输入名称；当您键入时，页面会刷新以显示匹配的名称。如果要清除名称过滤，请点击过滤器字段中的 **清除**（）。
- 管理变量 - 要管理变量集中包含的变量，请参阅管理变量，第 98 页。

创建变量集

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择**变量集 (Variable Set)**。

步骤 3 点击**添加变量集 (Add Variable Set)**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 输入**说明 (Description)**（可选）。

步骤 6 管理变量集中的变量；请参阅管理变量，第 98 页。

步骤 7 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

管理变量

您必须拥有 威胁 许可证（适用于 威胁防御 设备）或保护许可证（所有其他设备类型）。

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择**变量集 (Variable Set)**。

步骤 3 点击要编辑的变量集旁边的 **编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 管理变量：

- 显示 - 如果要显示变量的完整值，请将指针悬停在变量旁边的**值 (Value)** 列中的值上方。
- 添加 - 如果要添加变量，请点击**添加 (Add)**；请参阅添加变量， 第 99 页。
- 删除 - 点击变量旁边的 **删除**（）。如果自添加变量后已保存变量集，请点击**是 (Yes)** 以确认是否要删除变量。

  不能删除以下变量：

  - 默认变量
  - 入侵规则或其他变量所使用的用户定义的变量
  - 属于祖先域的变量

- 编辑 - 点击要编辑的变量旁边的 **编辑**（）；请参阅 编辑变量， 第 100 页。
- 重置 - 如果要将已修改变量重置为其默认值，请点击已修改变量旁边的 **重置** 。如果重置呈灰色显示，则表明以下情况之一成立：

  - 当前值已是默认值。
  - 配置属于祖先域。

  提示 将指针悬停在活动的重置图标上可显示默认值。

步骤 5 点击**保存 (Save)** 以保存变量集。如果变量集正在供访问控制策略使用，请点击**是 (Yes)** 以确认要保存更改。

由于默认变量集中的当前值决定所有其他变量集中的默认值，因此，修改或重置默认变量集中的变量会更改未对该变量默认值进行自定义的那些变量集中的该变量当前值。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

添加变量

您必须拥有 威胁 许可证（适用于 威胁防御 设备）或保护许可证（所有其他设备类型）。

过程

步骤 1 在变量集编辑器中，点击**添加 (Add)**。

步骤 2 在 **Name** 字段中为变量输入一个唯一名称。

步骤 3 从**类型 (Type)** 下拉列表中，选择**网络 (Network)** 或**端口 (Port)**。

步骤 4 为变量指定值：

- 如果要将项目从可用网络或端口列表移动到包含或排除项目列表，可以选择一个或多个项目，然后进行拖放，或者点击**包含 (Include)** 或**排除 (Exclude)**。

  提示 如果网络或端口变量的包含变量列表和排除变量列表中的地址或端口重叠，排除的地址或端口优先。

- 输入一个文字值，然后点击**添加 (Add)**。对于网络变量，可以输入单个 IP 地址或地址块。对于端口变量，可以添加单个端口或端口范围，用连字符(-)隔开上限和下限值。如有需要，可重复此步骤输入多个文字值。
- 如果要从包含或排除列表中删除项目，请点击该项目旁边的 **删除**（ ）。

注释 要包含或排除的项目列表可以包括原义字符串和现有变量、对象及网络对象组（对于网络变量）的任意组合。

步骤 5 点击 **Save** 保存变量。如果是添加自定义变量集中的新变量，可以选择以下选项：

- 点击**是 (Yes)** 添加使用配置值作为默认变量集中的自定义值（进而也是其他自定义变量集中的默认值）的变量。
- 点击**否 (No)** 将变量添加为默认变量集中的默认值 `any`（进而在其他自定义变量集中也使用此默认值）。

步骤 6 点击**保存 (Save)** 以保存变量集。更改保存成功，与该变量集链接的所有访问控制策略均显示为过期状态。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

编辑变量

您必须拥有 威胁 许可证（适用于 威胁防御 设备）或保护许可证（所有其他设备类型）。

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

可以同时编辑自定义变量和默认变量。

无法更改现有变量中的**名称 (Name)** 或**类型 (Type)** 值。

过程

步骤 1 在变量集编辑器中，点击要修改的变量旁边的 **编辑**（ ）。

如果显示**视图**（ ），则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 2 修改变量：

- 如果要将项目从可用网络或端口列表移动到包含或排除项目列表，可以选择一个或多个项目，然后进行拖放，或者点击**包含 (Include)** 或**排除 (Exclude)**。

  提示 如果网络或端口变量的包含变量列表和排除变量列表中的地址或端口重叠，排除的地址或端口优先。

- 输入一个文字值，然后点击**添加 (Add)**。对于网络变量，可以输入单个 IP 地址或地址块。对于端口变量，可以添加单个端口或端口范围，用连字符(-)隔开上限和下限值。如有需要，可重复此步骤输入多个文字值。
- 如果要从包含或排除列表中删除项目，请点击该项目旁边的 **删除**（ ）。

注释 要包含或排除的项目列表可以包括原义字符串和现有变量、对象及网络对象组（对于网络变量）的任意组合。

步骤 3 点击 **Save** 保存变量。

步骤 4 点击**保存 (Save)** 以保存变量集。如果变量集正在供访问控制策略使用，请点击**是 (Yes)** 以确认要保存更改。更改保存成功，与该变量集链接的所有访问控制策略均显示为过期状态。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

VLAN 标签

配置的每个 VLAN 标记对象代表一个 VLAN 标记或标记范围。

可以将VLAN标记对象进行分组。组表示多个对象；就此意思而言，在单个对象中使用一系列VLAN标记不被视为组。

可以在系统 Web 界面中的各种位置使用 VLAN 标记对象和组，包括规则和事件搜索。例如，可以编写仅适用于特定 VLAN 的访问控制规则。

创建 VLAN 标记对象

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中，选择 **VLAN 标记 (VLAN Tag)**。

步骤 3 从**添加 VLAN 标记 (Add VLAN Tag)** 下拉列表中，选择**添加对象 (Add Object)**。

步骤 4 输入 **Name**。

步骤 5 输入 **Description**。

步骤 6 在 **VLAN 标记 (VLAN Tag)** 字段中输入值。使用连字符可指定 VLAN 标记范围。

步骤 7 管理对象的覆盖：

- 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 13 页。
- 如果要将覆盖值添加到此对象，请展开“覆盖”(Override) 部分并点击**添加 (Add)**；请参阅添加对象覆盖，第 13 页。

步骤 8 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

VPN

您可以在 威胁防御 设备上使用以下 VPN 对象。要使用这些对象，您必须具有管理员权限，并且您的智能许可证帐户必须满足导出控制要求。您只能在分叶域中配置这些对象。

威胁防御 IKE 策略

互联网密钥交换 (IKE) 是用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的密钥管理协议。IKE 协商包含两个阶段。第 1 阶段协商两个 IKE 对等体之间的安全关联，使对等体能够在第 2 阶段中安全通信。在第 2 阶段协商期间，IKE 为其他应用建立 SA，例如 IPsec。两个阶段在协商连接时均使用提议。IKE 提议是一组两个对等体用于保护其之间的协商的算法。在各对等体商定公共（共享）IKE 策略后，即开始 IKE 协商。此策略声明哪些安全参数用于保护后续 IKE 协商。

对于 IKEv1，IKE 方案包含单个算法集和模数组。您可以创建确保多个优先化的策略来确保至少一个策略与远程对等体的策略匹配。与 IKEv1 不同，在 IKEv2 方案中，您可以在一个策略中选择多个算法和模数组。由于对等体在第 1 阶段协商期间进行选择，因此可创建单个 IKE 方案，但是考虑多个不同的方案，以向最需要的方案提供更高的优先级。对于 IKEv2，策略对象不指定身份验证，其他策略必须定义身份验证要求。

当配置站点间 IPsec VPN 时，需要 IKE 策略。有关详细信息，请参阅VPN。

配置 IKEv1 策略对象

使用“IKEv1 策略”(IKEv1 Policy) 页面创建、编辑或删除 IKEv1 策略对象。这些策略对象包含 IKEv1 策略所需的参数。

过程

步骤 1 依次选择**对象 (Objects)** > **对象管理 (Object Management)** 并从目录中选择 **VPN** > **IKEv1 策略 (IKEv1 Policy)**。

系统将列出之前配置的策略，包括系统定义的默认值。根据您的访问级别，您可以 **编辑**（）、查看 **视图**（） 或 **删除**（） 方案。

步骤 2 （可选） 选择**添加**（）**添加 IKEv1 策略 (Add IKEv1 Policy)** 以创建新策略对象。

步骤 3 为此策略输入**名称 (Name)**。最多允许 128 个字符。

步骤 4 （可选） 为此方案输入**说明 (Description)**。最多允许 1,024 个字符。

步骤 5 在**优先级 (Priority)** 中输入 IKE 策略的优先级值。

当尝试查找常见安全关联 (SA) 时，优先级值可确定两个协商对等体比较的 IKE 策略顺序。如果远程 IPsec 对等体不支持在您的第一个策略中选定的参数，它会尝试使用下一个优先级中定义的参数。有效值范围为 1 到 65,535。数值越低，优先级越高。如果将此字段留空，管理中心将分配最低的未分配值，从 1 开始然后为 5，并以 5 为增量继续。

步骤 6 在**加密**中选择加密方法。

在决定为 IKEv1 策略使用哪种加密和散列算法时，您的选择限于对等设备支持的算法。对于 VPN 拓扑中的外部设备，必须选择与两个对等体匹配的算法。对于 IKEv1，选择相关选项之一。 有关选项的完整说明，请参阅决定使用哪个加密算法。

步骤 7 选择创建消息摘要的**散列 (Hash)** 算法，用于确保消息的完整性。

在决定为IKEv1方案使用哪种加密和散列算法时，您的选择限于受管设备支持的算法。对于VPN拓扑中的外部设备，必须选择与两个对等体匹配的算法。 有关选项的完整说明，请参阅决定使用哪些散列算法。

步骤 8 设置 **Diffie-Hellman 组**。

用于加密的Diffie-Hellman组。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。选择要在 VPN 中允许的组。有关选项的完整说明，请参阅决定要使用的 Diffie-Hellman 模数组。

步骤 9 设置安全关联 (SA) 的**持续期限 (Lifetime)**（以秒为单位）。可指定 120 到 2,147,483,647 秒之间的值。默认值为 86400。

当超过持续期限时，SA 到期且必须在两个对等体之间重新协商。通常，持续期限越短（某种程度上），IKE协商越安全。但是，持续期限越长，将来设置IPsec安全关联的速度相比较短持续期限的更快。

步骤 10 设置在两个对等体之间使用的**身份验证方法 (Authentication Method)**。

- **预共享密钥 (Preshared Key)** - 在身份验证阶段，预共享密钥允许密钥在两个对等体之间共享并由 IKE 使用。如果未使用同一预共享密钥配置其中一个参与的对等体，则无法建立 IKE SA。
- **证书 (Certificate)** - 当您将“证书”(Certificate)用作 VPN 连接的身份验证方法时，对等体从 PKI 基础设施中的 CA 服务器获取数字证书，并用其相互进行身份验证。

注释 在支持IKEv1的VPN拓扑中，所选IKEv1策略对象中指定的**身份验证方法**会成为IKEv1**身份验证类型**设置的默认设置。这些值必须匹配，否则，您的配置将出错。

步骤 11 点击**保存**
IKEv1 策略添加到列表中。

配置 IKEv2 策略对象

使用“IKEv2 策略”(IKEv2 Policy)对话框来创建、删除和编辑 IKEv2 策略对象。这些策略对象包含 IKEv2 策略所需的参数。

过程

步骤 1 依次选择**对象 (Objects)** > **对象管理 (Object Management)**，然后从目录中选择 **VPN** > **IKEv2 策略 (IKEv2 Policy)**。

系统将列出之前配置的策略，包括系统定义的默认值。根据您的访问级别，您可以**编辑**（）、**视图**（）或**删除**（）策略。

步骤 2 选择**添加**（）**添加 IKEv2 策略 (Add IKEv2 Policy)** 以创建新策略。

步骤 3 为此策略输入**名称 (Name)**。

策略对象的名称。最多允许 128 个字符。

步骤 4 为此策略输入**说明 (Description)**。

策略对象的说明。最多允许 1024 个字符。

步骤 5 输入**优先级 (Priority)**。

IKE 方案的优先级值。当尝试查找常见安全关联 (SA) 时，优先级值可确定两个协商对等体比较的 IKE 方案顺序。如果远程 IPsec 对等体不支持在您的第一个策略中选定的参数，它会尝试使用下一个最低优先级策略中定义的参数。有效值范围为 1 到 65535。数值越低，优先级越高。如果将此字段留空，管理中心将分配最低的未分配值，从 1 开始然后为 5，并以 5 为增量继续。

步骤 6 设置安全关联 (SA) 的**持续期限 (Lifetime)**（以秒为单位）。可指定 120 到 2,147,483,647 秒之间的值。默认值为 86400。

当超过持续期限时，SA 到期且必须在两个对等体之间重新协商。通常，持续期限越短（某种程度上），IKE 协商越安全。但是，持续期限越长，将来设置 IPsec 安全关联的速度相比较短持续期限的更快。

步骤 7 选择 IKE 策略中使用的散列算法的**完整性算法 (Integrity Algorithms)** 部分。散列算法创建消息摘要，它用于确保消息的完整性。

在决定为 IKEv2 方案使用哪种加密和散列算法时，您的选择限于受管设备支持的算法。对于 VPN 拓扑中的外部设备，必须选择与两个对等体匹配的算法。选择要在 VPN 中允许的所有算法。有关选项的完整说明，请参阅决定使用哪些散列算法。

步骤 8 选择用于建立第 1 阶段 SA（用于保护第 2 阶段协商）的**加密算法 (Encryption Algorithm)**。

在决定为 IKEv2 方案使用哪种加密和散列算法时，您的选择限于受管设备支持的算法。对于 VPN 拓扑中的外部设备，必须选择与两个对等体匹配的算法。选择要在 VPN 中允许的所有算法。 有关选项的完整说明，请参阅决定使用哪个加密算法。

步骤 9 选择**PRF 算法 (PRF Algorithm)**。

IKE 策略中使用的散列算法的伪随机函数 (PRF) 部分。在 IKEv1 中，完整性和 PRF 算法不分开，但在 IKEv2 中，可以为这些元素指定不同的算法。选择要在 VPN 中允许的所有算法。 有关选项的完整说明，请参阅决定使用哪些散列算法。

步骤 10 选择并**添加 DH 组 (DH Group)**。

用于加密的 Diffie-Hellman 组。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。选择您想要在 VPN 中允许的组。 有关选项的完整说明，请参阅决定要使用的 Diffie-Hellman 模数组。

步骤 11 点击**保存**

如果已选择有效的选项组合，则新的 IKEv2 策略会添加到列表中。如果未选择，在会显示错误消息，且必须相应地做出更改，以便成功保存此策略。

威胁防御 IPSec 提议

在配置 VPN 拓扑时，使用 IPsec 方案（或转换集）。在与 ISAKMP 进行 IPsec 安全关联协商期间，对等体同意使用特定方案来保护特定数据流。两个对等体的方案必须相同。

根据 IKE 版本（IKEv1 或 IKEv2），存在不同的 IPsec 方案对象：

- 当创建 IKEv1 IPsec 方案（转换集）对象时，可以选择 IPsec 运行的模式，并定义所需的加密和身份验证类型。您可以为算法选择单一选项。如果要在VPN中支持多个组合，请创建多个IKEv1 IPsec 方案对象。
- 当创建 IKEv2 IPsec 方案对象时，可以选择 VPN 中允许的所有加密和散列算法。在 IKEv2 协商期间，对等体选择其分别支持的最合适选项。

IKEv1 和 IKEv2 IPsec 方案都使用封装安全协议 (ESP)。它可以提供身份验证、加密和反重播服务。ESP 为 IP 协议类型 50。

注释 我们建议对 IPsec 隧道使用加密和身份验证。

配置 IKEv1 IPsec 方案对象

过程

步骤 1 依次选择**对象 (Objects)** > **对象管理 (Object Management)**，然后从目录中选择 **VPN** > **IPsec IKev1 方案 (IPsec IKev1 Proposal)**。

系统将列出以前配置的方案，包括系统定义的默认值。根据您的访问级别，您可以 **编辑**（）、查看 **视图**（）或 **删除**（）方案。

步骤 2 选择**添加**（）**添加 IPsec IKEv1 方案 (Add IPsec IKEv1 Proposals)** 以创建新的方案。

步骤 3 为此方案输入**名称 (Name)**

策略对象的名称。最多允许 128 个字符。

步骤 4 为此方案输入**说明 (Description)**。

策略对象的说明。最多允许 1024 个字符。

步骤 5 选择 **ESP 加密**方法。此方案的封装安全协议 (ESP) 加密算法。

对于IKEv1，选择相关选项之一。在决定用于IPsec方案的加密和散列算法时，您的选择仅限于VPN中的设备所支持的算法。 有关选项的完整说明，请参阅决定使用哪个加密算法。

步骤 6 为 **ESP 散列 (ESP Hash)** 选择一个选项。

有关选项的完整说明，请参阅决定使用哪些散列算法。

步骤 7 点击**保存**
将新方案添加到列表中。

配置 IKEv2 IPsec 方案对象

过程

步骤 1 依次选择**对象 (Objects)** > **对象管理 (Object Management)**，然后从目录中选择 **VPN** > **IKEv2 IPsec 方案 (IKEv2 IPsec Proposal)**。

系统将列出以前配置的方案，包括系统定义的默认值。根据您的访问级别，可以编辑 **编辑**（）、查看 **视图**（） 或删除 **删除**（） 方案。

步骤 2 选择**添加**（）**添加 IKEv2 IPsec 方案 (Add IKEv2 IPsec Proposal)** 以创建新的方案。

步骤 3 为此方案输入**名称 (Name)**

策略对象的名称。最多允许 128 个字符。

步骤 4 为此方案输入**说明 (Description)**。

策略对象的说明。最多允许 1024 个字符。

步骤 5 选择要在方案中用于身份验证的 **ESP 散列 (ESP Hash)** 方法、散列或完整性算法。

注释 威胁防御 不支持使用 NULL 加密的 IPSec 隧道。确保不为 IPSec IKEv2 提议选择 NULL 加密。

对于 IKEv2，选择要用于支持 **ESP 散列 (ESP Hash)** 的所有选项。 有关选项的完整说明，请参阅决定使用哪些散列算法。

步骤 6 选择 **ESP 加密**方法。此方案的封装安全协议 (ESP) 加密算法。

对于 IKEv2，点击“选择”(Select) 以打开一个对话框，在对话框中可以选择要支持的所有选项。在决定用于 IPsec 方案的加密和散列算法时，您的选择仅限于 VPN 中的设备所支持的算法。 有关选项的完整说明，请参阅决定使用哪个加密算法。

步骤 7 点击**保存**
将新方案添加到列表中。

威胁防御组策略对象

组策略是存储在组策略对象中的一组属性和值对，用于定义远程接入VPN体验。例如，在组策略对象中，可以配置地址、协议和连接设置等常规属性。

在建立VPN隧道时，将确定应用于用户的组策略。RADIUS授权服务器将会分配组策略，或从当前连接配置文件中获取。

注释 威胁防御 上没有任何组策略继承属性。对于用户使用完整的组策略对象。使用登录时 AAA 服务器识别的组策略对象；如果未指定组策略对象，则使用为VPN连接配置的默认组策略。提供的默认组策略可以设置为默认值，但仅在将该策略分配给连接配置文件且用户未识别其他组策略时使用该策略。

要使用组对象，您必须有与您的智能许可证帐户关联的这些 AnyConnect 客户端 许可证之一，并启用了导出控制功能：

- 仅限 AnyConnect VPN
- AnyConnect Plus
- AnyConnect Apex

相关主题

配置组策略对象，第 107 页

配置组策略对象

请参阅威胁防御组策略对象，第 106 页。

过程

步骤 1 选择**对象** > **对象管理** > **VPN** > **组策略**。

系统将列出之前配置的策略，包括系统默认值。根据您的访问级别，可以编辑、查看或删除组策略。

步骤 2 点击**添加组策略**或选择要编辑的当前策略。

步骤 3 输入该策略的**名称**，还可以选择输入**说明**。

此名称最多可包含 64 个字符，允许使用空格。说明最多可以有 1,024 个字符。

步骤 4 如组策略常规选项，第 108 页中所述，为此组策略指定**常规**参数。

步骤 5 如组策略 AnyConnect 客户端 选项，第 110 页中所述，为此组策略指定 **AnyConnect** 参数。

步骤 6 如组策略高级选项，第 113 页中所述，为此组策略指定**高级**参数。

步骤 7 点击**保存 (Save)**。

新的策略组将添加到列表中。

下一步做什么

将组策略对象添加到远程接入 VPN 连接配置文件。

组策略常规选项

导航路径

对象 > **对象管理** > **VPN** > **组策略**，点击 点击**添加组策略**或选择要编辑的当前策略。，然后选择**常规**选项卡。

VPN 协议字段

指定应用此组策略时可使用的远程接入 VPN 隧道的类型。**SSL** 或 **IPsec IKEv2**。

IP 地址池

指定根据特定于远程接入 VPN 中用户组的地址池应用的 IPv4 地址分配。对于远程接入 VPN，可以为识别的使用 RADIUS/ISE 进行授权的用户组分配特定地址池中的 IP 地址。通过为特定用户组配置特定的组策略作为“RADIUS 授权”属性 (GroupPolicy/Class)，可以为系统中不知道身份的用户或用户组无缝执行策略实施。例如，您必须为使用这些地址的承包商和策略实施选择一个特定的地址池，以允许他们限制性地访问内部网络。

威胁防御 设备向客户端分配 IPv4 地址池的优先顺序：

1. IPv4 地址池的 RADIUS 属性
2. 组策略的 RADIUS 属性
3. 映射到连接配置文件的组策略中的地址池
4. 连接配置文件中的 IPv4 地址池

关于组策略中使用 IP 地址池的一些限制：

- 不支持 IPv6 地址池。
- 一个组策略中最多可配置六个 IPv4 地址池。
- 修改使用中的地址池时会出现部署失败。在对地址池进行任何更改前，必须注销所有用户。
- 重命名地址池或配置的地址池重叠时，部署可能会失败。您必须删除旧地址池，稍后再部署更改的地址池，以此来部署更改。

  部分故障排除命令：

  - `show ip local pool <address-pool-name>`
  - `show vpn-sessiondb detail anyconnect`
  - `vpn-sessiondb loggoff all noconfirm`

横幅字段

指定登录时要向用户显示的横幅文本。长度最多可以为491个字符。没有默认值。IPsec VPN客户端对于条幅支持完全HTML，但AnyConnect客户端仅支持部分HTML。要确保向远程用户正确显示横幅，请对IPsec客户端使用/n标记，对SSL客户端使用
标记。

DNS/WINS字段

域命名系统(DNS)和Windows Internet命名系统(WINS)服务器。用于AnyConnect客户端名称解析。

- **主DNS服务器**和**辅助DNS服务器** - 选择或创建一个网络对象，定义希望此组使用的DNS服务器的IPv4或IPv6地址。
- **主WINS服务器**和**辅助WINS服务器** - 选择或创建一个网络对象，其中包含希望此组使用的WINS服务器的IP地址。
- **DHCP网络范围**-选择或创建一个网络对象，其中包含一个可路由的IPv4地址，与所需池子在同一子网，但不在池子内。DHCP服务器确定此IP地址所属的子网并从该地址池分配IP地址。如果未正确设置，VPN策略部署将失败。

  如果在连接配置文件中为地址池配置了DHCP服务器，DHCP作用域会标识要用于此组的地址池的子网。DHCP服务器的地址还必须来自此作用域标识的同一个子网。作用域允许您选择DHCP服务器中定义的部分地址池，用于此特定组。

  如未定义网络范围，则DHCP服务器将按地址池配置顺序分配IP地址。它将检查各个池，直到发现未分配的地址为止。

  建议尽可能将接口的IP地址用于路由目的。例如，如果池为10.100.10.2-10.100.10.254，接口地址为10.100.10.1/24，则使用10.100.10.1作为DHCP范围。请不要使用网络编号。DHCP仅可用于IPv4寻址。如果您选择的地址不是接口地址，可能需要为范围地址创建静态路由。

  目前不支持LINK-SELECTION（RFC 3527）和SUBNET-SELECTION（RFC 3011）。
- **默认域** - 默认域的名称。指定顶级域，例如example.com。

拆分隧道字段

拆分隧道引导一些网络流量通过VPN隧道（加密），将剩下的网络流量引导至VPN隧道外部（未加密或“以明文形式”）。

- **IPv4拆分隧道/IPv6拆分隧道** - 默认情况下，不启用拆分隧道。对于IPv4和IPv6，此字段均设置为**允许所有流量通过隧道**。如果保留此设置，来自终端的所有流量都将通过VPN连接。

  要配置拆分隧道，请选择**下面指定的隧道网络**或**排除下面指定的网络**策略。然后为该策略配置访问控制列表。
- **拆分隧道网络列表类型** - 选择所使用的访问列表类型。然后选择或创建**标准访问列表**或**扩展访问列表**。有关详细信息，请参阅访问列表，第19页。
- **DNS请求拆分隧道** - 也称为拆分DNS。配置环境中预期的DNS行为。

默认情况下，不启用拆分 DNS，并将其设置为**按拆分隧道策略发送 DNS 请求**。选择**始终通过隧道发送 DNS 请求**强制将所有 DNS 请求通过隧道发送到专用网络。

要配置拆分 DNS，请选择**仅通过隧道发送指定的域**，然后在**域列表**字段中输入域名列表。这些请求通过拆分隧道解析到专用网络。所有其他名称使用公用DNS服务器进行解析。在域列表中最多输入十个条目，条目之间用逗号分隔。整个字符串的长度不能超过 255 个字符。

相关主题

配置组策略对象，第 107 页

组策略 AnyConnect 客户端 选项

这些规范适用于 AnyConnect 客户端 VPN 客户端的操作。

导航

对象 > 对象管理 > VPN > 组策略。点击**添加组策略**或选择要编辑的当前策略。然后选择 **AnyConnect** 选项卡。

配置文件字段

配置文件 - 选择或创建包含 AnyConnect 客户端配置文件 的文件对象。有关对象创建详细信息，请参见 文件对象，第 114 页。

AnyConnect 客户端配置文件 是存储在 XML 文件中的一组配置参数。AnyConnect 客户端 软件使用它来配置出现在客户端用户界面中的连接条目。这些参数（XML标记）还配置相应设置以启用更多 AnyConnect 客户端 功能。

使用基于 GUI 的 AnyConnect 配置文件编辑器（一个独立的配置工具）来创建 AnyConnect 客户端配置文件。有关详细信息，请参阅相应版本的《Cisco Secure 客户端（包括 AnyConnect）管理员指南》的 *AnyConnect* 配置文件编辑器 一章。

管理配置文件字段

管理 VPN 隧道可提供在终端开启时连接到企业网络，即使最终用户未通过 VPN 连接也是如此。

管理 VPN 配置文件-管理配置文件包含用于在终端上启用和建立管理 VPN 隧道的设置。

独立管理VPN隧道配置文件编辑器可用于创建新的配置文件或修改现有的配置文件。您可以从思科软件下载中心下载配置文件编辑器。

有关添加配置文件的详细信息，请参阅 文件对象，第 114 页。

客户端模块字段

Cisco 仅限 AnyConnect VPN 通过各种内置模块提供增强的安全性。这些模块提供网络安全，终端流量的网络可视性和网络外漫游保护等服务。每个客户端模块都包含一个客户端配置文件，其中包含根据您的要求的一组自定义配置。

以下 AnyConnect 客户端 模块是可选的，您可以将这些模块配置为在 VPN 用户下载 AnyConnect 时下载 AnyConnect 客户端：

- **AMP 启用程序** - 为终端部署高级恶意软件防护 (AMP) 。
- **DART**-捕获系统日志和其他诊断信息的快照，可将其发送到 Cisco TAC 进行故障排除。
- **ISE 终端安全评估** - 使用 OPSWAT v3 库执行终端安全评估检查，评估终端的合规性。
- **网络访问管理器** -为有线和无线网络访问提供 802.1X（第 2 层）和设备身份验证。
- **网络可视性** -可提升企业管理员执行容量和服务规划、审计、合规性和安全分析的能力。
- **登录前启动 (Start Before Login)** - 通过在 Windows 登录对话框出现之前启动 AnyConnectAnyConnect 客户端，强制用户在登录到 Windows 之前通过 VPN 连接而连接到企业基础设施。
- **Umbrella 漫游安全** -在没有处于活动状态的 VPN 时提供 DNS 层安全。
- **网络安全**-根据定义的安全策略分析网页的元素，允许可接受的内容，并阻止恶意或不可接受的内容。

点击 **添加** 并为每个客户端模块选择以下选项：

- **客户端模块 (Client Module)** - 从列表中选择 AnyConnect 客户端 模块。
- **要下载的配置文件 (Profile to download)** - 选择或创建包含 AnyConnect 客户端配置文件 的文件对象。有关对象创建详细信息，请参见 文件对象，第 114 页。
- **启用模块下载**-选择启用终端以下载客户端模块以及配置文件。如果未选择，则终端只能下载客户端配置文件。

使用基于 GUI 的 AnyConnect 配置文件编辑器（一个独立的配置工具）来创建每个模块的客户端分析文件 。您可以从 Cisco 软件下载中心下载 AnyConnect 配置文件编辑器 。有关详细信息，请参见相应版本的《思科 AnyConnect 安全移动客户端管理员指南》 中的 *AnyConnect* 配置文件编辑器 一章。

SSL 设置字段

- **SSL 压缩** - 是否启用数据压缩，如果是，则设置要使用的数据压缩方法：Deflate 或 LZS。默认情况下会禁用 SSL 压缩。

  数据压缩加快了传输速率，但也增加了每个用户会话的内存需求和 CPU 使用率。因此，降低了安全设备的总体吞吐量。

- **DTLS 压缩** - 是否使用 LZS 为此组压缩数据报传输层安全 (DTLS) 连接。默认情况下会禁用 DTLS 压缩。
- **MTU 大小 (MTU Size)** - 思科 仅限 AnyConnect VPN 为 SSL VPN 连接建立的最大传输单位 (MTU) 大小。默认值为 1406 字节，有效范围为 576 到 1462 字节。
  - **忽略 DF 位** - 是否忽略需要分片的数据包中的“不分片 (df)”位。允许强制将已设置 DF 位的数据包分片，从而使其能够通过隧道传递。

连接设置字段

- **在 Anyconnect 客户端和 VPN 网关之间启用保持连接消息**。及其**间隔**设置 - 是否在对等体之间交换保持连接消息，以证明它们可用于在隧道中发送和接收数据。默认设置为启用。保持连接消息以设置的时间间隔传输。如果启用，请输入远程客户端在发送 IKE 保持连接数据包之间等待的时间间隔（以秒为单位）。默认间隔为 20 秒，有效范围为 15 到 600 秒。
- **启用失效对等体检测...** 。及其**间隔**设置 - 死对等检测 (DPD) 可确保 VPN 安全网关或 VPN 客户端快速检测到对等体不再响应以及连接失败的情况。默认情况下，会为网关和客户端启用该设置。DPD 消息以设置的时间间隔传输。如果启用，请输入远程客户端在发送 DPD 消息之间等待的时间间隔（以秒为单位）。默认间隔为 30 秒，有效范围为 5 到 3600 秒。
- **启用客户端绕行协议** - 使您可以配置安全网关管理 IPv4 流量（安全网关仅允许 IPv6 流量时）或管理 IPv4 流量（安全网关仅允许 IPv4 流量时）的方式。

  当 AnyConnect 客户端 建立与头端的 VPN 连接时，头端可以为客户端分配 IPv4 和/或 IPv6 地址。如果头端对 AnyConnect 客户端 连接仅分配一个 IPv4 地址或一个 IPv6 地址，则您可以配置 Client Bypass Protocol 以丢弃头端尚未分配 IP 地址（默认、已禁用、未检查）的网络流量，或允许该流量绕过头端并从客户端以未加密或“明文形式”发送（已启用、已检查）。

  例如，假设安全网关只将一个 IPv4 地址分配给 AnyConnect 客户端 连接，且终端为双协议栈。当终端尝试访问 IPv6 地址时，如果禁用客户端旁路协议，则会丢弃 IPv6 流量；但是，如果启用客户端旁路协议，则会从客户端以明文形式发送 IPv6 流量。

- **SSL 重新生成密钥** - 使客户端能够为连接重新生成密钥，重新协商加密密钥和初始化向量，从而提高连接的安全性。默认情况下，此设置处于禁用状态。启用后，可以在指定的时间间隔进行重新协商，对现有隧道重新生成密钥，或通过设置以下字段来创建新隧道：
  - **方法** - 启用 SSL 重新生成密钥时可用。创建**新隧道**（默认）或重新协商**现有隧道**的规范。
  - **间隔** - 启用 SSL 重新生成密钥时可用。设置为 4 分钟的默认值，其范围为 4-10080 分钟（1 周）。
- **客户端防火墙规则** - 使用客户端防火墙规则为 VPN 客户端的平台配置防火墙设置。规则基于诸如源地址、目标地址和协议等条件。扩展访问控制列表构建块对象用于定义流量过滤条件。选择或创建此组策略的扩展 ACL。定义**专用网络规则**以控制流向专用网络的数据，且/或定义**公用网络规则**以控制在已建立的 VPN 隧道之外以“明文”形式传输的数据。

注释 确保 ACL 仅包含 TCP/UDP/ICMP/IP 端口以及“任意”、“任意 IPv4”或“任意 IPv6”类型的源网络。

只有运行 Microsoft Windows 的 VPN 客户端才能使用这些防火墙设置。

自定义属性字段

本部分列出 AnyConnect 客户端 用于配置 Per App VPN，允许或延迟升级和动态分割隧道等功能的 AnyConnect 自定义属性。点击 **添加** 以向组策略添加自定义属性。

1. 选择 **AnyConnect 属性 (AnyConnect Attribute)**：Per App VPN、允许延迟更新或动态分割隧道。
2. 从列表中选择 **自定义属性对象** 。

注释 点击添加（+）以为所选 AnyConnect 属性创建新的自定义属性对象。您还可以在 **对象** > **对象管理** > **VPN** > **自定义属性**中创建自定义属性对象。请参阅添加 AnyConnect 客户端 自定义属性对象，第 117 页。

3. 点击 **添加** 将属性保存到组策略，然后点击 **保存** 将更改保存到组策略。

相关主题

配置组策略对象 ， 第 107 页

组策略高级选项

导航路径

对象 > **对象管理** > **VPN** > **组策略**，点击点击**添加组策略**或选择要编辑的当前策略。，然后选择**高级**选项卡。

流量过滤器字段

- **访问列表过滤器** - 这些过滤器包含相应规则来确定是允许还是阻止通过 VPN 连接隧道传输的数据包。规则基于诸如源地址、目标地址和协议等条件。请注意，VPN 过滤器仅适用于初始连接。它不适用于因应用检查操作而打开的辅助连接，例如 SIP 媒体连接。扩展访问控制列表构建块对象用于定义流量过滤条件。选择或创建此组策略的新扩展 ACL。
- **限制 VPN 到 VLAN** - 也称为“VLAN 映射”，此参数指定该组策略应用到的会话的出口 VLAN 接口。ASA 将所有流量从该组转发到所选 VLAN。

  使用此属性向组策略分配 VLAN 以简化访问控制。向此属性赋值是在会话中使用 ACL 过滤流量的替代方法。除默认值（未限制）外，该下拉列表仅显示此 ASA 中配置的 VLAN。允许的值范围为 1 到 4094。

会话设置字段

- **访问时间** - 选择或创建时间范围对象。此对象指定该组策略可用于远程访问用户的时间范围。有关详细信息，请参阅时间范围 ， 第 83 页。
- **每个用户的同时登录数** - 指定允许某个用户执行的最多同时登录数。默认值为 3。最小值为 0，表示禁止登录并阻止用户访问。允许多个同时连接可能会危害安全性并影响性能。
- **最大连接时间/警报间隔** - 指定最大用户连接时间，以分钟为单位。此时间结束时，系统会终止连接。最小值为 1 分钟)。警报间隔指定在到达最大连接时间以向用户显示消息之前的时间间隔。

- **空闲超时/警报间隔** - 指定此用户的空闲超时时间，以分钟为单位。如果在此时间段内用户连接上没有通信活动，则系统会终止连接。最短时间为 1 分钟。默认值为 30 分钟。警报间隔指定在到达空闲时间以向用户显示消息之前的时间间隔。

相关主题

配置组策略对象 ，第 107 页

文件对象

使用“添加文件对象”和“编辑文件对象”对话框可以创建和编辑文件对象。文件对象表示配置中使用的文件，通常适用于远程接入 VPN 策略。它们可以包含 AnyConnect 客户端配置文件和 AnyConnect 客户端映像文件。

还使用独立的配置文件编辑器为每个 AnyConnect 模块和 AnyConnect 客户端 管理 VPN 创建配置文件，并作为 AnyConnect 的一部分部署到管理员定义的终端用户要求和端点上的身份验证策略，他们将预配置的网络配置文件提供给终端用户使用。

在创建文件对象时，管理中心将在其存储库中创建该文件的副本。在创建数据库的备份时，将备份这些文件；如果恢复该数据库，也将恢复这些文件。在将文件复制到 平台以用于文件对象时，请不要将该文件直接复制到文件存储库。

在部署指定文件对象的配置时，会将相关联的文件下载到相应目录中的设备。

您可以针对每个文件点击以下选项之一：

- **下载 (Download)** - 点击下载 AnyConnect 文件。
- **编辑** -修改文件对象详细信息。
- **删除 (Delete)** - 删除 AnyConnect 客户端 文件对象。 在删除文件对象时，不会从文件存储库中删除相关联的文件，而只会删除该对象。

导航路径

对象 (Objects) > **对象管理 (Object Management)** > **VPN** > **AnyConnect 文件 (AnyConnect File)**。

字段

- **名称**-输入文件的名称以识别文件对象；最多可以添加 128 个字符。
- **文件名称**-点击 **浏览** 以选择文件。选择文件时，系统会添加文件名和完整路径。
- **文件类型**-选择与所选文件对应的文件类型。以下文件类型可用：
  - **AnyConnect 客户端映像 (AnyConnect Client Image)** - 当您添加从 Cisco 软件下载中心下载的 AnyConnect 客户端 映像时，请选择此类型。

    您可以将新的或附加的 AnyConnect 客户端 映像与 VPN 策略相关联。您也可以取消关联不受支持的或生命周期终止的客户端程序包。

- **AnyConnect VPN 配置文件 (AnyConnect VPN Profile)** - 为 AnyConnect VPN 配置文件选择此类型。

  使用基于GUI的 AnyConnect 配置文件编辑器（独立配置工具）来创建配置文件。有关详细信息，请参见相应版本的《思科 AnyConnect 安全移动客户端管理员指南》 中的 *AnyConnect* 配置文件编辑器 一章。

- **AnyConnect 管理 VPN 配置文件 (AnyConnect Management VPN Profile)** - 在为 AnyConnect 管理 VPN 隧道添加配置文件时选择此类型。

  从 Cisco 软件下载中心下载 AnyConnect **VPN 管理隧道独立配置文件编辑器**（如果尚未下载），并使用 AnyConnect 管理 VPN 隧道的所需设置创建配置文件。

- **AMP 启用程序服务配置文件 (AMP Enabler Service Profile)** - 该配置文件用于 AnyConnect AMP 启用程序。当远程访问 VPN 用户连接到 VPN 时，AMP 启动器和此配置文件会从 威胁防御 推送到终端。

- **反馈配置文件**-您可以添加客户体验反馈配置文件并选择此类型，以接收有关客户已启用和使用的功能和模块的信息。

- **ISE 终端安全评估配置文件 (ISE Posture Profile)** - 如果要为 AnyConnect ISE 终端安全评估模块添加配置文件，请选择此选项。

- **NAM 服务配置文件**-使用网络访问管理器配置文件编辑器配置和添加 NAM 配置文件。

- **网络可视性服务配置文件 (Network Visibility Service Profile)** - AnyConnect 网络可视性模块的配置文件。您可以使用 NVM 配置文件编辑器创建配置文件。

- **Umbrella 漫游安全配置文件**-如果使用使用配置文件编辑器创建的 .json 文件部署 Umbrella 漫游安全模块，则必须选择此文件类型。

- **网络安全服务配置文件**-在为网络安全模块添加配置文件时选择此文件类型。

- **HostScan 软件包**-添加 HostScan 软件包文件时选择此文件类型。此文件在配置动态访问策略（DAP）时用于收集有关终端上安装的操作系统，防病毒，反间谍软件和防火墙软件的信息。

- **AnyConnect 外部浏览器软件包 (AnyConnect External Browser Package)** - 此文件类型用于为 SAML 单点登录网络身份验证选择外部浏览器软件包文件。

  您可以在新版本的外部软件包文件可用时添加软件包文件。

  有关详细信息，请参阅配置远程访问 VPN 的 AAA 设置。

- **说明**-添加可选说明。

相关主题

思科 AnyConnect 安全移动客户端 映像

组策略 AnyConnect 客户端 选项 ， 第 110 页

证书映射对象

证书映射对象是一组命名的证书匹配规则。这些对象用于在接收的证书和远程接入VPN连接配置文件之间提供关联。连接配置文件和证书映射对象都是远程接入VPN策略的一部分。如果接收的证书与证书映射中包含的规则相匹配，则连接将被“映射”，或者与指定的连接配置文件相关联。规则按优先级顺序排列，并且按照它们在UI中的显示顺序进行匹配。当证书映射对象中的第一个规则产生一个匹配时，匹配结束。

导航

对象 > **对象管理** > **VPN** > **证书映射**

字段

- **名称** - 标识此对象，以便可以从其他配置（如远程接入 VPN）引用该对象。
- **映射条件** - 指定要评估的证书的内容。如果证书认为这些规则满足要求，则用户将被映射到包含此对象的连接配置文件。
  - **组件** - 选择要用于匹配规则的客户端证书的组件。
  - **字段** - 根据客户端证书的使用者或颁发者选择匹配规则的字段。

    如果**字段**设置为替代使用者或扩展密钥用法，则该组件将被冻结为整个字段
  - **运算符** - 为匹配规则选择运算符，如下所示：
    - 等于 - 证书组件必须与输入的值匹配。如果它们不完全匹配，则连接将被拒绝。
    - 包含 - 证书组件必须包含输入的值。如果组件不包含该值，则连接将被拒绝。
    - 不等于 - 证书组件不能等于输入的值。例如，对于一个选定的“国家/地区”证书组件，以及输入的“美国”值，如果客户的“国家/地区”值等于“美国”，则连接将被拒绝。
    - 不包含 - 证书组件不能包含输入的值。例如，对于一个选定的“国家/地区”证书组件，以及输入的“美国”值，如果客户的“国家/地区”值包含“美国”，则连接将被拒绝。
- **值** - 匹配规则的值。输入的值域所选的组件和运算符关联。

相关主题

配置证书映射

AnyConnect 客户端 自定义属性对象

自定义属性由 AnyConnect 客户端 用于配置 Per App VPN、允许或延迟升级和动态拆分隧道等功能。一个自定义属性有一个类型和一个命名值。先定义属性的类型，然后可以定义此类型的一个或多个命名值。您可以使用 管理中心 来创建 AnyConnect 自定义属性对象，将对象添加到组策略，并将组策略与远程接入 VPN 关联，以启用 VPN 客户端的功能。

威胁防御 使用自定义属性对象支持以下功能：

- **Per App VPN**- Per App VPN 功能可帮助识别 威胁防御 管理员通过 VPN 允许的应用和仅隧道应用。
- **允许或延迟升级** - 延迟升级允许 AnyConnect 客户端 用户延迟 AnyConnect 客户端 升级的下载。如果有客户端更新，您可以配置 AnyConnect 客户端 的属性，以便打开一个询问用户是想要进行更新还是想要延迟升级的对话框。
- **动态拆分隧道 (Dynamic Split Tunneling)** - 通过动态拆分隧道，您可以调配在 VPN 隧道中包含或排除 IP 地址或网络的策略。通过创建自定义属性并将其添加到组策略，可配置动态分割隧道。

有关配置 AnyConnect 客户端 自定义属性的分步说明，请参阅 添加 AnyConnect 客户端 自定义属性对象，第 117 页 和

有关为某个功能配置特定自定义属性的详细信息，请参阅所用 AnyConnect 客户端 版本的《*Cisco Secure* 客户端（包括 *AnyConnect*）管理员指南》。

相关主题

组策略 AnyConnect 客户端 选项，第 110 页

添加 AnyConnect 客户端 自定义属性对象

开始之前

在为Per App VPN添加自定义属性对象之前，请确保已完成以下操作：

- Per App VPN 必须通过 MDM 正确配置，并且每个设备都必须注册到 MDM 服务器
- 使用 Cisco AnyConnect 客户端 企业应用选择器工具为每个应用创建 base64 编码字符串。
  1. 从这里下载 Cisco AnyConnect 客户端 企业应用选择器工具。
  2. 打开应用选择工具，然后从左上角的下拉菜单中选择移动平台。
  3. 通过输入友好名称和应用 ID 添加规则；其余字段为可选字段。
  4. 在菜单栏上，点击 **策略 (Policy)**。编码的 base65 规则以其编码格式显示。
  5. 选择并复制策略字符串，并将其保存以供稍后在创建 AnyConnect 客户端 自定义属性对象时使用。

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)** > **VPN** > **自定义属性 (Custom Attribute)**。

步骤 2 点击**添加 AnyConnect 自定义属性 (Add AnyConnect Custom Attribute)**。

步骤 3 输入 **名称** 和可选属性的 **说明** 。

步骤 4 从 **AnyConnect 属性 (AnyConnect Attribute)** 下拉列表中选择一个属性：

- **Per App VPN**-选择此选项并在 **属性值** 框中指定 base64 编码的字符串。
- **允许延迟更新**-选择以下选项之一并指定所需的信息以允许或延迟 AnyConnect 客户端 客户端更新：
  - **显示提示直到用户执行操作**-显示提示给 VPN 用户，直到用户选择允许或推迟 VPN 客户端更新。
  - **显示提示直到超时**-选择此选项可显示指定持续时间的提示，并在 **超时** 框中指定持续时间。
  - **不显示提示并采取自动操作**-选择此选项以自动允许或推迟 VPN 更新。
  - **默认操作**-选择在用户不响应时或在您希望配置自动操作而无需用户干预时要采取的默认操作。您可以选择更新 AnyConnect 客户端 客户端或推迟更新。
  - **最低版本**-指定客户端系统上允许或推迟更新的最低 AnyConnect 版本。
- **动态拆分隧道**-选择此选项可在 VPN 隧道中包含或排除 IP 地址或网络。
  - **包含域**-指定将包含在远程访问 VPN 隧道中的域名。
  - **排除域**-指定将从远程访问 VPN 隧道中排除的域名。

步骤 5 选中 **允许覆盖** 复选框，允许对此对象组进行覆盖。

步骤 6 点击**保存**。
自定义属性对象添加到列表中。

下一步做什么

将自定义属性与组策略相关联。请参阅向组策略中添加自定义属性，第 118 页。

向组策略中添加自定义属性

您必须将 AnyConnect 自定义属性与组策略相关联，才能将其用于远程访问 VPN 连接。您

过程

步骤 1 选择 **对象** > **对象管理** > **VPN** > **组策略**。

步骤 2 添加新的组策略或编辑现有组策略。

步骤 3 点击 **AnyConnect** > **自定义属性 (Custom Attributes)**。

步骤 4 点击**添加 (Add)**。

步骤 5 选择 **AnyConnect 属性 (AnyConnect Attribute)**：Per App VPN、允许延迟更新或动态分割隧道。

步骤 6 从列表中选择 **自定义属性对象** 。

注释 点击添加（+）以为所选 AnyConnect 属性创建新的自定义属性对象。您还可以在 **对象** > **对象管理** > **VPN** > **自定义属性**中创建自定义属性对象。请参阅添加 AnyConnect 客户端自定义属性对象，第 117 页。

步骤 7 点击 **添加** 将属性保存到组策略，然后点击 **保存** 将更改保存到组策略。

相关主题

组策略 AnyConnect 客户端 选项，第 110 页

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。