身份策略

您可以使用身份策略从连接中收集用户身份信息。然后，可以在控制面板中基于用户身份查看使用情况，并根据用户或用户组配置访问控制。

身份策略概述

您可以使用身份策略检测与连接关联的用户。通过识别用户身份，可以将威胁、终端和网络智能与用户身份信息关联。通过将网络行为、流量和事件直接与单个用户相关联，系统可帮助您确定策略违规、攻击或网络漏洞的来源。

例如，可以确定入侵事件所攻击的主机的所有人是谁，并确定是谁发起了内部攻击或端口扫描。此外，还可以确定高带宽用户，以及正在访问不良网站或应用的用户。

用户检测不仅仅是收集数据进行分析，您也可以基于用户名或用户组名编写访问规则，根据用户身份选择性允许或阻止到资源的访问。

可以使用以下方法获取用户身份：

- 被动身份验证 - 对所有类型的连接，从其他身份验证服务获取用户身份而不提示输入用户名和密码。
- 主动身份验证 - 提示输入用户名和密码，并根据指定身份源进行身份验证，获取源 IP 地址的用户身份（仅限于 HTTP 连接）。

以下主题提供了有关用户身份的详细信息。

通过被动身份验证确定用户身份

被动身份验证在收集用户身份信息时不提示用户输入用户名和密码。系统会从您指定的身份源获取映射。

您可以从以下源被动获取用户到 IP 地址的映射：

- 远程访问 VPN 登录。被动身份支持以下用户类型：
  - 在外部验证服务器中定义的用户账户。
  - 在 防火墙设备管理器中定义的本地用户账户。
- 思科身份服务引擎 (ISE)；思科身份服务引擎被动身份连接器 (ISE-PIC)。

如果给定用户是通过多个源所识别，则 RA VPN 身份占优先地位。

通过主动身份验证确定用户身份

身份验证是确认用户身份的行为。

如果 HTTP 流量来自系统没有其用户身份映射的 IP 地址，通过主动身份验证，您可以决定是否针对为系统配置的目录对发起该流量的用户进行身份验证。如果身份验证成功，该 IP 地址则被视为具有该通过身份验证的用户的身份。

如身份验证不成功，用户对网络的访问并不会受阻。为这些用户提供哪些访问权限最终由访问规则决定。

处理未知用户

当您为身份策略配置目录服务器后，系统会从目录服务器下载用户和组成员信息。此信息每24小时在午夜刷新一次，或在每次您编辑和保存目录配置时刷新（即使您未进行任何更改）。

如果某用户在活动身份验证身份规则提示时成功进行了身份验证，但该用户的名称不在下载的用户身份信息中，则该用户会被标记为“未知”。您不会在与身份相关的控制面板中看到该用户的ID，该用户也不会匹配组规则。

但是，系统将应用面向未知用户的任何访问控制规则。例如，如果您阻止未知用户的连接，那么即使这些用户成功进行了身份验证（即目录服务器可识别用户并且密码有效），他们也会被阻止。

因此，当您对目录服务器进行更改（例如添加或删除用户，或更改组成员身份）时，直到系统从目录下载更新之后这些更改才会反映在策略实施中。

如果您不希望每天都等到午夜进行更新，可以通过编辑目录领域信息（依次选择**对象** > **身份源**，然后编辑领域）强制进行更新。点击**保存**，然后部署更改。系统随即会下载更新。

注释 您可以依次转至**策略** > **访问控制**，点击**添加规则 (+)** 按钮，并在**用户**选项卡上查看用户列表，从而检查系统上是否有新的或已删除的用户信息。如果找不到新用户，或者还是可以找到已删除的用户，则系统的信息未更新。

如何实施身份策略

要启用用户身份采集，以便得知与 IP 地址与关联的用户，您需要配置多个项目。正确配置后，您将能够看到监控控制面板和事件中的用户名。您还将能够在访问控制和 SSL 解密规则中使用用户身份作为流量匹配条件。

以下过程概述您必须配置哪些内容才能正常使用身份策略。

过程

步骤 1 配置 AD 身份领域。

不论您是主动（提示进行用户验证）使用用户身份，还是被动使用，都需要配置包含用户身份信息的 Active Directory (AD) 服务器。请参阅配置 AD 身份领域。

如果配置被动身份，则可以创建 AD 领域序列，使系统可以提取多个 AD 领域中的身份。如果您的网络中有多个 AD 域，此方法将非常有用。

步骤 2 如果您想要使用被动身份验证身份规则，请配置被动身份源。

根据您要在设备中实现的服务和网络中可用的服务，您可以配置任何以下内容。

- 远程访问 VPN - 如果您要支持到设备的远程访问 VPN 连接，用户登录可以提供基于 AD 服务器或本地用户（ 防火墙设备管理器中定义的用户）的身份。有关配置远程访问 VPN 的信息，请参阅配置远程访问 VPN。
- 思科身份服务引擎 (ISE) 或思科身份服务引擎被动身份连接器 (ISE PIC) - 如果您使用这些产品，您可以将设备配置为 pxGrid 订阅方，并从 ISE 获取用户身份。请参阅配置身份服务引擎。

步骤 3 依次选择**策略** > **身份**，并启用身份策略。请参阅配置身份策略，第 5 页。

步骤 4 配置身份策略设置，第 6 页。

基于您在系统中配置的源，自动选择被动身份源。如果您想要配置主动身份验证，您必须为强制网络门户和 SSL 重签解密（如果尚未启用 SSL 解密策略）配置证书。

步骤 5 配置身份策略默认操作，第 7 页。

如果您打算仅使用被动身份验证，您可以将默认操作设置为被动身份验证，无需创建特定规则。

步骤 6 配置身份规则，第 8 页。

创建将从相关网络收集被动或主动用户身份的规则。

主动身份验证最佳实践

如果身份规则要求对用户进行主动身份验证，则该用户将重定向到连接该用户所通过的界面上的强制网络门户，然后系统会提示用户进行身份验证。

由于此重定向指向接口 IP 地址，因此身份策略证书不完全匹配，并且用户会收到不受信任的证书错误。用户必须接受证书才能继续操作并对设备进行身份验证。由于这种行为类似于中间人攻击，用户不愿意接受不受信任的证书。

为避免此问题，您可以将主动身份验证配置为使用设备上一个接口的完全限定域名 (FQDN)。使用正确配置的证书时，用户不会收到不受信任的证书错误，并且身份验证将更加无缝，且看起来更加安全。

开始之前

主动身份验证仅适用于 HTTP 流量，只要设备没有用户工作站或其他客户端设备的当前用户映射，就会对最终用户造成中断。您可以通过实施被动身份验证来避免中断。

过程

步骤 1 在 DNS 服务器中，为要用于收集主动身份验证的接口的接口 IP 地址定义完全限定域名 (FQDN)。

也称为强制网络门户，这必须是路由接口。

步骤 2 使用证书颁发机构 (CA)，获取此 FQDN 的证书。

您可以为特定的 FQDN 创建证书，例如 ftd1.captive-port.example.com。或者，您可以：

- 获取可应用于许多不同设备上的强制网络门户接口的通配符证书，例如 *.captive-port.example.com。通配符也可以更广泛，适用于各种终端，例如 *.eng.example.com，甚至是 *.example.com。
- 在证书中包含多个使用者备选名称 (SAN)。

步骤 3 选择**对象** > **证书**，并上传证书。

步骤 4 选择**对象** > **网络**，并为 DNS 名称创建 FQDN 网络对象。

步骤 5 在**策略 (Policies)** > **身份 (Identity)** 页面上，使用证书和 FQDN 对象更新身份策略设置。

步骤 6 在身份策略中创建使用主动身份验证的规则。

步骤 7 限制主动身份验证时可使用的密码套件。

默认情况下，浏览器连接至身份 Web 服务器（强制网络门户）进行主动身份验证时，可使用任何可用密码。为增强安全性，您可限制允许的密码套件。有关详细信息，请参阅配置 TLS/SSL 密码设置。

配置身份策略

您可以使用身份策略从连接中收集用户身份信息。然后，可以在控制面板中基于用户身份查看使用情况，并根据用户或用户组配置访问控制。

下文概述了如何配置通过身份策略获取用户身份所需的元素。

过程

步骤 1 依次选择**策略** > **身份**。

如果尚未定义身份策略，请点击**启用身份策略**并按配置身份策略设置，第 6 页中的说明配置设置。

步骤 2 管理身份策略。

在配置身份设置后，此页面将按顺序列出所有规则。规则依据流量按照从上到下的顺序进行匹配，由第一个匹配项确定要应用的操作。从此页面中可以执行以下操作：

- 要启用或禁用身份策略，请点击**身份策略**开关。
- 要更改身份策略设置，请点击**身份策略配置**按钮（  ）。
- 要更改**默认操作**，请点击操作并选择所需的操作。请参阅配置身份策略默认操作，第 7 页。
- 要移动规则，请编辑规则并从**顺序**下拉列表中选择新位置。
- 要配置规则，请执行以下操作：
  - 要创建新规则，请点击 + 按钮。
  - 要编辑现有规则，请点击该规则的编辑图标 ()（在“操作”列中）。也可以选择在表中点击某规则属性来编辑该属性。
  - 要删除不再需要的规则，请点击该规则的删除图标 ()（在“操作”列中）。

有关创建和编辑身份策略的更多信息，请参阅配置身份规则，第 8 页。

配置身份策略设置

要正常使用身份策略，必须配置提供用户身份信息的源。必须配置的设置因配置的规则类型而异，而规则类型可以是被动和/或主动的。

这些设置显示在设置对话框的不同部分。您可以看到两个部分，也可以看到一个部分，具体取决于如何访问对话框。如果您尝试创建身份验证类型的规则，而没有事先配置所需的设置，系统将自动显示对话框。

以下过程介绍完整对话框。

开始之前

确保目录服务器、Firewall Threat Defense设备和客户端之间的时间设置一致。这些设备间的时间偏差可能会导致用户身份验证操作失败。“一致”说明您可以使用不同的时区，但时间相对于这些时区应是相同的；例如，10 AM PST = 1 PM EST。

过程

步骤 1 依次选择**策略** > **身份**。

步骤 2 点击**身份策略配置**按钮（  ）。

步骤 3 配置**被动身份验证**选项。

对话框显示已经配置的被动身份验证源。

如有必要，您可以通过此对话框配置 ISE。如果您尚未配置 ISE 对象，可以点击**集成 ISE** 链接，立即创建对象。如果对象存在，将显示对象及其状态（已启用或已禁用）。

必须配置至少一个已启用被动身份源，才能创建被动身份验证规则。

步骤 4 配置**主动身份验证**选项。

如果身份规则要求对用户进行主动身份验证，则该用户将被重定向到强制网络门户端口，然后系统会提示他们进行身份验证。在配置这些设置之前，请阅读主动身份验证最佳实践，第 4 页。

- **服务器证书** - 选择在主动身份验证期间提供给用户的内部证书。如果尚未创建所需的证书，请点击下拉列表底部的**创建新的内部证书**。

  如果用户不上传其浏览器已经信任的证书，则必须接受该证书。

- **重定向到主机名**（仅限 Snort 3.0）- 选择定义接口的完全限定主机名的网络对象，该接口应用作主动身份验证请求的强制网络门户。如果该对象尚不存在，请点击**创建新网络**。

  FQDN 必须解析为设备上接口之一的 IP 地址。通过使用 FQDN，您可以为客户端将识别的主动身份验证分配证书，从而避免用户在被重定向到 IP 地址时收到不受信任证书警告。证书可以在证书的使用者备选名称 (SAN) 中指定 FQDN、通配符 FQDN 或多个 FQDN。

  如果身份规则要求对用户进行主动身份验证，但您未指定重定向 FQDN，则用户将被重定向到他们连接的接口上的强制网络门户端口。

- **端口** - 强制网络门户端口。默认端口是 885 (TCP)。如果配置了其他端口，则该端口必须在 1025-65535 的范围内。

  注释
  如果您不提供**重定向到主机名** FQDN，HTTP Basic、HTTP 响应页面和 NTLM 身份验证方法会使用接口的 IP 地址将用户重定向到强制网络门户。但对于 HTTP 协商，用户将使用完全限定 DNS 名称 *firewall-hostname.AD-domain-name* 进行重定向。如果您想在不提供**重定向到主机名** FQDN 的情况下使用 HTTP 协商，还必须更新 DNS 服务器以将此名称映射到您需要进行主动身份验证的所有内部接口的 IP 地址。否则，将无法进行重定向，用户也无法进行身份验证。建议您始终提供**重定向到主机名** FQDN 以确保行为一致，而无论采用哪种身份验证方法。

步骤 5 （仅主动身份验证。）在**解密重签名证书**中，选择相应内部 CA 证书，以用于利用重签名证书实施解密的规则。

您可以使用预定义的 NGFW-Default-InternalCA 证书，也可以使用您创建或上传的证书。如果尚无证书，请点击**创建内部 CA** 进行创建。

如果尚未在客户端浏览器中安装证书，请点击下载按钮 () 获取副本。有关如何安装证书的信息，请参阅各浏览器文档。另请参阅为解密重签名规则下载 CA 证书。

注释
只有在未配置 SSL 解密策略的情况下，系统才会提示您进行 SSL 解密设置。要在启用身份策略之后更改这些设置，请编辑 SSL 解密策略设置。

步骤 6 点击**保存**。

配置身份策略默认操作

身份策略对不匹配任何身份规则的连接实施默认操作。

实际上，不设置规则是策略的有效配置。如果想在所有流量源上使用被动身份验证，只需将被动身份验证配置为默认操作。

过程

步骤 1 依次选择**策略** > **身份**。

步骤 2 点击**默认操作**，并从以下选项中选择一个：

- **被动身份验证（任何身份源）**-通过对不匹配任何身份规则的连接使用所有配置的被动身份源，确定用户身份。如果不配置任何被动身份源，使用被动身份验证作为默认选择等同于使用“无身份验证”。
- **无身份验证（不需要身份验证）**- 不对不匹配任何身份规则的连接确定用户身份。

配置身份规则

身份规则确定是否应收集用户身份信息以匹配流量。如果您不想获取用户身份信息以匹配流量，则可以配置“无身份验证”。

请记住，无论规则配置如何，都仅对HTTP流量进行主动身份验证。因此，无需创建规则将非HTTP流量从主动身份验证中排除。如果您希望获取所有 HTTP 流量的用户身份信息，只需将主动身份验证规则应用于所有源和目的。

注释 而且请记住，身份验证失败对网络访问没有影响。身份策略仅收集用户身份信息。如果要阻止无法进行身份验证的用户访问网络，则必须使用访问规则。

开始之前

规则自上而下进行评估。对于与给定规则的指定网络条件匹配的连接，系统将根据规则中指定的身份领域对用户进行评估。如果用户不属于该领域，他们将被标记为未知，并且不会评估身份策略中的其他规则。因此，如果有多个领域需要评估，请务必使用领域序列而不是单个领域。

过程

步骤 1 依次选择**策略** > **身份**。

步骤 2 执行以下任一操作：

- 要创建新规则，请点击 + 按钮。
- 要编辑现有规则，请点击规则的编辑图标 ( )。

要删除不再需要的规则，请点击该规则的删除图标 ( )。

步骤 3 在**顺序**中，选择要将该规则插入在已排序有序规则列表插入该规则的位置。

先匹配的规则先应用，所以您必须确保流量匹配条件条件较具体的规则显示在次之用来匹配流量的较通用条件条件的策略上方。

默认将规则添加到列表的末尾。如果以后要更改规则的位置，请编辑此选项。

步骤 4 在**名称**中输入规则的名称。

步骤 5 选择**操作**，如有必要，还要选择 **AD 身份源**。

您必须选择包括用于被动和主动身份验证规则的用户账户的 AD 身份领域。如果所需的领域尚不存在，请点击**创建新身份领域**并立即创建。对于被动身份验证，您可以选择 AD 领域序列，而不是单个 AD 领域对象。

- **被动身份验证** - 使用被动身份验证确定用户身份。系统将会显示所有已配置的身份源。此规则会自动使用所有已配置的源。

- **主动身份验证** — 使用主动身份验证确定用户身份。主动身份验证仅适用于 HTTP 或已解密的 HTTPS 流量。如果任何其他类型的流量与要求或允许主动身份验证的身份策略匹配，则不会尝试进行主动身份验证。
- **无身份验证** - 不获取用户身份。基于身份的访问规则不会应用于此流量。这些用户将标记为**无需身份验证**。

步骤 6 （仅主动身份验证。）选择您的目录服务器支持的身份验证方法（**类型**）。

- **HTTP 基本身份验证** - 使用未加密的 HTTP 基本身份验证 (BA) 连接对用户进行身份验证。用户通过其浏览器的默认身份验证弹出窗口登录网络。这是默认值。
- **NTLM** - 使用 NT LAN Manager (NTLM) 连接对用户进行身份验证。仅当选择了一个 AD 领域时，此选项才可用。用户使用其浏览器的默认身份验证弹出窗口登录网络，不过您可以将 IE 和 Firefox 浏览器配置为使用其 Windows 登录域信息以透明方式进行身份验证（请参阅启用透明用户身份验证，第 11 页）。
- **HTTP 协商** - 允许设备协商用于用户代理（用户发起流量流所用的应用）和 Active Directory 服务器之间的方法。协商有助于使用广受支持的最强方法，顺序为先 NTLM，然后是 Basic 方法。用户通过其浏览器的默认身份验证弹出窗口登录网络。
- **HTTP 响应页面** - 提示用户使用系统提供的网页进行身份验证。这是一种 HTTP Basic 身份验证方法。

注释
如果您不提供**重定向到主机名** FQDN，HTTP Basic、HTTP 响应页面和 NTLM 身份验证方法会使用接口的 IP 地址将用户重定向到强制网络门户。但对于 HTTP 协商，用户将使用完全限定 DNS 名称 *firewall-hostname.AD-domain-name* 进行重定向。如果您想在不提供**重定向到主机名** FQDN 的情况下使用 HTTP 协商，还必须更新 DNS 服务器以将此名称映射到您需要进行主动身份验证的所有内部接口的 IP 地址。否则，将无法进行重定向，用户也无法进行身份验证。建议您始终提供**重定向到主机名** FQDN 以确保行为一致，而无论采用哪种身份验证方法。

步骤 7 （仅主动身份验证。）依次选择**以访客身份回退** > **开/关**，确定是否将未通过主动身份验证的用户标记为访客用户。

用户有三次机会成功进行身份验证。如果仍不成功，选择此选项可以确定是否标记用户。您可以根据这些值编写访问规则。

- **以访客身份回退** > **开** - 系统将用户标记为**访客**。
- **以访客身份回退** > **关** - 系统将用户标记为**未通过身份验证**。

步骤 8 在**源/目标**选项卡上定义流量匹配条件。

请记住，仅在使用 HTTP 流量时才会尝试进行主动身份验证。因此，无需为非 HTTP 流量配置无身份验证规则，也无需为任何非 HTTP 流量创建主动身份验证规则。但是，被动身份验证适用于任何类型的流量。

身份规则的源/目标条件定义了流量通过的安全区（接口）、IP 地址或该 IP 地址所在的国家/地区或大洲（地理位置）或是流量中所用的协议和端口。默认设置为任何区域、地址、地理位置、协议和端口。

要修改条件，请点击该条件内的 + 按钮，选择所需的对象或元素，然后在弹出对话框中点击**确定**。如果条件需要对象，而所需的对象不存在，您可以点击**创建新对象**。点击对象或元素对应的 **x**，可将其从策略中移除。

可以配置以下流量匹配条件。

源区域、目标区域

安全区对象，定义通过其传递流量的接口。可以定义一个或两个条件，也可以不定义任何条件：未指定的任何条件都将应用到任何接口上的流量。

- 要匹配从区域中的接口离开设备的流量，请将该区域添加至**目标区域**。
- 要匹配从区域中的接口进入设备的流量，请将该区域添加至**源区域**。
- 如果同时向一条规则添加源区域和目标区域条件，匹配流量必须源自其中一个指定源区域并通过其中一个目标区域流出。

如果应基于流量进入或离开设备的位置来应用规则，请使用此条件。例如，如果要确保从源自内部网络的所有流量收集用户身份，请选择内部区域作为**源区域**，同时将目标区域留空。

注释
不能在同一规则中搭配使用被动和路由安全区。此外，被动安全区只能被指定为源区域，不能作为目标区域。

源网络、目标网络

定义流量的网络地址或位置的网络对象或地理位置。

- 要匹配来自某个 IP 地址或地理位置的流量，请配置**源网络**。
- 要匹配流向 IP 地址或地理位置的流量，请配置**目标网络**。
- 如果同时向一条规则添加源网络条件和目标网络条件，匹配流量必须源自其中一个指定 IP 地址并流向其中一个目标 IP 地址。

添加此条件时，可从以下选项卡中进行选择：

- **网络** - 为您要控制的流量选择定义源或目标 IP 地址的网络对象或组。
- **地理位置** - 选择要基于流量的源或目的国家/地区或大洲控制流量的地理位置。选择大洲将会选择该大洲内的所有国家/地区。除了直接在规则中选择地理位置外，也可以选择您创建的地理位置对象来定义位置。使用地理位置，可以便捷地限制对特定国家/地区的访问，而不需要知道此位置所用的全部潜在 IP 地址。

  注释
  为了确保使用最新地理位置数据过滤流量，思科强烈建议您定期更新地理位置数据库(GeoDB)。

源端口、目标端口/协议

定义流量中所用协议的端口对象。对于 TCP/UDP，这可能包括端口。

- 要匹配来自协议或端口的流量，请配置**源端口**。源端口只能为 TCP/UDP。

- 要匹配流向协议或端口的流量，请配置**目标端口/协议**。
- 要同时匹配来自特定 TCP/UDP 端口的流量和流向特定 TCP/UDP 端口的流量，请配置源端口和目标端口。如果同时将源和目标端口添加至条件，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，您可以匹配从端口 TCP/80 流至端口 TCP/8080 的流量。

步骤 9 点击**确定**。

启用透明用户身份验证

如果将身份策略配置为允许进行主动身份验证，可以使用以下身份验证方法获取用户身份：

HTTP Basic

使用 HTTP Basic 身份验证时，系统会始终提示用户使用其目录用户名和密码进行身份验证。密码以明文形式传输。因此，Basic 身份验证不是一种安全的身份验证。

Basic 身份验证方法是默认的身份验证机制。

HTTP Response Page

这是一种 HTTP Basic 身份验证类型，使用时，用户会看到登录浏览器页面。

NTLM、HTTP Negotiate（适用于 Active Directory 的集成 Windows 身份验证）

使用集成的 Windows 身份验证，用户可以登录到域来使用其工作站。访问服务器（包括主动身份验证期间的 Firewall Threat Defense强制网络门户）时，浏览器将尝试使用此域登录。密码不进行传输。如果身份验证成功，则以透明方式对用户进行身份验证；用户不了解存在或解决的任何身份验证挑战。

如果浏览器使用域登录凭证无法满足某个身份验证请求，则系统会提示用户提供用户名和密码，这与 Basic 身份验证的用户体验是相同的。因此，如果配置集成的 Windows 身份验证，用户无需在访问同一域内的网络或服务器时提供凭证。

请注意，HTTP Negotiate 会选择 Active Directory 服务器和用户代理支持的最强方法。如果协商选择 HTTP Basic 作为身份验证方法，则不会获取透明身份验证。强度顺序依次为 NTLM、Basic。协商必须选择 NTLM，才能进行透明身份验证。

您必须将客户端浏览器配置为支持集成的 Windows 身份验证才能进行透明身份验证。以下部分介绍了支持集成的 Windows 身份验证的一些常用浏览器的集成 Windows 身份验证常规要求和基本配置。有关更详细的信息，用户应参阅其浏览器（或其他用户代理）的帮助，因为各方法可能会因软件版本而不同。

提示 并非所有浏览器都支持集成的 Windows 身份验证，例如 Chrome 和 Safari（基于编写本文档时可用版本）。系统会提示用户提供用户名和密码。请参阅浏览器的文档确定您使用的版本是否支持。

透明身份验证的要求

用户必须将其浏览器或用户代理配置为实施透明身份验证。用户可以单独执行此操作，您也可以代其进行配置，并使用软件分发工具将此配置推送至客户端工作站。如果您选择让用户自己执行此操作，请确保提供适用于您的网络的特定配置参数。

无论是浏览器还是用户代理，您都必须实施以下常规配置：

- 将用户连接网络所采用的 Firewall Threat Defense重定向主机名或接口添加到“受信任站点”列表。如果不使用重定向主机名，可以使用 IP 地址，也可以使用完全限定域名（如果可用，例如，inside.example.com）。也可以使用通配符或部分地址创建一个通用的受信任站点。例如，使用 *.example.com 或只是 example.com 通常可以覆盖所有内部站点，从而信任您网络中的所有服务器（使用您自己的域名）。如果添加接口的物理地址，可能需要将多个地址添加到受信任站点，从而涵盖用户对网络的所有接入点。
- 集成的 Windows 身份验证不通过代理服务器工作。因此，您要么不使用代理，要么必须将 Firewall Threat Defense重定向主机名或接口添加到被排除通过该代理的地址中。如果您决定必须使用代理，系统会提示用户进行身份验证，即使使用 NTLM 亦是如此。

提示 配置透明身份验证不是必须的，却可为最终用户提供方便。如果不配置透明身份验证，系统会向用户显示所有身份验证方法的登录质询。

配置 Internet Explorer 以进行透明身份验证

要配置 Internet Explorer 以进行 NTLM 透明身份验证，请执行以下操作：

过程

步骤 1 依次选择**工具** > **互联网选项**。

步骤 2 依次选择**安全**选项卡和**本地 Intranet** 区域，然后执行以下操作：

a) 点击**站点**按钮，打开受信任站点列表。

b) 确保至少选择以下其中一个选项：

- **自动检测 Intranet 网络**。如果选择此选项，系统将禁用其他所有选项。
- **包括所有不使用代理服务器的站点**。

c) 点击**高级**打开“本地 Intranet 站点”对话框，然后将您要信任的站点添加到**添加站点**框中，然后点击**添加**。

如果您有多个URL，请重复该过程。使用通配符指定部分URL，例如**`http://*.example.com`**或只是**`*.example.com`**。

关闭对话框返回到“互联网选项”对话框。

d) 在**本地 Intranet** 仍处于选中状态的情况下，点击**自定义级别**打开“安全设置”对话框。找到**用户身份验证** > **登录**设置，然后选择**只在 Intranet 区域自动登录**。点击**确定**。

步骤 3 在“互联网选项”对话框中，点击**连接**选项卡，然后点击 **LAN 设置**。

如果选中**为 LAN 使用代理服务器**，您需要确保 Firewall Threat Defense接口绕过该代理。适当执行以下任一操作：

- 选择**对于本地地址不使用代理服务器**。
- 点击**高级**并将地址输入**对于以下列字符开头的地址不使用代理服务器**框。您可以使用通配符，例如 **`*.example.com`**。

配置 Firefox 以进行透明身份验证

要配置 Firefox 进行 NTLM 透明身份验证，请执行以下操作：

过程

步骤 1 打开 **about:config**。借助过滤器栏找到您需要修改的首选项。

步骤 2 要支持 NTLM，请修改以下首选项（在 network.automatic 上过滤）：

- **network.automatic-ntlm-auth.trusted-uris** - 双击首选项，输入 URL，然后点击**确定**。您可以通过将 URL 以逗号分隔来输入多个 URL；包括该协议是可选的。例如：

  ```
  http://host.example.com, http://hostname, myhost.example.com
  ```

  您也可以 使用部分URL。Firefox匹配该字符串的末尾，而不是一个随机子字符串。因此，您可以仅指定域名来包括您的整个内部网络。例如：

  ```
  example.com
  ```

- **network.automatic-ntlm-auth.allow-proxies** - 确保值为 **true**，这是默认值。如果值当前为 false，请双击以更改该值。

步骤 3 检查 HTTP 代理设置。可以通过选择**工具 (Tools)** > **选项 (Options)**，然后点击“选项”对话框中的**网络 (Network)** 选项卡来查找这些设置。点击“连接”(Connection) 组中的**设置 (Settings)** 按钮。

- 如果选择**无代理**，则无需进行任何配置。
- 如果选择**使用系统代理设置**，则需要修改 about:config 中的 **network.proxy.no_proxies_on** 属性，以添加您在 **network.automatic-ntlm-auth.trusted-uris** 中包括的可信赖 URI。
- 如果选择**手动代理配置**，则更新**无代理对象**列表以包括这些可信赖的 URI。

- 如果选择其他某个选项，请确保用于这些配置的属性不包括这些可信赖的 URI。

监控身份策略

如果要求身份验证的身份策略正常工作，您应该会在**监控** > **用户**控制面板和其他有用户信息的控制面板上看到用户信息。

此外，**监控** > **事件**中显示的事件应该有用户信息。

如果没有看到任何用户信息，请验证目录服务器是否在正常运行。使用目录服务器配置对话框中的**测试**按钮验证连接。

如果目录服务器在正常运行并且可用，请验证要求主动身份验证的身份规则的流量匹配条件是否是以与您的用户匹配的方式编写的。例如，请确保源区域有用户流量进入设备的接口。主动身份验证身份规则仅与 HTTP 流量匹配，因此用户必须通过设备发送该类型的流量。

对于被动身份验证，使用ISE对象中的**测试**按钮（如果您在使用该源）。如果您使用远程访问VPN，请验证服务正常运行，并且用户可以进行VPN连接。有关识别和解决问题的更多详细信息，请参阅这些功能的故障排除主题。

身份策略示例

使用案例章节涵盖实施身份策略的示例。请参阅如何深入了解您的网络流量。

当地语言翻译版本说明

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

当地语言翻译版本说明

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

当地语言翻译版本说明

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

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。