用户身份策略

以下主题讨论如何创建和管理身份规则及身份策略：

关于身份策略

身份策略包含身份规则。身份规则会将流量集与领域和身份验证方法相关联：被动身份验证、主动身份验证或无身份验证。

除了下面段落提到的例外之外，您必须配置计划使用的领域和身份验证方法，然后才能在身份规则中进行调用：

- 在**系统 (System)** > **集成 (Integration)** > **领域 (Realms)**中，配置身份策略外的领域。有关详细信息，请参阅创建 LDAP 领域或 Active Directory 领域和领域目录。
- 在 **系统** > **集成** > **身份源**中，配置 ISE/ISE-PIC 被动身份验证身份源。
- 在系统外，配置被动身份验证身份源：TS 代理。有关详细信息，请参阅《思科终端服务 *(TS)* 代理指南》。
- 在身份策略中，配置主动身份验证身份源：强制网络门户。有关详细信息，请参阅如果为用户控制配置强制网络门户。
- 您可以在远程访问 VPN 策略中配置远程访问 VPN，即主动身份验证身份源。有关详细信息，请参阅远程访问 VPN 身份验证。

向一个身份策略添加多个身份规则后，对规则排序。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。流量匹配的第一个规则是处理该流量的规则。

您可以选择配置身份策略，以按网络对象过滤流量，从而在设备达到或接近其内存限制时限制每个设备监控的网络。设备必须运行 威胁防御 6.7 或更高版本，才能对其应用网络过滤。

配置一个或多个身份策略后，必须将一个身份策略与访问控制策略相关联。当网络上的流量与身份规则中的条件匹配时，系统会将流量与指定领域相关联并使用指定身份源对流量中的用户进行身份验证。

如果不配置身份策略，则系统不会执行用户身份验证。

创建身份策略的例外

如果满足以下所有条件，则不需要身份策略：

- 您使用 ISE/ISE-PIC 身份源。
- 您未在访问控制策略中使用用户或组。
- 您在访问控制策略中使用安全组标记 (SGT)。有关详细信息，请参阅 ISE SGT 与自定义 SGT 规则条件。

相关主题

如何设置身份策略

身份策略的许可证要求

威胁防御 许可证

Any

经典许可证

控制

身份策略的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

创建身份策略

此任务讨论如何创建身份策略。

开始之前

在访问控制策略内使用领域中的用户和组需要身份策略。创建并启用一个或多个领域，如创建LDAP领域或 Active Directory 领域和领域目录中所述。

（可选。）如果特定受管设备监控大量用户组，则由于内存限制，系统可能会根据组丢弃用户映射。因此，带有领域或用户条件的规则可能不会按预期执行。如果设备运行的是版本 6.7 或更高版本，您可以将身份规则配置为仅按一个网络或网络组对象监控流量。要创建网络对象，请参阅 创建网络对象。

如果满足以下所有条件，则不需要身份策略：

- 您使用 ISE/ISE-PIC 身份源。
- 您未在访问控制策略中使用用户或组。
- 您在访问控制策略中使用安全组标记 (SGT)。有关详细信息，请参阅 ISE SGT 与自定义 SGT 规则条件。

过程

步骤 1 登录管理中心。

步骤 2 点击**策略** > **访问控制** > **身份** ，然后点击**新建策略 (New Policy)**。

步骤 3 输入**名称 (Name)** 和**说明 (Description)**（后者为可选项）。

步骤 4 点击**保存 (Save)**。

步骤 5 要将规则添加到策略，请点击**添加规则 (Add Rule)**，如创建身份规则，第 11 页中所述。

步骤 6 要创建规则类别，请点击**添加类别 (Add Category)**。

步骤 7 要配置强制网络门户主动身份验证，请点击**主动身份验证 (Active Authentication)** 并查看 配置强制网络门户第 2 部分：创建身份策略和主动身份验证规则。

步骤 8 （可选。）要按网络对象过滤流量，请点击**身份源 (Identity Source)** 选项卡。从列表中，点击要用于过滤此身份策略流量的网络对象。点击 **添加**（＋） 以创建新的网络对象。

步骤 9 点击**保存 (Save)** 保存身份策略。

下一步做什么

- 将规则添加到指定要匹配的用户和其他选项的身份策略；请参阅创建身份规则，第 11 页。
- 将身份策略与访问控制策略相关联，以允许或阻止选定用户访问指定的资源；请参阅将其他策略与访问控制相关联。
- （Microsoft Azure AD 领域不需要。）将配置更改部署到受管设备；请参阅部署配置更改。

如果您遇到问题，请参阅用户控制故障排除，第 21 页。

相关主题

配置强制网络门户第 2 部分：创建身份策略和主动身份验证规则
创建身份映射过滤器，第 4 页
强制网络门户字段
用户控制故障排除，第 21 页

创建身份映射过滤器

身份映射过滤器可用于限制应用身份规则的网络。例如，如果您的 管理中心 管理的FTD 内存有限，则可以限制其监控的网络。

（可选）从接收 ISE 的用户到 IP 和安全组标记 (SGT) 到 IP 的映射中排除子网。您通常应对内存较低的受管设备执行此操作，以防止 Snort 身份运行状况监控器内存错误。

开始之前

执行以下任务：

1. 创建身份策略所需的领域。请参阅创建 LDAP 领域或 Active Directory 领域和领域目录。
2. 创建身份策略。请参阅创建身份策略，第 3 页。
3. （可选。）创建网络对象或网络组对象，如创建网络对象中所述。您创建的网络对象或组应定义您希望托管设备在身份策略中监控的网络。

   此步骤为可选，因为您可以在配置身份映射过滤器时创建一个。

过程

步骤 1 登录管理中心。

步骤 2 点击**策略 (Policies)** > **身份 (Identity)**。

步骤 3 请点击 **编辑**（  ）。

步骤 4 点击**身份源 (Identity Source)** 选项卡。

步骤 5 从 **身份映射过滤器** 列表中，点击要用作过滤器的网络对象的名称，或点击 **加号**（+） 以创建新的过滤器。

要创建新的网络对象，请参阅创建网络对象。

步骤 6 单击**保存**。

步骤 7 （Microsoft Azure AD 领域不需要。）将配置更改部署到受管设备；请参阅部署配置更改。

下一步做什么

（Microsoft Azure AD 领域不需要。）将身份策略与访问控制策略相关联，如将其他策略与访问控制相关联中所述。

要检查或更改 ISE 身份映射过滤器（也称为 子网过滤器），请使用以下命令：

```
show identity-subnet-filter
configure identity-subnet-filter { add | remove } subnet
```

身份规则条件

通过规则条件，您可以微调身份策略，以您要控制的用户和网络为目标。有关详细信息，请参阅以下各节之一：

相关主题

安全区域规则条件
网络规则条件
VLAN 标记规则条件
端口规则条件
领域和设置规则条件，第 9 页

安全区域规则条件

安全区域可对网络进行分段，以通过跨多个设备将接口分组来帮助管理和分类流量。

区域规则条件可根据其源和目标安全区域控制流量。如果将源区域和目标区域均添加到区域条件中，则匹配流量必须源自其中一个源区域的接口，并通过其中一个目标区域的接口流出。

正如区域中的所有接口都必须为同一类型（均为内联、被动、交换或路由），区域条件中使用的所有区域也必须为同一类型。由于被动部署的设备不会传输流量，因此不能使用具有被动接口的区域作为目标区域。

尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。

提示 按区域限制规则是提高系统性能的一种最佳方式。如果规则不适用于通过设备任意接口的流量，则该规则不影响该设备的性能。

安全区域条件和多租户

在多域部署中，在祖先域中创建的区域可以包含位于不同域中的设备上的接口。在后代域中配置区域条件时，您的配置仅适用于可以看到的接口。

网络规则条件

网络规则条件使用内部报头按流量的源和目标 IP 地址来控制流量。使用外部报头的隧道规则具有隧道终端条件而不是网络条件。

您可以使用预定义对象构建网络条件，或手动指定单个 IP 地址或地址块。

注释 您 不能 在身份规则中使用 FDQN 网络对象。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。

重定向到主机名网络规则条件

（仅限 Snort 3.0）—你可以使用一个网络对象，其中包含强制网络门户可用于主动认证请求的接口的完全限定主机名（FQDN）。

FQDN 必须解析为受管设备上接口之一的 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受管设备的 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替代名称 (SAN) 中指定一个 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受管设备接口上的强制网络门户端口。

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.directory-server-domain-name*进行重定向。要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。

VLAN 标记规则条件

注释 访问规则中的 VLAN 标记仅适用于内联集。带 VLAN 标记的访问规则与防火墙接口上的流量不匹配。

VLAN 规则条件可控制 VLAN 标记的流量，包括 Q-in-Q（堆栈 VLAN）流量。系统使用最内层的 VLAN 标记过滤 VLAN 流量，但不包括预过滤器策略，因为它在其规则中使用最外层的 VLAN 标记。

请注意以下 Q-in-Q 支持：

- Firepower 4100/9300 上的威胁防御 -不支持 Q-in-Q （仅支持一个 VLAN 标记）。
- 所有其他型号上的威胁防御：
  - 内联集和被动接口-支持 Q-in-Q，最多2个 VLAN 标记。
  - 防火墙接口-不支持 Q-in-Q （仅支持一个 VLAN 标记）。

可以使用预定义对象构建 VLAN 条件，或手动输入从 1 到 4094 之间的任意 VLAN 标记。使用连字符可指定 VLAN 标记范围。

在集群中，如果遇到 VLAN 匹配问题，请编辑访问控制策略高级选项“传输/网络预处理器设置”(Transport/Network Preprocessor Settings)，然后选择**跟踪连接时忽略 VLAN 信头 (Ignore the VLAN header when tracking connections)** 选项。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 VLAN 标记限制此配置可产生意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

端口规则条件

通过端口条件，您可以按流量的源端口和目标端口控制该流量。

尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。

基于端口的规则的最佳实践

指定端口是目标应用的传统方式。但是，可以将应用配置为使用唯一端口绕过访问控制块。因此，尽可能使用应用过滤条件而不是端口条件来确定流量目标。

应用过滤也建议用于动态打开单独通道的应用（如 FTD），以实现控制和数据流。使用基于端口的访问控制规则可能会阻止此类应用正确执行，并可能导致阻止所需的连接。

使用源端口和目标端口限制

如果同时添加源端口和目标端口限制，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，如果添加经由 TCP 的 DNS 作为源端口，则可以添加 Yahoo Messenger Voice Chat (TCP) 而不是 Yahoo Messenger Voice Chat (UDP) 作为目标端口。

如果仅添加源端口或仅添加目标端口，则可以添加使用不同传输协议的端口。例如，在单一访问控制规则中，可以将经由 TCP 的 DNS 和经由 UDP 的 DNS 二者添加为源端口条件。

端口、协议和 ICMP 代码规则条件

端口条件根据源和目标端口匹配流量。根据规则类型，“端口”可以表示以下任何一项：

- TCP 和 UDP - 可以根据端口控制 TCP 和 UDP 流量。系统使用括号内的协议号，以及可选的关联端口或端口范围来表示此配置。例如：TCP(6)/22。
- ICMP - 可以根据 ICMP 和 ICMPv6 (IPv6-ICMP) 流量的互联网层协议及可选类型和代码控制该流量。例如：ICMP(1):3:3。
- 协议-您可以借助于未使用端口的其他协议控制流量。

尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。

基于端口的规则的最佳实践

指定端口是目标应用的传统方式。但是，可以将应用配置为使用唯一端口绕过访问控制块。因此，尽可能使用应用过滤条件而不是端口条件来确定流量目标。请注意，应用过滤在预过滤器规则中不可用。

应用过滤也建议用于动态打开单独通道的应用（如 FTP），以实现控制和数据流。使用基于端口的访问控制规则可能会阻止此类应用正确执行，并可能导致阻止所需的连接。

使用源端口和目标端口限制

如果同时添加源端口和目标端口限制，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，如果添加经由 TCP 的 DNS 作为源端口，则可以添加 Yahoo Messenger Voice Chat (TCP) 而不是 Yahoo Messenger Voice Chat (UDP) 作为目标端口。

如果仅添加源端口或仅添加目标端口，则可以添加使用不同传输协议的端口。例如，在单一访问控制规则中，可以将经由 TCP 的 DNS 和经由 UDP 的 DNS 二者添加为目标端口条件。

将非 TCP 流量与端口条件相匹配

您可以匹配非基于端口的协议。默认情况下，如果不指定端口条件，则匹配 IP 流量。虽然可以将端口条件配置为与非 TCP 流量相匹配，但有一些限制：

- 访问控制规则 - 对于典型设备，可以通过使用 GRE (47) 协议作为目标端口条件将 GRE 封装的流量与访问控制规则相匹配。对于 GRE 限制的规则，只能添加基于网络的条件：区域、IP 地址、端口和 VLAN 标签。此外，系统使用外部报头将访问控制策略中的**所有**流量与 GRE 限制

的规则相匹配。对于 威胁防御设备，请使用预过滤器策略中的隧道规则来控制 GRE 封装的流量。

- 解密 规则 - SSL 规则仅支持 TCP 端口条件。
- IMCP 回应 - 类型设置为 0 的目标 ICMP 端口或类型设置为 129 的目标 ICMPv6 端口仅与主动回应回复相匹配。为应答 ICMP 回应请求而发送的 ICMP 回应回复被忽略。为使某个规则匹配任何 ICMP 回应，请使用 ICMP 类型 8 或 ICMPv6 类型 128。

领域和设置规则条件

通过**领域和设置 (Realm & Settings)** 选项卡页面，您可以选择要应用身份规则的领域或领域序列。如果您使用的是强制网络门户，则还可以选择其他选项。

身份验证领域 (Authentication Realm)

从**领域 (Realm)** 列表中，点击领域或领域序列。

包含要对其执行指定**操作 (Action)** 的用户的领域或领域序列。必须在选择作为身份规则中的领域或领域序列之前，对领域进行完全配置。

注释 如果启用了 VPN 远程接入，而且您的部署正在使用 RADIUS 服务器组进行 VPN 身份验证，请确保您指定的领域与此 RADIUS 服务器组相关联。

仅主动身份验证：其他选项

如果选择**主动身份验证 (Active Authentication)** 作为身份验证类型，或者选中**如果无法建立被动或 VPN 身份则使用主动身份验证 (Use active authentication if passive or VPN identity cannot be established)** 框，您将看到以下选项。

如果无法建立被动或 VPN 身份，请使用主动身份验证

（仅限被动身份验证规则。）如果被动身份验证或VPN身份验证无法标识用户，选择此选项将通过强制网络门户主动身份验证来验证用户。您必须在身份策略中配置主动身份验证规则，才能选择此选项。（即，用户必须使用强制网络门户进行身份验证。）

如果禁用此选项，没有 VPN 身份或被动身份验证不能标识的用户将被标识为“未知”。

另请参阅本主题后面对 **身份验证领域** 列表的讨论，

如果身份验证无法识别用户，则识别为特殊身份/访客 (Identify as Special Identities/Guest if authentication cannot identify user)

选择此选项允许执行强制网络门户主动身份验证时而失败指定次数的用户以访客身份访问您的网络。这些用户显示在以其用户名（如果 AD 或 LDAP 服务器中有他们的用户名）或**访客**（如果他们的用户名未知）标识的 管理中心 中。其领域是在身份规则中指定的领域。（默认情况下，失败的登录次数为 3。）

仅当您将**主动身份验证**（即，强制网络门户身份验证）配置为规则**操作**时，才会显示此字段。

身份验证协议

要用于执行强制网络门户主动身份验证的方法。用户在使用响应页面登录时看到的内容的示例如 使用主动身份验证规则创建示例身份策略，第 16 页中所示。

选项因领域、LDAP 或 AD 的类型而有所不同。

- 如果要使用未加密的 HTTP 基本身份验证 (BA) 连接对用户进行身份验证，请选择 **HTTP 基本身份验证**。用户通过其浏览器的默认身份验证弹出窗口登录网络。

  大多数 Web 浏览器会从 HTTP 基本身份验证登录中缓存凭证，并在旧会话超时后使用这些凭证无缝开始新会话。

- 选择 **NTLM** 以使用 NT LAN Manager (NTLM) 连接对用户进行身份验证。仅在选择 AD 领域时，此选项才可用。如果在用户的浏览器中配置了透明身份验证，则该用户自动登录。如果未配置透明身份验证，则用户使用其浏览器的默认身份验证弹出窗口进行登录。

- 选择 **Kerberos** 以使用 Kerberos 连接对用户进行身份验证。仅在为已启用安全 LDAP (LDAPS) 的服务器选择 AD 领域时，此选项才可用。如果在用户的浏览器中配置了透明身份验证，则该用户自动登录。如果未配置透明身份验证，则用户使用其浏览器的默认身份验证弹出窗口进行登录。

注释 您选择的**领域**必须配置 **AD 加入用户名**和 **AD 加入密码**，才能执行 Kerberos 强制网络门户主动身份验证。

注释 如果您要创建身份规则来执行 Kerberos 强制网络门户，并且已配置了 DNS 解析，则必须配置 DNS 服务器来解析强制网络门户设备的完全限定域名 (FQDN)。FQDN 必须与您配置 DNS 时提供的主机名匹配。

对于 威胁防御 设备，FQDN 必须解析为用于强制网络门户的路由接口的 IP 地址。

- 选择 **HTTP 协商**以允许强制网络门户服务器选择“HTTP 基本”、“Kerberos”或“NTLM”进行身份验证连接。仅在选择 AD 领域时，此类型才可用。

注释 您选择的**领域**必须配置 **AD 加入用户名**和 **AD 加入密码**，这样一来，**HTTP 协商**才能选择 Kerberos 强制网络门户主动身份验证。

注释 如果您要创建身份规则来执行 **HTTP 协商**强制网络门户，并且已配置了 DNS 解析，则必须配置 DNS 服务器来解析强制网络门户设备的完全限定域名 (FQDN)。用于强制网络门户的设备的 FQDN 必须与您配置 DNS 时提供的主机名匹配。

- 选择 **HTTP 响应页面**，使用户能够选择要登录的领域。

  您可以选择自定义响应页面；例如，符合公司风格标准。

主动身份验证领域

（仅限被动身份验证规则。）如果您点击了 **如果无法建立被动或 VPN 身份，则使用主动身份验证**，则必须点击领域或领域序列的名称。领域或领域序列的可用性取决于您对身份验证协议的选择，如下所示：

- **HTTP 基本** 或 **HTTP 响应页面** 身份验证协议：您可以选择领域或领域序列。
- **NTLM**、 **Kerberos**或 **HTTP 协商** 身份验证协议：只能选择领域。您 不能 选择领域序列。

创建身份规则

有关身份规则的配置选项的详细信息，请参阅身份规则字段，第 12 页。

开始之前

您必须创建并启用领域 或领域序列。

- 创建 Microsoft Active Directory 领域和领域目录，如创建 LDAP 领域或 Active Directory 领域和领域目录所述。
- （仅限 Microsoft AD 领域。）下载用户和组并启用领域，如 同步用户和组中所述。
- 创建 Microsoft Azure Active Directory 领域，如创建 Azure AD 领域中所述。
- （可选。）按创建领域序列中所述创建领域序列。

注意 在禁用了 TLS/SSL 解密（即，当访问控制策略不包括 a 解密策略 时）时添加第一个主动身份验证规则或删除最后一个主动身份验证规则 在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为。

请注意，主动身份验证规则具有 **主动身份验证** 规则操作或 **被动身份验证** 规则操作，并且 **如果无法建立被动或 VPN 识别，则使用主动身份验证** 已选中。

过程

步骤 1 登录管理中心。

步骤 2 请点击 **策略** > **访问控制** > **身份** 。

步骤 3 点击要将身份规则添加到的身份策略旁边的 **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**添加规则 (Add Rule)**。

步骤 5 输入 **Name**。

步骤 6 如果指定规则适用，请选中**已启用 (Enabled)** 复选框。

步骤 7 要将规则添加到现有类别，请指明要**插入**规则的位置。要添加新类别，请点击**添加类别 (Add Category)**。

步骤 8 从列表中选择一个规则**操作**。

步骤 9 如果您正在配置强制网络门户，请参阅如果为用户控制配置强制网络门户。

步骤 10 （可选）要向身份规则中添加条件，请参阅身份规则条件，第 5 页。

步骤 11 点击**添加 (Add)**。

步骤 12 在策略编辑器中，设置规则位置。点击并拖动，或使用右键点击菜单剪切并粘贴。规则从 1 开始进行编号。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。流量匹配的第一条规则是处理该流量的规则。适当的规则顺序可减少处理网络流量所需的资源，并防止规则抢占。

步骤 13 点击**保存 (Save)**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

身份规则字段

使用以下字段配置身份规则。

启用

启用此选项可启用身份策略中的身份规则。取消选择此选项可禁用身份规则。

操作

指定要对指定领域中的用户执行的身份验证的类型：**被动身份验证**（默认）、**主动身份验证**或**无身份验证**。必须完全配置身份验证方法或身份源，然后再选择其作为身份规则中的操作。

此外，如果启用了 VPN（至少在一台受管设备上配置），远程访问 VPN 会话将通过 VPN 进行主动身份验证。其他会话使用规则操作。这意味着，如果启用了 VPN，会首先确定所有会话的 VPN 身份，而不考虑所选的操作。如果在指定领域发现 VPN 身份，将使用此身份源。不再执行任何其他强制网络门户主动身份验证，即便已选择。

如果未发现 VPN 身份源，该过程将根据指定操作继续。不能将身份策略仅限制为仅使用 VPN 身份验证，因为如果未找到 VPN 身份源，将根据所选的操作应用规则。

注意 在禁用了 TLS/SSL 解密（即，当访问控制策略不包括 SSL 策略时）时添加第一个主动身份验证规则或删除最后一个主动身份验证规则 在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为。

请注意，主动身份验证规则具有 **主动身份验证** 规则操作或 **被动身份验证** 规则操作，并且 **如果无法建立被动或 VPN 识别，则使用主动身份验证** 已选中。

有关您的系统版本支持哪些被动和主动身份验证方法的信息，请参阅关于用户身份源。

身份策略和规则示例

以下各节提供使用被动身份验证规则或主动身份验证规则配置身份策略的示例。此外，由于您可以使用领域或领域序列通过主动身份验证对用户进行身份验证，因此提供了单独的示例。

主动身份验证 意味着用户使用强制网络门户进行身份验证；用户在被允许访问允许的资源之前输入网络凭证。（RA-VPN 是另一种类型的主动身份验证，但它不能与强制网络门户身份验证一起使用。有关详细信息，请参阅远程访问 VPN 身份源。）

被动身份验证 涵盖所有其他类型。被动身份验证包括使用 Microsoft Active Directory 领域、Microsoft Azure Active Directory 领域、思科身份服务引擎等。

您可以使用 Microsoft Azure Active Directory 领域以不同的方式对用户进行身份验证，此处未讨论。有关详细信息，请参阅创建 Microsoft Azure AD 领域。

假定条件

示例使用以下假设：

- Microsoft Active Directory (AD) 领域，名为 forest.example.com，其中两个子域配置为信任关系：
  - 美国西部
  - 美国东部地区
- 包含两个领域的名为 US 的领域序列
- 使用领域序列对用户进行身份验证的被动身份验证规则
- 两个主动身份验证规则：
  - 通过领域对用户进行身份验证并使用 NTLM 身份验证协议的一个规则
  - 使用领域序列对用户进行身份验证并使用 HTTP 响应页面身份验证协议的一个规则
- 每个示例身份规则与不同的身份策略相关联

被动身份验证身份规则

配置被动身份验证身份规则时，可以选择使用 LDAP（Microsoft Active Directory 领域），或 Microsoft AD 领域序列对用户进行身份验证。您可以使用领域对任何身份验证类型进行身份验证；领域序列限制您可以使用的身份验证类型。有关示例，请参阅使用被动身份验证规则创建身份策略，第 14 页。

主动身份验证身份规则

配置主动身份验证身份规则时，可以选择使用 LDAP（Microsoft Active Directory 领域），或 Microsoft AD 领域序列对用户进行身份验证。您可以使用领域对任何身份验证类型进行身份验证；领域序列限制您可以使用的身份验证类型。

您还可以使用 Microsoft Active Directory 领域序列对用户进行身份验证，但以下身份验证类型除外：

- NTLM
- Kerberos
- HTTP 协商

有关示例，请参阅使用主动身份验证规则创建示例身份策略，第 16 页。

使用被动身份验证规则创建身份策略

此任务讨论如何使用被动身份验证规则创建身份策略，该规则使用美国领域序列对用户进行身份验证。如果在序列中的第一个领域中未找到用户，系统将按领域序列中列出的顺序搜索序列中的其他领域。如果仍未在领域或领域序列找到用户，则会将该用户标识为“未知”。

如果在序列中的任何领域均未找到用户，则可以选择使用强制网络门户对用户进行身份验证（即主动身份验证）。有关详细信息，请参阅 强制网络门户指南和限制。

过程

步骤 1 登录管理中心。

步骤 2 请点击 **策略** > **访问控制** > **身份** 。

步骤 3 点击**新建策略**。

步骤 4 输入策略的 **名称** 和可选 **说明**。

步骤 5 单击**保存**。

步骤 6 点击**添加规则**。

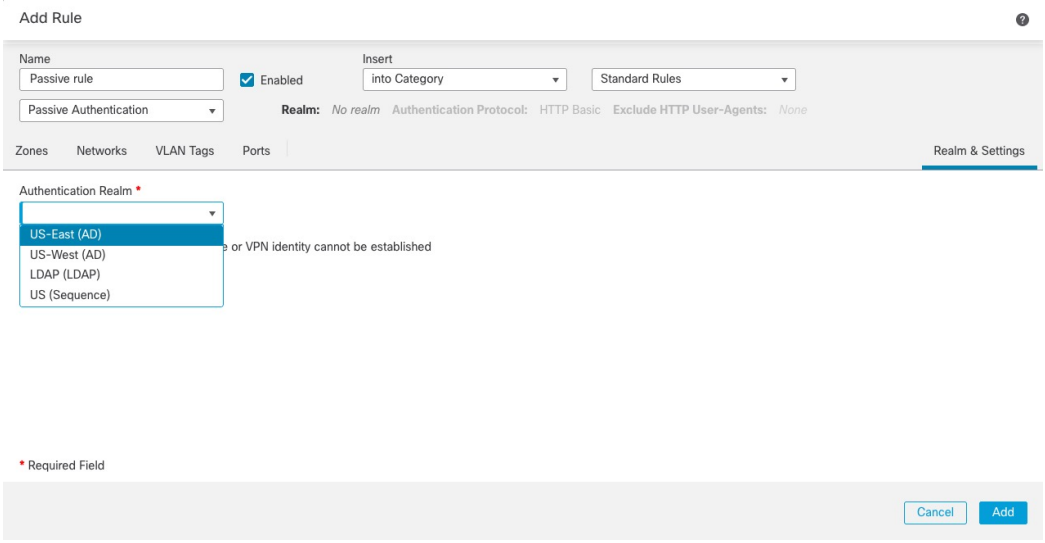
步骤 7 为规则输入**名称 (Name)**。

步骤 8 从“操作”列表中，点击 **被动身份验证**。

步骤 9 点击 **领域和设置** 选项卡页面。

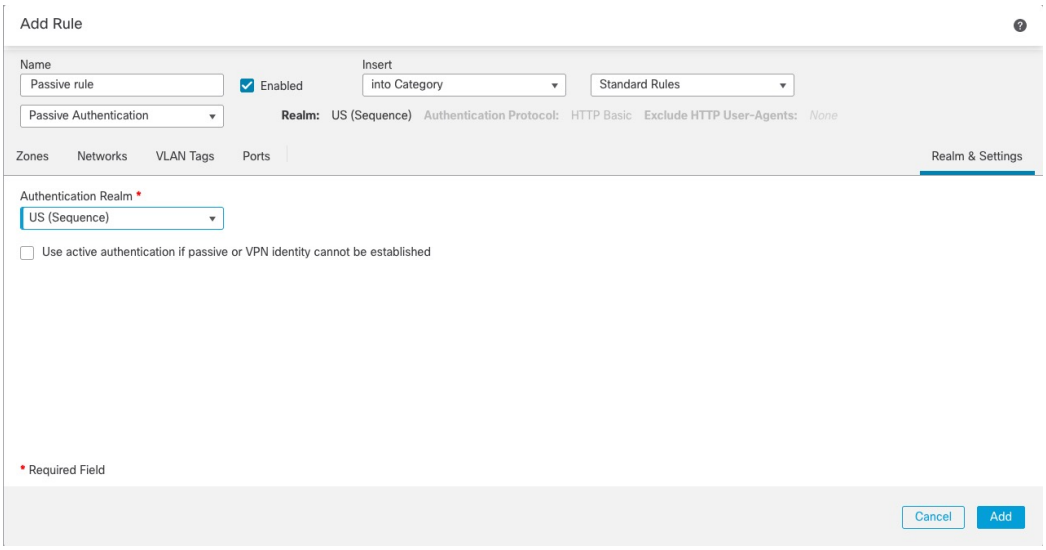
步骤 10 从列表中，点击领域或领域序列的名称。

下图显示了一个示例。



- 如果您选择一个领域（例如示例中的**美国东部**），则系统会搜索该领域以查找与规则匹配的用户。如果未找到用户，则会将该用户标识为“未知”(Unknown)。
- 如果选择领域序列（在示例中的**美国（序列）**），则系统将按照序列中指定的顺序在该序列中的每个领域搜索用户。如果未找到用户，则会将该用户标识为“未知”(Unknown)。
- 您还可以选择 LDAP 领域。
- 对于用户身份验证的额外方法，请选中 **如果无法建立被动或 VPN 身份，请使用主动身份验证**。有关详细信息，请参阅 强制网络门户指南和限制。

下图显示配置为在美国领域序列中搜索用户的被动身份策略示例。



步骤 11 （可选。）要按网络对象过滤流量，请点击**身份源 (Identity Source)** 选项卡。从列表中，点击要用于过滤此身份策略流量的网络对象。点击 **添加**（+） 以创建新的网络对象。

步骤 12 设置身份规则条件，如中所述 身份规则条件 ， 第 5 页。

步骤 13 将身份规则与访问控制规则相关联，如 将其他策略与访问控制相关联中所述。

步骤 14 将配置更改部署到受管设备；请参阅部署配置更改。

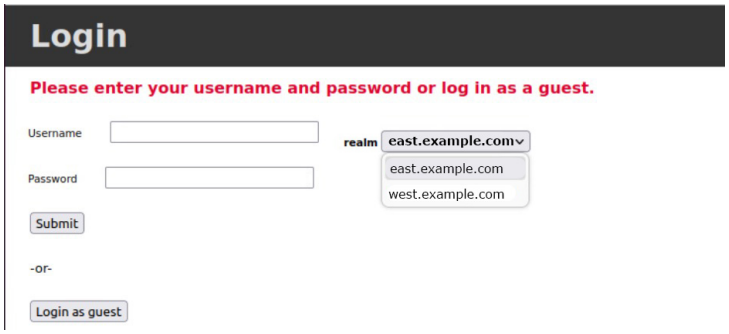
使用主动身份验证规则创建示例身份策略

关联的任务显示使用 **主动身份验证** 规则配置身份策略的示例，其中使用领域或领域序列执行身份验证。

差异如下：

- 领域 是您可以使用任何受支持的身份验证类型（当前， **HTTP Basic**、 **NTLM**、 **Kerberos**、 **HTTP Negotiate**或 **HTTP Response Page**）。
- 领域序列 将您限制为仅 **HTTP Basic** 或 **HTTP 响应页面** 身份验证类型。

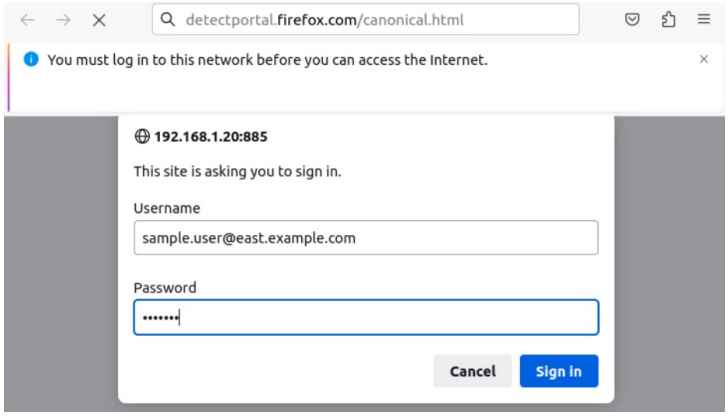
  使用领域序列和 HTTP 响应页面身份验证类型进行身份验证的用户默认会看到以下内容：



  用户可以通过以下任何一种方式进行身份验证：

  - 如果显示领域序列中的领域列表（如图所示），则用户必须在提供的字段中输入用户名和密码，然后从列表中单击其领域名称。
  - 如果领域未显示在列表中，则用户可以按照 `username@domain` 格式输入其凭证。

  使用领域和 HTTP 基本身份验证页面进行身份验证的用户会看到以下内容：



用户必须以 `username@domain` 格式来输入其用户名。

过程

步骤 1 登录管理中心。

步骤 2 请点击 **策略** > **访问控制** > **身份** 。

步骤 3 点击**新建策略**。

步骤 4 输入策略的 **名称** 和可选 **说明**。

步骤 5 单击**保存**。

步骤 6 点击**主动身份验证**选项卡。

步骤 7 输入以下信息：

- **服务器证书**：从列表中，点击要用于与 威胁防御 设备安全连接的内部证书对象，或点击 **添加**（+） 以添加一个。
- **要重定向到的主机名**：（可选。）从列表中，点击要将强制网络门户请求重定向到的网络对象。

  如果省略此值，请求将重定向到受管设备的 IP 地址。点击 **添加**（+） 以创建新的网络对象。有关详细信息，请参阅重定向到主机名网络规则条件，第 6 页。

  受管设备必须启用 Snort 3 才能使用此选项。
- **端口**：输入要供强制网络门户使用的端口。此端口对于强制网络门户必须是唯一的，并且必须与您设置的访问控制规则相匹配，如 配置强制网络门户第 3 部分：创建 TCP 端口访问控制规则 中所述。（默认值为 885。）
- **最大登录尝试次数**：输入登录失败前的最大登录尝试次数。（默认值为 3。）
- **跨防火墙共享主动身份验证**：取消选中以便让管理中心强制要求用户在每次使用与上次不同的托管设备访问您的网络时重新进行身份验证。

  有关此选项的详细信息，请参阅强制网络门户字段。
- **主动身份验证响应页面**：为强制网络门户用户选择系统提供的或自定义的登录页面。有关您的选项的更多信息，请参阅 强制网络门户字段。

步骤 8 点击 **保存** 保存身份策略的更改。

步骤 9 点击**规则**选项卡。

步骤 10 点击**添加规则**。

步骤 11 为规则输入**名称 (Name)**。

步骤 12 从列表中，点击 **主动身份验证**。

步骤 13 点击 **领域和设置** 选项卡页面，然后继续以下部分之一。

下一步做什么

继续执行以下部分之一：

- 使用领域的主动身份验证， 第 18 页
- 使用领域序列的主动身份验证， 第 19 页

使用领域的主动身份验证

此任务讨论如何使用领域和任何可用的身份验证协议（当前为 **HTTP Basic**、**NTLM**、**Kerberos**、**HTTP Negotiate** 或 **HTTP Response Page**）对强制网络门户用户进行身份验证。

开始之前

完成 使用主动身份验证规则创建示例身份策略， 第 16 页中讨论的任务。

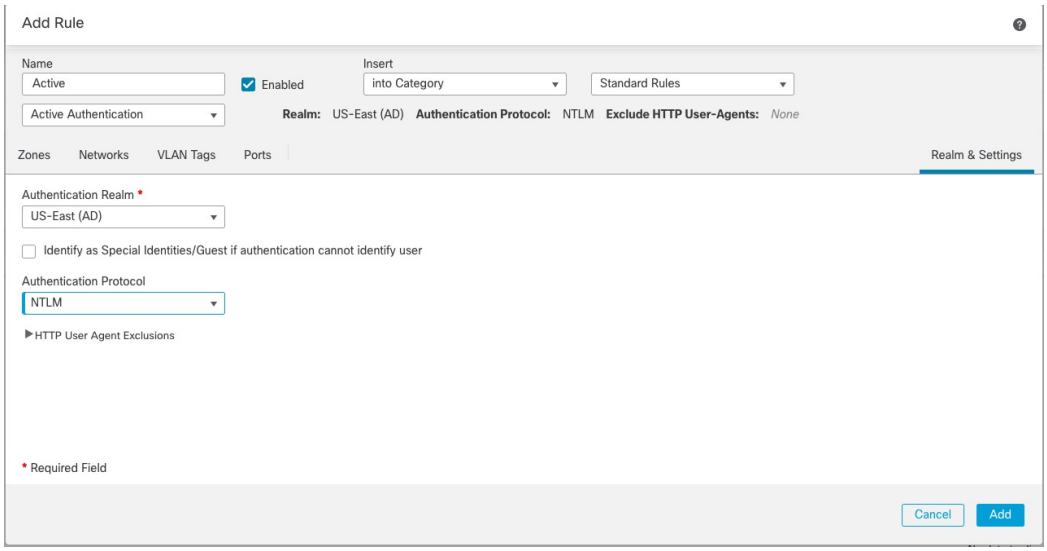
过程

步骤 1 继续 使用主动身份验证规则创建示例身份策略， 第 16 页。

步骤 2 在**领域和设置 (Realms & Settings)** 选项卡页面中，点击**美国东部 (US-East)**。

步骤 3 在**身份验证协议 (Authentication Protocol)** 列表中，点击 **NTLM**。

下图显示了一个示例。



如果您选择一个领域（如示例中），则系统会搜索该领域以查找与规则匹配的用户。如果未找到用户，则会将该用户标识为“未知”(Unknown)。

步骤 4 点击**添加**。

步骤 5 （可选。）要按网络对象过滤流量，请点击**身份源 (Identity Source)** 选项卡。从列表中，点击要用于过滤此身份策略流量的网络对象。点击 **添加**（＋） 以创建新的网络对象。

步骤 6 设置身份规则条件，如中所述 身份规则条件，第 5 页。

步骤 7 将身份规则与访问控制规则相关联，如 将其他策略与访问控制相关联中所述。

步骤 8 将配置更改部署到受管设备；请参阅部署配置更改。

使用领域序列的主动身份验证

此任务讨论如何使用领域序列对强制网络门户用户进行身份验证，这会将您限制为 **HTTP 基本** 或 **HTTP 响应页面** 身份验证协议。

开始之前

完成 使用主动身份验证规则创建示例身份策略，第 16 页中讨论的任务。

过程

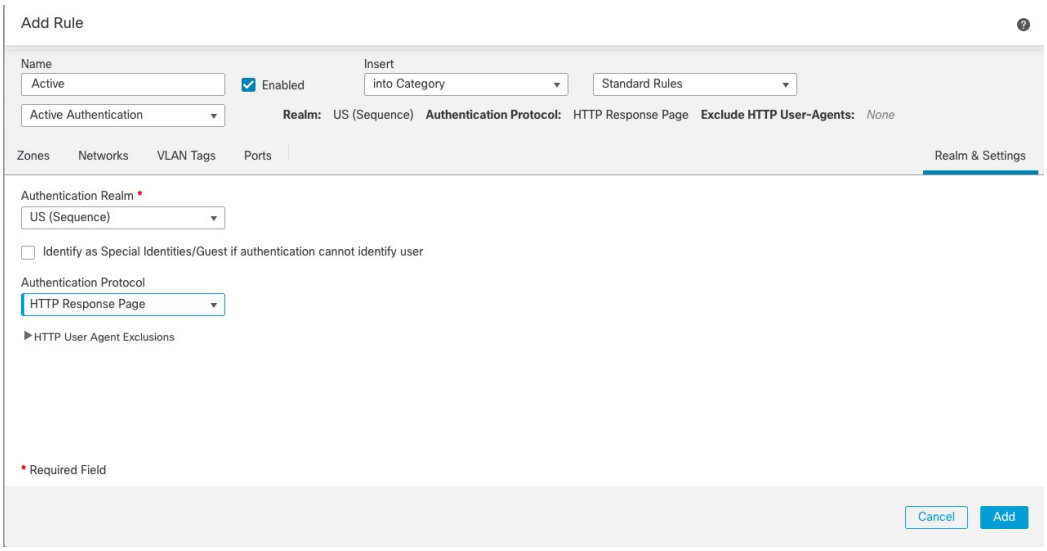
步骤 1 继续 使用主动身份验证规则创建示例身份策略，第 16 页。

步骤 2 在 **领域和设置** 选项卡页面上，点击列表中的领域的名称。

步骤 3 从列表中，点击**美国东部 (US-East)**。

步骤 4 从**协议 (Protocol)** 列表中，点击 **HTTP 响应页面 (HTTP Response Page)**。

下图显示了一个示例。



如果选择了领域序列（如本例所示），系统会按照领域序列中指定的顺序来搜索序列中的领域。序列中的第一个领域可以称为默认领域；如果用户没有更改，则会使用该领域。如果未找到用户，则会将该用户标识为“未知”(Unknown)。

（仅当您从较早版本升级到版本 7.4.1 时。）编辑 HTTP 响应页面，使其显示序列中的领域列表，如更新自定义身份验证表单中所述。

步骤 5 点击**添加**。

步骤 6 （可选。）要按网络对象过滤流量，请点击**身份源 (Identity Source)** 选项卡。从列表中，点击要用于过滤此身份策略流量的网络对象。点击 **添加**（＋） 以创建新的网络对象。

步骤 7 设置身份规则条件，如中所述 身份规则条件，第 5 页。

步骤 8 将身份规则与访问控制规则相关联，如 将其他策略与访问控制相关联中所述。

步骤 9 将配置更改部署到受管设备；请参阅部署配置更改。

管理身份策略

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 登录管理中心。

步骤 2 请点击 **策略** > **访问控制** > **身份** 。

步骤 3 要删除策略，请点击 **删除**（🗑） 。 如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 要编辑策略，请点击策略旁边的 **编辑**（ ） 并进行更改，如创建身份策略， 第 3 页中所述。 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 5 要复制策略，请点击 **复制**（ ）。

步骤 6 要生成该策略的报告，请点击 **报告**（ ），如生成当前策略报告中所述。

步骤 7 要比较策略，请参阅比较策略。

步骤 8 要创建用于组织策略的文件夹，请点击**添加类别 (Add Category)**。

下一步做什么

部署配置更改；请参阅 部署配置更改。

管理身份规则

过程

步骤 1 登录管理中心。

步骤 2 请点击 **策略** > **访问控制** > **身份** 。

步骤 3 点击您要编辑的策略旁边的**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 如创建身份策略， 第 3 页中所述，要编辑身份规则，请点击 **编辑**（ ） 并进行更改。

步骤 5 要删除身份规则，请点击 **删除**（ ）。

步骤 6 要创建规则类别，请点击**添加类别**并选择位置和规则。

步骤 7 点击**保存 (Save)**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

用户控制故障排除

如果您发现意外的用户规则行为，请考虑调整规则、身份源或领域配置。有关其他相关故障排除信息，请参阅：

- 排除 ISE / ISE-PIC 或 Cisco TrustSec 问题
- TS 代理身份源故障排除
- 强制网络门户身份源故障排除

- 领域和用户下载故障排除

针对领域、用户或用户组的规则与流量不匹配

如果将 TS 代理或 ISE/ISE-PIC 设备配置为监控大量用户组，或者如果将大量用户映射到网络上的主机，则系统可能会由于 Cisco Secure Firewall Management Center 用户限制而丢弃用户记录。因此，具有用户条件的规则可能不会按预期与流量匹配。

针对用户组或用户组内的用户的规则不是按预期与流量匹配

如果配置具有用户组条件的规则，则 LDAP 或 Active Directory 服务器必须配置用户组。如果服务器按照基本对象层次结构组织用户，系统无法执行用户组控制。

针对辅助组中的用户的规则不是按预期与流量匹配

如果配置具有用户组条件的规则，并且该条件包含或排除属于 Active Directory 服务器中辅助组的成员的用户，则服务器可能会限制其报告的用户数。

默认情况下，Active Directory 服务器会限制它们从辅助群组报告的用户数量。您必须自定义此限制，以便辅助组中的所有用户都报告给 Cisco Secure Firewall Management Center并可用于具有用户条件的规则中。

规则与首次发现的用户不匹配

在系统检测到先前未发现的用户的活动后，会从服务器检索其有关信息。直到系统成功检索此信息后，此用户发现的活动才不由匹配规则处理。相反，用户会话由其匹配的下一个规则（或适用时的策略默认操作）处理。

例如，这可能解释以下情形：

- 属于用户组成员的用户与具有用户组条件的规则不匹配。
- 当用于用户数据检索的服务器是 Active Directory 服务器时，由 TS 代理或 ISE/ISE-PIC 设备报告的用户与规则不匹配。

请注意，这可能会导致系统延迟显示事件视图和分析工具中的用户数据。

规则与所有 ISE 用户都不匹配

这是预期行为。可以对由 Active Directory 域控制器进行身份验证的 ISE 用户执行用户控制。不能对由 LDAP、RADIUS 或 RSA 域控制器进行身份验证的 ISE 用户执行用户控制。

规则与所有 ISE/ISE-PIC 用户都不匹配

这是预期行为。可以对由 Active Directory 域控制器进行身份验证的 ISE/ISE-PIC 用户执行用户控制。不能对由 LDAP、RADIUS 或 RSA 域控制器进行身份验证的 ISE/ISE-PIC 用户执行用户控制。

使用过多内存的用户和组

如果处理用户和组使用的内存过多，则会显示运行状况警报。请记住，所有用户会话都会传播到 管理中心 管理的所有设备。如果 管理中心 管理具有不同内存量的设备，则内存量最少的设备将确定系统可以处理的无错误用户会话数。

如果问题仍然存在，您可以选择以下选项：

- 隔离子网上容量较低的受管设备，并将 ISE/ISE-PIC 配置为不向这些子网报告被动身份验证数据。

  请参阅 《*Cisco* 身份服务引擎管理员指南》中关于管理网络设备的章节。

- 取消订阅安全组标记（SGT）。

  有关详细信息，请参阅配置用户控制 ISE。

- 将受管设备升级为内存更高的型号。

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。