通过强制网络门户的用户控制

强制网络门户身份源

强制网络门户是系统支持的授权身份源之一。强制网络门户是一种主动身份验证方法，其中用户可以使用托管设备验证网络登录。（RA-VPN 是另一种类型的主动身份验证。）主动身份验证与被动身份验证的不同之处在于，托管设备会向用户显示登录页面，而被动身份验证会查询身份验证领域（例如 Microsoft AD）来对用户进行身份验证。

通常使用强制网络门户要求身份验证访问互联网，或者访问受限制的内部资源；可以选择配置对资源的访客访问。在系统对强制网络门户用户进行身份验证后，会根据访问控制规则处理其用户流量。强制网络门户仅会对 HTTP 和 HTTPS 流量执行身份验证。

注释 要将 Microsoft Azure AD (SAML) 领域用于强制网络门户，请参阅创建一个 用于主动身份验证的 Microsoft Azure AD (SAML) 领域（强制网络门户）。

注释 必须先对 HTTPS 流量进行加密，然后强制网络门户才能执行身份验证。

强制网络门户还记录失败的身份验证尝试。如果尝试失败，则不会将新用户添加到数据库的用户列表中。强制网络门户报告的身份验证活动失败的用户活动类型是**身份验证失败的用户 (Failed Auth User)**。

从强制网络门户获取的身份验证数据可用于用户感知和用户控制。

相关主题

如果为用户控制配置强制网络门户，第 5 页

关于主机名重定向

（仅限 Snort 3。）主动身份验证身份规则会使用其配置的接口重定向到强制网络门户端口。由于重定向通常是指向 IP 地址，因此用户会收到不受信任的证书错误，并且由于此行为类似于中间人攻击，因此用户可能不愿意接受不受信任的证书。

为避免此问题，您可以将强制网络门户配置为使用托管设备的完全限定域名 (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。

相关主题

重定向到主机名网络规则条件

强制网络门户的许可证要求

威胁防御 许可证

任意

强制网络门户的要求和前提条件

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

强制网络门户准则和限制

在身份策略中配置和部署强制网络门户时，来自指定领域的用户会使用威胁防御来进行身份验证，以访问您的网络。

注释 如果远程接入VPN用户已通过作为安全网关的托管设备进行主动身份验证，则不会执行强制网络门户主动身份验证，即便身份策略中配置了该验证方式。

强制网络门户和策略

在身份策略中配置强制网络门户并在身份规则中调用主动身份验证。身份策略与访问控制策略相关联，访问控制策略定义对网络中资源的访问。例如，您可以排除 US-West/Finance 组中的用户访问 Engineering 服务器，也可以禁止用户访问网络上的非安全应用。

您可以在身份策略的**主动身份验证**选项卡页面上配置一些强制网络门户身份策略设置，并在与访问控制策略关联的身份规则中配置其余部分。

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。不管上述哪种情况，系统都会透明地启用或禁用 TLS/SSL 解密，从而重启 Snort 进程。

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。

当强制网络门户对与身份规则匹配的用户进行身份验证时，Active Directory 或 LDAP 组中尚未下载的任何 Microsoft 用户都将被识别为“未知”(Unknown)。为避免用户被识别为未知，请将领域 或领域序列 配置为下载您希望通过强制网络门户进行身份验证的所有组中的用户。未知用户根据关联的访问控制策略处理；如果访问控制策略配置为阻止未知用户，则会阻止这些用户。

要确保系统下载领域 或领域序列中的所有用户，请确保组位于领域配置的可用组列表中。

有关同步用户和组的详细信息，请参阅 同步用户和组。

需要路由接口

只有配置了路由接口的设备，才能执行强制网络门户主动身份验证。如果要为强制网络门户配置身份规则，并且您的强制网络门户设备包含内联接口和路由接口，则必须在访问控制策略中配置接口规则条件，以便仅针对设备上的路由接口。

如果访问控制策略相关的身份策略包含一个或多个强制网络门户身份规则，并且您在管理一个或多个配置了路由接口的设备的 Cisco Secure Firewall Management Center 上部署策略，则策略部署成功且路由接口执行主动身份验证。

所需的证书和证书颁发机构

在使用强制网络门户进行用户控制和感知之前，您必须满足以下所有条件：

- 要使用 Microsoft AD 进行身份验证，请导出服务器的根证书并将其作为受信任的 CA 证书导入到 Cisco Secure Firewall Management Center 中。

- 用于向部署了身份策略的托管设备进行身份验证的内部证书对象。
- 所需解密规则的内部证书颁发机构。

您可以在创建解密策略时创建内部证书和内部证书颁发机构。

强制网络门户要求和限制

请注意以下要求和限制：

- 强制网络门户不支持 HTTP/3 QUIC 连接。
- 系统每秒最多支持 20 次强制网络门户登录。
- 对于计入最大登录尝试次数的失败登录尝试，失败登录尝试之间存在最长五分钟的时间限制。该五分钟限制不可配置。

  （最大登录尝试次数显示在连接事件中：**分析** > **连接** > **事件**。）

  如果失败登录之间的间隔时间超过五分钟，则用户将被重定向到强制网络门户进行身份验证，而不会被指定为登录失败的用户或访客用户，也不会报告给 Cisco Secure Firewall Management Center。
- 强制网络门户不会协商 TLS v1.0 连接。

  仅支持 TLS v1.1、v1.2 和 TLS 1.3 连接。
- 要从强制网络门户安全地注销用户并防止用户再次登录，管理员可以关闭其会话：**分析** > **用户** > **用户活动**。如果用户关闭浏览器，则浏览器不会自动重新进行身份验证。
- 如果为父域创建了领域，并且托管设备检测到有用户登录到该父域的子域，则托管设备不会检测用户的后续注销。
- 您的访问控制规则必须允许流量流向计划用于强制网络门户的设备的 IP 地址和端口。
- 要对 HTTPS 流量执行强制网络门户主动身份验证，必须使用 a 解密策略解密来自要对其进行身份验证的用户的流量。您无法解密托管设备上强制网络门户用户的 Web 浏览器和强制网络门户后台守护程序之间的连接中的流量；此连接用于对强制网络门户用户进行身份验证。
- 要限制允许流经托管设备的非 HTTP 或 HTTPS 流量的量，您应在身份策略的**端口**选项卡页面中输入典型的 HTTP 和 HTTPS 端口。

  托管设备在确定传入请求未使用 HTTP 或 HTTPS 协议时，会将先前未发现的用户从**待定**更改为**未知**。托管设备将用户从 **待定** 状态更改为其他状态之后，访问控制、服务质量和 解密策略 便可以应用到该流量。如果您的其他策略不允许非 HTTP 或 HTTPS 流量，则在强制网络门户身份策略上配置端口可以防止允许不需要的流量流经托管设备。

Kerberos 前提条件

如果使用 Kerberos 身份验证，则托管设备的主机名必须少于 15 个字符（这是 Windows 设置的 NetBIOS 限制）；否则，强制网络门户身份验证失败。您在设置设备时设置托管设备主机名。有关详细信息，请参阅 Microsoft 文档网站上的此类文章： Active Directory 中计算机、域、站点和 OU 的命名约定。

DNS 必须向主机名返回 64KB 或更少的响应；否则，AD 连接测试失败。此限制在两个方向上都适用，将在 RFC 6891 第 6.2.5 节中讨论。

如果为用户控制配置强制网络门户

开始之前

要使用强制网络门户进行主动身份验证，必须设置一个 LDAP 领域；或者一个Microsoft AD 领域 或领域序列；Microsoft Azure AD (SAML) 领域；访问控制策略；一个身份策略；a 解密策略；并将身份和解密策略与相同的访问控制策略关联。最后，必须将这些策略部署到托管设备。此主题介绍这些任务的高度概要。

注释 要将 Microsoft Azure AD (SAML) 领域用作强制网络门户，请参阅如何创建 用于主动身份验证的 Microsoft Azure AD (SAML) 领域（强制网络门户）。

首先，请执行以下任务：

- 确认您的 Cisco Secure Firewall Management Center 使用已配置的路由接口管理一台或多台设备。
- 要将加密身份验证用于强制网络门户，要么为进行身份验证的托管设备创建一个 PKI 对象，要么使证书数据和密钥可在用于访问 Cisco Secure Firewall Management Center的机器上使用。要创建 PKI 对象，请参阅PKI。

过程

步骤 1 按照以下主题中所述，创建一个 LDAP 领域并将其启用；或者创建一个 Microsoft AD 领域以及可选的领域序列并将其启用：

- 创建 LDAP 领域或 Active Directory 领域和领域目录
- 同步用户和组

要确保系统下载领域 或领域序列中的所有用户，请确保组位于领域配置的可用组列表中。

有关详细信息，请参阅同步用户和组。

步骤 2 获取所需的证书和证书颁发机构
您必须具备以下所有条件：

- 要使用 Microsoft AD 进行身份验证，请导出服务器的根证书并将其作为受信任的 CA 证书导入到 Cisco Secure Firewall Management Center 中。
- 用于向部署了身份策略的托管设备进行身份验证的内部证书对象。
- 所需解密规则的内部证书颁发机构。

您可以在创建解密策略时创建内部证书和内部证书颁发机构。

步骤 3 使用关联的证书颁发机构创建网络对象。

请参阅 配置强制网络门户第 1 部分：创建网络主体，第 6 页。

步骤 4 使用主动身份验证规则创建身份策略。

在使用强制网络门户执行身份验证后，该身份策略将在您的领域访问资源内启用所选用户。

有关详细信息，请参阅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，第 8 页。

步骤 5 为强制网络门户配置允许强制网络门户端口（默认情况下为 TCP 885）上的流量的访问控制规则。

您可以为要使用的强制网络门户选择任何可用的 TCP 端口。无论选择哪个端口，都必须创建一条允许该端口上的流量的规则。

有关详细信息，请参阅配置强制网络门户第 3 部分：创建 TCP 端口访问控制规则，第 10 页。

步骤 6 再添加一条访问控制规则，以允许所选领域或领域序列中的用户使用强制网络门户访问资源。

有关详细信息，请参阅配置强制网络门户第 4部分：创建用户访问控制规则，第 11 页。

步骤 7 为 **未知** 用户配置 a 解密策略 和 **解密 - 重签** 规则，以使强制网络门户用户能够使用 HTTPS 协议访问网页。

仅当HTTPS流量在流量发送到强制网络门户之前被解密的情况下，强制网络门户才能进行用户身份验证。系统本身将强制网络门户视为**未知**用户。

强制网络门户示例：通过出站规则来创建解密策略，第 12 页

步骤 8 将身份和 解密策略 与第 3 步的访问控制策略相关联。

这是最后一步，此后系统即可使用强制网络门户进行用户身份验证。

有关详细信息，请参阅 配置强制网络门户第 6 部分：将身份和 解密策略 与访问控制策略关联起来，第 14 页。

下一步做什么

请参阅配置强制网络门户第 1 部分：创建网络主体，第 6 页。

相关主题

排除强制网络门户中的应用，第 16 页
PKI
强制网络门户身份源故障排除，第 17 页
Snort 重新启动场景

配置强制网络门户第 1 部分：创建网络主体

此任务讨论如何开始将强制网络门户配置为身份源。

开始之前

（仅限 Snort 3。）使用 DNS 服务器创建完全限定的主机名 (FQDN) 并将 威胁防御 的内部证书上传至 管理中心。如果您之前从未使用过例如 此类 资源，可以咨询此类资源。在 管理中心 托管的一台设备上指定路由接口的 IP 地址。

有关网络对象的详细信息，请参阅 重定向到主机名网络规则条件。

过程

步骤 1 如果尚未这样子，请登录 管理中心。

步骤 2 请点击 **对象** > **对象管理**。

步骤 3 展开 **PKI**。

步骤 4 点击 **内部证书**。

步骤 5 点击 **Add Internal Cert**。

步骤 6 在**名称 (Name)** 字段中，输入名称以标识内部证书（例如，**`MyCaptivePortal`**）。

步骤 7 在 **证书数据** 字段中，粘贴证书或使用 **浏览** 按钮查找证书。

证书公用名必须与您想要强制网络门户用户进行身份验证的 FDQN 完全匹配。

步骤 8 在 **密钥** 字段中，粘贴证书的私钥或使用 **浏览** 按钮查找证书。

步骤 9 如果证书已加密，请选中 **已加密** 复选框并在相邻字段中输入密码。

步骤 10 点击**保存 (Save)**。

步骤 11 点击**网络 (Network)**。

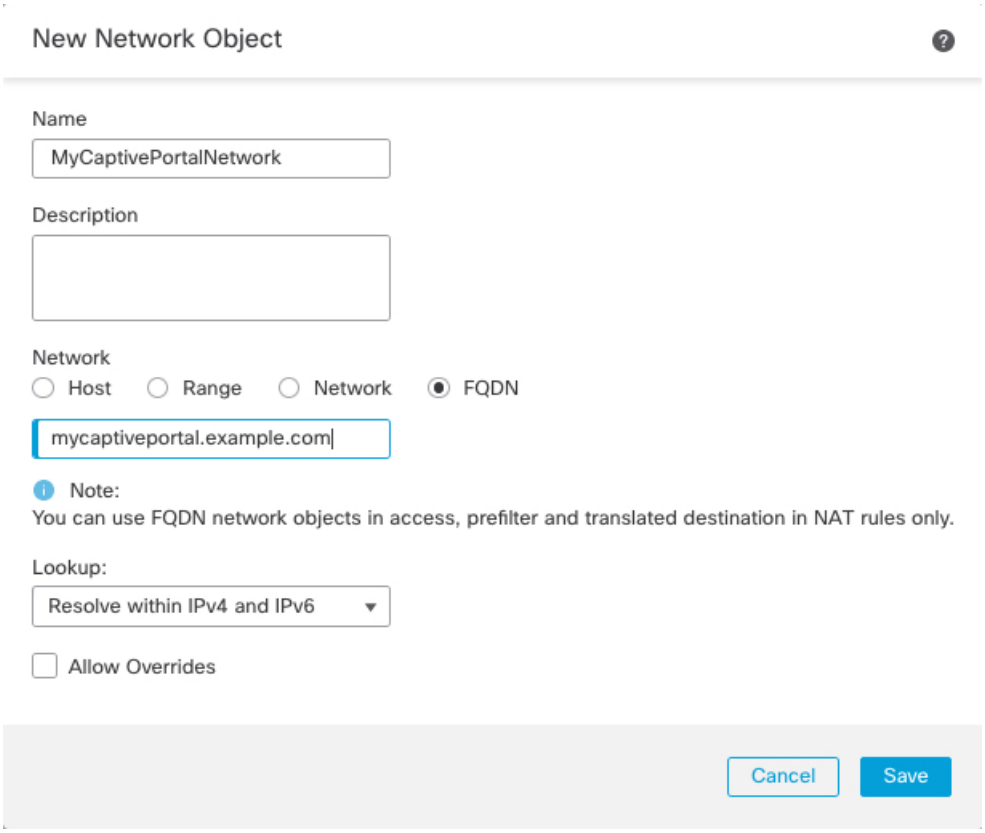
步骤 12 点击 **添加网络 (Add Network)** > **添加对象 (Add Object)**。

步骤 13 在 **名称** 字段中，输入名称以标识对象（例如， **`MyCaptivePortalNetwork`**）。

步骤 14 点击 **FDQN** ，然后在字段中输入强制网络门户的FDQN的名称。

步骤 15 点击 **查找**选项。

下图显示了一个示例。



步骤 16 点击保存 **(Save)**。

下一步做什么

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 ， 第 8 页

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

开始之前

此由多个部分组成的程序展示如何使用默认 TCP 端口 885 以及将 管理中心 服务器证书用于强制网络门户和 TLS/SSL 解密来设置强制网络门户。本示例中的每个部分介绍启用强制网络门户来执行主动身份验证所需的一项任务。

如果您遵循此程序中的所有步骤，则可以将强制网络门户配置为供您的域中的用户使用。您可以选择执行在程序的各个部分中介绍的其他任务。

有关完整程序的概述，请参阅如果为用户控制配置强制网络门户 ， 第 5 页。

过程

步骤 1 如果尚未登录，请登录 管理中心。

步骤 2 依次点击**策略** > **访问控制** > **身份**，然后创建或编辑身份策略。

步骤 3 （可选。）点击**添加类别**，为强制网络门户身份规则添加类别，然后为该类别输入一个**名称**。

步骤 4 点击**主动身份验证**选项卡。

步骤 5 从列表中选择适当的 **服务器证书** ，或者点击 **添加** (+) 以添加证书。

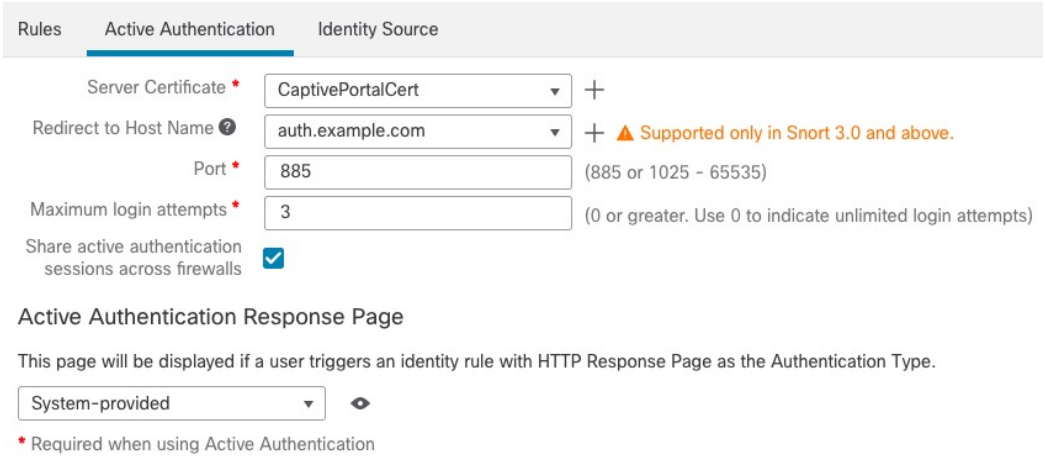
注释
强制网络门户 不 支持使用数字签名算法（DSA）或椭圆曲线数字签名算法（ECDSA）证书。

步骤 6 从 **重定向到主机名 (Redirect to Host Name)** 字段中，点击之前创建的网络对象或者点击 **添加** (+)。

步骤 7 在**端口**字段中输入 **885**，然后指定**最大登录尝试次数**。

步骤 8 取消选中 **跨防火墙共享主动身份验证 (Share active authentication across firewalls)** ，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 ， 第 15 页。

步骤 9 （可选。）选择**主动身份验证响应页面**，如强制网络门户字段 ， 第 15 页中所述。



步骤 10 （如果仅从早期版本升级到版本 7.4.1，并且使用领域序列对用户进行身份验证。）点击 **编辑** (✎) 并查看 更新自定义身份验证表单 ， 第 10 页。

步骤 11 点击**保存 (Save)**。

步骤 12 点击**规则 (Rules)**。

步骤 13 点击 **添加规则** 以添加新的强制网络门户身份策略规则，或者点击 **编辑** (✎) 以编辑现有规则。

步骤 14 为规则输入**名称 (Name)**。

步骤 15 从**操作**列表中，选择**主动身份验证**。

步骤 16 点击 **领域和设置**。

步骤 17 从**领域 (Realms)** 列表中，选择要用于用户身份验证的领域或领域序列。

步骤 18 （可选。）选中**如果身份验证无法识别用户，则识别为访客**。有关详细信息，请参阅强制网络门户字段，第 15 页。

步骤 19 从列表中选择**身份验证协议 (Authentication Protocol)**。

如果选择 **NTLM**、 **Kerberos**或 **HTTP 协商 (HTTP Negotiate)** 身份验证协议，则无法使用领域序列来对用户进行身份验证。改为选择 **HTTP 基本 (HTTP Basic)** 或 **HTTP 响应页面 (HTTP Response Page)** 。

步骤 20 （可选。）要豁免强制网络门户中的特定应用流量，请参阅排除强制网络门户中的应用，第 16 页。

步骤 21 向规则（端口、网络等）添加条件，如身份规则条件中所述。

步骤 22 点击**添加 (Add)**。

步骤 23 在该页面顶部，点击**保存 (Save)**。

下一步做什么

继续执行配置强制网络门户第 3 部分：创建 TCP 端口访问控制规则，第 10 页。

更新自定义身份验证表单

从早期版本升级到版本 7.4.1（或更高版本）后，必须将以下行添加到自定义身份验证表单，用户才能在使用强制网络门户进行身份验证时查看域列表。（如果使用 HTTP 响应页面身份验证类型，则始终需要执行此任务；如果用户使用其他身份验证类型对领域进行身份验证，则此任务为可选任务。）

在身份规则的**主动身份验证 (Active Authentication)** 选项卡页面上，点击 **编辑** (✎) 并在表单中要求用户登录的部分输入以下内容：

```
<select name="realm" id="realm"></select>
```

配置强制网络门户第 3 部分：创建 TCP 端口访问控制规则

该程序的这一部分显示如何创建访问控制规则，以允许强制网络门户使用 TCP 端口 885（它是强制网络门户的默认端口）与客户端通信。如果您希望，也可以选择另一个端口，但该端口必须与您在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，第 8 页中选择的端口匹配。

开始之前

有关整个强制网络门户配置的概述，请参阅如果为用户控制配置强制网络门户，第 5 页。

过程

步骤 1 如果尚未登录，请登录 管理中心。

步骤 2 如果尚未进行此操作，则请创建强制网络门户证书，如 PKI中所述。

步骤 3 依次点击**策略 (Policies)** > **访问控制 (Access Control)** > **访问控制 (Access Control)** 然后创建或编辑访问控制策略。

步骤 4 点击**添加规则 (Add Rule)**。

步骤 5 为规则输入**名称 (Name)**。

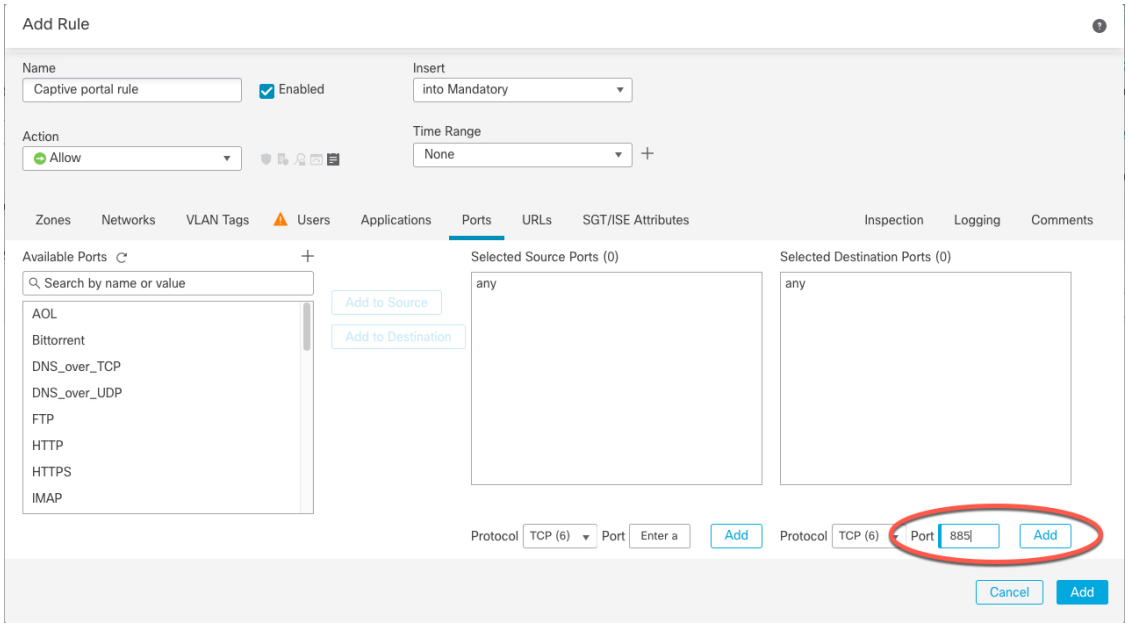
步骤 6 从**操作**列表中选择**允许**。

步骤 7 点击**端口 (Ports)**。

步骤 8 从**所选目标端口**字段下的**协议**列表中，选择 **TCP**。

步骤 9 在**端口**字段中，输入 **885**。

步骤 10 点击**端口 (Port)** 字段旁边的**添加 (Add)**。
下图显示了一个示例。



步骤 11 点击页面底部的**添加 (Add)**。

下一步做什么

继续执行配置强制网络门户第 4部分：创建用户访问控制规则 ， 第 11 页。

配置强制网络门户第 4部分：创建用户访问控制规则

该过程的此部分讨论如何添加访问控制规则，以使领域中的用户能够使用强制网络门户进行身份验证。

开始之前

有关整个强制网络门户配置的概述，请参阅如果为用户控制配置强制网络门户 ， 第 5 页。

过程

步骤 1 在规则编辑器中，点击**添加规则 (Add Rule)**。

步骤 2 为规则输入**名称 (Name)**。

步骤 3 从**操作**列表中选择**允许**。

步骤 4 点击“**用户**”。

步骤 5 在**可用领域**列表中，点击要允许的领域。

步骤 6 如果没有显示领域，则请点击 **刷新** ( )。

步骤 7 在**可用用户**列表中，选择要添加到规则的用户，然后点击**添加到规则**。

步骤 8 （可选。）向访问控制策略添加条件，如身份规则条件中所述。

步骤 9 点击**添加 (Add)**。

步骤 10 在访问控制规则页面上，点击**保存 (Save)**。

步骤 11 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。

下一步做什么

强制网络门户示例：通过出站规则来创建解密策略 ， 第 12 页

强制网络门户示例：通过出站规则来创建解密策略

程序的此部分介绍如何创建 a 解密策略 ， 以在流量到达强制网络门户之前解密和重签流量。强制网络门户仅可对解密的流量进行身份验证。

开始之前

您的出站服务器必须具有内部证书颁发机构 (CA)；换言之，是指为强制网络门户用户解密流量以进行身份验证的托管设备。该证书必须不同于用于验证托管设备的强制网络门户的内部证书。

过程

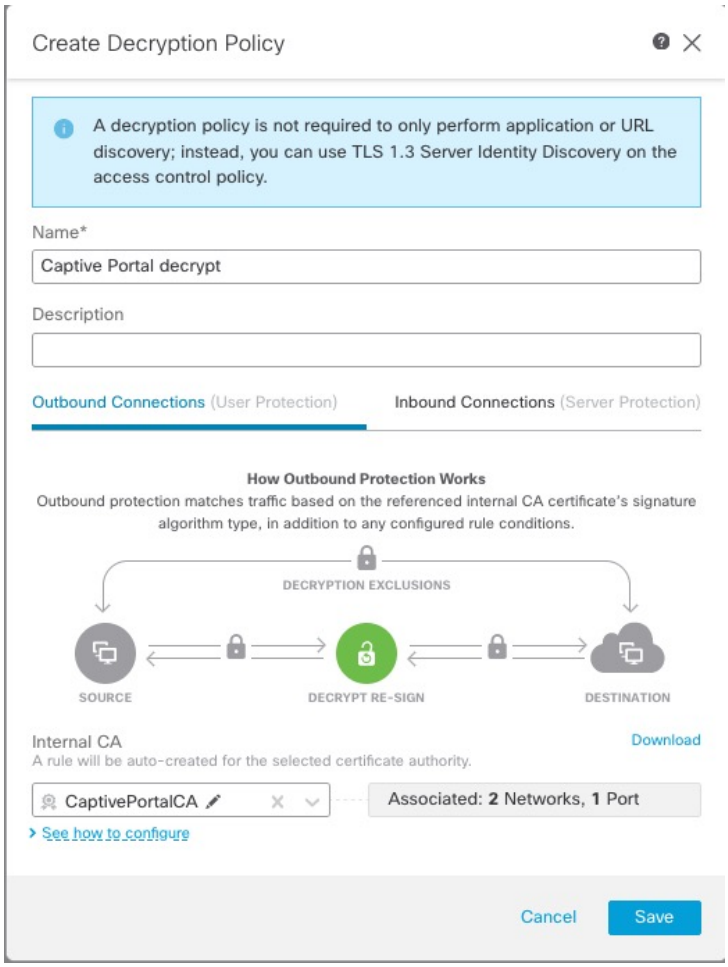
步骤 1 如果尚未登录，请登录管理中心。

步骤 2 请点击 **策略** > **访问控制标题** > **解密**。

步骤 3 点击**新建策略 (New Policy)**。

步骤 4 在 **Name** 和 **Description** 中为策略提供唯一名称和说明（后者为可选项）。

步骤 5 点击**出站连接 (Outbound Connections)** 选项卡。



步骤 6 为规则上传或选择证书。

系统会根据 CA 和网络/端口的组合创建一条规则。

步骤 7 （可选。）选择网络和端口。

更多详细信息：

- 解密规则 条件
- 网络规则条件
- 端口规则条件

步骤 8 点击**保存 (Save)**。

步骤 9 点击您创建的解密策略旁边的 **编辑** (✎)。

步骤 10 点击强制网络门户的解密规则旁边的 **编辑** (✎)。

步骤 11 点击“**用户**”。

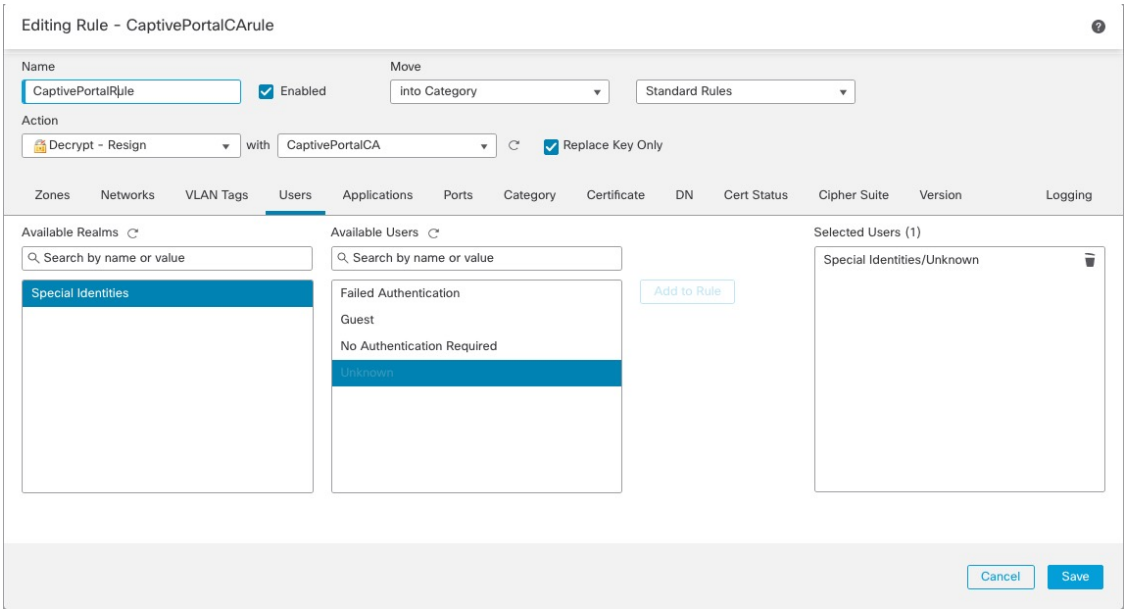
步骤 12 在 **可用领域** 列表上方，点击 **刷新** (↻)。

步骤 13 在**可用领域**列表中，点击**特殊身份**。

步骤 14 在**可用用户**列表中，点击**未知**。

步骤 15 点击**添加至规则**。

下图显示了一个示例。



步骤 16 （可选。）设置其他选项，如解密规则 条件中所述。

步骤 17 点击**添加 (Add)**。

下一步做什么

配置强制网络门户第 6 部分：将身份和 解密策略 与访问控制策略关联起来，第 14 页

配置强制网络门户第6部分：将身份和解密策略与访问控制策略关联起来

该程序的这一部分讨论如何将身份策略和 TLS/SSL **解密 - 重新签名**规则与您先前创建的访问控制规则关联起来。在此之后，用户可以使用强制网络门户进行身份验证。

开始之前

有关整个强制网络门户配置的概述，请参阅如果为用户控制配置强制网络门户，第 5 页。

过程

步骤 1 点击**策略 (Policies)** > **访问控制 (Access Control)** > **访问控制 (Access Control)**，然后按照配置强制网络门户第 3 部分：创建 TCP 端口访问控制规则，第 10 页中所述编辑您创建的访问控制策略。 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 2 创建新的访问控制策略，或者编辑现有策略。

步骤 3 在该页面顶部，点击**身份 (Identity)** 字样。

步骤 4 从该列表中，选择身份策略的名称，然后在该页面顶部，点击**保存 (Save)**。

步骤 5 重复前面的步骤，以使强制网络门户 解密策略与访问控制策略相关联。

步骤 6 如果尚未进行此操作，则请将托管设备作为该策略的目标，如设置访问控制策略的目标设备中所述。

下一步做什么

- 将身份和访问控制策略部署到托管设备，如部署配置更改中所述。
- 监控用户活动，如 《Cisco Secure Firewall Management Center 管理指南》 中使用工作流程所述。

强制网络门户字段

使用以下字段，在身份策略的**主动身份验证**选项卡页面上配置强制网络门户设置。另请参阅身份规则字段和排除强制网络门户中的应用，第 16 页。

服务器证书 (Server Certificate)

强制网络门户后台守护程序显示的内部证书。

注释 强制网络门户 不 支持使用数字签名算法（DSA）或椭圆曲线数字签名算法（ECDSA）证书。

端口

要用于强制网络门户连接的端口号。您必须使用 TCP 端口设置访问控制规则以用于强制网络门户，然后将身份策略与该访问控制策略相关联。有关详细信息，请参阅配置强制网络门户第 3 部分：创建 TCP 端口访问控制规则，第 10 页。

最大登录尝试次数 (Maximum login attempts)

系统拒绝用户登录请求前允许的最大失败登录尝试的次数。

跨防火墙共享主动身份验证会话

确定当用户的身份验证会话被发送到与之前连接的设备不同的托管设备时是否需要进行身份验证。如果您的组织要求用户在每次更改位置或站点时进行身份验证，则应禁用此选项。

- （默认，继续之前的行为。）选中此复选框可允许用户使用与主动身份验证身份规则相关联的任何托管设备进行身份验证。
- 清除复选框可要求用户使用不同的托管设备进行身份验证，即使他们已经使用部署了主动身份验证规则的另一个托管设备进行了身份验证。如果您的组织要求按位置或站点进行身份验证，并且按站点部署托管设备，请使用此选项。

托管设备要么是集群设备，要么是高可用性对，就好像它们是同一台设备；特别是

- 同一集群或高可用性对中的托管设备：保存用户会话以保持集群对的一致性。在故障转移时，辅助设备具有当前用户会话数据。
- 不同集群或高可用性对中的托管设备：不会共享用户会话数据，因此不存储在这些设备上。

主动身份验证响应页面 (Active Authentication Response Page)

要向强制网络门户用户显示的系统提供或自定义 HTTP 响应页面。在身份策略主动身份验证设置中选择**主动身份验证响应页面**后，还必须使用 **HTTP 响应页面**配置一个或更多个身份规则作为**身份验证协议**。

系统提供的 HTTP 响应页面包括**用户名 (Username)** 和**密码 (Password)** 字段，如果选择使用域序列进行身份验证，则还包括一个领域列表以及用于允许用户以访客身份访问网络的**以访客身份登录 (Login as guest)** 按钮。要显示单点登录方法，请配置自定义 HTTP 响应页面。

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中所示。

选择以下选项：

- 要使用通用响应，请选择**系统提供**。可以点击 **视图** (👁) 以查看此页面的 HTML 代码。
- 要创建自定义响应，请选择**自定义**。将显示一个具有系统提供的代码的窗口，您可以替换或修改该代码。完成时，保存更改。可以通过点击 **编辑** (✎) 来编辑自定义页面。

相关主题

内部证书对象

排除强制网络门户中的应用

您可以选择应用（通过其 HTTP 用户-代理 字符串标识）并免于对它们执行强制网络门户主动身份验证。这允许所选应用的流量在未经身份验证的情况下通过身份策略。

注释 此列表中仅显示带有**用户代理排除标记**的应用。

过程

步骤 1 如果尚未登录，请登录 管理中心。

步骤 2 请点击 **策略** > **访问控制标题** > **身份** 。

步骤 3 编辑包含强制网络门户规则的身份策略。

步骤 4 在 **领域和设置** 选项卡页面上， 展开**HTTP 用户代理排除**。

- 在第一列中，选中要过滤应用的每个项目旁边的复选框，然后选择一个或多个应用，然后点击 **添加到规则 (Add to Rule)**。

  复选框与 ANDed 在一起。

- 要减少显示的过滤器，请在 **按名称搜索** 字段中键入搜索字符串；这对类别和标记尤其有用。要清除搜索，请点击 **清除** (✕)。

- 要刷新过滤器列表并清除所有所选过滤器，请点击 **重新加载** (↻)。

注释
该列表每次显示 100 个应用。

步骤 5 从**可用应用**列表中选择要添加到过滤器的应用：

- 要减少显示的应用，请在**按名称搜索**字段中输入搜索字符串。要清除搜索，请点击 **清除** (✕)。
- 使用位于列表底部的页码可浏览各个可用应用的列表。
- 要刷新应用列表并清除所有所选应用，请点击 **重新加载** (↻)。

步骤 6 添加所选应用以免除外部身份验证。可以点击并拖动，也可以点击**添加到规则 (Add to Rule)**。由此则得到您所选的应用过滤器组合。

下一步做什么

- 继续配置身份规则，如创建身份规则中所述。

强制网络门户身份源故障排除

有关其他相关故障排除信息，请参阅领域和用户下载故障排除和用户控制故障排除。

如果您遇到强制网络门户证问题，请检查以下事项：

- 强制网络门户托管设备上的时间必须与 管理中心上的时间同步。

- 如果您已配置DNS解析并创建了身份规则来执行**Kerberos**（或**HTTP 协商**，如果希望Kerberos作为选项）强制网络门户，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。

  有关详细信息，请参阅关于主机名重定向，第 2 页。

- 如果使用 Kerberos 身份验证，则托管设备的主机名必须少于 15 个字符（这是 Windows 设置的 NetBIOS 限制）；否则，强制网络门户身份验证失败。您在设置设备时设置托管设备主机名。有关详细信息，请参阅 Microsoft 文档网站上的此类文章：Active Directory 中计算机、域、站点和 OU 的命名约定。

- DNS 必须向主机名返回 64KB 或更少的响应；否则，AD 连接测试失败。此限制在两个方向上都适用，将在 RFC 6891 第 6.2.5 节中讨论。

- 如果强制网络门户配置正确，但重定向到 IP 地址或完全限定域名 (FQDN) 失败，请禁用终端安全软件。此类软件可能会干扰重定向。

- 如果您选择**Kerberos**（或**HTTP 协商**，如果您要将 Kerberos 作为一个选项）作为身份规则的**身份验证类型**，则您选择的**领域**必须配置**AD 加入用户名**和**AD 加入密码**，以便执行 Kerberos 强制网络门户主动身份验证。

- 如果选择 **HTTP 基本身份验证** 作为身份规则中的 **身份验证类型**，则您的网络上的用户可能不会注意到其会话超时。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。

- 如果您的管理中心和托管设备之间的连接失败，则无法在停机期间识别设备报告的所有强制网络门户登录，除非以前查看过这些用户并已将他们下载到管理中心。无法识别的用户在管理中心上记录为“未知”(Unknown) 未知用户。停机时间过后，系统将根据身份策略中的规则重新识别和处理“未知”(Unknown) 用户。

- 如果要用于强制网络门户的设备包含内联接口和路由接口，则必须在强制网络门户身份规则中配置区域条件，以便仅针对强制网络门户设备上的路由接口。

- 托管设备的主机名必须少于 15 个字符，Kerberos 身份验证才能成功。

- 要从强制网络门户安全地注销用户并防止用户再次登录，管理员可以关闭其会话：**分析** > **用户标题** > **活动会话**。如果用户关闭浏览器，则浏览器不会自动重新进行身份验证。

- 活动FTP会话在事件中显示为**Unknown**用户。此为正常现象，因为在活动FTP中，会由服务器（而非客户端）发起连接，而 FTP 服务器则不应具有关联的用户名。有关活动 FTP 的详细信息，请参阅 RFC 959。

- 当强制网络门户对与身份规则匹配的用户进行身份验证时，Active Directory 或 LDAP 组中尚未下载的任何 Microsoft 用户都将被识别为“未知”(Unknown)。为避免用户被识别为未知，请将领域 或领域序列 配置为下载您希望通过强制网络门户进行身份验证的所有组中的用户。未知用户根据关联的访问控制策略处理；如果访问控制策略配置为阻止未知用户，则会阻止这些用户。

  要确保系统下载领域 或领域序列中的所有用户，请确保组位于领域配置的可用组列表中。

  有关详细信息，请参阅 同步用户和组。

强制网络门户的历史记录

功能	管理中心最低版本管理中心	威胁防御最低版本	详细信息
使用领域或领域序列进行身份验证。	7.4.1	7.4.1	您可以为 LDAP 领域、Microsoft Active Directory 领域或领域序列配置主动身份验证。此外，您还可以配置被动身份验证规则，使用领域或领域序列退回到主动身份验证。您可以选择在访问控制规则中共享相同身份策略的托管设备之间共享会话。 此外，您可以选择要求用户在使用不同于之前访问的托管设备访问系统时再次进行身份验证。 Microsoft Azure Active Directory 不能与强制网络门户一起使用。 新增/修改的菜单项： • **策略 (Policies)** > **身份 (Identity)** > （编辑策略） > **主动身份验证 (Active Authentication)** > **跨防火墙共享主动身份验证会话 (Share active authentication sessions across firewalls)** • **身份策略 (Identity policy)** > （编辑） > **添加规则 (Add Rule)** > **被动身份验证 (Passive Authentication)** > **领域和设置 (Realms & Settings)** > **如果无法建立被动或 VPN 身份，则使用主动身份验证 使用主动身份验证 (Use active authentication if passive or VPN identity cannot be established)** • **身份策略 (Identity policy)** > （编辑） > **添加规则 (Add Rule)** > **主动身份验证 (Active Authentication)** > **领域和设置 (Realms & Settings)** > **如果无法建立被动或 VPN 身份，则使用主动身份验证 使用主动身份验证 (Use active authentication if passive or VPN identity cannot be established)**
跨防火墙共享主动身份验证会话。	7.4.1	7.4.1	确定当用户的身份验证会话被发送到与之前连接的设备不同的托管设备时是否需要进行身份验证。如果您的组织要求用户在每次更改位置或站点时进行身份验证，则应禁用此选项。 • （默认。）启用可允许用户使用与主动身份验证身份规则相关联的任何托管设备进行身份验证。 • 禁用可要求用户使用不同的托管设备进行身份验证，即使他们已经使用部署了主动身份验证规则的另一个托管设备进行了身份验证。 新增/修改的屏幕： **策略 (Policies)** > **身份 (Identity)** > （编辑策略） > **主动身份验证 (Active Authentication)** > **跨防火墙共享主动身份验证会话 (Share active authentication sessions across firewalls)**

功能	管理中心最低版本管理中心	威胁防御最低版本	详细信息
主机名重定向。	7.1.0	7.1.0 与 Snort 3	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）。
访客登录。	6.1.0	6.1.0	用户可以使用强制网络门户以访客身份登录。
强制网络门户。	6.0.0	6.0.0	引入的功能。可以使用强制网络门户要求用户在浏览器窗口出现提示时输入其凭证。映射还允许策略基于用户或用户组。

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。