AnyConnect俘虏门户检测和修正

目录

简介

本文描述思科AnyConnect移动性客户端俘虏门户检测功能和需求它的能正确地作用。在旅馆、餐馆、机场和其他公共场所的许多无线热点使用俘虏门户为了阻止对互联网的用户访问。他们重定向HTTP请求到要求用户输入他们的凭证或确认热点主机的条款和条件的他们自己的网站。

先决条件

要求

思科建议您有Cisco AnyConnect安全移动客户端的知识。

使用的组件

本文档中的信息基于以下软件版本：

- AnyConnect版本3.1.04072
- Cisco可适应安全工具(ASA)版本9.1.2

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

提供wi-fi和有线访问，例如机场，咖啡店和旅馆的许多设施，要求用户支付，在他们获取访问前，同意遵守可接受的使用规定或者两个。这些设施使用呼叫俘虏门户的一个技术为了防止应用程序连接，直到用户打开浏览器并且接受访问的条件。

俘虏门户修正需求

俘虏门户检测和修正的支持要求这些许可证之一：

- AnyConnect高级版(安全套接字协议层(SSL) VPN版本)
- 思科AnyConnect安全移动性

您能使用思科AnyConnect安全移动性许可证为了为俘虏门户检测和修正提供支持与AnyConnect精华或AnyConnect优质许可证的组合。

> **Note**: 是在使用中的AnyConnect的版本支持的Microsoft Windows和Macintosh OS X操作系统支持俘虏门户检测和修正。

俘虏门户热点检测

AnyConnect显示**无法与VPN**在GUI的**服务器**消息联系，如果不能连接，不管原因。VPN服务器指定安全网关。如果不间断工作的启用，并且一个俘虏门户不存在，客户端继续尝试连接到VPN并且相应地更新状态消息。

如果不间断工作的VPN启用，连接失败策略关闭，俘虏门户修正禁用，并且AnyConnect检测一个俘虏门户的出现，则AnyConnect GUI显示此消息一次每连接，并且一次每请重新连接：

```
The service provider in your current location is restricting access to the Internet.
The AnyConnect protection settings must be lowered for you to log on with the service
provider. Your current enterprise security policy does not allow this.
```

如果AnyConnect检测出现一俘虏门户，并且AnyConnect配置与以前描述的那有所不同，AnyConnect GUI显示此消息一次每连接，并且一次每请重新连接：

```
The service provider in your current location is restricting access to the Internet.
You need to log on with the service provider before you can establish a VPN session.
You can try this by visiting any website with your browser.
```

> **Caution**:默认情况下俘虏门户检测启用并且是不可配置的。 AnyConnect不在俘虏门户检测时修改任何浏览器配置设置。

俘虏门户热点修正

俘虏门户修正是您满足一个俘虏门户热点要求为了获取网络访问的进程。

AnyConnect不修正俘虏门户;它依靠最终用户执行修正。

为了执行俘虏门户修正，最终用户符合热点供应商的要求。这些需求也许包括成本的付款访问网络，在可接受的使用规定，或者由供应商定义的某个其他要求的一个签名。

在AnyConnect VPN客户端配置文件必须明确地允许俘虏门户修正，如果不间断工作的AnyConnect启用，并且连接失败策略设置对已关闭。如果不间断工作的启用，并且连接失败策略设置打开，您不需要明显地允许在AnyConnect VPN客户端配置文件的俘虏门户修正，因为用户没有从网络访问限制。

错误俘虏门户检测

AnyConnect能错误地假设在这些情况下在一个俘虏门户。

- 如果AnyConnect尝试与与包含一个不正确服务器名的证书的ASA联系(CN)，则AnyConnect客户端认为在一个俘虏门户环境。

  为了防止此问题，请确保ASA证书适当地配置。在证书的CN值必须匹配ASA服务器的名称在VPN客户端配置文件的。

- 如果有在响应对客户端的尝试由对ASA的阻塞HTTPS访问与ASA联系的网络的另一个设备，在ASA前，则AnyConnect客户端认为在一个俘虏门户环境。当用户是在内部网络并且通过防火墙连接为了连接到ASA时，此情况能发生。

  如果必须从公司里边限制对ASA的访问，请配置您的防火墙这样HTTP和HTTPS流量对ASA的地址不返回HTTP状态。应该允许或完全阻塞对ASA的HTTP/HTTPS访问(亦称黑洞)为了保证HTTP/HTTPS请求发送对ASA不会返回一意外的答复。

AnyConnect行为

此部分描述AnyConnect如何正常运行。

1. AnyConnect尝试HTTPS探测器对在XML配置文件定义的完全合格的域名(FQDN)。

2. 如果有验证错误(没有委托/错误FQDN)，则AnyConnect尝试HTTP探测器对在XML配置文件定义的FQDN。如果比HTTP 302有其他答复，则认为自己是在俘虏门户后。

俘虏门户不正确地检测与IKEV2

当您尝试运行端口的443可适应安全设备管理器对ASA的一互联网密钥交换版本2 (IKEv2)时连接与禁用的SSL验证(ASDM)门户，为俘虏门户检测执行的HTTPS探测器导致重定向到ASDM门户(**/admin/public/index.html**)。因为这没有由客户端预计，看起来象俘虏门户重定向，并且连接尝试被防止，因为看起来俘虏门户修正要求。

应急方案

如果遇到此问题，这是一些应急方案：

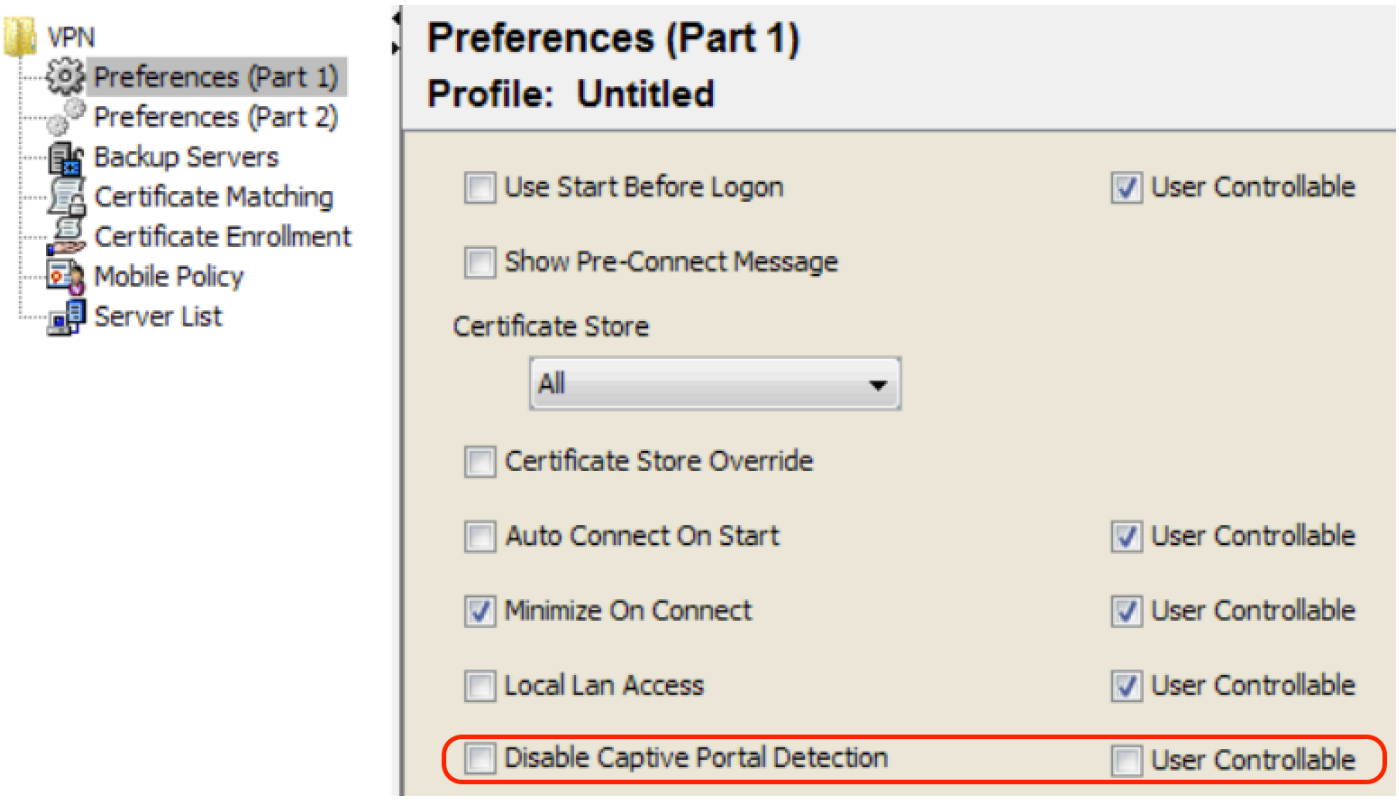
- 取消建立接口的HTTP on命令，以便ASA不会听在接口的HTTP连接。
- 删除在接口的SSL信任点。
- 启用IKEV2客户端服务。
- 启用在接口的WebVPN。

此问题由在版本3.1(3103)的Cisco Bug ID CSCud17825解决。

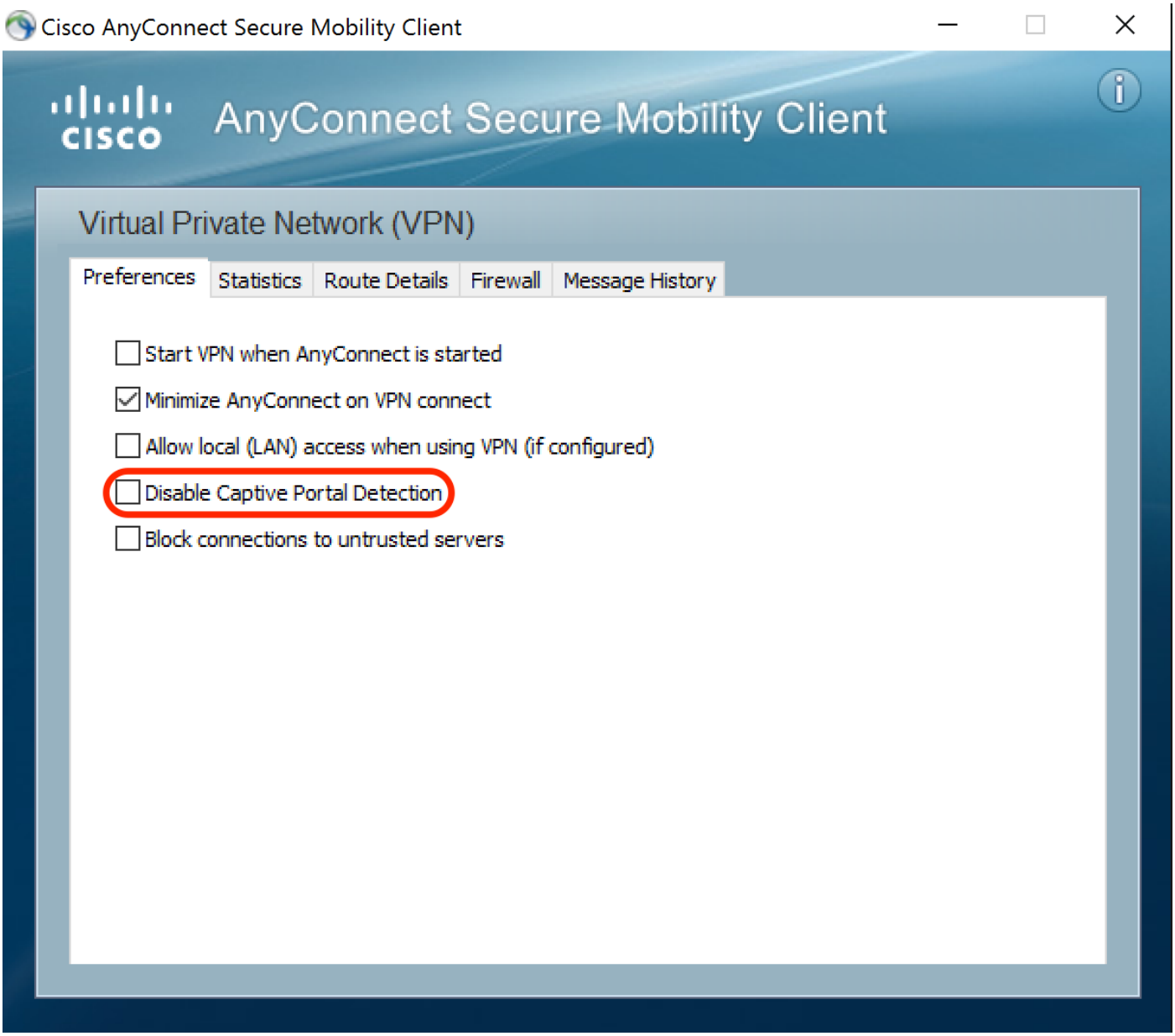
Caution:同一问题为Cisco IOS路由器存在。如果**ip http server**在Cisco IOS启用，要求，如果同一个方框使用作为PKI服务器， AnyConnect错误地检测俘虏门户。应急方案是使用**IP HTTP access-class**为了终止对AnyConnect HTTP请求的答复，而不是请求验证。

禁用俘虏门户功能

是可能的禁用在AnyConnect客户端版本4.2.00096的俘虏门户功能及以后(请参阅Cisco Bug ID CSCud97386)。管理员能确定选项应该是否是已禁用的用户可配置或。此选项是可用的在首选(在配置文件编辑器的部分1)部分下。管理员能选择**禁用俘虏门户检测**或**用户可控制**如此所显示配置文件编辑器快照：



如果可控制的用户被检查，复选框出现在AnyConnect安全移动性客户端UI的首选选项卡如显示此处：


Cisco AnyConnect Secure Mobility Client
AnyConnect Secure Mobility Client
Virtual Private Network (VPN)
Preferences
Statistics
Route Details
Firewall
Message History
Start VPN when AnyConnect is started
Minimize AnyConnect on VPN connect
Allow local (LAN) access when using VPN (if configured)
Disable Captive Portal Detection
Block connections to untrusted servers