了解CSC的DNS和SWG回退设置

目录

简介

先决条件

- 要求
- 使用的组件

概述

哪些DNS回退设置会导致SWG回退？

哪些DNS回退设置不会导致SWG回退？

独立SWG回退设置

简介

本文档介绍思科安全客户端(CSC)的DNS和安全网络网关(SWG)回退设置。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Cisco安全客户端。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

概述

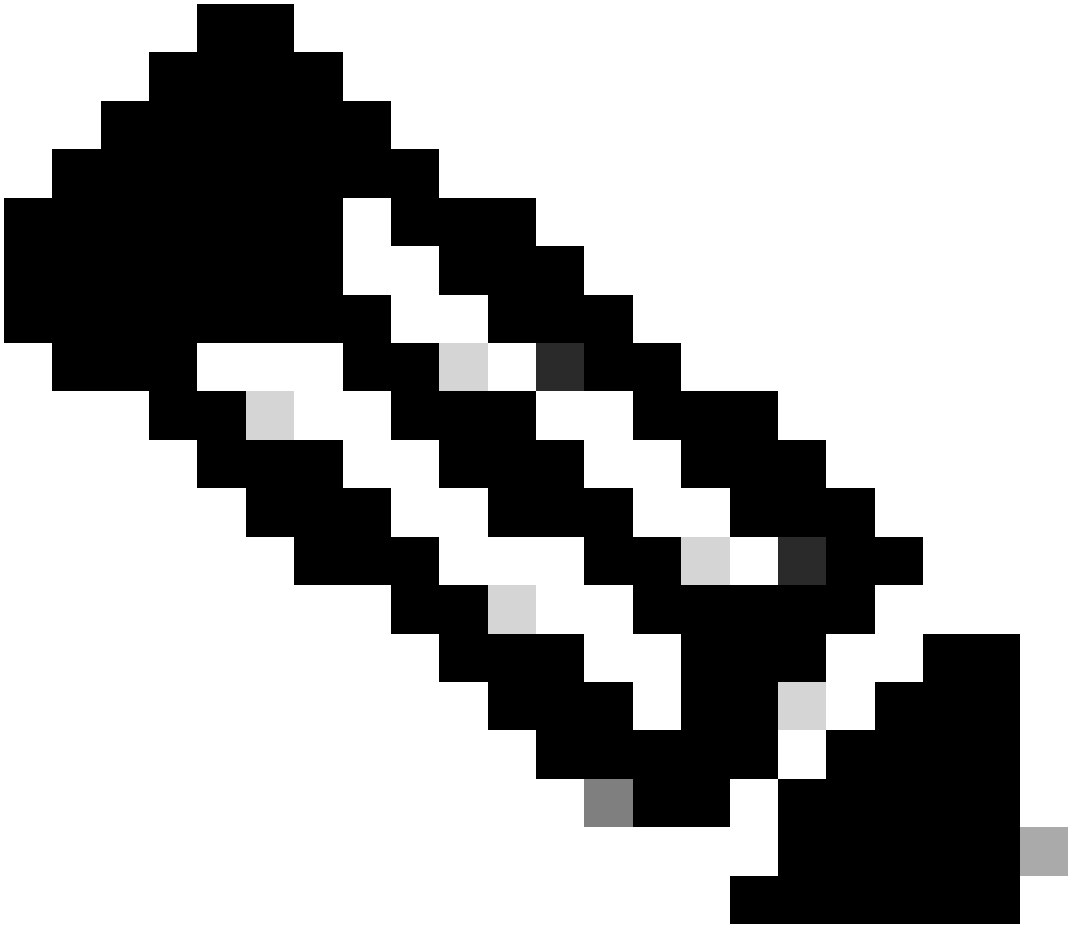
直到2024年4月25日左右，思科安全客户端的SWG模块回退行为无法控制，而无论DNS模块的状态如何，并且取决于DNS回退设置来启用/禁用SWG保护。为了解决这个问题，Umbrella已将DNS模块和SWG模块的行为分离，从而根据需要实现独立管理。5.1.3.62版及更高版本上的Cisco Secure Clients可以使用此功能，其中Umbrella将DNS和SWG回退设置分离，以便实现增强的精细控制。旧版本上的客户端未遵循单独的SWG模块回退。

当启用DNS退避后安全网关退避功能时，CSC的SWG模块将遵循DNS模块的行为。但是，并非所有DNS回退设置都会发生这种情况。在下一部分中，详细介绍SWG模块执行或不执行的DNS回退设置。

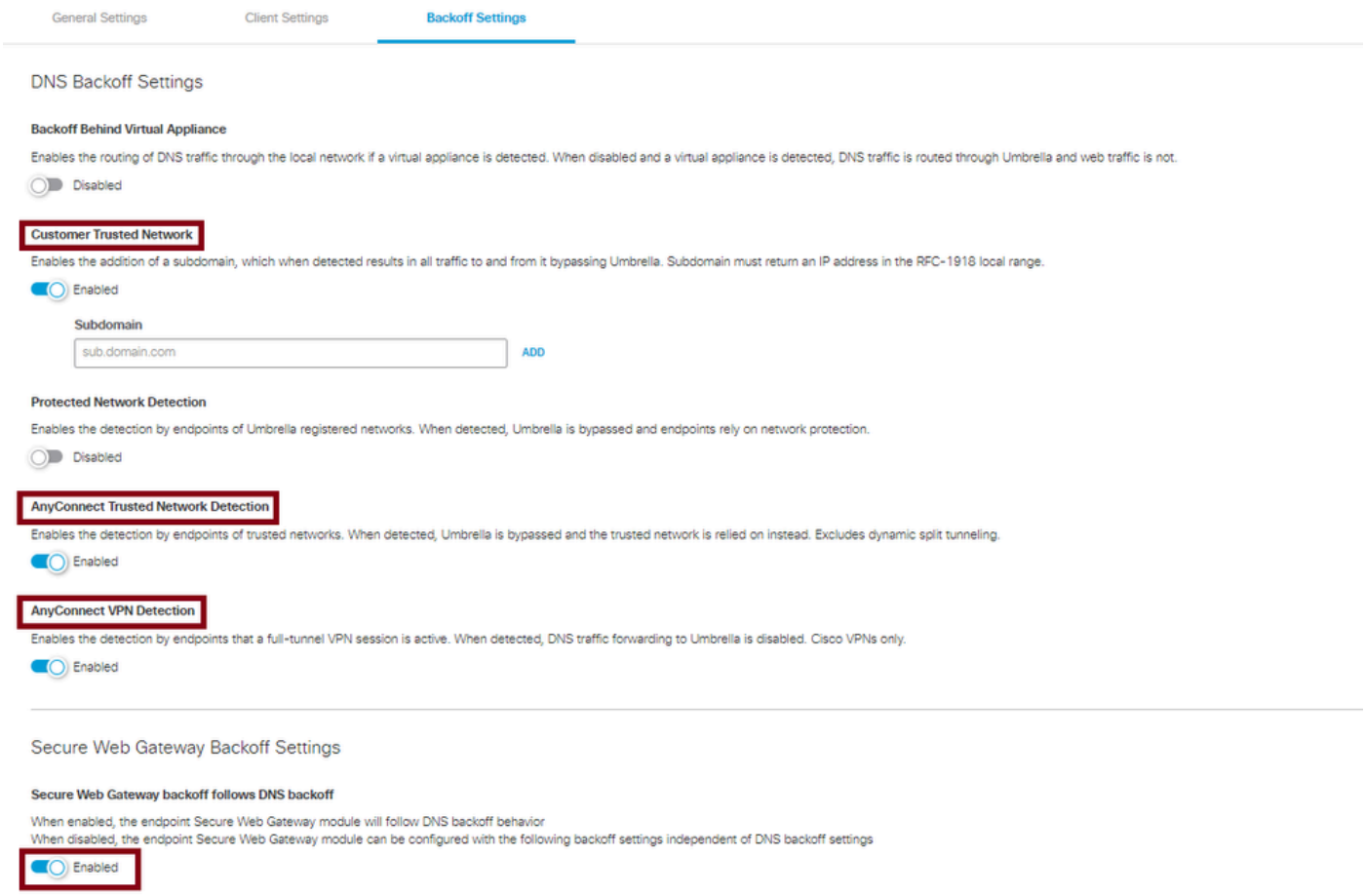
哪些DNS回退设置会导致SWG回退？

以下DNS回退设置会导致SWG回退：

- 客户信任网络：在DNS回退设置中设置Customer Trusted Network域是最简单的方法之一。通过托管解析为RFC1918地址的内部域，DNS和SWG可以同时回退。Umbrella的客户端被编码为查询该域。如果成功将域解析为私有IP地址，则会将设备识别为位于私有受保护的网络上，从而导致DNS模块退出。Web模块也遵循这种回退机制，当DNS模块成功解析域时，同样可以采用这种回退机制。
- AnyConnect受信任网络检测
- AnyConnect VPN检测



注意：DNS回退设置在运行早于5.1.3.62版本的Cisco安全客户端上仍然有效，因为它是在DNS和SWG回退设置分离之前实施的。

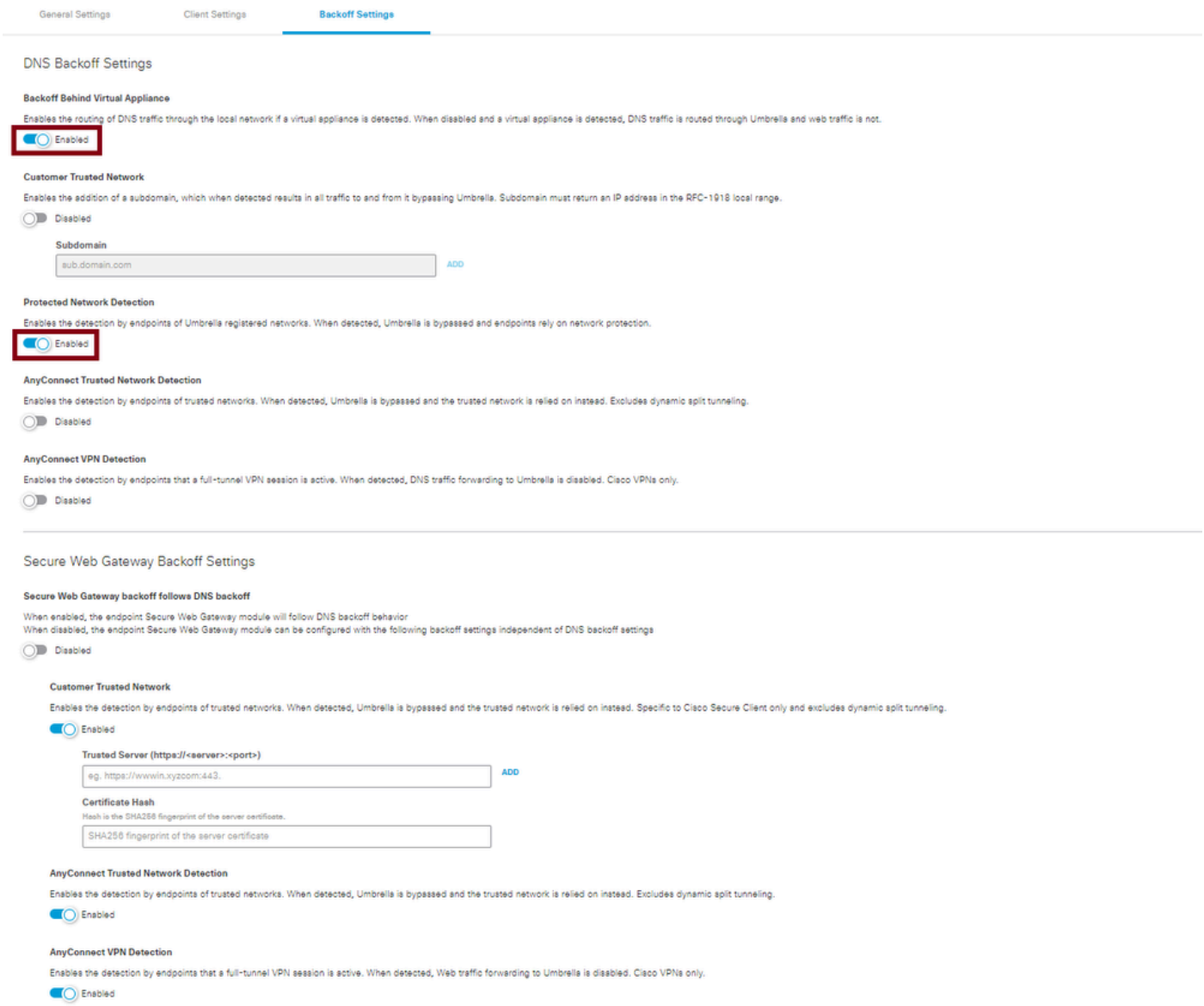


27885424859028

哪些DNS回退设置不会导致SWG回退？

配置这两个DNS回退功能不会导致SWG回退。因此，您必须有选择性地配置SWG回退设置，而与DNS配置状态无关。这将在下一节中详细讨论。

- 虚拟设备后退：从AnyConnect 4.10.07061(MR7)和Secure Client 5.0.02075(MR2)开始，SWG模块可以在存在Umbrella虚拟设备的网络上保持启用状态。如果您以前依靠虚拟设备在给定网络上禁用SWG模块和Web重定向，则可以改为使用受信任网络域或AnyConnect受信任网络检测。
- 受保护网络检测



27885587178772

独立SWG回退设置

如果您的环境中未启用这些DNS回退功能，您可以专门利用此处介绍的SWG回退设置之一，以确保SWG保持禁用状态：

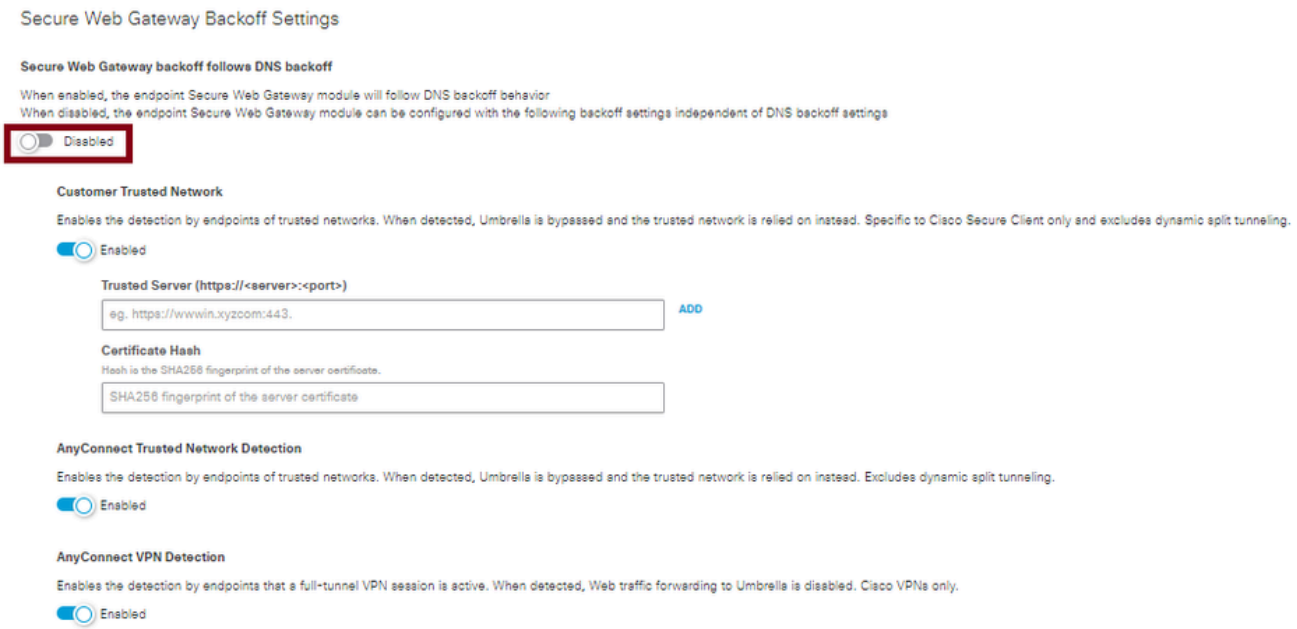
- 客户信任网络
- AnyConnect受信任网络检测
- AnyConnect VPN检测

这一新功能允许SWG模块独立于DNS模块运行。此功能适用于使用5.1.3.62及更高版本的思科安全客户端。在控制面板中配置一个显式SWG回退切换：

- 客户信任网络：一个选项是使用SWG回退设置下的Customer Trusted Network选项，在该选项中，您可以配置客户端可以联系的内部服务器，以确认该服务器位于受保护的网络中。您需要确保客户端可以访问Web服务器，获取该服务器上的证书，并将证书哈希复制到Umbrella控制面板。

其他两个选项仅适用于VPN连接：

- AnyConnect受信任网络检测
- AnyConnect VPN检测



27886005743764

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。