DNS- und SWG-Backoff-Einstellungen für CSC verstehen

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

Überblick

Welche DNS-Backoff-Einstellungen führen dazu, dass die SWG abgeschaltet wird?

Welche DNS-Backoff-Einstellungen führen nicht dazu, dass die SWG deaktiviert wird?

Unabhängige SWG-Backoff-Einstellungen

Einleitung

In diesem Dokument werden die Backoff-Einstellungen für DNS und Secure Web Gateway (SWG) für Cisco Secure Client (CSC) beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Secure Client.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

Bis etwa zum 25. April 2024 konnte das Abschaltverhalten des Cisco Secure Client für die SWG-Module nicht unabhängig vom Status des DNS-Moduls gesteuert werden und war zur Aktivierung/Deaktivierung des SWG-Schutzes von den DNS-Abschalteinstellungen abhängig. Um diesem Problem zu begegnen, hat Umbrella das Verhalten für das DNS-Modul und das SWG-Modul entkoppelt, wodurch bei Bedarf eine unabhängige Verwaltung möglich ist. Diese Funktion

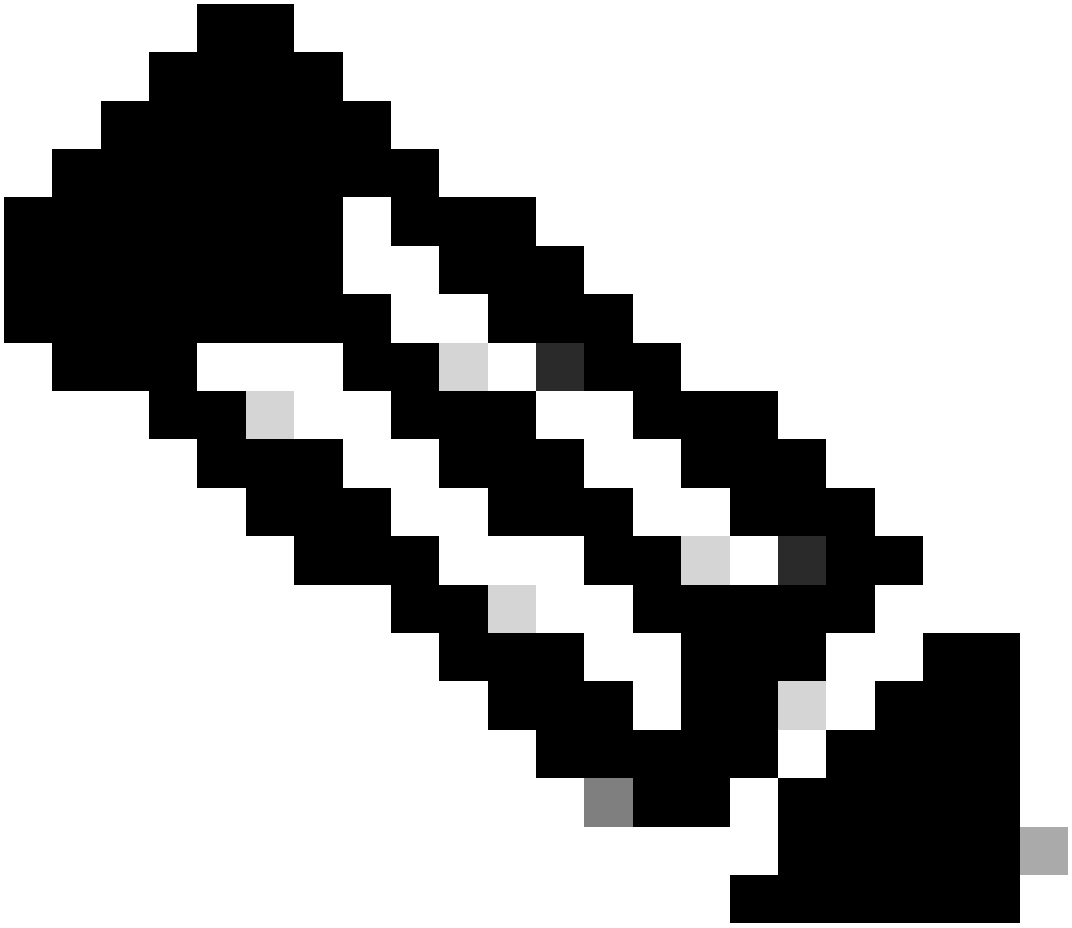
steht Cisco Secure Clients ab Version 5.1.3.62 zur Verfügung, bei der Umbrella die DNS- und SWG-Backoff-Einstellungen entkoppelt hat, um eine erweiterte präzise Kontrolle zu ermöglichen. Clients älterer Versionen folgten nicht der separaten Absicherung des SWG-Moduls.

Wenn die Funktion zum Sicheren Web-Gateway-Backoff nach dem DNS-Backoff aktiviert ist, folgt das SWG-Modul des CSC dem Verhalten des DNS-Moduls. Dies ist jedoch nicht bei allen DNS-Backoff-Einstellungen der Fall. Im nächsten Abschnitt werden die DNS-Backoff-Einstellungen erläutert, die vom SWG-Modul verwendet werden oder nicht.

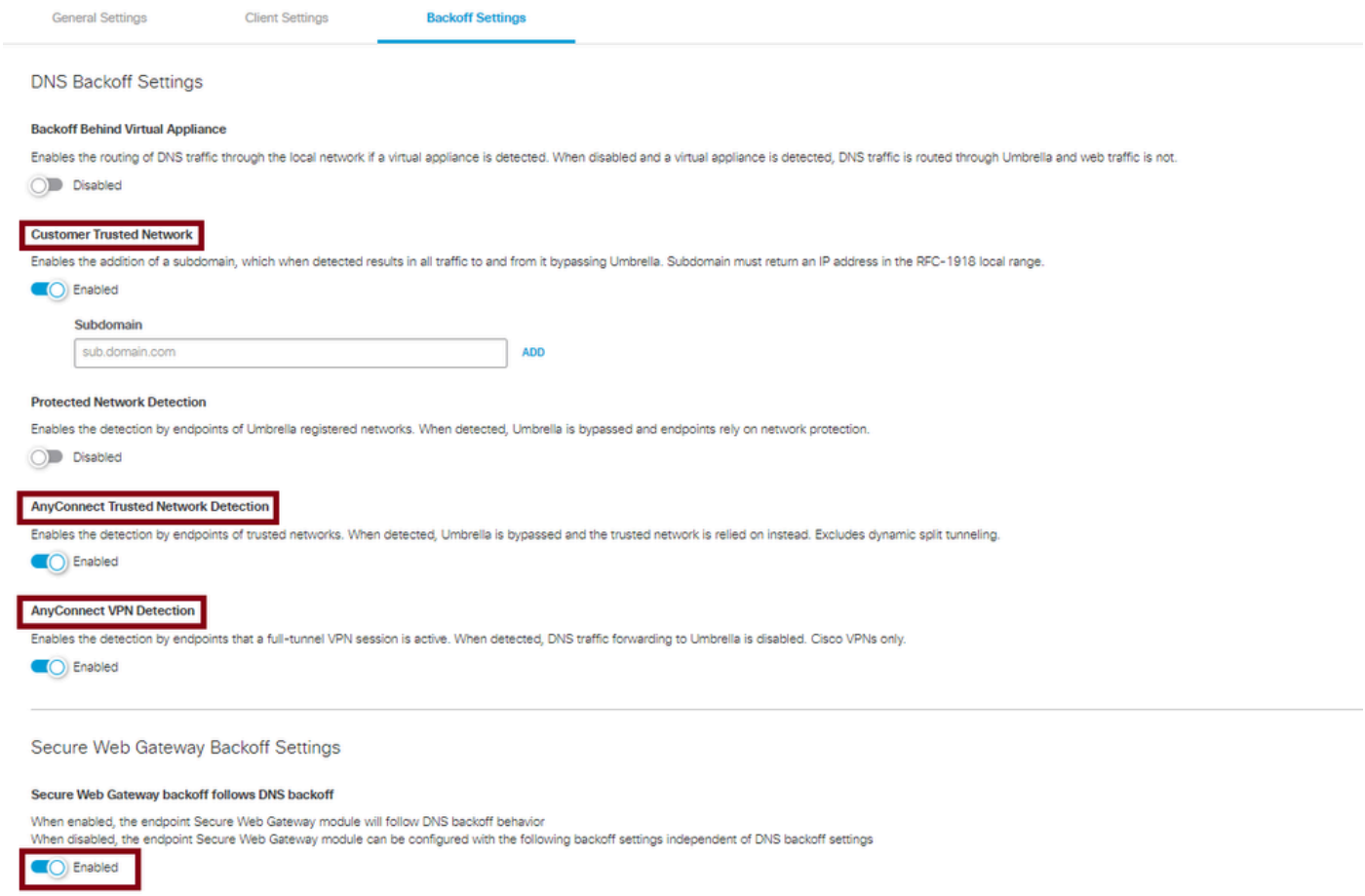
Welche DNS-Backoff-Einstellungen führen dazu, dass die SWG abgeschaltet wird?

Diese DNS-Backoff-Einstellungen veranlassen die SWG zum Backoff:

- Kundenorientiertes Netzwerk: Die Einrichtung einer Customer Trusted Network-Domäne in den DNS-Backoff-Einstellungen ist eine der einfachsten Methoden. Durch das Hosten einer internen Domäne, die in eine RFC1918-Adresse aufgelöst wird, können sowohl DNS als auch SWG gleichzeitig ein Backoff durchführen. Der Umbrella-Client ist codiert, um diese Domäne abzufragen. Wenn die Domäne erfolgreich in eine private IP-Adresse aufgelöst wird, wird das Gerät als in einem privaten und geschützten Netzwerk befindlich identifiziert, wodurch das DNS-Modul zurückgesetzt wird. Dieser Backoff-Mechanismus wird auch vom Web-Modul beachtet, das ebenfalls zurücktreten kann, wenn das DNS-Modul die Domäne erfolgreich auflöst.
- Erkennung vertrauenswürdiger AnyConnect-Netzwerke
- AnyConnect VPN-Erkennung



Anmerkung: Die DNS-Backoff-Einstellungen bleiben auf Cisco Secure Clients mit älteren Versionen als 5.1.3.62 funktionsfähig, da sie vor der Entkopplung der DNS- und SWG-Backoff-Einstellungen implementiert wurden.

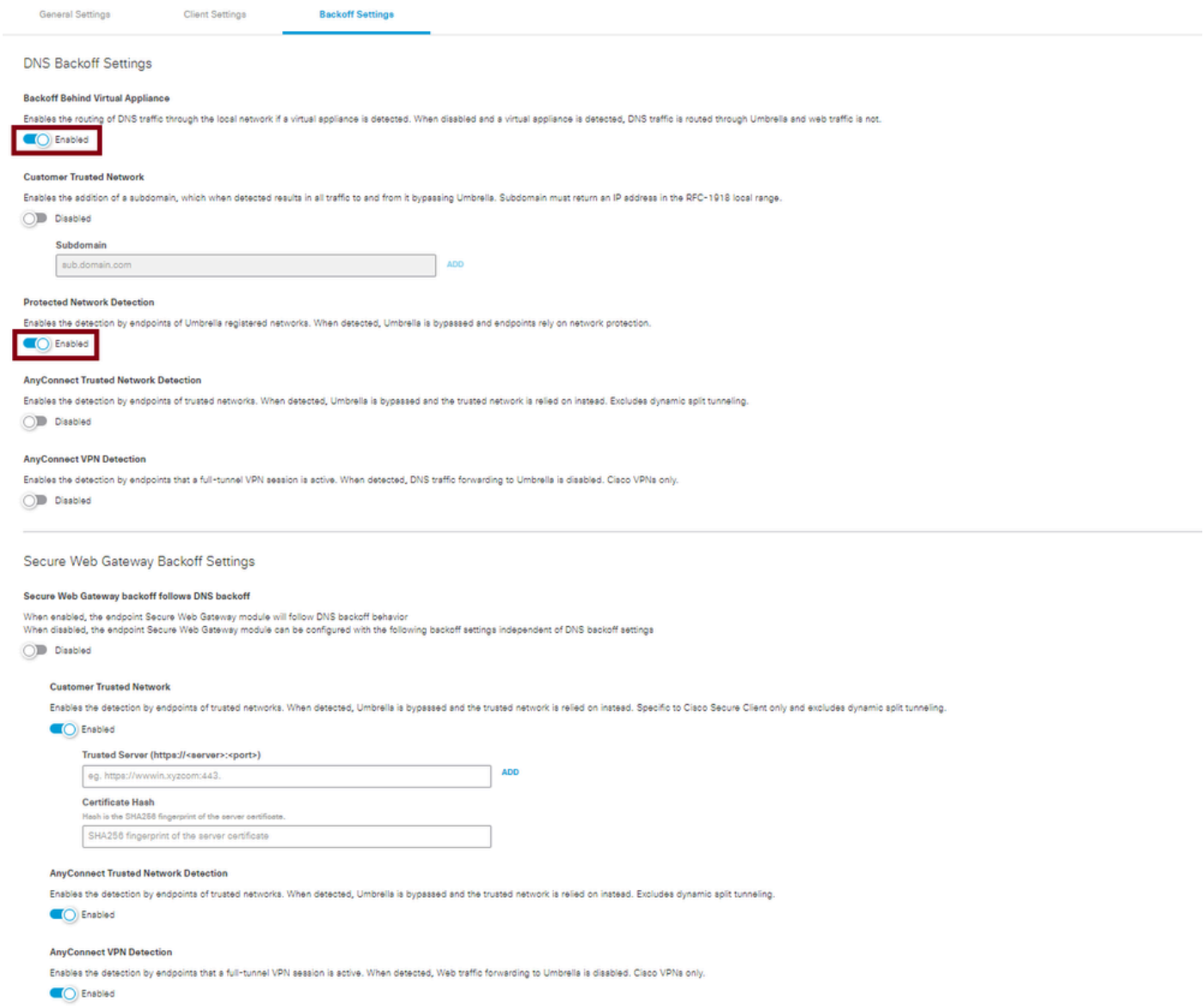


27885424859028

Welche DNS-Backoff-Einstellungen führen nicht dazu, dass die SWG deaktiviert wird?

Die Konfiguration dieser beiden DNS-Backoff-Funktionen führt nicht dazu, dass die SWG abgewinkt ist. Daher müssen Sie die SWG-Backoff-Einstellungen unabhängig vom DNS-Konfigurationsstatus selektiv konfigurieren. Dies wird im nächsten Abschnitt ausführlicher behandelt.

- Backoff Behind Virtual Appliance: Ab AnyConnect 4.10.07061 (MR7) und Secure Client 5.0.02075 (MR2) kann das SWG-Modul in Netzwerken aktiviert bleiben, in denen eine virtuelle Umbrella-Appliance vorhanden ist. Wenn Sie zuvor auf das Vorhandensein einer virtuellen Appliance zur Deaktivierung des SWG-Moduls und der Web-Umleitung in einem bestimmten Netzwerk angewiesen waren, können Sie stattdessen Trusted Network Domain (vertrauenswürdige Netzwerkdomäne) oder AnyConnect Trusted Network Detection (Erkennung vertrauenswürdiger Netzwerke über AnyConnect) verwenden.
- Erkennung geschützter Netzwerke



27885587178772

Unabhängige SWG-Backoff-Einstellungen

Wenn diese DNS-Backoff-Funktionen in Ihrer Umgebung nicht aktiviert sind, können Sie ausschließlich eine der hier beschriebenen SWG-Backoff-Einstellungen verwenden, um sicherzustellen, dass die SWG deaktiviert bleibt:

- Kundenorientiertes Netzwerk
- Erkennung vertrauenswürdiger AnyConnect-Netzwerke
- AnyConnect VPN-Erkennung

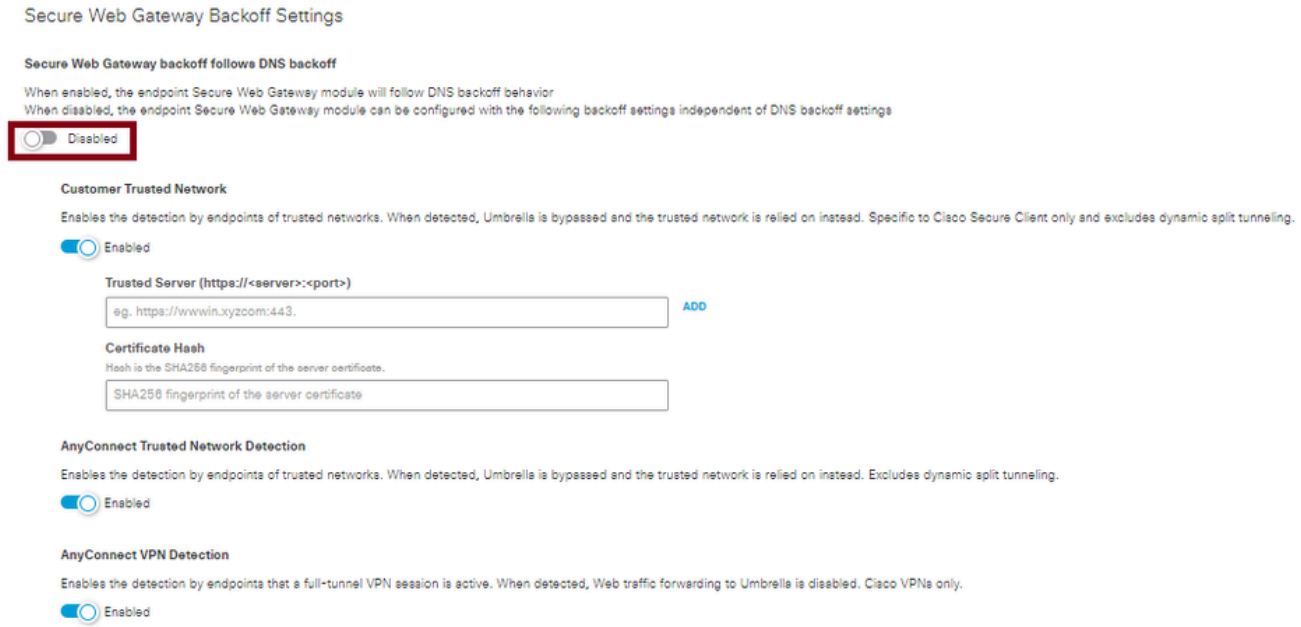
Dank dieser neuen Funktion kann das SWG-Modul unabhängig vom DNS-Modul betrieben werden. Diese Funktion steht Cisco Secure Clients ab Version 5.1.3.62 zur Verfügung. Konfigurieren Sie einen der expliziten SWG-Backoff-Umschalter im Dashboard:

- Kundenorientiertes Netzwerk: Eine Option besteht darin, die Option "Customer Trusted Network" unter den SWG-Backoff-Einstellungen zu verwenden, mit der Sie einen internen

Server konfigurieren können, den der Client erreichen kann, um zu bestätigen, dass er sich im geschützten Netzwerk befindet. Sie müssen sicherstellen, dass der Webserver vom Client erreichbar ist, ein Zertifikat auf diesem Server abrufen und den Zertifikats-Hash in das Umbrella Dashboard kopieren.

Die beiden anderen Optionen gelten ausschließlich für VPN-Verbindungen:

- Erkennung vertrauenswürdiger AnyConnect-Netzwerke
- AnyConnect VPN-Erkennung



27886005743764

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.