Instellingen voor DNS- en SWG-back-off voor CSC begrijpen

Inhoud

Inleiding

In dit document worden de back-upinstellingen voor DNS en Secure Web Gateway (SWG) voor Cisco Secure Client (CSC) beschreven.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Secure Client.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

Tot ongeveer 25 april 2024 kon het back-offgedrag van de SWG-module van de Cisco Secure Client niet worden gecontroleerd, ongeacht de status van de DNS-module en was het afhankelijk van de DNS-back-offinstellingen om SWG-beveiliging in of uit te schakelen. Om dit aan te pakken, heeft Umbrella het gedrag voor de DNS-module en de SWG-module ontkoppeld, waardoor onafhankelijk beheer mogelijk is als dat nodig is. Dit is beschikbaar voor Cisco Secure Clients op versie 5.1.3.62 en nieuwer waar Umbrella de DNS- en SWG-back-offinstellingen ontkoppelde om

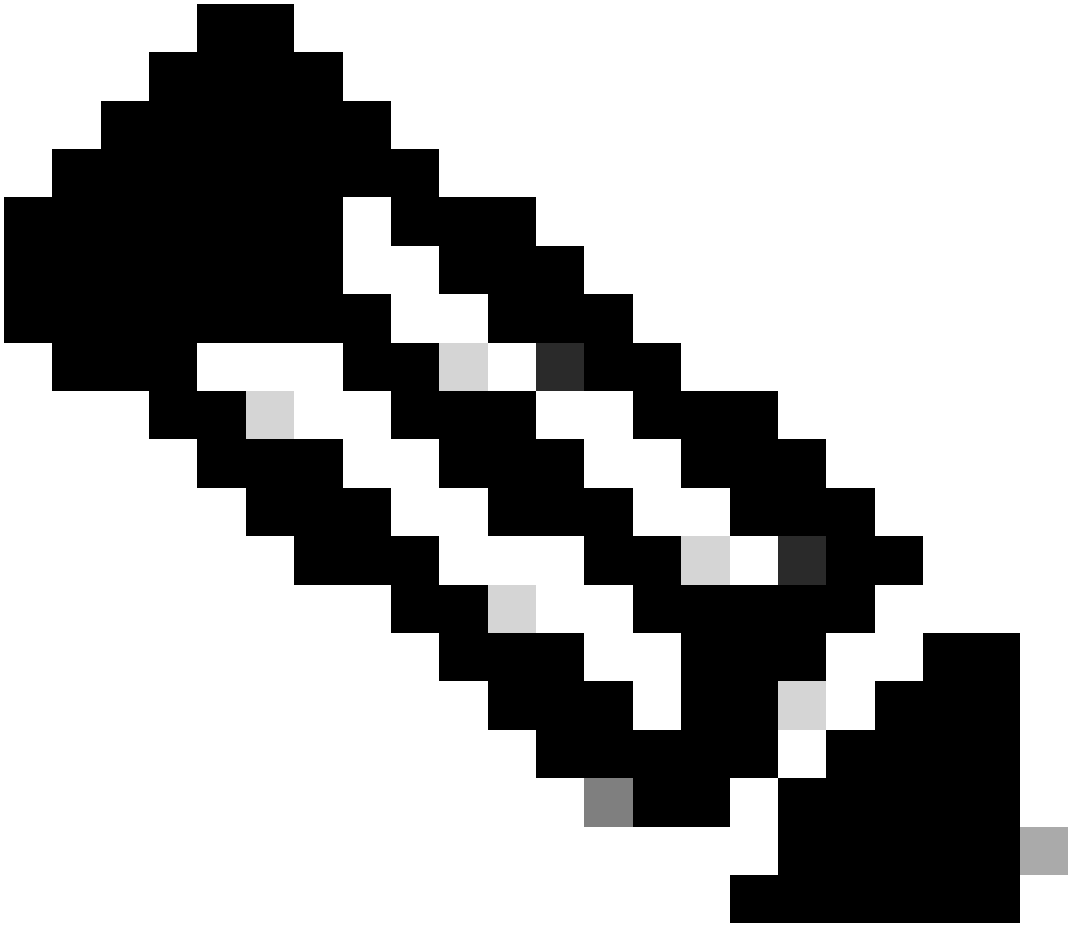
verbeterde granulaire controle mogelijk te maken. Cliënten op oudere versies volgden de afzonderlijke back-up van de SWG-module niet.

Wanneer de Secure Web Gateway-back-up volgt nadat de DNS-back-offfunctie is ingeschakeld, volgt de SWG-module van de CSC het gedrag van de DNS-module. Dit gebeurt echter niet bij alle DNS-back-off-instellingen. In de volgende sectie worden de DNS-back-offinstellingen die de SWG-module wel of niet volgt, gedetailleerd weergegeven.

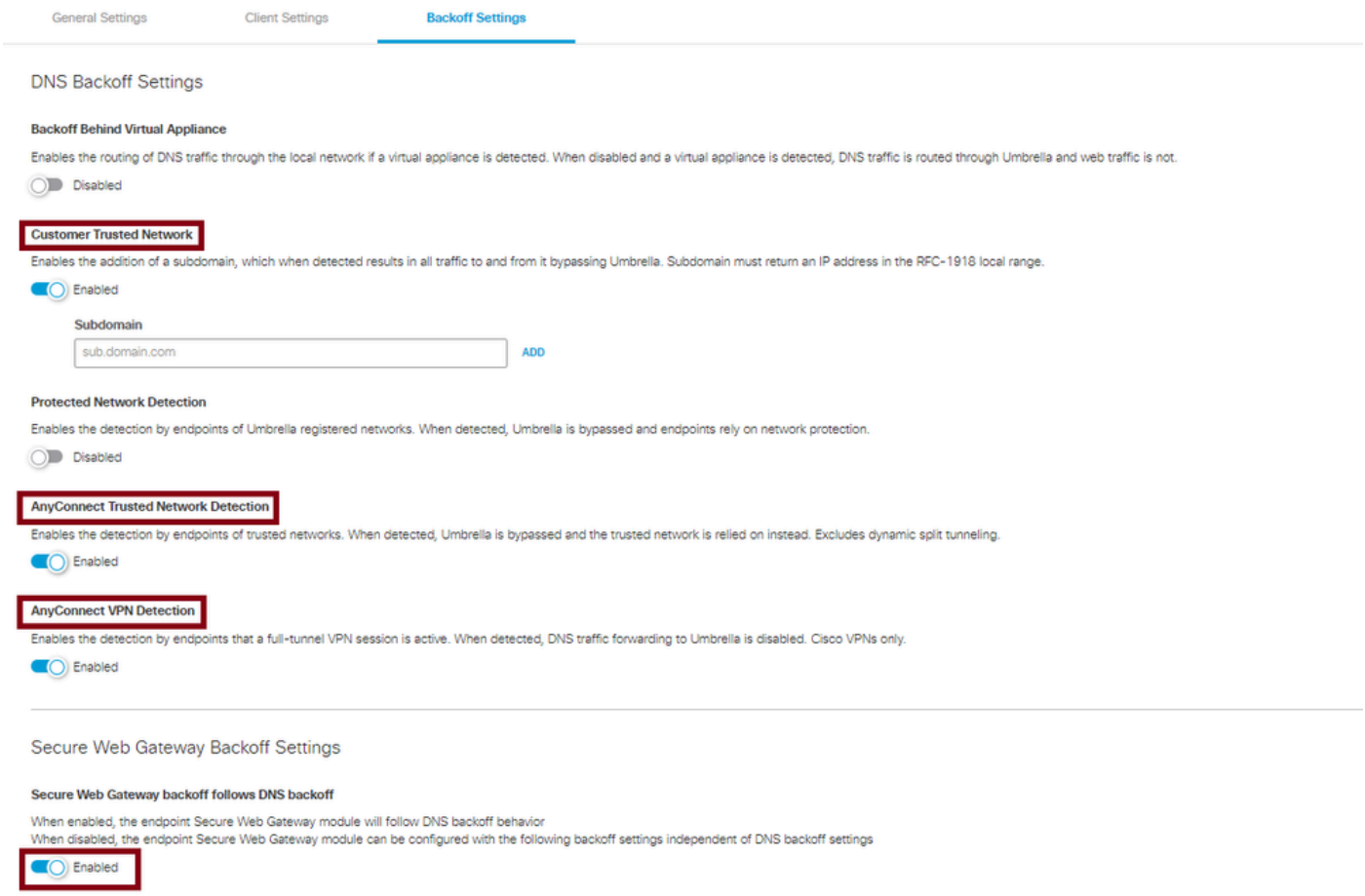
Welke DNS-back-off-instellingen zorgen ervoor dat SWG wordt uitgeschakeld?

Deze DNS-back-off-instellingen zorgen ervoor dat SWG terugkeert:

- Customer Trusted Network: Het instellen van een Customer Trusted Network-domein in de DNS-back-offinstellingen is een van de eenvoudigste methoden. Door een intern domein te hosten dat oplost naar een RFC1918-adres, kunnen zowel DNS als SWG tegelijkertijd back-off maken. Umbrella's client is gecodeerd om dat domein te bevragen. Als het domein met succes wordt opgelost in een privé-IP-adres, wordt het apparaat geïdentificeerd als onderdeel van een privé en beveiligd netwerk, waardoor de DNS-module een back-up maakt. Dit back-offmechanisme wordt ook gerespecteerd door de webmodule, die op dezelfde manier een back-off kan maken wanneer de DNS-module het domein met succes oplost.
- Trusted Network Detection van AnyConnect
- AnyConnect VPN-detectie



Opmerking: De DNS-back-offinstellingen blijven functioneel op Cisco Secure Clients met versies ouder dan 5.1.3.62, omdat deze is geïmplementeerd vóór de ontkoppeling van de DNS- en SWG-back-offinstellingen.

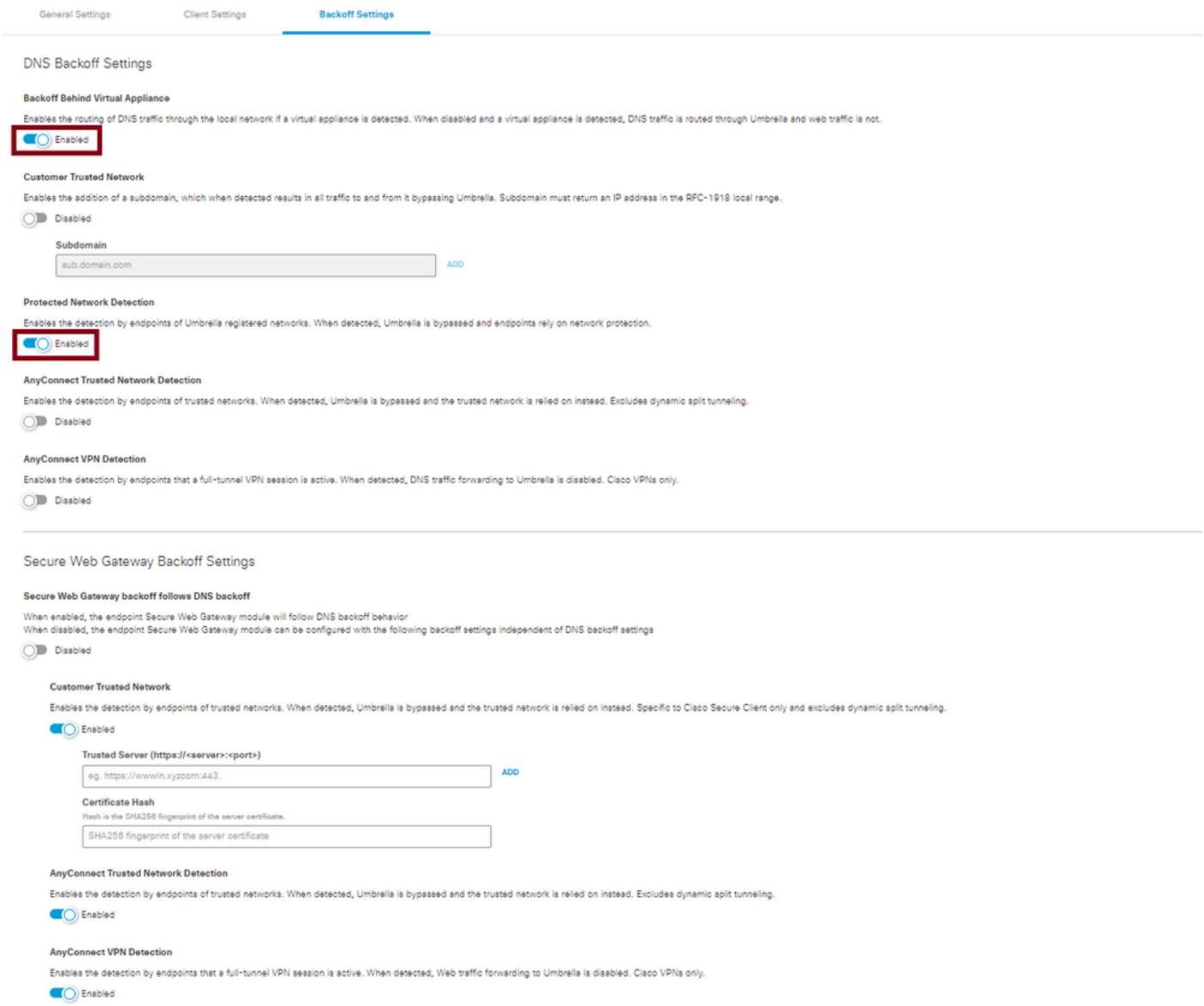


27885424859028

Welke DNS-back-off-instellingen zorgen er niet voor dat SWG wordt uitgeschakeld?

Het configureren van deze twee DNS-back-offfuncties zorgt er niet voor dat SWG zich terugtrekt. Daarom moet u SWG-back-offinstellingen selectief configureren, onafhankelijk van de DNS-configuratiestatus. Dit wordt in het volgende gedeelte nader besproken.

- Back-off achter virtuele apparaten: vanaf AnyConnect 4.10.07061 (MR7) en Secure Client 5.0.02075 (MR2) kan de SWG-module ingeschakeld blijven op netwerken waar een virtuele Umbrella-apparaat aanwezig is. Als u eerder afhankelijk was van de aanwezigheid van een virtueel toestel om de SWG-module en webomleiding op een bepaald netwerk uit te schakelen, kunt u in plaats daarvan Trusted Network Domain of AnyConnect Trusted Network Detection gebruiken.
- Beveiligde netwerkdetectie



27885587178772

Onafhankelijke back-upinstellingen voor SWG

Als deze DNS-back-upfuncties niet zijn ingeschakeld in uw omgeving, kunt u uitsluitend een van de hier beschreven SWG-back-upinstellingen gebruiken om ervoor te zorgen dat SWG uitgeschakeld blijft:

- Vertrouwd netwerk van klant
- Trusted Network Detection van AnyConnect
- AnyConnect VPN-detectie

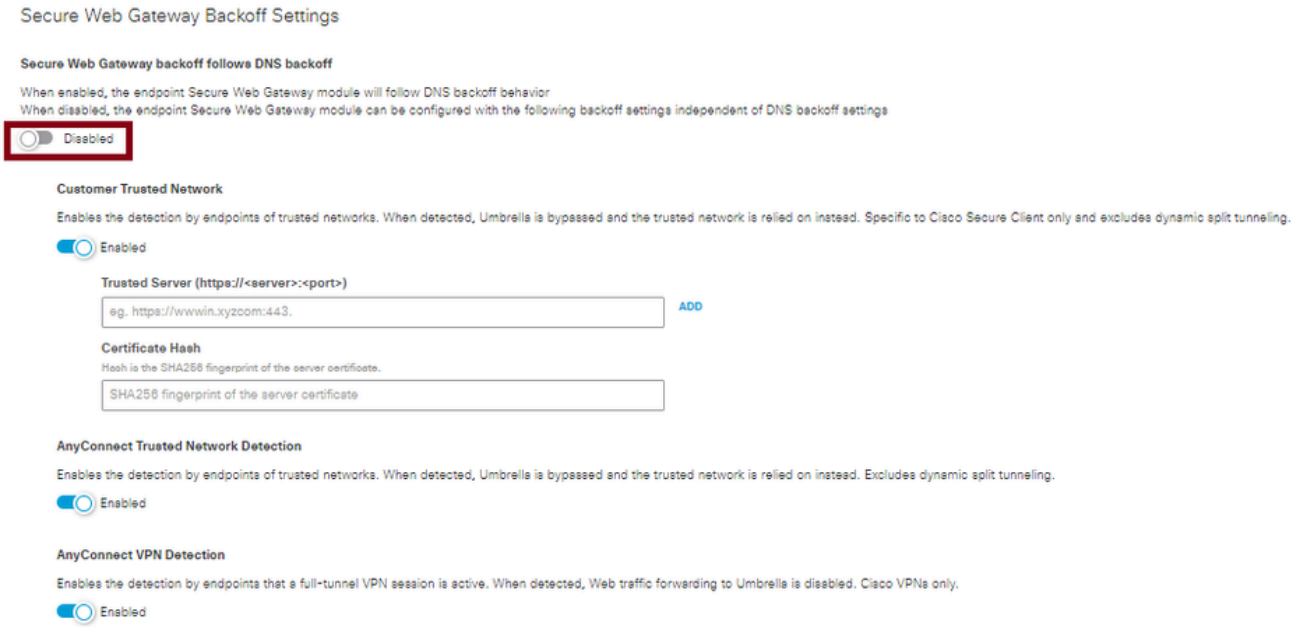
Met deze nieuwe mogelijkheid kan de SWG-module onafhankelijk van de DNS-module werken. Deze functie is beschikbaar voor Cisco Secure Clients met behulp van versie 5.1.3.62 en nieuwer. Configureer een van de expliciete SWG-back-offschakelaars in het dashboard:

- Vertrouwd netwerk van de klant: een optie is om de optie Vertrouwd netwerk van de klant te gebruiken onder de back-upinstellingen van SWG, waarbij u een interne server kunt

configureren die de client kan bereiken om te bevestigen dat deze zich op het beveiligde netwerk bevindt. U moet ervoor zorgen dat de webserver bereikbaar is voor de client, een certificaat op die server verkrijgen en de hash van het certificaat naar het Umbrella-dashboard kopiëren.

De andere twee opties zijn uitsluitend van toepassing op VPN-verbindingen:

- Trusted Network Detection van AnyConnect
- AnyConnect VPN-detectie



27886005743764

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.