Entender as configurações de backoff de DNS e SWG para CSC

Contents

Introdução

Este documento descreve o DNS e as configurações de retirada do Secure Web Gateway (SWG) para o Cisco Secure Client (CSC).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Secure Client.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

Até por volta de 25 de abril de 2024, o comportamento de backoff do módulo SWG do Cisco Secure Client não podia ser controlado independentemente do estado do módulo DNS e dependia das configurações de backoff de DNS para ativar/desativar a proteção SWG. Para lidar com isso, a Umbrella dissociou o comportamento do módulo DNS e do módulo SWG, permitindo o gerenciamento independente conforme necessário. Ele está disponível para Cisco Secure

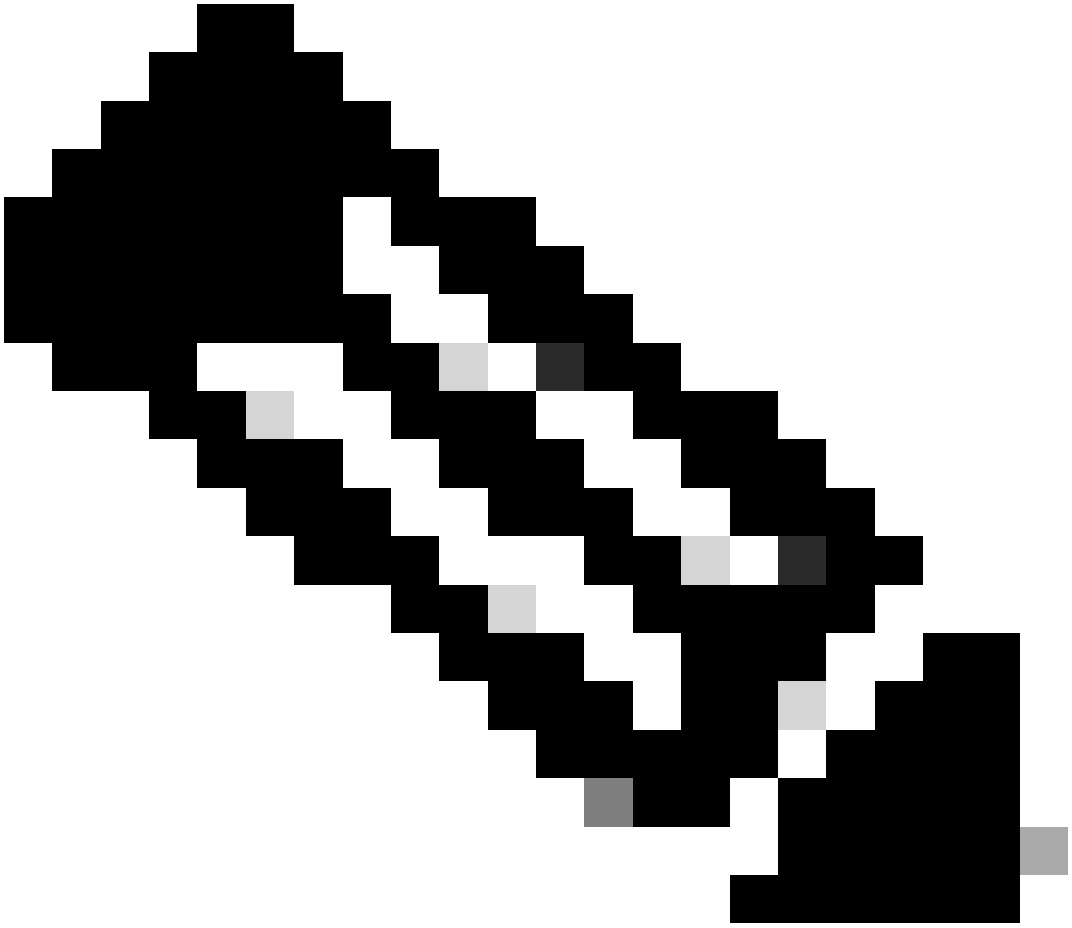
Clients na versão 5.1.3.62 e mais recente, onde a Umbrella desacoplou as configurações de backoff de DNS e SWG para permitir um controle granular aprimorado. Os clientes de versões mais antigas não seguiram o backoff do módulo SWG separado.

Quando o recurso backoff do Secure Web Gateway segue o backoff de DNS está habilitado, o módulo SWG do CSC segue o comportamento do módulo DNS. No entanto, isso não ocorre com todas as configurações de backoff de DNS. Na próxima seção, as configurações de backoff de DNS que o módulo SWG segue ou não segue são detalhadas.

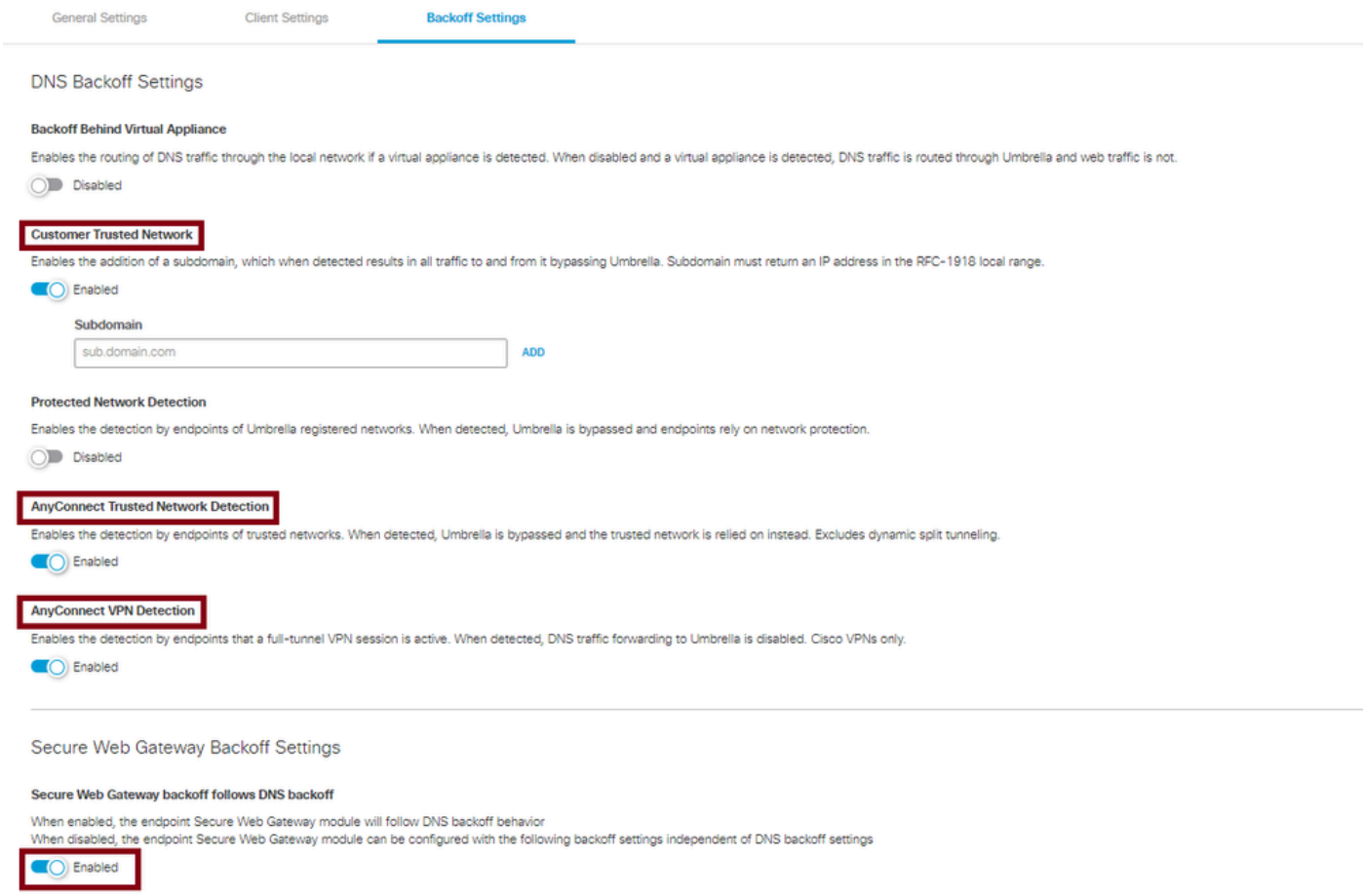
Quais configurações de retirada de DNS fazem com que o SWG seja desativado?

Estas configurações de backoff de DNS fazem com que o SWG seja backoff:

- Rede confiável do cliente: A configuração de um domínio de Rede confiável do cliente nas configurações de backoff de DNS é um dos métodos mais simples. Ao hospedar um domínio interno que resolve para um endereço RFC1918, o DNS e o SWG podem recuar simultaneamente. O cliente do Umbrella é codificado para consultar esse domínio. Se resolver com êxito o domínio para um endereço IP privado, ele identificará o dispositivo como estando em uma rede privada e protegida, fazendo com que o módulo DNS seja desativado. Esse mecanismo de recuo também é respeitado pelo módulo Web, que pode recuar de forma semelhante quando o módulo DNS resolve com êxito o domínio.
- Detecção de rede confiável AnyConnect
- Detecção de VPN AnyConnect



Note: As configurações de backoff de DNS permanecem funcionais nos Cisco Secure Clients que executam versões anteriores a 5.1.3.62, pois foram implementadas antes da dissociação das configurações de backoff de DNS e SWG.

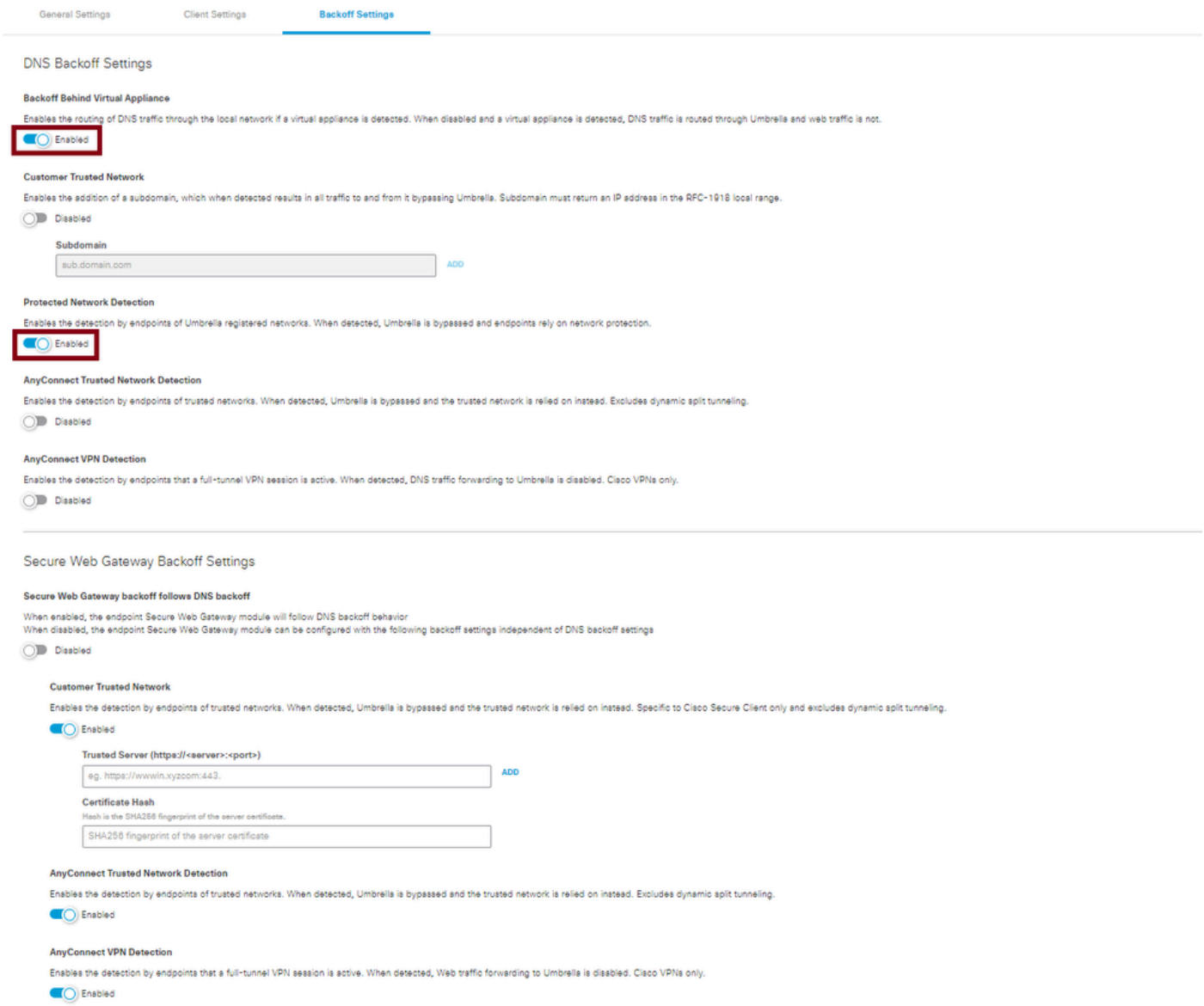


27885424859028

Quais configurações de retirada de DNS não fazem com que o SWG seja desativado?

A configuração desses dois recursos de backoff de DNS não faz com que o SWG se afaste. Portanto, você deve definir as configurações de backoff do SWG de forma seletiva, independentemente do estado de configuração do DNS. Isso será discutido com mais detalhes na próxima seção.

- Retrocesso atrás do dispositivo virtual: A partir do AnyConnect 4.10.07061 (MR7) e Secure Client 5.0.02075 (MR2), o módulo SWG pode permanecer ativado em redes onde um dispositivo virtual Umbrella está presente. Se você estava anteriormente confiando na presença de um dispositivo virtual para desabilitar o módulo SWG e o redirecionamento da Web em uma determinada rede, você pode usar o Domínio de rede confiável ou a Detecção de rede confiável do AnyConnect.
- Detecção de rede protegida



27885587178772

Configurações de recuo de SWG independente

Se esses recursos de backoff de DNS não estiverem ativados em seu ambiente, você poderá utilizar exclusivamente uma das configurações de backoff de SWG descritas aqui para garantir que o SWG permaneça desativado:

- Rede confiável do cliente
- Detecção de rede confiável AnyConnect
- Detecção de VPN AnyConnect

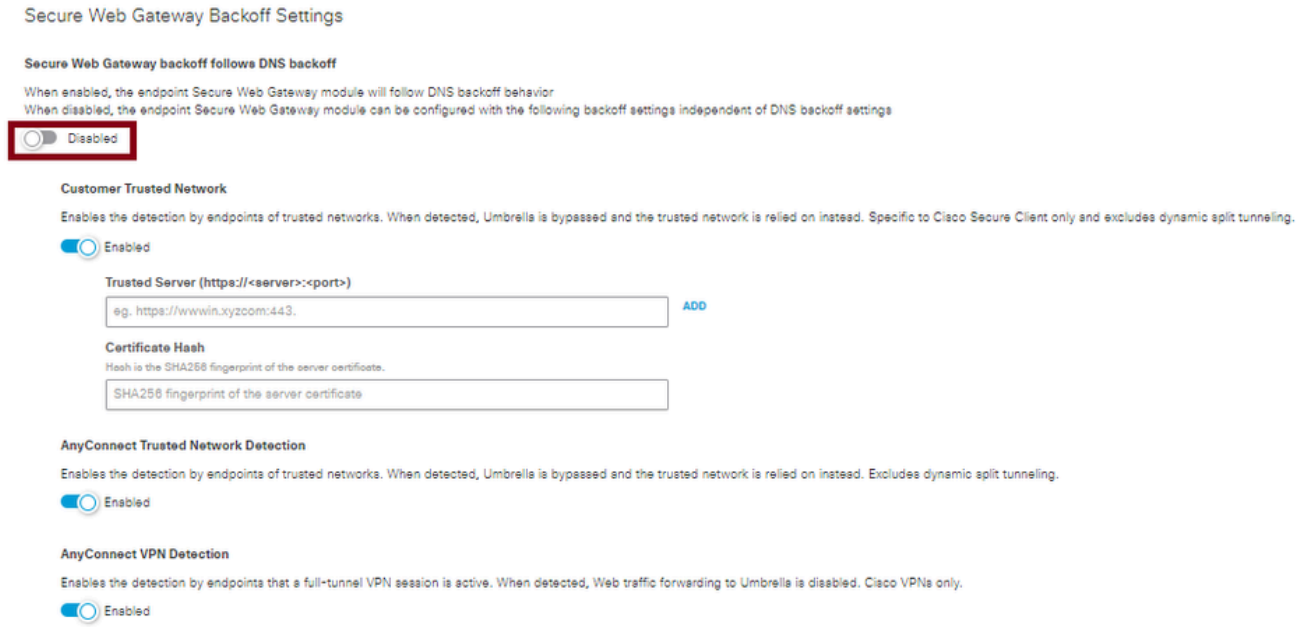
Esse novo recurso permite que o módulo SWG opere independentemente do módulo DNS. Esse recurso está disponível para Cisco Secure Clients usando a versão 5.1.3.62 e mais recente. Configure uma das alternâncias explícitas de backoff do SWG no painel:

- Rede confiável do cliente: Uma opção é usar a opção Rede confiável do cliente nas configurações de backoff do SWG, onde você pode configurar um servidor interno que o

cliente pode acessar para confirmar que está na rede protegida. Você precisa garantir que o servidor Web seja acessível pelo cliente, obter um certificado nesse servidor e copiar o hash do certificado para o painel do Umbrella.

As outras duas opções aplicam-se exclusivamente a conexões VPN:

- Detecção de rede confiável AnyConnect
- Detecção de VPN AnyConnect



27886005743764

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.