

CSCのDNSおよびSWGバックオフ設定について

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[概要](#)

[SWGのバックオフを引き起こすDNSバックオフ設定はどれか？](#)

[SWGのバックオフが行われないDNSバックオフ設定はどれか？](#)

[独立したSWGバックオフ設定](#)

はじめに

このドキュメントでは、Cisco Secure Client(CSC)のDNSおよびセキュアWebゲートウェイ(SWG)バックオフ設定について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco Secure Clientに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

2024年4月25日前後まで、Cisco Secure ClientのSWGモジュールのバックオフ動作は、DNSモジュールの状態に関係なく制御できず、SWG保護を有効/無効にするDNSバックオフ設定に依存していました。これに対処するため、UmbrellaはDNSモジュールとSWGモジュールの動作を分離し、必要に応じて独立した管理を可能にしました。これは、UmbrellaがDNSとSWGバックオフ設定を分離し、きめ細かい制御を強化したCisco Secure Client/バージョン5.1.3.62以降で使用できます。古いバージョンのクライアントは、個別のSWGモジュールのバックオフに従いませんでした。

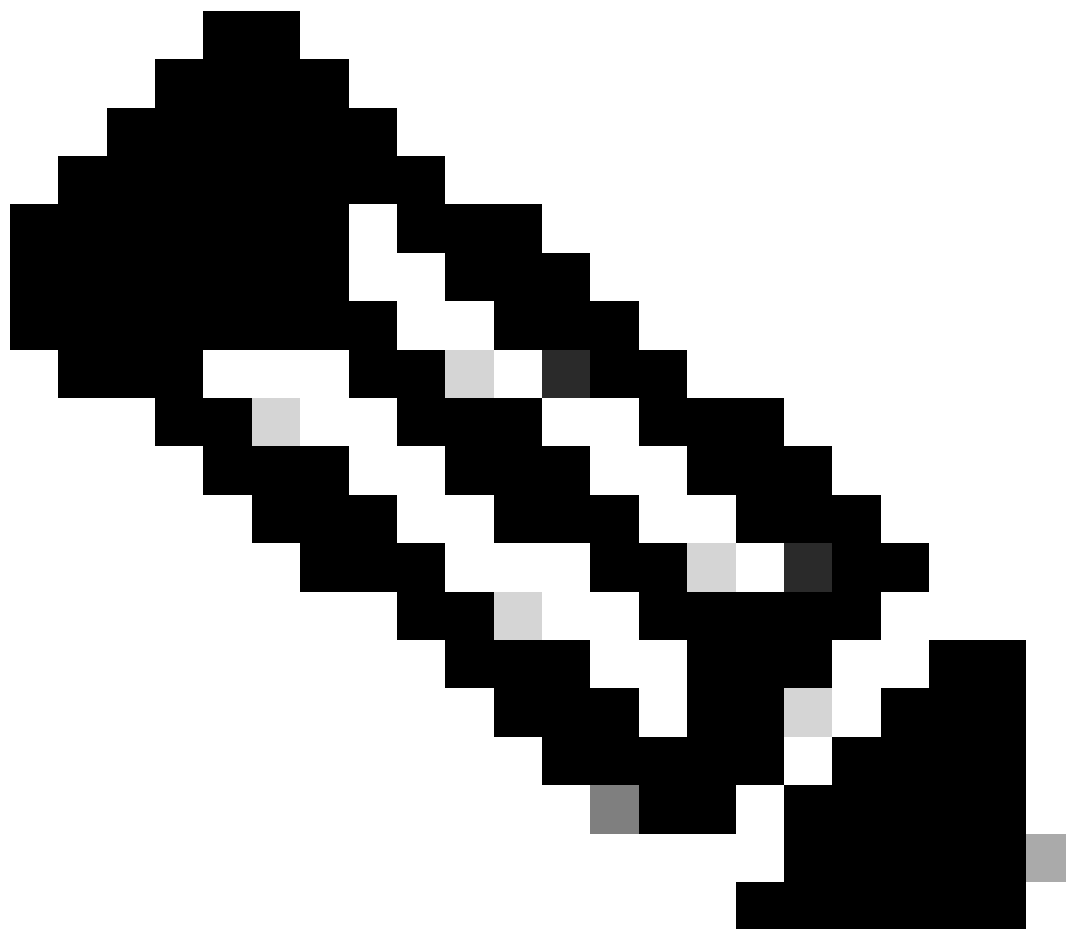
Secure Web Gateway backoff follows DNS backoff機能が有効になっている場合、CSCのSWGモ

ジュールはDNSモジュールの動作に従います。ただし、これは、すべてのDNSバックオフ設定で発生するわけではありません。次のセクションでは、SWGモジュールが従うDNSバックオフ設定または従わないDNSバックオフ設定について詳しく説明します。

SWGのバックオフを引き起こすDNSバックオフ設定はどれか？

次のDNSバックオフ設定により、SWGはバックオフします。

- Customer Trusted Network:DNSバックオフ設定でのCustomer Trusted Networkドメインの設定は、最も簡単な方法の1つです。RFC1918アドレスに解決される内部ドメインをホストすることで、DNSとSWGの両方を同時にバックオフできます。Umbrellaのクライアントは、そのドメインを照会するようにコーディングされています。ドメインがプライベートIPアドレスに正常に解決されると、デバイスがプライベートで保護されたネットワーク上にあることが識別され、DNSモジュールがバックオフします。このバックオフメカニズムは、DNSモジュールがドメインの解決に成功した場合にも同様にバックオフできるWebモジュールでも尊重されます。
- AnyConnect信頼ネットワーク検出
- AnyConnect VPNの検出



注:DNSバックオフ設定は、5.1.3.62より前のバージョンを実行しているCisco Secure Client上では、DNSとSWGバックオフ設定を分離する前に実装されているため、引き続き機能します。

DNS Backoff Settings

Backoff Behind Virtual Appliance

Enables the routing of DNS traffic through the local network if a virtual appliance is detected. When disabled and a virtual appliance is detected, DNS traffic is routed through Umbrella and web traffic is not.

☐ Disabled

Customer Trusted Network

Enables the addition of a subdomain, which when detected results in all traffic to and from it bypassing Umbrella. Subdomain must return an IP address in the RFC-1918 local range.

☒ Enabled

Subdomain

sub.domain.com

ADD

Protected Network Detection

Enables the detection by endpoints of Umbrella registered networks. When detected, Umbrella is bypassed and endpoints rely on network protection.

☐ Disabled

AnyConnect Trusted Network Detection

Enables the detection by endpoints of trusted networks. When detected, Umbrella is bypassed and the trusted network is relied on instead. Excludes dynamic split tunneling.

☒ Enabled

AnyConnect VPN Detection

Enables the detection by endpoints that a full-tunnel VPN session is active. When detected, DNS traffic forwarding to Umbrella is disabled. Cisco VPNs only.

☒ Enabled

Secure Web Gateway Backoff Settings

Secure Web Gateway backoff follows DNS backoff

When enabled, the endpoint Secure Web Gateway module will follow DNS backoff behavior

When disabled, the endpoint Secure Web Gateway module can be configured with the following backoff settings independent of DNS backoff settings

☒ Enabled

27885424859028

SWGのバックオフが行われないDNSバックオフ設定はどれか？

これら2つのDNSバックオフ機能を設定しても、SWGはバックオフしません。そのため、DNSの設定状態に関係なく、SWGバックオフ設定を選択的に設定する必要があります。これについては、次のセクションで詳しく説明します。

- 仮想アプライアンスの背後でのバックオフ：AnyConnect 4.10.07061(MR7)およびSecure Client 5.0.02075(MR2)以降では、Umbrella仮想アプライアンスが存在するネットワークでSWGモジュールを有効なままにできます。以前に仮想アプライアンスの存在に依存して特定のネットワークでSWGモジュールとWebリダイレクションを無効にしていた場合は、代わりにTrusted Network DomainまたはAnyConnect Trusted Network Detectionを使用できます。
- 保護されたネットワーク検出

DNS Backoff Settings

Backoff Behind Virtual Appliance

Enables the routing of DNS traffic through the local network if a virtual appliance is detected. When disabled and a virtual appliance is detected, DNS traffic is routed through Umbrella and web traffic is not.

☒ Enabled

Customer Trusted Network

Enables the addition of a subdomain, which when detected results in all traffic to and from it bypassing Umbrella. Subdomain must return an IP address in the RFC-1918 local range.

☐ Disabled

Subdomain

sub.domain.com

ADD

Protected Network Detection

Enables the detection by endpoints of Umbrella registered networks. When detected, Umbrella is bypassed and endpoints rely on network protection.

☒ Enabled

AnyConnect Trusted Network Detection

Enables the detection by endpoints of trusted networks. When detected, Umbrella is bypassed and the trusted network is relied on instead. Excludes dynamic split tunneling.

☐ Disabled

AnyConnect VPN Detection

Enables the detection by endpoints that a full-tunnel VPN session is active. When detected, DNS traffic forwarding to Umbrella is disabled. Cisco VPNs only.

☐ Disabled

Secure Web Gateway Backoff Settings

Secure Web Gateway backoff follows DNS backoff

When enabled, the endpoint Secure Web Gateway module will follow DNS backoff behavior.

When disabled, the endpoint Secure Web Gateway module can be configured with the following backoff settings independent of DNS backoff settings.

☐ Disabled

Customer Trusted Network

Enables the detection by endpoints of trusted networks. When detected, Umbrella is bypassed and the trusted network is relied on instead. Specific to Cisco Secure Client only and excludes dynamic split tunneling.

☒ Enabled

Trusted Server (https://<server>:<port>)

eg. https://www.xyzoom.com:443

ADD

Certificate Hash

Hash is the SHA256 fingerprint of the server certificate.

SHA256 fingerprint of the server certificate

AnyConnect Trusted Network Detection

Enables the detection by endpoints of trusted networks. When detected, Umbrella is bypassed and the trusted network is relied on instead. Excludes dynamic split tunneling.

☒ Enabled

AnyConnect VPN Detection

Enables the detection by endpoints that a full-tunnel VPN session is active. When detected, Web traffic forwarding to Umbrella is disabled. Cisco VPNs only.

☒ Enabled

27885587178772

独立したSWGバックオフ設定

ご使用の環境でこれらのDNSバックオフ機能が有効になっていない場合は、ここで説明するSWGバックオフ設定のいずれかを排他的に使用して、SWGを無効のままにすることができます。

- お客様の信頼ネットワーク
- AnyConnect信頼ネットワーク検出
- AnyConnect VPNの検出

この新しい機能により、SWGモジュールはDNSモジュールから独立して動作できます。この機能は、バージョン5.1.3.62以降を使用しているCisco Secure Clientで使用できます。ダッシュボードで、次のいずれかの明示的なSWGバックオフトグルを設定します。

- Customer Trusted Network : オプションの1つは、SWGバックオフ設定の下でCustomer Trusted Networkオプションを使用することです。このオプションでは、クライアントがア

クセスできる内部サーバを設定し、そのサーバが保護されたネットワーク上に存在することを確認できます。Webサーバがクライアントから到達可能であることを確認し、そのサーバ上の証明書を取得し、証明書ハッシュをUmbrellaダッシュボードにコピーする必要があります。

他の2つのオプションは、VPN接続にのみ適用されます。

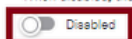
- AnyConnect信頼ネットワーク検出
- AnyConnect VPNの検出

Secure Web Gateway Backoff Settings

Secure Web Gateway backoff follows DNS backoff

When enabled, the endpoint Secure Web Gateway module will follow DNS backoff behavior.

When disabled, the endpoint Secure Web Gateway module can be configured with the following backoff settings independent of DNS backoff settings.



Customer Trusted Network

Enables the detection by endpoints of trusted networks. When detected, Umbrella is bypassed and the trusted network is relied on instead. Specific to Cisco Secure Client only and excludes dynamic split tunneling.

☒ Enabled

Trusted Server (https://<server>:<port>)

eg. https://www.xyz.com:443.

[ADD](#)

Certificate Hash

Hash is the SHA256 fingerprint of the server certificate.

SHA256 fingerprint of the server certificate

AnyConnect Trusted Network Detection

Enables the detection by endpoints of trusted networks. When detected, Umbrella is bypassed and the trusted network is relied on instead. Excludes dynamic split tunneling.

☒ Enabled

AnyConnect VPN Detection

Enables the detection by endpoints that a full-tunnel VPN session is active. When detected, Web traffic forwarding to Umbrella is disabled. Cisco VPNs only.

☒ Enabled

27886005743764

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。