企業ネットワークでのUmbrellaローミングクライアントの設定

内容

はじめに

このドキュメントでは、会社のネットワークでのUmbrellaローミングクライアントの設定について説明します。

概要

Umbrellaローミングクライアントは、リモートユーザを保護するための優れたツールですが、企業ネットワーク上のユーザを保護して、セキュリティのもう1つの層を追加することもできます。ビジネスのニーズに応じて、一部の管理者は社内ネットワークでUmbrellaローミングクライアントの継続的な保護を必要としますが、他の管理者はUmbrellaローミングクライアントを他のUmbrellaポリシーに従って「バックオフ」することを希望します。

Umbrellaは、Umbrellaローミングクライアントがネットワークに入ったときにどのように動作するかに関する柔軟性を提供します。この記事では、これらの異なるアプローチの概要を説明します。

目標

Q) 社内ネットワークでUmbrellaローミングクライアントを無効にする理由は何ですか。

通常、内部および外部DNSを機能させるためにUmbrellaローミングクライアントを無効にする必要はありません。Umbrellaローミングクライアントでは、ドメイン管理機能を使用して、内部DNSトラフィックを通常のDNSサーバに送信します。これにより、Umbrellaローミングクライアントがネットワーク上のエンドポイントで実行されている間、保護と接続の両方を維持できます。

ただし、Roaming Client保護を無効にすることを検討する理由がいくつかあります。

- ネットワークを離れるローミングユーザに対して、異なる「オンネットワーク」および「オフネットワーク」ポリシーを提供する。
- 社内ネットワークで内部DNSサーバを使用すると、キャッシングと発信DNSトラフィックの削減という点でいくつかの利点があります。
- Umbrellaローミングクライアントは、Umbrellaへの接続を確認するためにプローブメッセージを定期的に送信します。クライアントの数が非常に多い場合、この追加トラフィックは不要である可能性があります。

Q) Umbrellaローミングクライアントを会社のネットワーク上で有効のままにしておく必要があるのはなぜですか。

その一方で、ローミングクライアントを常に有効にしておく理由は非常に優れています。

- Umbrellaローミングクライアントコンピューターが常に同じポリシーを使用していることを確認します。
- きめ細かいレポートを作成するために、Umbrellaローミングクライアントのホスト名を（ネットワークIDではなく）レポートで識別可能な状態にします。
- Roaming Clientは、プライバシーを強化するために「暗号化されたDNS」トラフィックを使用します
- セキュアなWebゲートウェイユーザ（AnyConnectを使用）の場合、SWG Webフィルタリングを提供するには、クライアントを有効にしておく必要があります。

動作モード

常にオン

Umbrellaローミングクライアントは、会社のネットワークで使用されても有効なままです。このモードでは、Umbrellaローミングクライアントidを使用してポリシーが設定され、このIDがレポートに表示されます。

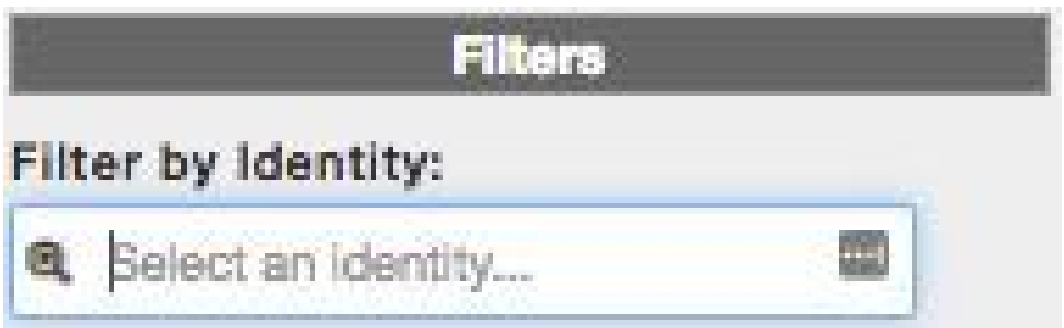
ポリシー	Umbrellaローミングクライアントidは常に使用されます。
レポート	Umbrellaローミングクライアントidは、マシン単位の精度を提供するレポートに常に表示されます
DNS トラフィック	• Umbrellaローミングクライアントは、企業ネットワーク上にある場合でも、Umbrellaに直接DNSクエリを送信し続けます。 • Umbrellaに送信されるクエリは暗号化され、セキュリティが強化されま

	す。 • 「内部ドメイン」のクエリは、通常のDNSサーバにルーティングされ、Umbrellaには送信されません。
プローブメッセージ	Umbrellaローミングクライアントは、引き続きプローブメッセージを送信して、Umbrellaの可用性を判断します。

Always ONモードを設定する方法：

1. Identities > Roaming Computersの順に移動します。
2. (Roaming client settings)アイコンをクリックします。
3. Disable DNS redirection while on an Umbrella Protected Networkをオフにして、Saveをクリックします。
4. Umbrellaローミングクライアント用に別のポリシーを作成し、それが最高の優先順位（リストの一番上）であることを確認します。 Umbrellaローミングクライアントポリシーは、ネットワークIDに基づくどのポリシーよりも高い優先順位にする必要があります。

通常のネットワークポリシーを使用する
Umbrellaローミングクライアントが有効になり、Umbrellaと直接通信し続けますが、ポリシーとレポートの両方の目的でネットワークIDが使用されます。このモードをアクティブにするには、単にネットワークポリシーをUmbrellaローミングクライアントポリシーよりも高い優先順位に設定します。

ポリシー	ネットワークポリシーは、保護されたネットワークで使用されます。これにより、異なるオン/オフネットワークポリシーが可能になります。
レポート	• レポートは、プライマリIDとしてネットワークIDに関連付けられます。 • レポーティングでは、Umbrellaローミングクライアントのホスト名を使用して検索し、そのクライアントのみの結果をフィルタリングできます。 

DNS トラフィック	• Umbrellaローミングクライアントは、企業ネットワーク上にある場合でも、Umbrellaに直接DNSクエリを送信し続けます。 • Umbrellaに送信されるクエリは暗号化され、セキュリティが強化されます。 • 「内部ドメイン」のクエリは、通常のDNSサーバにルーティングされ、Umbrellaには送信されません。
プローブメッセージ	Umbrellaローミングクライアントは、引き続きプローブメッセージを送信して、Umbrellaの可用性を判断します。

「通常のネットワークポリシーを使用する」方法:

1. Identities > Roaming Computersの順に移動します。
2. (Roaming client settings)アイコンをクリックします。
3. Disable DNS redirection while on an Umbrella Protected Networkをオフにして、Saveをクリックします。
4. ネットワーク用に別のポリシーを作成します。 ネットワークのポリシーが、ローミングクライアントに基づくすべてのポリシーよりも高い優先順位であることを確認します。

保護されたネットワークの背後で無効にする（小規模なネットワークに最適）
Umbrellaローミングクライアントは、保護されたネットワーク上にあることを検出すると、「バックオフ」できます。つまり、ポリシーとレポートの両方にネットワークIDが使用されます。

このモードは、「通常のネットワークポリシーの使用」モードの動作と似ていますが、Umbrellaローミングクライアントが実際に自身を無効にし、DNSトラフィックを干渉しない点が異なります。

ポリシー	ネットワークポリシーは、保護されたネットワークで使用されます。これにより、異なるオン/オフネットワークポリシーが可能になります。
レポート	保護されたネットワーク上では、レポートに対するマシン単位の粒度はありません。レポートはネットワークIDにのみ関連付けられます。
DNS トラフィック	保護されたネットワーク上では、Umbrellaローミングクライアントは DNSクエリに干渉せず、通常の内部DNSサーバに送信されます。

プローブメッセージ	Umbrellaローミングクライアントは、プローブメッセージを送信し続け、保護されたネットワーク上にあることを確認します。

保護されたネットワークの背後でディセーブルにするの設定方法：

1. Identities > Roaming Computersの順に移動します。
2. (Roaming client settings)アイコンをクリックします。
3. Disable DNS redirection while on an Umbrella Protected Networkを選択して、Saveをクリックします。
4. Policies > Policies Listの順に移動します。
5. ネットワーク用に別のポリシーを作成します。 ネットワークのポリシーが、Umbrellaローミングクライアントに基づくポリシーよりも高い優先順位であることを確認します。
6. ローカルDNSサーバがUmbrellaリゾルバに転送され、Umbrellaダッシュボードに正しく登録されている必要があります。
7. この機能が動作するには、クライアントワークステーションで使用される出力IPが、内部DNSサーバで使用される出力IPと同じネットワークIDに登録されている必要があります。詳細については、この記事を参照してください。

信頼されたネットワークドメインの背後で無効にする（大規模なネットワークに最適）

お客様が設定した「信頼できるネットワークドメイン」を選択できるようになりました。 クライアントはこのDNSドメイン（Aレコード）の解決を試み、ドメインが正常に解決されると保護を無効にします。 これは、クライアントが会社のネットワーク上にあるときにのみ解決される内部専用のDNSレコードです。

ポリシー	クライアントは、信頼される側のドメインが検出されるたびにバックオフを行い、必ずしもUmbrellaポリシーやフィルタリングを受信するとは限りません。 社内ネットワークにポリシーが適用されていることを確認するために、他のUmbrella機能（ネットワーク保護など）を追加することをお勧めします。
レポート	クライアントは、信頼される側のドメインが検出されるたびにバックオフを行い、必ずしもUmbrellaポリシーやフィルタリングを受信するとは限りません。 ネットワークが他のUmbrella機能（ネットワーク保護など）によって保護されている場合、トラフィックはネットワークIDの下のレポートに表示されます。
DNS トラフィック	信頼できるネットワークでは、Umbrellaローミングクライアントは DNSクエリに干渉せず、通常の内部DNSサーバに送信されます。

プローブメッセージ	Umbrellaローミングクライアントは、この状態のDNS「プローブ」テストの大部分を無効にし、ローミングクライアントによって生成されるトラフィックの量を大幅に削減します。

信頼できるネットワークドメインの設定方法：

1. 内部DNSサーバでDNS Aレコードを作成します（例： magic.mydomain.tld）。
    1. レコードは「サブドメイン」である必要があります（3つ以上のDNSラベル）。
    2. レコードは内部RFC-1918アドレスに解決される必要があります
    3. 記録が公に存在しないように注意してください
2. Identities > Roaming Computersの順に移動します。
3. (Roaming client settings)アイコンをクリックします。
4. Trusted Network Domainオプションを選択し、ドメイン名（例：magic.mydomain.tld）を入力します。 [Save] をクリックします。

Umbrella仮想アプライアンスでのUmbrella Roamingクライアントの使用

Umbrellaの「Insights」製品の一部として(Platform and Insightsパッケージ内)、ネットワーク内でDNSフォワーダとして機能する仮想アプライアンス(VA)を提供します。このVAは、ネットワーク上のDNS要求のソースに関する可視性を得るための鍵であり、Active Directoryの統合にも必要です。

デフォルトでは、Umbrellaローミングクライアントは、VAがDNS転送に使用されていることを検出すると無効になります。VAがDNSサーバとして割り当てられている場合（DHCPまたはスタティック設定を使用）、Umbrellaローミングクライアントはこれを検出し、自身を無効にします。

VAバックオフ

ポリシー	VA Backoffを有効にすると、選択したポリシーの決定にVA Identityが使用されます。ポリシーは、次のIDに基づいて作成できます。 • ADユーザ（AD統合が有効な場合のみ） • ADコンピュータ（AD統合が有効な場合のみ） • 内部ネットワーク • 包括サイト名。 ポリシーの優先順位の詳細については、ここをクリックしてください。
レポート	VAバックオフが有効になっていると、Umbrellaローミングクライアントは VAの背後では無効になり、レポートには表示されません。レポートは次のいずれかの形式

	で記録されます。 • ADユーザ（AD統合が有効な場合のみ） • ADコンピュータ（AD統合が有効な場合のみ） • 内部ネットワーク • 包括サイト名。 また、要求ごとに内部クライアントのIPアドレスが記録されます。 
DNS トラフィック	• Umbrellaローミングクライアントは DNSクエリに干渉せず、仮想アプライアンスに送信されます。 • VAは外部DNSクエリをUmbrella（暗号化）に転送します。 • VAは必要に応じて内部DNSクエリをルーティングし、設定された内部DNSサーバに転送します。
プローブメッセージ	Umbrellaローミングクライアントは引き続きUmbrellaにプローブメッセージを送信しますが、これは低いレートで行われます。

VAバックオフの設定方法：

1. この機能はデフォルトで有効になっていますが、ステータスを確認できます（オプションで無効にすることもできます）
2. Identities > Roaming Computersの順に移動します。
3. (Roaming client settings)アイコンをクリックします。
4. VA Backoffオプションを選択します

Cisco Umbrella AnyConnect Roamingセキュリティモジュール

Cisco AnyConnect用のUmbrellaモジュールは、上記と同じ動作モードをすべてサポートしています。 2つの追加のAnyConnect固有のモードも使用できます。 これらのモードは両方とも、Identities > Roaming ComputersページのUmbrellaダッシュボードでイネーブルにできますが、AnyConnect VPNプロファイル内で追加の設定が必要です。

- AnyConnectの信頼ネットワーク検出を尊重します。
  この機能により、Cisco AnyConnectが信頼ネットワーク上にあると判断した場合に、Umbrellaセキュリティモジュールが無効になります。 これは、AnyConnectの信頼ネットワーク検出機能を使用してネットワークを識別します。 信頼されたドメイン、DNSサーバ、およびURLを使用して、会社のネットワークを特定できます。 詳細については、AnyConnectのドキュメントを参照してください。

- フルトンネルVPNセッションがアクティブな間はローミングクライアントを無効にする
  この機能を有効にすると、AnyConnectがフルトンネル（またはTunnel All DNS）VPNに接続されている場合、Umbrellaモジュールは無効になります。

無効にすると、ローミングクライアントはDNSトラフィックをフィルタしません。そのため、ネットワーク保護機能などの他のセキュリティによってネットワークが保護されていることを確認することが重要です。

その他の情報

会社のネットワークでRoaming Clientを無効にしたいが、制御の強化が必要な場合、または他のオプションについて話し合う場合は、Cisco Umbrellaサポートにお問い合わせください。

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。