

セキュアコネクトユーザのリモートアクセスのためのSIGポリシーの設定

内容

[はじめに](#)

[概要](#)

[DNSポリシー](#)

[ファイアウォールポリシー](#)

[Webポリシー](#)

[WebユーザーID](#)

[DLPポリシー](#)

[DLPユーザID](#)

はじめに

このドキュメントでは、セキュアコネクトユーザのリモートアクセスのSIGポリシーを作成する方法について説明します。

概要

このKnowledgebaseの記事は、Umbrellaのリモートアクセス(VPNaaS)機能を含むSecure Connect/パッケージを使用しているお客様に適用されます。

管理者は、AnyConnect経由でリモートアクセスに接続されたローミングユーザに適用するUmbrellaファイアウォール、Web、およびデータ損失ポリシーを設定できます。

DNSポリシー

AnyConnectリモートアクセスVPN接続を介して、Umbrellaリゾルバ (例 : 208.67.222.222) にDNSクエリを送信することができます。ただし、UmbrellaダッシュボードでDNSトラフィックの識別、ポリシー、またはレポートを有効にすることはできません。

- これはDNS解決のみを提供するため、通常は推奨されません。
- VPN DNS設定で外部DNSリゾルバを使用すると、内部DNSゾーンの解決が妨げられます。

DNS Servers

Your organization's private DNS Servers. Up to 10 servers.

4410210378004

DNSクエリのID、ポリシー、およびレポートを追加するには、次の3つの方法のいずれかを検討する必要があります。

- ・（推奨） - [Umbrella AnyConnect Roamingモジュール](#)を展開します（[展開] > [コンピュータの移動]から）。外部DNSトラフィックは、「ローミングコンピュータ」IDが適用されたUmbrellaに直接送信されます。このモジュールでは、オプションの[ADユーザID](#)もサポートされています。
- ・ オンプレミスのDNSサーバからUmbrellaにトラフィックを転送し、[ネットワーク](#) IDを使用してトラフィックを識別します。すべてのユーザが同じポリシー/IDを受け取り、詳細なユーザレポートは作成されません。
- ・ オンプレミスネットワークで[Umbrella仮想アプライアンス](#)を使用して、トラフィックをUmbrellaに転送します。DNSクエリは、内部（VPNプールのIPアドレス）で識別できます。[AD統合](#)を追加できます。追加のオンプレミスコンポーネントのインストールが必要です。

次の例は、個々のAnyConnectクライアントに対してDNSポリシー(Policies > DNS Policies)を設定する方法を示しています。これは、Umbrella AnyConnect Roamingモジュールが展開されている場合にのみ可能です。

Policies dictate the security protection, category settings, and individual destination lists you can apply to some or all of your identities. Policies also control log levels and how block pages are displayed, in descending order, so your top policy will be applied before the second if they share the same identity. To change the priority of your policies, simply drag and drop the policy in the order you want.

Content Category Migration Incomplete.

You must migrate all legacy content categories. For more information, see [Umbrella's Help](#).

[MIGRATE CONTENT CATEGORIES](#)

What would you like to protect?

Select Identities

Search Identities

All Identities / Roaming Computers

☒ AC_W10

1 Selected

[REMOVE ALL](#)

☐ AC_W10

4410210455444



注:AnyConnectにUmbrellaモジュールを使用する場合、スプリットトンネリングの設定に応じて、オプションでDNSトラフィックをトンネルの内部または外部に送信できます。

ファイアウォールポリシー

ファイアウォールポリシーは、リモートアクセス(AnyConnect)クライアントとインターネットの間のトラフィックに適用されます。 Deployments > Firewall Policyの順に選択し、[Manage Firewall](#)のドキュメントに従ってルールを設定します。

既定のファイアウォール規則は、リモートアクセスクライアントに適用されます。 リモートアクセスユーザ用の特定のポリシーを作成する場合、オプションで新しいファイアウォールポリシーを作成し、ソーストンネルIDとして「Remote Access orgid:<ID>」を選択できます。 同じファイアウォールポリシーがすべてのリモートアクセスユーザに適用されます。

- ファイアウォールポリシーは、RAクライアントとプライベート/ブランチネットワーク間のアクセスの制御には使用されません。これは、オンプレミスファイアウォールで制御する必要があります。

- すべてのUmbrellaファイアウォールルールと同様に、これらのルールはリモートアクセスクライアントの発信接続を制御します。着信接続は許可されません。
- リモートアクセスクライアントの送信元IPアドレスは、常にVPNプールから動的に割り当てられます。
 - 「送信元IP」を使用して特定のコンピュータのルールを作成することは、IPが動的に再割り当てされるため、お勧めできません
 - 「ソースCIDR」範囲を使用することで、特定のリモートアクセスデータセンターのユーザに影響するルールを作成できます。各データセンターは、「Deployments > Remote Access」ページで設定される異なるVPNプール範囲を提供します。

Rule Criteria

Specify the protocols, IPs, network tunnels, and ports to be allowed or blocked.

Protocol

Any Protocol

Applications

Any

Source Tunnels

Specify Tunnels

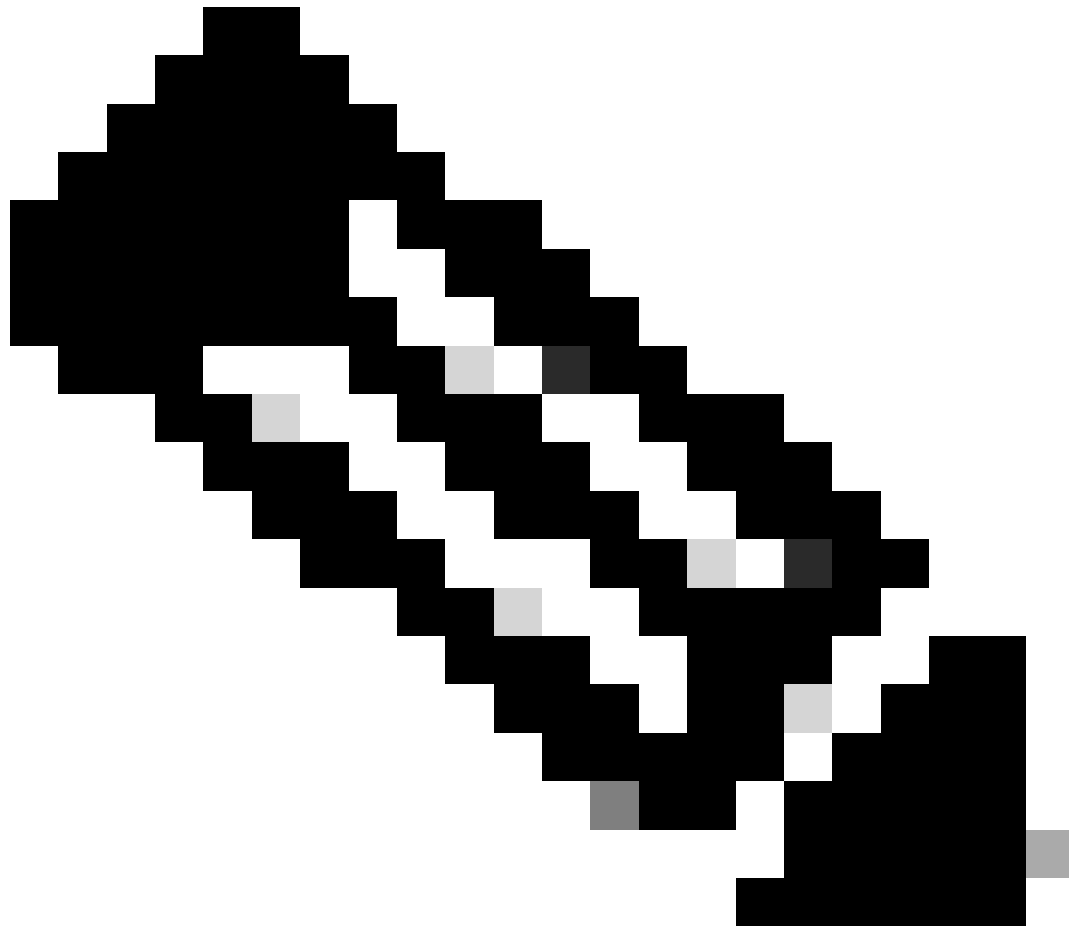
Remote Access orgId:5372429

CLEAR

Source IPs/CIDRs

Any

4409322341524



注：ユーザ単位のIDは、ファイアウォールポリシーでは使用できません。

Webポリシー

Webポリシーは、リモートアクセス(AnyConnect)クライアントとインターネットの間のトラフィックに適用されます。 Deployments > Web Policiesの順に選択し、Manage Web Policiesのドキュメントに従ってルールを設定します。

- Webポリシーは、RAクライアントとプライベート/ブランチWebサーバ間のアクセスを制御するために使用されません。 Webポリシーは外部Webサイトにのみ適用されます。

デフォルトのWebポリシーは、リモートアクセスクライアントに適用されます。 ただし、リモートアクセスクライアント専用のセキュリティ設定を定義する[新しいルールセットを作成すること](#)をお勧めします。 ルールセットのIDを定義するときに、トンネルのリストからRemote Access orgid:<ID> を選択します。 同じWebポリシーがすべてのリモートアクセスユーザーに適用されます。

ルールセットを作成した後、コンテンツカテゴリフィルタリングおよびアプリケーション設定を定義する[Webルールを追加](#)できます。

Ruleset Identities

You must select ruleset identities for them to be added to this ruleset and have this ruleset enabled. Identities matching the ruleset can then be evaluated against the rules within the ruleset. This has the effect of a logical AND between the ruleset identity and the rule identity. Identities are first added to Umbrella through the Identities page. For more information, see Umbrella's [Help](#).

☐  AD Groups

☐  AD Users 4 >

☒  Tunnels 12 >

☐  Networks 1 >

☐  Roaming Computers

☐  Internal Networks (All Tunnels)

1 Selected REMOVE ALL

 Remote Access orgId:5372429

CANCEL

SAVE

4409322363924

WebユーザーID

デフォルトでは、リモートアクセストラフィックをユーザ単位またはグループ単位で制御することはできません。同じポリシーが、「リモートアクセスグリッド」IDに基づくすべてのRAトラフィックに適用されます。ユーザ/グループIDを追加するには、次の2つのオプションがあります。

- [AnyConnect Umbrella Roaming](#)セキュリティモジュールをインストールし、[SWGエージェント機能](#)を有効にします。エージェントは、「ローミングコンピュータ」IDを適用したWebトラフィックをUmbrella SWGに直接送信します。このモジュールでは、オプションの[ADユーザID](#)もサポートされています。
- 「Remote Access orgid」IDに影響を与えるWebルールセットで[SAML](#)を有効にします。リモートアクセスに接続した後、Webブラウザトラフィックを生成するときに、RAユーザは2回目のSAMLによる認証を求められます。

注:AnyConnectにUmbrellaモジュールを使用する場合、スプリットトンネリングの設定に応じて、SWGトラフィックをトンネルの内部または外部にオプションで送信できます。

次の例は、個々のAnyConnectクライアントに対してDNSポリシーを設定する方法(Policies > DNS Policies)を示しています。これは、Umbrella AnyConnect Roaming Moduleが展開されている場合にのみ可能です。

Ruleset disabled. You must select at least one ruleset identity to enable this ruleset so that its settings and rules are evaluated and enforced.

Ruleset Rules

ADD RULE

Priority	Rule Name	Rule Action	Identities
1	Rule 1	Block	1 Anyconnect Client AC_W10

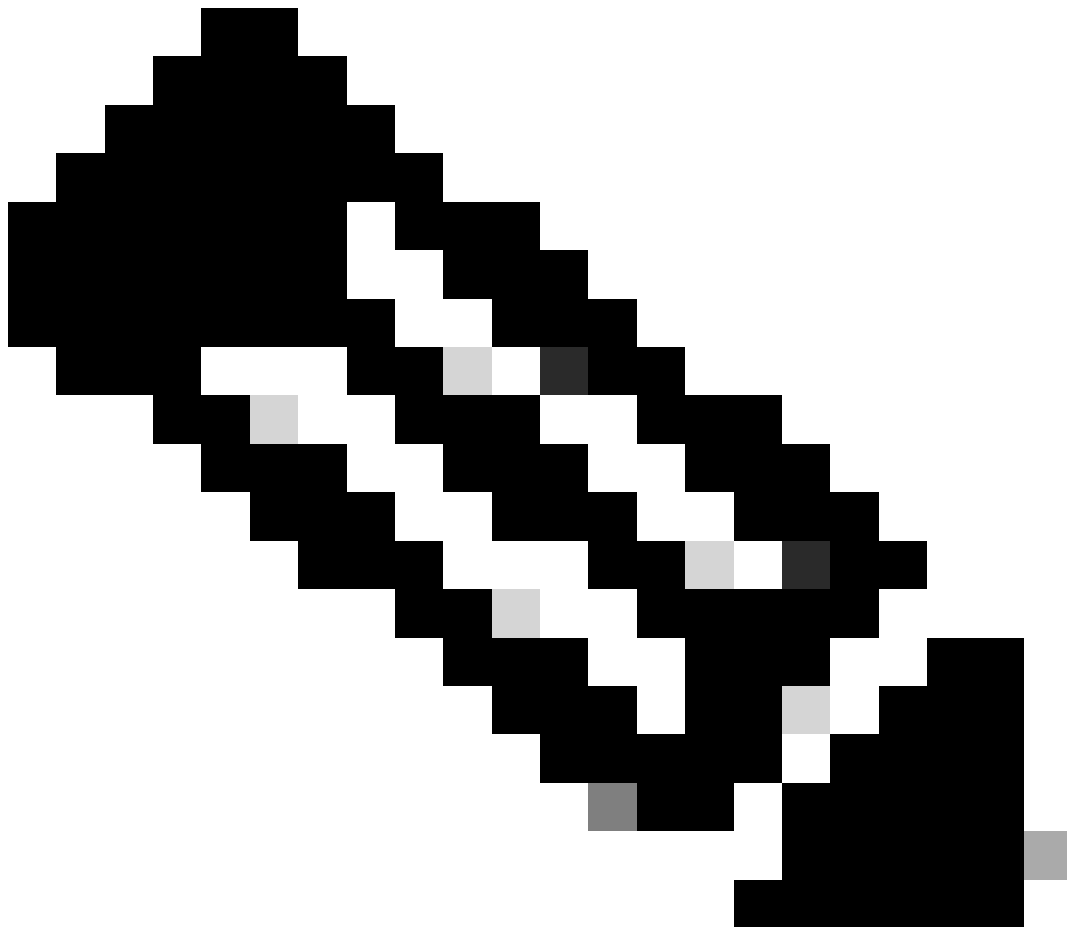
1 Selected

SAVE

DLPポリシー

データ損失ポリシーは、リモートアクセス(AnyConnect)クライアントとインターネットの間のトラフィックに適用されます。ドキュメント「[データ保護ポリシーの管理](#)」に従って、「展開」>「データ損失防止ポリシー」でルールを設定します。

- DLPポリシーは、RAクライアントとプライベート/ブランチWebサーバ間のアクセスを制御するために使用されません。DLPポリシーは、外部のトラフィックWebサイトにのみ適用されます。



注：DLPポリシーを適用するには、最初にリモートアクセスユーザー用のWebルールセットを作成しておく必要があります。WebルールセットでHTTPS復号化が有効になっている必要があります。

データ保護ルールのIDを選択する場合は、Remote Access orgid:<ID>.を選択します。同じデータ保護ポリシーがすべてのユーザーに適用されます。DLPルールを完成させるには、[DLP分類子](#)を選択または定義する必要があります。

Identities

Select identities to add them to this rule.

Search Identities

All Identities

☐

AD Groups

☐

AD Users

4 >

☒

Tunnels

12 >

☐

Networks

1 >

☐

Roaming Computers

☐

Internal Networks (All Tunnels)

1 Selected

REMOVE ALL

☒

Remote Access orgId:5372429

4409322428820

DLPユーザID

DLPは、セキュアなWebゲートウェイ (Webポリシー) からユーザIDを取得します。 ユーザIDを追加する方法については、「Webポリシー」セクションを参照してください。

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。