



Zero Trust アクセス

次のトピックでは、Zero Trust アプリケーションポリシーの概要、およびポリシーを設定および展開する方法について説明します。

- [Zero Trust アクセスについて \(1 ページ\)](#)
- [Threat Defense と Zero Trust アクセスの連携の仕組み \(3 ページ\)](#)
- [Zero Trust アクセスを使用する理由 \(4 ページ\)](#)
- [Zero Trust アクセス設定のコンポーネント \(4 ページ\)](#)
- [Zero Trust アクセスのワークフロー \(6 ページ\)](#)
- [Zero Trust アクセスの制限事項 \(7 ページ\)](#)
- [Zero Trust アプリケーションポリシーの前提条件 \(7 ページ\)](#)
- [Zero Trust アプリケーションポリシーの管理 \(8 ページ\)](#)
- [Zero Trust アプリケーションポリシーの作成 \(9 ページ\)](#)
- [アプリケーショングループの作成 \(10 ページ\)](#)
- [アプリケーションの作成 \(12 ページ\)](#)
- [Zero Trust アクセスポリシーの対象デバイスの設定 \(14 ページ\)](#)
- [Zero Trust アプリケーションポリシーの編集 \(15 ページ\)](#)
- [Zero Trust セッションのモニタリング \(17 ページ\)](#)
- [Zero Trust アクセスの履歴 \(19 ページ\)](#)

Zero Trust アクセスについて

Zero Trust アクセス機能は、Zero Trust ネットワークアクセス (ZTNA) の原則に基づいています。ZTNAは、暗黙の信頼を排除するゼロトラストセキュリティモデルです。このモデルは、ユーザーとリクエストのコンテキストを確認し、アクセスが許可された場合のリスクを分析した後、最小限のアクセス権を付与します。

Zero Trust アクセスにより、外部の SAML ID プロバイダー (IdP) ポリシーを使用して、ネットワークの内部 (オンプレミス) または外部 (リモート) から保護された Web ベースのリソースとアプリケーションへのアクセスを認証および承認できます。

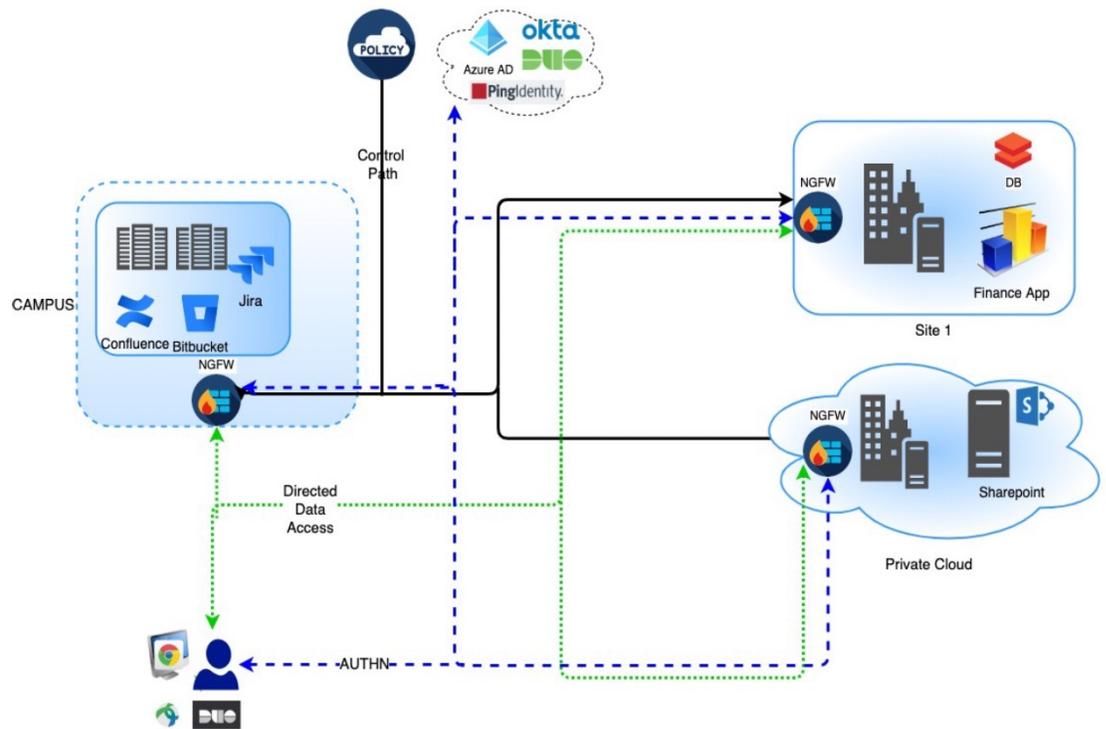
機能は以下のとおりです。

- Duo、Azure AD、Okta、およびその他のアイデンティティプロバイダーなど、複数の SAML ベースのアイデンティティプロバイダーをサポートします。
- Cisco Secure Client などのクライアントアプリケーションは、Secure Access 用のエンドポイント（クライアントデバイス）では必要ありません。
- アクセスと認証はブラウザを介して行われます。
- Web アプリケーション（HTTPS）のみをサポート。
- Duo Health などのエージェントを介してクライアントデバイスのポスチャがサポートされます。これを使用してデバイスのポスチャを Duo のポリシーで評価し、評価に基づいてアクセス権を付与します。同じ機能は、エージェントによるポスチャ評価をサポートするサードパーティのアイデンティティプロバイダー（Okta や PingID）と組み合わせて実行できます。
- HTTP リダイレクト SAML バインディングのサポート。
- 一連のアプリケーションで Zero Trust 保護を簡単に有効にできるアプリケーショングループのサポート。
- Zero Trust アプリケーショントラフィックでの Threat Defense の侵入とマルウェアの保護の活用。

Cisco Secure Firewall Management Center の Web インターフェイスを使用して、プライベートアプリケーションを定義し、定義したアプリケーションに脅威ポリシーを割り当てられる Zero Trust アプリケーションポリシーを作成できます。ポリシーはアプリケーション固有なので、管理者は、各アプリケーションの脅威認識に基づいてインスペクションレベルを決定します。

Threat Defense と Zero Trust アクセスの連携の仕組み

図 1: Threat Defense の展開



1. リモートまたはオンプレミスのユーザーは、ブラウザを使用して、エンドポイントからアプリケーションに接続するための HTTPS 要求を送信します。
2. HTTPS 要求は、アプリケーションを保護するファイアウォールによって代行受信されます。
3. ファイアウォールは、認証のためにアプリケーションに設定されている IdP にユーザーをリダイレクトします。



(注) この図では、各ファイアウォールが一連の Web アプリケーションを保護しています。ユーザーは、認証および承認後に、ファイアウォールの背後にあるアプリケーションに直接アクセスできます。

4. 認証および承認プロセスが完了すると、ファイアウォールにより、ユーザーはアプリケーションへのアクセスが許可されます。

Zero Trust アクセスを使用する理由

Zero Trust アクセスは、アプリケーションアクセスへの適用ポイントとして、Threat Defense の既存の展開を活用します。これにより、リモートおよびオンプレミスユーザーによる、アプリケーションごとの承認およびアプリケーションごとのトンネルを使用した、プライベートアプリケーションへのセグメント化されたアクセスが可能になります。

この機能により、ユーザーからネットワークが非表示になり、ユーザーは承認されたアプリケーションのみにアクセスできます。ネットワーク内の1つのアプリケーションに対して承認されても、ネットワーク上の他のアプリケーションに対する暗黙的な承認は与えられないため、攻撃対象領域が大幅に減少します。つまり、アプリケーションへのすべてのアクセスを明示的に承認する必要があります。

Threat Defense に Zero Trust アクセス機能を追加すると、ネットワークに別のデバイスを追加でインストールして管理することなく、より安全なアクセスモデルに移行できます。

この機能は、クライアントを必要とせず、アプリケーションごとのアクセスを実現できるため、管理が容易です。

Zero Trust アクセス設定のコンポーネント

新しい設定では、Zero Trust アプリケーションポリシー、アプリケーショングループ、およびアプリケーションを指定します。

- **Zero Trust アプリケーションポリシー** : アプリケーショングループ、グループ化されたアプリケーション、またはグループ化されていないアプリケーションを指定します。セキュリティゾーンとセキュリティ制御の設定は、グループ化されていないすべてのアプリケーションとアプリケーショングループに対してグローバルレベルで関連付けられます。

デフォルトで、グローバルポートプールがポリシーに割り当てられています。このプールから、設定されている各プライベートアプリケーションに一意のポートが自動的に割り当てられます。

Zero Trust アプリケーションポリシーでは、アプリケーショングループ、グループ化されたアプリケーション、またはグループ化されていないアプリケーションを指定します。

- **アプリケーショングループ** : SAML 認証設定を共有し、必要に応じてセキュリティゾーンとセキュリティ制御設定を共有できるアプリケーションの論理グループを指定します。

アプリケーショングループは、グローバルポリシーからセキュリティゾーンとセキュリティ制御の設定を継承し、値を上書きできます。

アプリケーショングループを作成すると、同じ SAML IdP 設定を使用して複数のアプリケーションを認証できます。アプリケーショングループの一部であるアプリケーションは、アプリケーショングループの SAML 設定を継承します。これにより、アプリケーションごとに SAML を設定する必要がなくなります。アプリケーショングループが作成されると、IdP を設定せずに新しいアプリケーションを追加できます。

エンドユーザーがグループの一部であるアプリケーションにアクセスしようとしたときに、ユーザーはアプリケーショングループに対して初回認証されます。ユーザーが同じアプリケーショングループの一部である他のアプリケーションにアクセスしようとするとき、ユーザーは認証のために IdP に再度リダイレクトされることなくアクセスできます。これにより、アプリケーションアクセスの要求で IdP が過負荷になるのを防ぎ、制限が有効になっている場合に IdP の使用を最適化できます。

- **アプリケーション**：以下の2つのタイプがあります。
 - **グループ化されていないアプリケーション**：スタンドアロンアプリケーションです。SAML設定は、アプリケーションごとに設定する必要があります。アプリケーションは、グローバルポリシーからセキュリティゾーンとセキュリティ制御の設定を継承し、アプリケーションによって上書きできます。
 - **グループ化されたアプリケーション**：アプリケーショングループの下にグループ化された複数のアプリケーションです。SAML設定はアプリケーショングループから継承され、上書きできません。ただし、セキュリティゾーンとセキュリティ制御の設定は、アプリケーションごとに上書きできます。

設定には以下の証明書が必要です。

- **アイデンティティ証明書**：この証明書は、Threat Defense がアプリケーションとしてマスカレードするために使用されます。Threat Defense は SAML サービスプロバイダー (SP) として動作します。この証明書は、プライベートアプリケーションの FQDN と一致するワイルドカードまたはサブジェクト代替名 (SAN) 証明書である必要があります。これは、Threat Defense で保護されているすべてのアプリケーションに共通の証明書です。
- **[IdP証明書 (IdP Certificate)]**：IdP は、定義されたアプリケーションまたはアプリケーショングループごとに証明書を提供します。この証明書は、Threat Defense が着信 SAML アサーションで IdP の署名を検証できるように設定する必要があります。



(注) IdP 証明書は通常、メタデータファイル内に含まれています。それ以外の場合、ユーザーはアプリケーションの設定中に IdP 証明書をすぐに使用できるようにしておく必要があります。

- **アプリケーション証明書**：ユーザーからアプリケーションに送信される暗号化トラフィックは、検査のためにこの証明書を使用して Threat Defense によって復号されます。

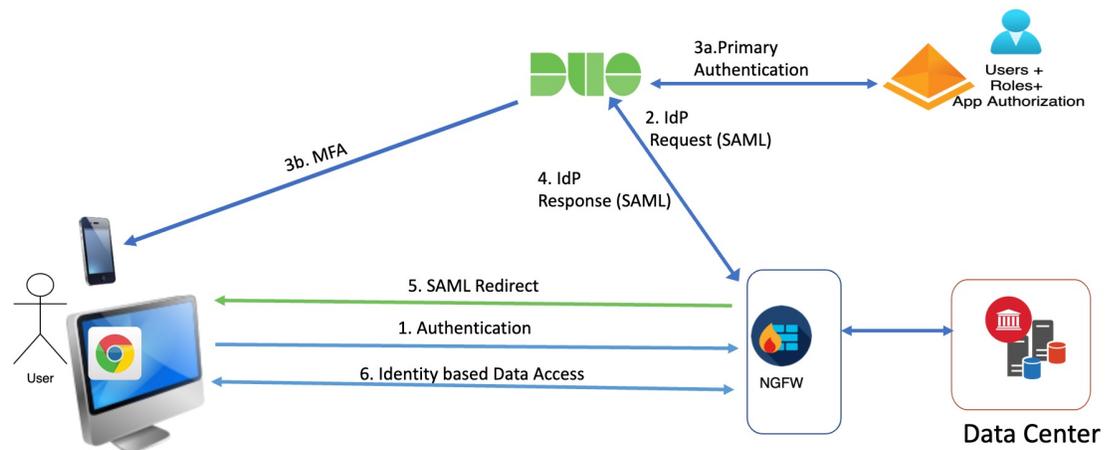


(注) この証明書は、IPS やマルウェア検査を実施していない場合でも、接続を許可するためにヘッダー内の Cookie を確認するために必要です。

Zero Trust アクセスのワークフロー

この図は、Zero Trust アクセスのワークフローを示しています。

図 2: Zero Trust アクセスのワークフロー



ワークフローは次のようになります。

1. ユーザーがブラウザにアプリケーションの URL を入力します。
 - HTTPS 要求が有効な場合、ユーザーはマッピングされたポートにリダイレクトされず（ステップ 6）。
 - HTTPS 要求が無効な場合、ユーザーはアプリケーションごとの認証のために送信されます（ステップ 2）。
2. ユーザーは、設定されたアイデンティティプロバイダー（IdP）にリダイレクトされます。
3.
 1. ユーザーは、設定されたプライマリ認証ソースにリダイレクトされます。
 2. ユーザーは、設定されたセカンダリ多要素認証（設定されている場合）で認証する必要があります。
4. IdP が Threat Defense に SAML 応答を送信します。ユーザー ID やその他の必要なパラメータが、ブラウザを介して SAML 応答から取得されます。
5. ユーザーはアプリケーションにリダイレクトされます。
6. 検証が成功すると、ユーザーにアプリケーションへのアクセスが許可されます。

Zero Trust アクセスの制限事項

- Webアプリケーション（HTTPS）のみがサポートされています。復号除外が必要なシナリオはサポートされていません。
- SAML IdP のみサポートしています。
- IPv6 はサポートされていません。NAT66、NAT64、および NAT46 のシナリオはサポートされていません。
- この機能は、Snort 3 が有効になっている場合にのみ Threat Defense で使用できます。
- 保護された Web アプリケーションのハイパーリンクにはすべて相対パスが必要で、個々のモードのクラスタではサポートされていません。
- 仮想ホストで、または内部ロードバランサの背後で実行されている保護された Web アプリケーションでは、同じ外部 URL と内部 URL を使用する必要があります。
- 個々のモードのクラスタではサポートされていません。
- 厳密な HTTP ホストヘッダー検証が有効になっているアプリケーションではサポートされません。
- アプリケーションサーバーが複数のアプリケーションをホストし、TLS Client Hello の Server Name Indication (SNI) ヘッダーに基づいてコンテンツを提供する場合、Zero Trust アプリケーション設定の外部 URL は、その特定のアプリケーションの SNI と一致する必要があります。

Zero Trust アプリケーションポリシーの前提条件

前提条件タイプ	説明
ライセンスング	<ul style="list-style-type: none"> • エクスポート制御機能を備えたスマートライセンスアカウント。 • (任意) IPS および脅威ライセンス：セキュリティ制御を使用する場合に必要です。

前提条件タイプ	説明
設定	プライベートアプリケーションのFQDNと一致するワイルドカードまたはサブジェクト代替名 (SAN) 証明書を作成します。詳細については、「 証明書の登録オブジェクトの追加 」を参照してください。
	プライベートアプリケーションへのアクセスが制限されるセキュリティゾーンを作成します。詳細については、「 セキュリティゾーンおよびインターフェイスグループオブジェクトの作成 」を参照してください。

Zero Trust アプリケーションポリシーの管理

Zero Trust アプリケーションポリシーを作成、編集、削除できます。

手順

ステップ 1 [ポリシー (Policies)] > [アクセス制御 (Access Control)] > [Zero Trustアプリケーション (Zero Trust Application)] の順に選択します。

ステップ 2 ゼロトラスト アクセス ポリシーを管理するには以下を実行します。

- 作成: [新規ポリシー (New Policy)] をクリックします。 [Zero Trust アプリケーションポリシーの作成 \(9 ページ\)](#) を参照してください。
- 編集: [編集 (Edit)] () をクリックします。 [Zero Trust アプリケーションポリシーの編集 \(15 ページ\)](#) を参照してください。
- レポート: [レポート (Report)] () をクリックします。
- 削除: [削除 (Delete)] () をクリックします。

ステップ 3 [Save (保存)] をクリックします。

次のタスク

Threat Defense に設定を展開する前に、警告が出ていないことを確認してください。設定変更を展開するには、『[Cisco Secure Firewall Management Center アドミニストレーションガイド](#)』の「設定変更の展開」をご覧ください。

Zero Trust アプリケーションポリシーの作成

このタスクでは、Zero Trust アプリケーションポリシーを設定します。

始める前に

[Zero Trust アプリケーションポリシーの前提条件 \(7 ページ\)](#) に示されているすべての前提条件を満たしていることを確認します。

手順

- ステップ 1** [ポリシー (Policies)] > [アクセス制御 (Access Control)] > [Zero Trust アプリケーション (Zero Trust Application)] の順に選択します。
- ステップ 2** [ポリシーを追加 (Add Policy)] をクリックします。
- ステップ 3** [全般 (General)] セクションで、[名前 (Name)] フィールドにポリシー名を入力します。説明フィールドは任意です。
- ステップ 4** [ドメイン名 (Domain Name)] フィールドに、ドメイン名を入力します。
ドメイン名が DNS に追加されていることを確認します。このドメイン名は、アプリケーションのアクセス元の Threat Defense ゲートウェイ インターフェイスに解決されます。このドメイン名は、アプリケーショングループ内のすべてのプライベートアプリケーションの ACS URL を生成するために使用されます。
- ステップ 5** [アイデンティティ証明書 (Identity Certificate)] ドロップダウンリストから既存の証明書を選択します。
Add (+) アイコンをクリックして、証明書登録オブジェクトを設定します。詳細については、「[証明書の登録オブジェクトの追加](#)」を参照してください。
- ステップ 6** [セキュリティゾーン (Security Zone)] ドロップダウンリストからセキュリティゾーンを選択します。
Add (+) アイコンをクリックして、新しいセキュリティゾーンを追加します。
セキュリティゾーンを追加するには、「[セキュリティゾーンおよびインターフェイス グループオブジェクトの作成](#)」を参照してください。
- ステップ 7** [グローバルポートプール (Global Port Pool)] セクションに、デフォルトのポート範囲が表示されます必要に応じて変更を加えます。ポート値の範囲は 1024 ~ 65535 です。このプールの一意のポートは、各プライベートアプリケーションに割り当てられます。
(注) このポート範囲は、既存の NAT 範囲と競合しない範囲にする必要があります。
- ステップ 8** (任意) [セキュリティ管理 (Security Controls)] セクションで、侵入またはマルウェアとファイルポリシーを追加します。

- [侵入ポリシー (Intrusion Policy)] : ドロップダウンリストからデフォルトのポリシーを選択するか、**Add (+)** アイコンをクリックして新しいカスタム侵入ポリシーを作成します。詳細については、最新バージョンの [Cisco Secure Firewall Management Center Snort 3 コンフィギュレーションガイド \[英語\]](#) の「Creating a Custom Snort 3 Intrusion Policy」のトピックを参照してください。
- [変数セット (Variable Set)] : ドロップダウンリストからデフォルトの変数セットを選択するか、**Add (+)** アイコンをクリックして新しい変数セットを作成します。詳細については、「[変数セットの作成](#)」を参照してください。
 - (注) 変数セットを使用するには、管理対象デバイスの Cisco Secure Firewall Threat Defense IPS ライセンスが必要です。
- [マルウェアおよびファイルポリシー (Malware and File Policy)] : ドロップダウンリストから既存のポリシーを選択します。**Add (+)** アイコンをクリックして、新しいマルウェアとファイルのポリシーを作成します。詳細については、[ファイルポリシーの管理](#)を参照してください。

ステップ 9 [保存 (Save)] をクリックして、ポリシーを保存します。

次のタスク

1. アプリケーショングループの作成 [アプリケーショングループの作成 \(10 ページ\)](#) を参照してください。
2. アプリケーションを作成します。 [アプリケーションの作成 \(12 ページ\)](#) を参照してください。
3. Zero Trust アプリケーションポリシーをデバイスに関連付けます。 [Zero Trust アクセスポリシーの対象デバイスの設定 \(14 ページ\)](#) を参照してください。
4. 設定変更を展開します。『[Cisco Secure Firewall Management Center アドミニストレーションガイド](#)』の「設定変更の展開」をご覧ください。

アプリケーショングループの作成

始める前に

[Zero Trust アプリケーションポリシーの作成 \(9 ページ\)](#)

手順

ステップ 1 [アプリケーショングループの追加 (Add Application Group)] をクリックします。

- ステップ 2** [アプリケーショングループ (Application Group)] セクションで、[名前 (Name)] フィールドに名前を入力し、[次へ (Next)] をクリックします。
- ステップ 3** [SAML サービスプロバイダー (SP) メタデータ (SAML Service Provider (SP) Metadata)] セクションで、データが動的に生成されます。[エンティティ ID (Entity ID)] フィールドと [Assertion Consumer Service (ACS) URL] フィールドの値をコピーするか、[SP メタデータのダウンロード (Download SP Metadata)] をクリックして、このデータを XML 形式でダウンロードして IdP に追加します。[次へ (Next)] をクリックします。
- ステップ 4** [SAML ID プロバイダー (IdP) メタデータ (SAML Identity Provider (IdP) Metadata)] セクションで、以下のいずれかの方法でメタデータを追加します。
- **XML ファイルのアップロード** : ファイルを選択するか、XML ファイルをドラッグアンドドロップします。

[エンティティ ID (Entity ID)]、[シングルサインオン URL (Single Sign-On URL)]、および [IdP 証明書 (IdP Certificate)] の詳細が表示されます。
 - **手動設定** : 以下の手順を実行します。
 - [エンティティ ID (Entity ID)] : サービスプロバイダーを一意に識別するために SAML IdP で定義されている URL を入力します。
 - [シングルサインオン URL (Single Sign-On URL)] : SAML ID プロバイダーサーバーにサインインするための URL を入力します。
 - [IdP 証明書 (IdP Certificate)] : IdP によって署名されたメッセージを検証するために、Threat Defense に登録された IdP の証明書を選択します。

Add (+) アイコンをクリックして、新しい証明書登録オブジェクトを設定します。詳細については、[証明書の登録の追加](#)を参照してください。
 - [後で設定 (Configure Later)] : IdP メタデータがない場合は、後で設定できます。
- [次へ (Next)] をクリックします。
- ステップ 5** [再認証間隔 (Re-authentication Interval)] セクションで、[タイムアウト間隔 (Timeout Interval)] フィールドに値を入力し、[次へ (Next)] をクリックします。

[再認証間隔 (Re-authentication Interval)] では、ユーザーが再認証する必要があるタイミングを決める値を入力できます。
- ステップ 6** [セキュリティゾーンとセキュリティ管理 (Security Zones and Security Controls)] セクションでは、セキュリティゾーンと脅威の設定が親ポリシーから継承されます。これらの設定は上書きできます。[次へ (Next)] をクリックします。
- ステップ 7** 設定のサマリーを確認します。[編集 (Edit)] をクリックして、いずれかのセクションの詳細を変更します。[終了 (Finish)] をクリックします。
- ステップ 8** [保存 (Save)] をクリックします。

アプリケーショングループが作成され、[Zero Trustアプリケーション (Zero Trust Application)] ページに表示されます。

次のタスク

1. [アプリケーションの作成 \(12 ページ\)](#)。
2. 設定変更を展開します。『[Cisco Secure Firewall Management Center アドミニストレーションガイド](#)』の「設定変更の展開」をご覧ください。

アプリケーションの作成

このタスクを使用して、グループ化されたアプリケーションまたはグループ化されていないアプリケーションを作成します。

始める前に

1. [Zero Trust アプリケーションポリシーの作成 \(9 ページ\)](#)。
2. [アプリケーショングループの作成 \(10 ページ\)](#) (グループ化されたアプリケーションにのみ必要)。

手順

ステップ 1 [ポリシー (Policies)] > [アクセス制御 (Access Control)] > [Zero Trustアプリケーション (Zero Trust Application)] の順に選択します。

ステップ 2 ポリシーを選択します。

ステップ 3 [アプリケーションの追加 (Add Application)] をクリックします。

ステップ 4 [アプリケーション設定 (Application Settings)] セクションで、以下のフィールドに入力します。

- [アプリケーション名 (Application Name)] : アプリケーション名を入力します。
- [外部URL (External URL)] : ユーザーがアプリケーションにアクセスするために使用する URL を入力します。
- [アプリケーションURL (Application URL)] : デフォルトでは、外部 URL がアプリケーションURLとして使用されます。別のURLを指定するには、[外部URLをアプリケーションURLとして使用 (Use External URL as Application URL)] チェックボックスをオフにします。

Threat Defense で内部 DNS を使用する場合、アプリケーションへの解決を確実にするために、アプリケーション URL はその DNS 内のエントリと一致している必要があります。

- [アプリケーション証明書 (Application Certificate)] : プライベートアプリケーションの証明書を選択します。Add () アイコンをクリックして、内部証明書オブジェクトを設定します。詳細については、「[内部証明書オブジェクトの追加](#)」を参照してください。

- [IPv4送信元変換 (IPv4 Source Translation)] : ドロップダウンリストから NAT の送信元ネットワークを選択します。Add () アイコンをクリックして、ネットワークオブジェクトを作成します。詳細については、「[ネットワーク](#)」を参照してください。

このネットワークオブジェクトまたはオブジェクトグループは、着信要求のパブリックネットワーク送信元 IP アドレスを企業のネットワーク内のルーティング可能な IP アドレスに変換するために使用されます。

(注) [ホスト (Host)] または [範囲 (Range)] タイプのオブジェクトまたはオブジェクトグループのみがサポートされます。

- [アプリケーショングループ (Application Group)] : ドロップダウンリストからアプリケーショングループを選択します。[アプリケーショングループの作成 \(10 ページ\)](#) を参照してください。

(注) このフィールドは、グループ化されていないアプリケーションには適用されません。

ステップ 5 [次へ (Next)] をクリックします。

ステップ 6 アプリケーションのタイプに応じて処理が異なります。

- グループ化されたアプリケーションの場合、[SAMLサービスプロバイダー (SP) メタデータ (SAML Service Provider (SP) Metadata)]、[SAML IDプロバイダー (IdP) メタデータ (SAML Identity Provider (IdP) Metadata)]、および[再認証間隔 (Re-authentication Interval)] はアプリケーショングループから継承されるため、ユーザーが設定する必要はありません。

- グループ化されていないアプリケーションの場合は、以下の手順を実行します。

1. [SAMLサービスプロバイダー (SP) メタデータ (SAML Service Provider (SP) Metadata)] セクションで、データが動的に生成されます。IdP の [エンティティID (Entity ID)] または [Assertion Consumer Service (ACS) URL] をコピーするか、[SPメタデータのダウンロード (Download SP Metadata)] をクリックして、このデータを XML 形式でダウンロードして IdP に追加します。[次へ (Next)] をクリックします。

2. [SAML IDプロバイダー (IdP) メタデータ (SAML Identity Provider (IdP) Metadata)] セクションで、以下のいずれかの方法でメタデータを追加します。

- **XML ファイルのアップロード** : ファイルを選択するか、XML ファイルをドラッグアンドドロップします。

[エンティティID (Entity ID)]、[シングルサインオンURL (Single Sign-On URL)]、および [IdP証明書 (IdP Certificate)] の詳細が表示されます。

- **手動設定** : 以下の手順を実行します。

- [エンティティID (EntityID)] : サービスプロバイダーを一意に識別するために SAML IdP で定義されている URL を入力します。
- [シングルサインオンURL (Single Sign-On URL)] : SAML ID プロバイダーサーバーにサインインするための URL を入力します。
- [IdP証明書 (IdP Certificate)] : IdP によって署名されたメッセージを検証するために、Threat Defense に登録された IdP の証明書を選択します。

Add(+) アイコンをクリックして、新しい証明書登録オブジェクトを設定します。詳細については、[証明書の登録の追加](#)を参照してください。

- [後で設定 (Configure Later)] : IdP メタデータがない場合は、後で設定できます。

[次へ (Next)] をクリックします。

3. [再認証間隔 (Re-authentication Interval)] セクションで、[タイムアウト間隔 (Timeout Interval)] フィールドに値を入力し、[次へ (Next)] をクリックします。[再認証間隔 (Re-authentication Interval)] では、ユーザーが再認証する必要があるタイミングを決める値を入力できます。

ステップ7 [セキュリティゾーンとセキュリティ管理 (Security Zones and Security Controls)] セクションでは、セキュリティゾーンと脅威の設定が親ポリシーまたはアプリケーショングループから継承されます。これらの設定は上書きできます。[次へ (Next)] をクリックします。

ステップ8 設定のサマリーを確認します。[編集 (Edit)] をクリックして、いずれかのセクションの詳細を変更します。[終了 (Finish)] をクリックします。

ステップ9 [保存 (Save)] をクリックします。

アプリケーションは、[Zero Trustアプリケーション (Zero Trust Application)] ページに一覧表示され、デフォルトで有効になっています。

次のタスク

1. [Zero Trust アクセスポリシーの対象デバイスの設定 \(14 ページ\)](#)。
2. 設定変更を展開します。『[Cisco Secure Firewall Management Center アドミニストレーションガイド](#)』の「設定変更の展開」をご覧ください。

Zero Trust アクセスポリシーの対象デバイスの設定

各 Zero Trust アクセスポリシーは、複数のデバイスを対象にできますが、各デバイスで一度に展開されるポリシーは1つです。

始める前に

1. [Zero Trust アプリケーションポリシーの作成 \(9 ページ\)](#)。
2. [アプリケーショングループの作成 \(10 ページ\)](#)。
3. [アプリケーションの作成 \(12 ページ\)](#)。

手順

ステップ 1 [ポリシー (Policies)] > [アクセス制御 (Access Control)] > [Zero Trust アプリケーション (Zero Trust Application)] の順に選択します。

ステップ 2 ポリシーを選択します。

ステップ 3 [対象デバイス (Targeted Devices)] をクリックします。

ステップ 4 以下のメソッドの 1 つを使用してポリシーを展開するデバイスを選択します。

- [使用可能なデバイス (Available Devices)] リストでデバイスを選択し、[>>] または **Add** (+) アイコンをクリックします。
- [選択されたデバイス (Selected Devices)] リストからデバイスを削除するには、デバイスを選択し、[<<] または [削除 (Delete)] (🗑️) アイコンをクリックします。

ステップ 5 [適用 (Apply)] をクリックしてポリシーの割り当てを保存します。

ステップ 6 [保存 (Save)] をクリックしてポリシーを保存します。

次のタスク

設定変更を展開します。『[Cisco Secure Firewall Management Center アドミニストレーション ガイド](#)』の「設定変更の展開」をご覧ください。

Zero Trust アプリケーションポリシーの編集

Zero Trust アプリケーションポリシー、アプリケーショングループ、またはアプリケーションの設定を編集できます。

手順

ステップ 1 [ポリシー (Policies)] > [アクセス制御 (Access Control)] > [Zero Trust アプリケーション (Zero Trust Application)] の順に選択します。

ステップ 2 編集する Zero Trust アプリケーションポリシーの横にある [編集 (Edit)] (✎) をクリックします。

ステップ 3 Zero Trust アプリケーションポリシーを編集します。

次のような設定の変更やアクションの実行が可能です。

- 名前と説明：ポリシー名の横の **[編集 (Edit)]** (✎) をクリックして変更を加え、**[適用 (Apply)]** をクリックします。
- ポリシー設定を変更するには、以下の手順を実行します。
 - **[設定 (Settings)]** をクリックします。
 - 必要に応じて設定を変更します。

重要 SAML ACS URL のドメイン名を編集すると、アプリケーションへのアクセスが中断されます。
 - **[Save (保存)]** をクリックします。
- アプリケーショングループの設定を変更するには、以下の手順を実行します。
 - **[アプリケーション (Applications)]** をクリックします。
 - 編集するアプリケーショングループの横にある **[編集 (Edit)]** (✎) をクリックします。
 - 各セクションで **[編集 (Edit)]** をクリックして、必要に応じて設定を変更します。

重要 アプリケーショングループ名を編集すると、アプリケーションへのアクセスが中断されます。
 - セクションの設定を変更したら、**[適用 (Apply)]** をクリックします。
 - **[終了 (Finish)]** をクリックします。
 - **[保存 (Save)]** をクリックします。
- アプリケーション設定を変更するには、以下の手順を実行します。
 - **[アプリケーション (Applications)]** をクリックします。
 - 編集するアプリケーションの横にある **[編集 (Edit)]** (✎) をクリックします。
 - 各セクションで **[編集 (Edit)]** をクリックして、必要に応じて設定を変更します。

重要 アプリケーション名を編集すると、アプリケーションへのアクセスが中断されます。
 - セクションの設定を変更したら、**[適用 (Apply)]** をクリックします。
 - **[終了 (Finish)]** をクリックします。
 - **[保存 (Save)]** をクリックします。
- 複数のアプリケーションを有効化、無効化、または削除するには、アプリケーションを選択し、必要な一括アクションをクリックして **[保存 (Save)]** をクリックします。

(注) これらのアクションは、右クリックメニューでも実行できます。

- すべてのアプリケーションを有効にするには、[一括アクション (Bulk Actions)] > [有効化 (Enable)] をクリックします。
- すべてのアプリケーションを無効にするには、[一括アクション (Bulk Actions)]、[無効化 (Disable)] をクリックします。
- すべてのアプリケーションを削除するには、[一括アクション (Bulk Actions)] > [削除 (Delete)] をクリックします。
- [Zero Trustアプリケーションに戻る (Return to Zero Trust Application)] をクリックして、ポリシーページに戻ります。

次のタスク

設定変更を展開します。『[Cisco Secure Firewall Management Center アドミニストレーション ガイド](#)』の「設定変更の展開」をご覧ください。

Zero Trust セッションのモニタリング

Connection Events

Zero Trust アプリケーションポリシーが展開されると、新しいフィールドが使用可能になります。テーブルビューにフィールドを追加するには、次の手順を実行します。

1. [分析 (Analysis)] > [接続 (Connections)] > [イベント (Events)] を選択します。
2. [接続イベントのテーブルビュー (Table View of Connection Events)] タブに移動します。
3. イベントのテーブルビューでは、デフォルトで複数のフィールドが非表示になっています。表示されるフィールドを変更するには、任意の列名の [x] アイコンをクリックして、フィールド選択ツールを表示します。
4. 次のフィールドを選択します。
 - [認証ソース (Authentication Source)]
 - [Zero Trustアプリケーション (Zero Trust Application)]
 - [Zero Trustアプリケーショングループ (Zero Trust Application Group)]
 - Zero Trust アプリケーションポリシー
5. [Apply] をクリックします。

接続イベントの詳細については、『Cisco Secure Firewall Management Center 管理ガイド』の「接続およびセキュリティ関連の接続イベント」を参照してください。

Zero Trust ダッシュボード

Zero Trust ダッシュボードでは、デバイス上のアクティブな Zero Trust セッションからのリアルタイムデータを監視できます。

Zero Trust ダッシュボードには、管理センターによって管理されている上位の Zero Trust アプリケーションと Zero Trust ユーザーの概要が表示されます。[概要 (Overview)] > [ダッシュボード (Dashboards)] > [Zero Trust] の順に選択して、ダッシュボードにアクセスします。

ダッシュボードには以下のウィジェットがあります。

- [上位の Zero Trust アプリケーション (Top Zero Trust Application)]
- [上位の Zero Trust ユーザー (Top Zero Trust Users)]

CLI コマンド

デバイス CLI にログインして次のコマンドを使用します。

CLI コマンド	説明
<code>show running-config zero-trust</code>	Zero Trust 設定の実行コンフィギュレーションを表示する
<code>show zero-trust</code>	ランタイムの Zero Trust 統計情報とセッション情報を表示する
<code>show cluster zero-trust</code>	クラスタ内のノード全体の Zero Trust 統計情報の概要を表示する
<code>clear zero-trust</code>	Zero Trust セッションと統計情報をクリアする
<code>show counters protocol zero_trust</code>	Zero Trust フローでヒットしたカウンタを表示する

診断ツール

診断ツールは、Zero Trust 設定で発生する可能性のある問題を検出することでトラブルシューティングを容易にします。診断は、次の 2 つのタイプに分類できます。

- **アプリケーション固有の診断**は、次のような問題を検出するために使用されます。
 - DNS 関連の問題
 - ソケットが開いていないなどの設定の誤り、または分類および NAT ルールの問題。
 - Zero Trust ポリシーまたは SSL ルールの展開に関する問題
 - 送信元 NAT の問題と PAT プールの枯渇に関する問題

- 一般的な診断は、次のような問題を検出するために使用されます。
 - 強力な暗号ライセンスが有効になっていない
 - 無効なアプリケーション証明書
 - SAML 関連の問題
 - ホームエージェントとクラスタの一括同期の問題

診断ツールを実行するには以下を実行します。

1. トラブルシューティングする Zero Trust アプリケーションの横にある [診断 (Diagnostics)] (🔧) をクリックします。[診断 (Diagnostics)] ダイアログボックスが表示されます。
2. [デバイスの選択 (Select Device)] ドロップダウンリストからデバイスを選択し、[実行 (Run)] をクリックします。診断プロセスが完了すると、[レポート (Reports)] タブにレポートが生成されます。
3. ログを表示、コピー、ダウンロードするには、[ログ (Logs)] タブをクリックします。

Zero Trust アクセスの履歴

機能	最小 Management Center	最小 Threat Defense	詳細
Zero Trust アクセスの機能拡張	7.4.1	7.4.1	<ul style="list-style-type: none"> • アプリケーションの NAT の送信元ネットワークを設定できるようになりました。設定されたネットワークオブジェクトまたはオブジェクトグループは、着信要求のパブリックネットワーク送信元 IP アドレスをアプリケーション ネットワーク内のルーティング可能な IP アドレスに変換するために使用されます。 • トラブルシューティングプロセスを容易にする診断ツールを使用できるようになりました。この診断ツールは、Zero Trust 設定で発生する可能性のある問題を検出します。
Zero Trust アクセス	7.4.0	7.4.0	プライベートアプリケーションへのアクセスをユーザーに許可できます。ユーザーは個人デバイスに追加のソフトウェアをインストールする必要がありません。この機能は、SAML ベースの認証を活用し、Duo およびその他すべての主要な ID プロバイダーをサポートします。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。