Cisco Secure Firewall で Zero Trust アクセスを使用してアプリケーションを保護する方法

初版：2024 年 1 月 29 日

ゼロトラスト ネットワーク アクセスの概要

Cisco Secure Firewall を使用した Zero Trust Secure Access

Zero Trust アクセスは、継続的な認証と各ネットワークアクセス試行のモニタリングによって信頼を確立するセキュリティモデルに基づいています。Secure Firewall Management Center 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（ZTA）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。

本書では、アプリケーションを保護し、脅威とマルウェアの保護を実装する完全なプロセスを示すシナリオの概要を示します。本書には、アプリケーションにアクセスし、脅威やマルウェアからアプリケーションを保護し、Zero Trust セッションをモニターするための検証手順も含まれています。

Secure Firewall Management Center の Zero Trust アクセスの機能

- Duo、Microsoft Azure Active Directory、Okta など、複数の SAML ベースの ID プロバイダーのサポート。
- Secure Access 用のエンドポイント（クライアントデバイス）の Cisco AnyConnect などのアプリケーション。
- ブラウザを介したアクセスと認証のサポート。
- 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をサポート。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を提供します。同じ機能をサードパーティの ID プロバイダーと協力して実行して、エージェントによるポスチャ評価をサポートできます。
- 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。

Zero Trust アクセスを使用するための前提条件

本書は、読者が Zero Trust の概念の基本を理解し、Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド [英語] バージョン 7.4 以降の「Zero Trust Access」の章を読み終えていることを前提としています。

この使用例の対象者

この使用例では、クライアントレス ゼロトラスト ネットワーク アクセス モデルを使用してプライベートアプリケーションとリソースにアクセスするプロセスの概要を示します。クライアントベースのセキュアなネットワークおよびアプリケーションアクセスには、Cisco Secure Client を使用することを推奨します。詳細については、「Cisco Secure Client」を参照してください。

この使用例の目的は、Secure Firewall Management Center で Zero Trust 機能を使用することを計画しているネットワーク管理者を支援して、ハイブリッドワークフォースが保護されたリソースと Web アプリケーションにアクセスできるようにし、保護されたリソースとアプリケーションをマルウェアから保護することです。

Zero Trust アクセスを実装するシナリオ

分散型ワークフォースで、従業員と請負業者がさまざまな場所で作業し、企業のファイアウォールの背後でホストされているプライベートアプリケーションやリソースにアクセスする大企業の場合、管理者は、ワークフォースが保護されたアプリケーションにアクセスするときに、悪意のあるアクティビティを実行するのを防ぎたいと考えます。

リスクがあるもの

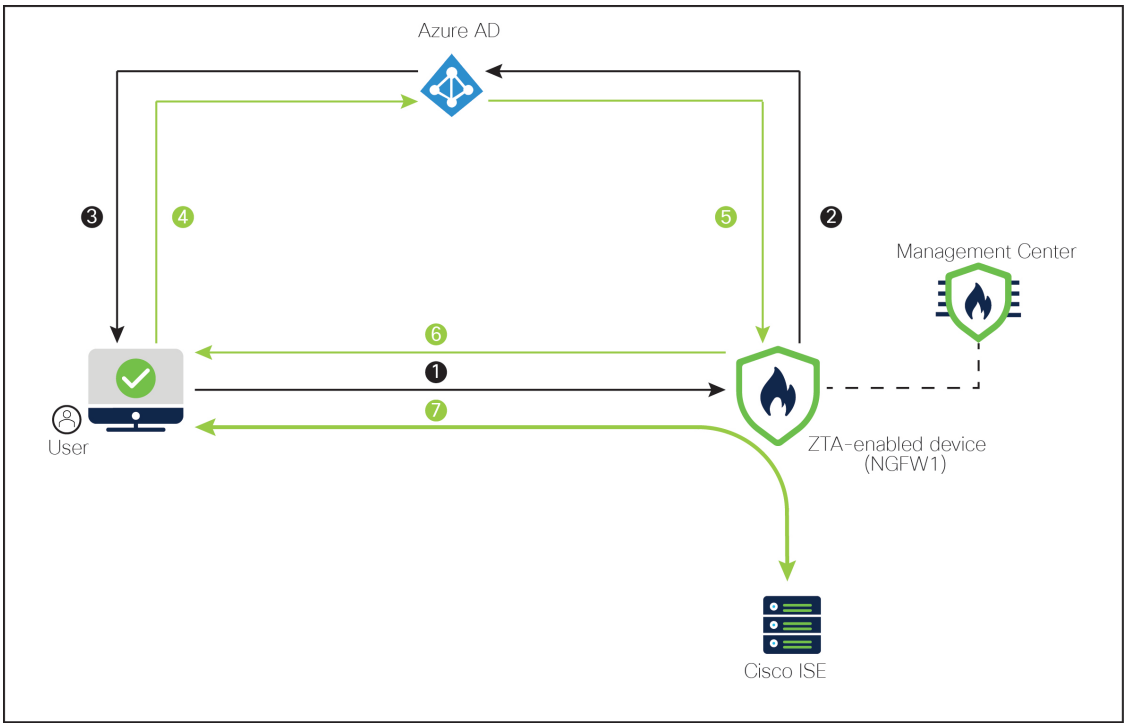
ワークフォースは完全なネットワークアクセスを取得できるため、攻撃対象領域が拡大し、ネットワークが攻撃に対して脆弱になります。ワークフォースは、悪意のあるコンテンツを含む可能性があるファイルもアップロードできます。

Secure Firewall Management Center Zero Trust アクセスポリシーによるアプリケーションの保護方法

ネットワーク管理者は、ファイアウォールへの Zero Trust アクセスを組み込み、すべてのエンドポイントデバイスにソフトウェアをインストールすることなく、重要なリソースやアプリケーションへのセキュアなリモートアクセスを可能にできます。この機能によりパフォーマンスは向上しますが、許可は単一のアプリケーションに制限されるため、潜在的な攻撃ポイントは最小限に抑えられます。機密情報やアプリケーションへのアクセスは、ユーザーのアイデンティティを検証し、リクエストのコンテキストを確認し、リスク分析を実行した後にのみ許可されます。さらに、Zero Trust アプリケーション トラフィックを保護するために、マルウェアとファイルポリシーが設定されます。

ネットワーク トポロジ

次のネットワークトポロジには、データセンターに設定された Threat Defense デバイスが含まれています。セキュリティゾーンは、デバイスのアウトバウンドインターフェイスで確立されます。



前述の図では、ネットワーク管理者は Management Center を使用して Zero Trust ポリシーを設定し、**NGFW1** というラベルの付いた Threat Defense を展開しています。**Cisco ISE** アプリケーションは、ファイアウォールの背後にあるデータセンターでホストされ、ユーザーは Zero Trust アプリケーションを介してアクセスします。注：ISE は認証、許可、およびアカウンティング（AAA）には使用されていません。Microsoft Azure Active Directory は、認証と許可に使用される SAML IdP サーバーです。ネットワークオブジェクトは、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作成されます。

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。
2. ZTA 対応の管理対象デバイスが、設定された IdP にユーザーを誘導します。
3. IdP がユーザーにログイン情報の入力を求めます。
4. ユーザーがユーザー名とパスワードを入力します。
5. IdP がファイアウォールに 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。
6. 検証が成功すると、ユーザーがアプリケーションにリダイレクトされます。

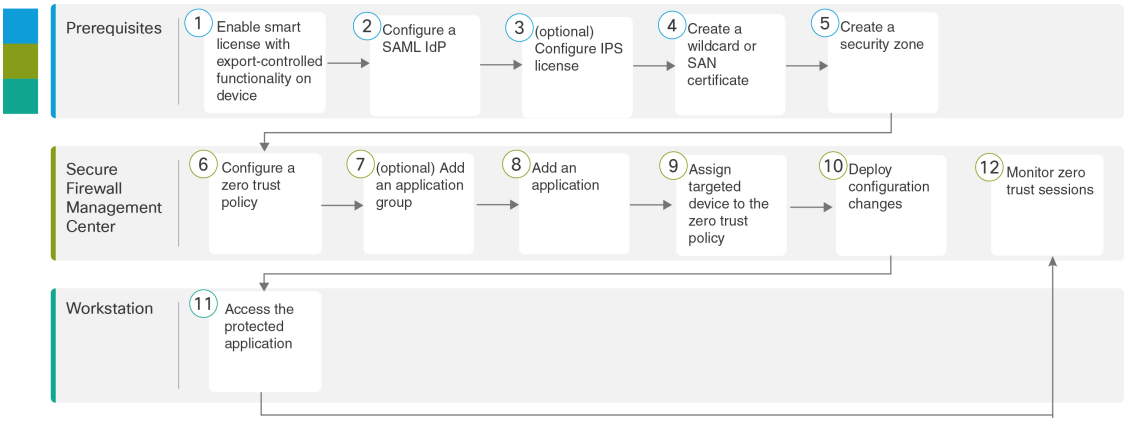
7. ユーザーがアプリケーションへのアクセスを許可されます。必要に応じて、アプリケーションにアクセス中に脅威とマルウェアの保護が適用されます。

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 アプリケーションを設定するためのエンドツーエンドの手順

次のフローチャートは、Secure Firewall Management Center で Zero Trust アクセスを設定するためのワークフローを示しています。



ステップ	説明
1	（前提条件）Threat Defense で輸出管理機能を備えたスマートライセンスを有効にします。
2	（前提条件）SAML IdP を設定します。
3	（前提条件）（任意）侵入防御システム（IPS）ライセンスを設定します。
4	（前提条件）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。
5	（前提条件）セキュリティゾーンを作成します。
6	Zero Trust アプリケーションポリシーの作成
7	アプリケーショングループの作成。
8	アプリケーションの作成。
9	Zero Trust アクセスポリシーの対象デバイスの設定。
10	デバイスに設定を導入。
11	保護されたアプリケーションにアクセス。
12	Zero Trust セッションのモニタリング。

Zero Trust アプリケーションポリシーの前提条件

次の条件が満たされていることを確認します。

- 輸出管理機能を備えたスマート ライセンス アカウント。
- プライベート アプリケーションにアクセスするための認証および許可用に SAML ID プロバイダー（IdP）を設定している。
- セキュリティ管理を有効にするために IPS および脅威ライセンスを設定している。
- 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）証明書を作成している。詳細については、Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド、X.Y [英語] の「Object Management」の章にある「Adding Certificate Enrollment Objects」の項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 Management Center に作成している。詳細については、Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド、X.Y [英語] の「Interface Overview」の章にある「Create Security Zone and Interface Group Object」の項を参照してください。
- パブリック DNS が更新されている。

証明書

次の証明書を作成してください。

- [アイデンティティ証明書（Identity Certificate）]：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。

  詳細については、Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド、X.Y [英語] の「Object Management」の章にある「Adding Certificate Enrollment Objects」の項を参照してください。

  この例では、アイデンティティ証明書 **ZTAA-ID-Certificate** を作成しました。

- [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。

  詳細については、Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド、X.Y [英語] の「Object Management」の章にある「Adding Certificate Enrollment」の項を参照してください。

  この例では、IdP 証明書 **Azure-AD-SAML-Certificate** を作成します。

- [アプリケーション証明書（Application Certificate）]：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 によって復号化されます。

  詳細については、Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド、X.Y [英語] の「Object Management」の章にある「Adding Internal Certificate Objects」の項を参照してください。

  この例では、アプリケーション **ZTAA-ISE-GUI-Certificate** の内部証明書を作成しました。

（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

次の条件が満た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。
- プライベートアプリケーションへのアクセスは、セキュリティゾーンによって制限されます。詳細については、Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド、X.Y [英語] の「Interface Overview」の章にある「Create Security Zone and Interface Group Objects」の項を参照してください。

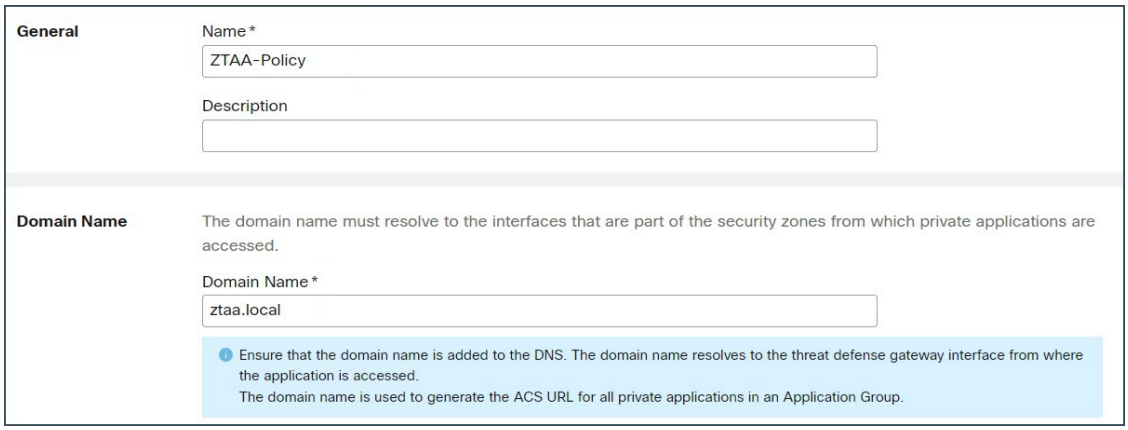
手順

ステップ 1 Management Center で、[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。

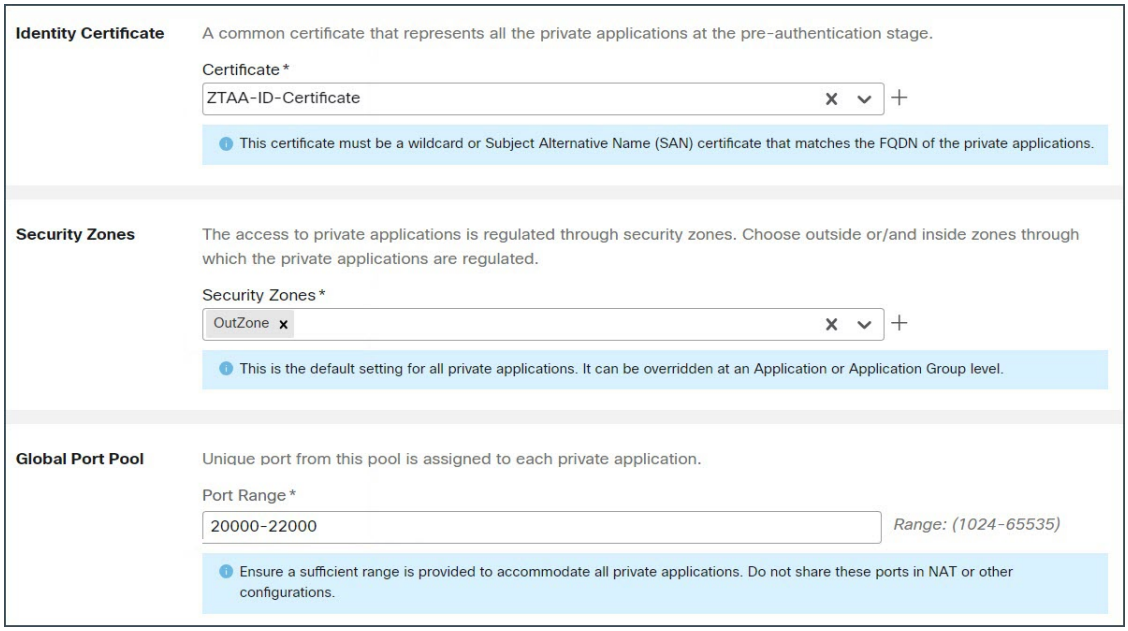
ステップ 2 [ポリシーを追加（Add Policy）] をクリックします。

ステップ 3 以下の説明に従って、Zero Trust ポリシーを設定します。

- [名前（Name）]：ポリシー名を入力します。この例では、Zero Trust ポリシー名は **ZTAA-Policy** です。
- [ドメイン名（Domain Name）]：ドメイン名を入力します。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 Assertion Consumer Service（ACS）URL を生成するために使用されます。この例では、ドメイン名は **ztaa.local** です。



- [IdP証明書（IdP Certificate）]：[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。この例では、作成されたアイデンティティ証明書 **ZTAA-ID-Certificate** を選択します。
- [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。この例では、セキュリティゾーン **OutZone** を作成しました。
- [ポート範囲（Port Range）]：このプールから一意のポートが各プライベート アプリケーションに割り当てられます。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。この例では、デフォルト値の **20000-22000** を使用します。

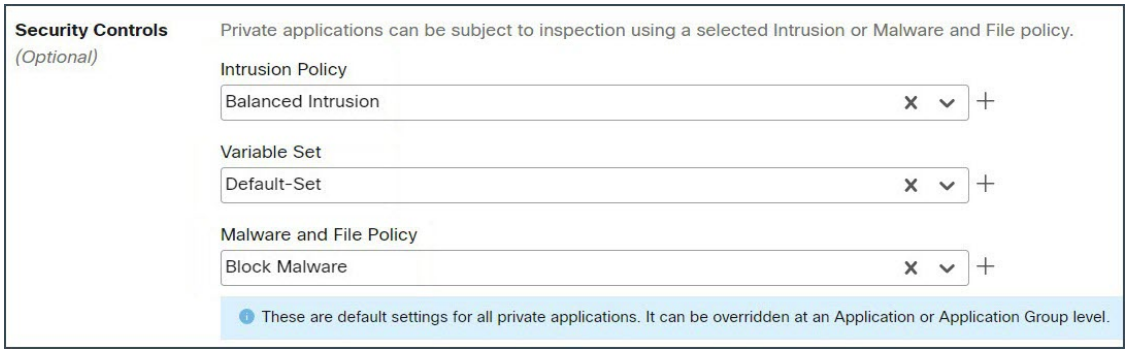


ステップ 4 [セキュリティ管理（Security Controls）]セクションで、侵入またはマルウェアとファイルポリシーを追加します。この設定により、Zero Trust アプリケーション トラフィックに対する侵入およびマルウェアの保護が提供されます。

- [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、[追加（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 CenterSnort 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。この例では、侵入ポリシー **Balanced Instrusion** を作成しました。
- [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、[追加（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、Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド、X.Y [英語] の「Object Management」の章にある「Creating Variable Sets」の項を参照してください。この例では、デフォルト値の **Default-Set** を使用しました。
- **マルウェアとファイルポリシー**：

  ドロップダウンリストから既存のポリシーを選択するか、[追加（Add）]（➕）アイコンをクリックして新しいカスタムマルウェアポリシーを作成します。

  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。詳細については、Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド、X.Y [英語] の「Network Malware Protection and File Policies」の章にある「Managing File Policies」の項を参照してください。この例では、**Block Malware** というマルウェアポリシーを作成しました。



ステップ 5 [保存（Save）] をクリックします。

アプリケーショングループの作成

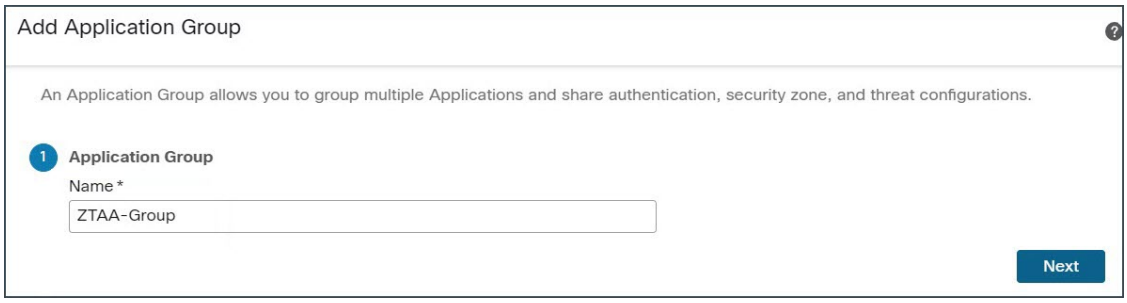
手順

ステップ 1 Management Center で、[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 [ポリシーの編集（Edit Policy）] をクリックします。

ステップ 3 [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 4 [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。この例では、アプリケーショングループ名は **ZTAA-Group** です。

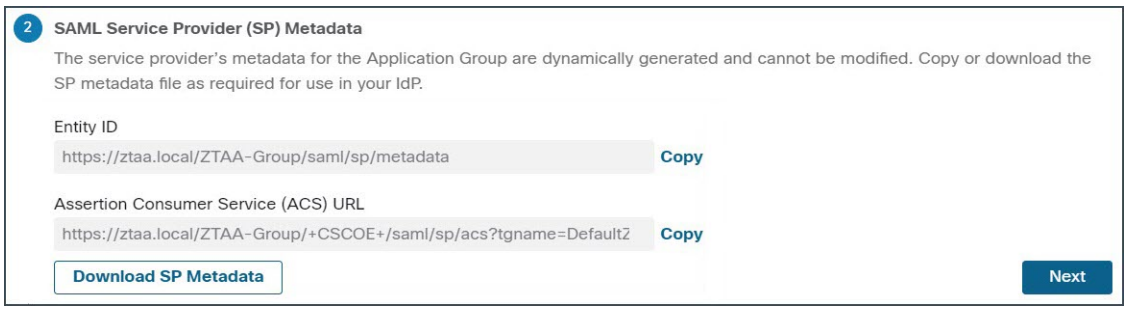


ステップ 5 [SAMLサービスプロバイダー（SP）メタデータ（SAML Service Provider (SP) Metadata）] セクションで、前の手順で指定した構成要素からデータが動的に生成されます。

- アプリケーショングループ：ZTAA-Group
- ドメイン名：ztaa.local

[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。

この例では、データは XML 形式でダウンロードされ、Azure Active Directory IdP にアップロードされます。



[次へ（Next）] をクリックします。

ステップ 6 [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、メタデータを追加します。

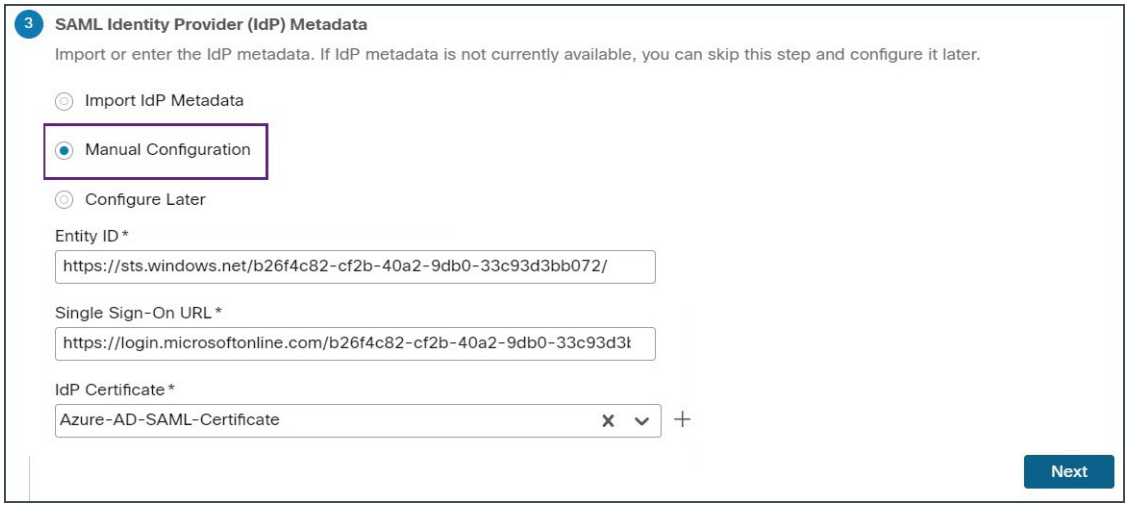
この例では、メタデータを手動で入力します。

[手動設定（Manual Configuration）] を選択して、メタデータを入力します。

- [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。この例では、**https://sts.windows.net/b26f4c82-cf2b-40a2-9db0-33c93d3bb072/** を使用します。

- [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。この例では、**https://login.microsoftonline.com/b26f4c82-cf2b-40a2-9db0-33c93d3bb072/saml2** を使用します。
- [IdP証明書（IdP Certificate）]：Threat Defense に登録されている IdP の証明書を選択します。

  この例では、作成した IdP 証明書 **Azure-AD-SAML-Certificate** を選択します。



この例では、[手動設定（Manual Configuration）] が選択されています。

[次へ（Next）] をクリックします。

ステップ 7 [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。この例では、デフォルト値の **1440** を使用します。

ステップ 8 [セキュリティゾーンとセキュリティ管理（Security Zones and Security Controls）] では、セキュリティゾーンと脅威の設定が親から継承されます。この例では、デフォルト値が保持されます。[次へ（Next）] をクリックします。

ステップ 9 設定のサマリーを確認します。[終了（Finish）] をクリックします。

ステップ 10 [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。

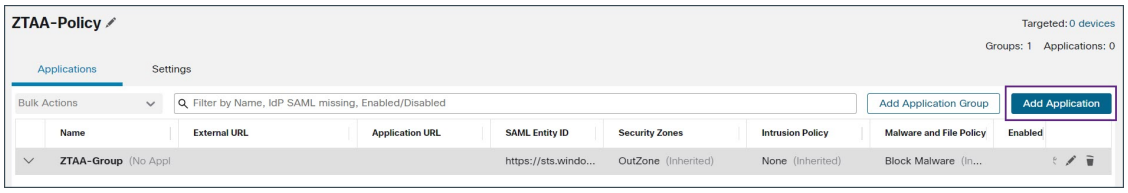
アプリケーションの作成

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。この例では、**ZTAA-Policy** 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）] で、次のフィールドを設定します。

- [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。この例では、アプリケーション名は **ZTAA-ISE-GUI-Access** です。

- [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。この例では、**https://ise-external.local** を使用します。
- [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。この例では、**https://ise.local** を使用します。

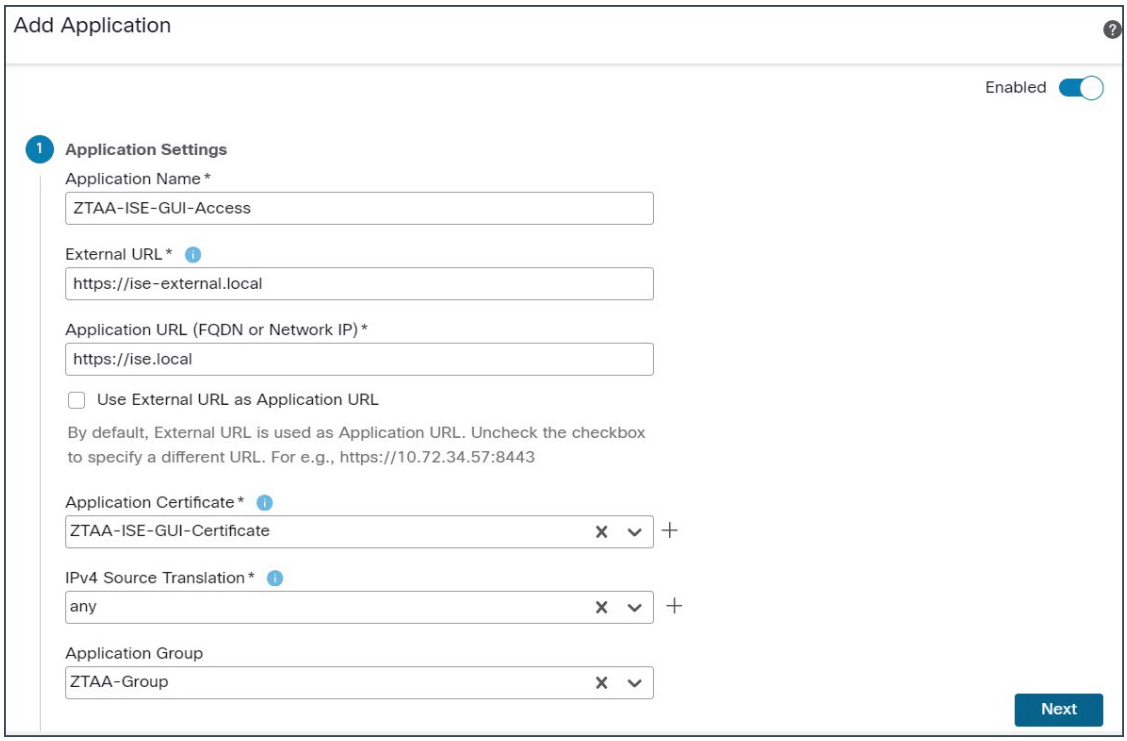
  Threat Defense で内部 DNS を使用する場合、アプリケーションへの解決を確実にするために、アプリケーション URL はその DNS 内のエントリと一致している必要があります。
- [アプリケーション証明書（Application Certificate）]：プライベートアプリケーションの証明書を選択します。

  この例では、作成された内部証明書 **ZTAA-ISE-GUI-Certificate** を選択します。
- [IPv4送信元の変換（IPv4 Source Translation）]：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。詳細については、Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド、X.Y [英語] の「Object Management」の章にある「Create Network Objects」の項を参照してください。

  （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」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。

この例では、**ZTAA-Group** アプリケーショングループを使用します。



[次へ（Next）] をクリックします。

ステップ 5 設定のサマリーを確認し、[終了（Finish）] をクリックします。

ステップ 6 [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。

（注） Management Center は、各アプリケーションの診断ツールを提供し、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。詳細については、Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド、X.Y [英語] の「Zero Trust Access」の章にある「Monitor Zero Trust Sessions」の項を参照してください。

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。

手順

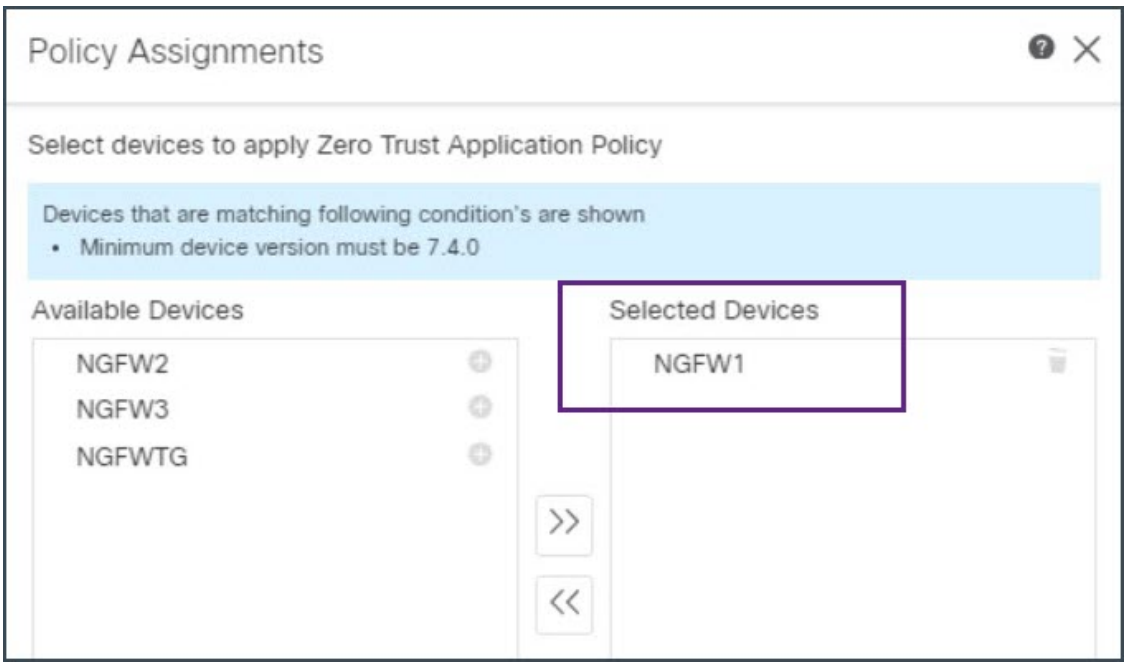
ステップ 1 [ポリシー（Policies）]>[アクセス制御（Access Control）]>[Zero Trustアプリケーション（Zero Trust Application）] の順に選択します。

ステップ 2 ポリシーを選択します。この例では、**ZTAA-Policy** 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 展開するデバイスを選択します。

この例では、**NGFW1** を選択します。



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）] をクリックします。

次のタスク

デバイスに設定を導入

デバイスに設定を導入

すべての設定が完了したら、管理対象デバイスに設定を展開します。

手順

ステップ 1 Management Center メニューバーで、[展開（Deploy）] をクリックします。展開準備が完了しているデバイスのリストが表示されます。

ステップ 2 設定変更を展開するデバイスの横にあるチェックボックスをオンにします。この例では、デバイスは **NGFW1** です。

ステップ 3 [展開（Deploy）] をクリックします。[展開（Deploy）] ダイアログボックスで展開が [完了（Completed）] とマークされるまで待ちます。

ステップ 4 展開する変更に関するエラーや警告がシステムによって識別された場合は、[検証エラー（Validation Errors）] または [検証の警告（Validation Warnings）] ウィンドウにその内容が表示されます。完全な詳細を表示するには、[検証エラー（Validation Errors）] または [検証の警告（Validation Warnings）] リンクをクリックします。

次の選択肢があります。

- [展開の続行（Proceed with Deploy）]：警告状態を解決せずに展開を続行します。システムがエラーを確認した場合は続行できません。
- [閉じる（Close）]：展開せずに終了します。エラーおよび警告状態を解決し、設定の再展開を試行します。

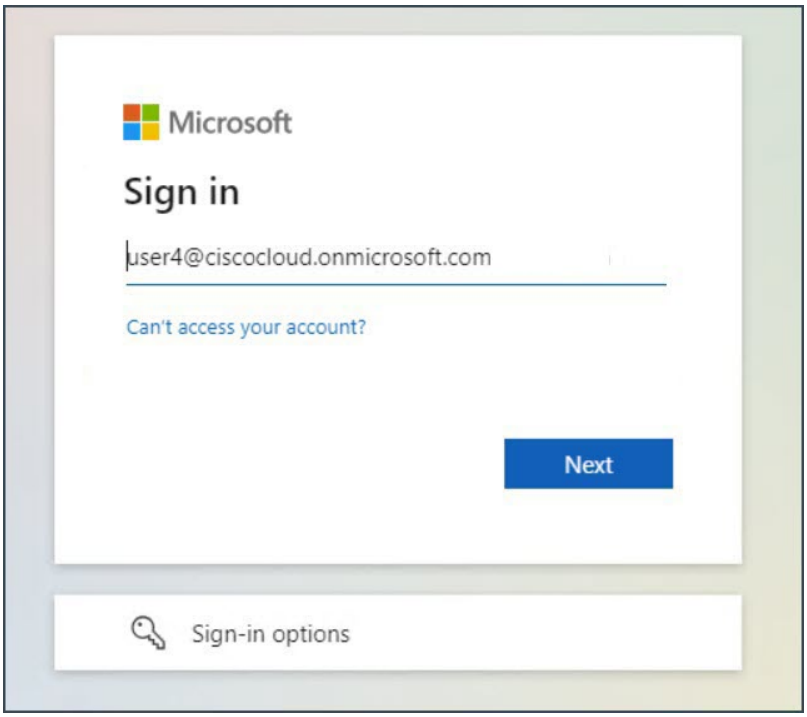
保護されたアプリケーションにアクセス

設定の展開が正常に完了すると、アプリケーションの外部 URL を使用してアプリケーションにアクセスできます。

手順

ステップ 1 クライアントマシンでブラウザを開き、外部 URL を使用して保護されたアプリケーションにアクセスします。この例では、使用される外部 URL は **https://ise-external.local** です。

ユーザーがログインページにリダイレクトされ、ログイン情報の入力を求めるプロンプトが SAML IdP から表示されます。この例では、使用される SAML IdP は Microsoft Azure Active Directory です。



ステップ 2 ログイン情報を送信後、IdP がユーザーを認証および承認し、Threat Defense デバイスへの応答で SAML アサーションを送信すると、ユーザーがアプリケーションにリダイレクトされます。

ステップ 3 認証に成功すると、ユーザーはアプリケーションにアクセスできます。この例では、Cisco ISE ホームページが表示されます。

ステップ 4 ユーザーはログイン情報を使用して Cisco ISE にログインします。

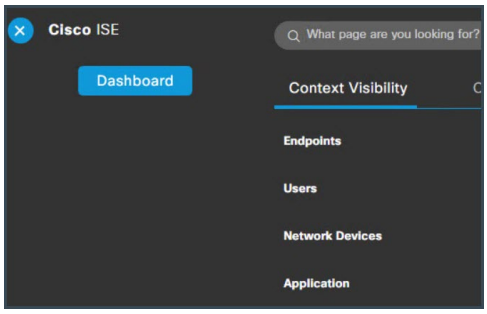
Zero Trust アプリケーション トラフィックにおけるマルウェアの保護のテスト

ユーザーが保護されたアプリケーションにマルウェアファイルをアップロードしようとすると、ネットワーク上のマルウェアファイルのアップロードが ZTA ポリシーによってブロックされます。

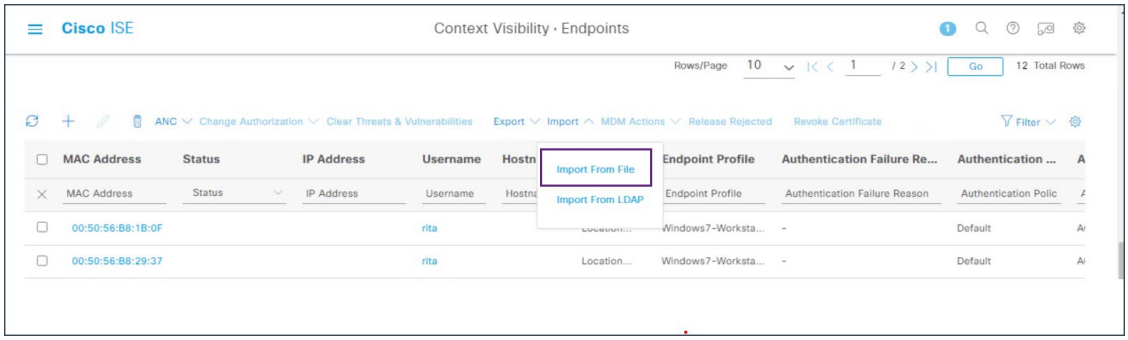
手順

ステップ 1 Cisco ISE アプリケーションにログインします。

ステップ 2 Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] の順に選択します。



ステップ 3 このページを下にスクロールしてエンドポイントのリストを見つけ、[インポート（Import）] > [ファイルからインポート（Import From File）] の順に選択します。

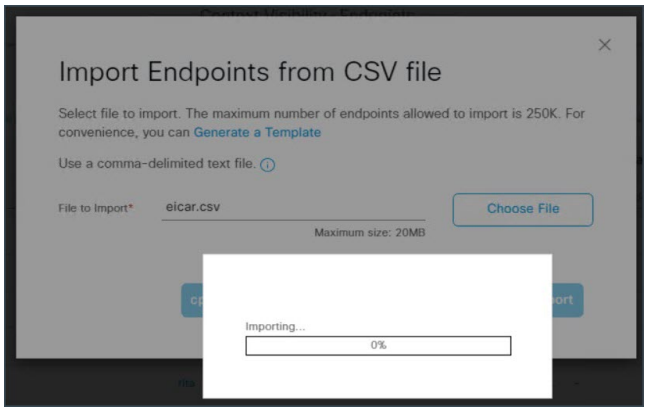


ステップ 4 [ファイルの選択（Choose File）]をクリックし、アップロードするファイルを選択します。ファイルを選択するためのナビゲーション手順は、オペレーティングシステムによって異なる場合があります。

この例では、事前に作成されたサンプルマルウェアファイルを選択しています。

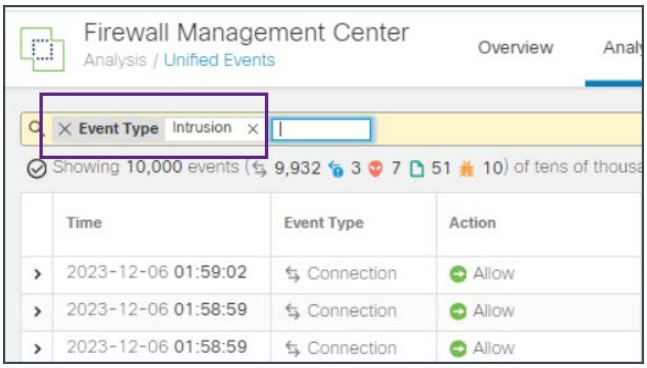
ステップ 5 [インポート（Import）] をクリックします。

アップロードアクションは 0% を超えて進行しません。これはマルウェアファイルであり、ZTA ポリシーによりファイルのアップロードがブロックされています。



ステップ 6 Management Center にログインし、[分析（Analysis）] > [統合イベント（Unified Events）] の順に選択します。

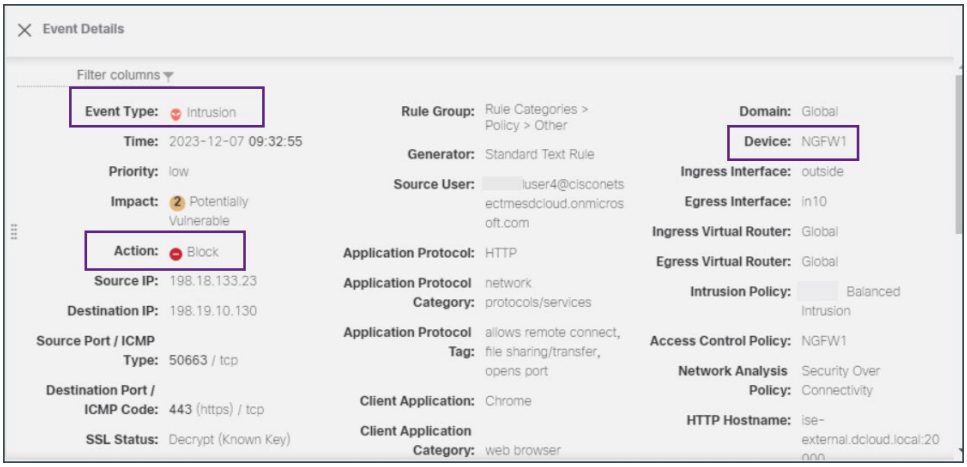
ステップ 7 検索バーで、フィルタの [イベントタイプ（Event Type）] を [侵入（Intrusion）] に設定し、[適用（Apply）] をクリックします。



この例では、スライドする時間枠をデフォルトの **5 分** に設定しています。[スライド時間範囲（Sliding Time Range）] をクリックします。

イベントページには、悪意のあるファイルが検出され、ブロックされたことが表示されます。

イベントをダブルクリックすると、[イベントの詳細（Event Details）] ページに詳細情報が表示されます。



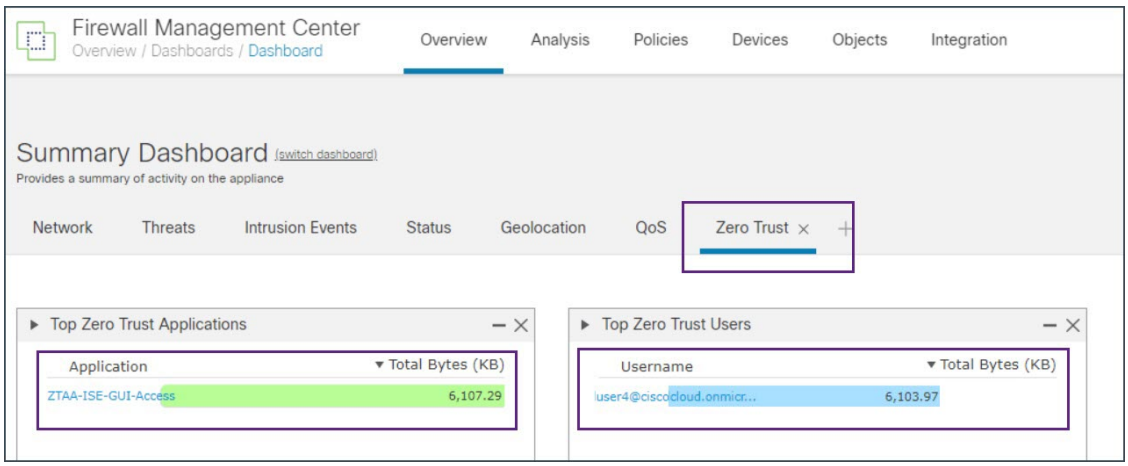
Zero Trust セッションのモニタリング

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、Management Center 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。

この例では、[上位のZero Trustアプリケーション（Top Zero Trust Applications）] ウィジェットに、Zero Trust アプリケーション **ZTAA_ISE_GUI_Access** と、アプリケーションにアクセスしているユーザーのユーザー名が表示されます。

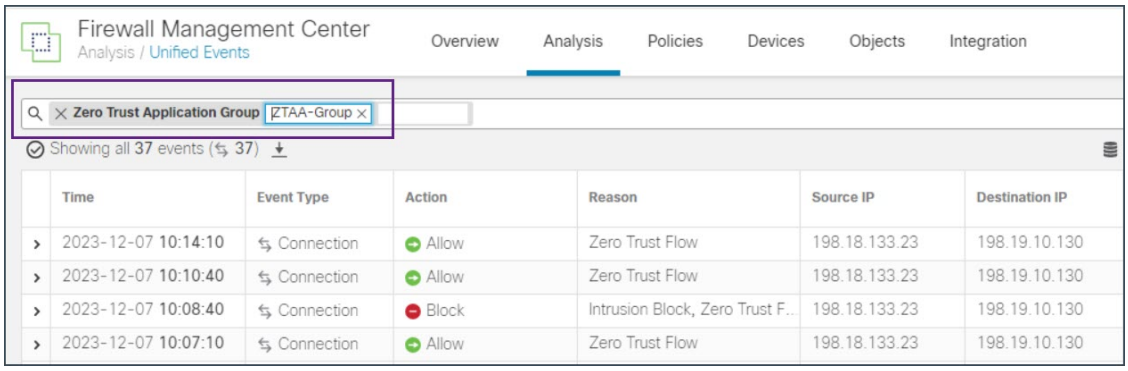


接続イベント

Zero Trust セッションを確立後、Zero Trust セッションに関連付けられているイベントを表示し、ユーザーのアクティビティをモニターできます。

1. Management Center で、[分析（Analysis）] > [統合イベント（Unified Events）] の順に選択します。
2. 検索バーで、[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）]、または [Zero Trustアプリケーションポリシー（Zero Trust Application Policy）] を検索し、その作成時に指定した対応する名前を入力します。

   この例では、[Zero Trustアプリケーショングループ（Zero Trust Application Group）]（**ZTAA-Group**）を使用してイベントを検索します。



スライダを右にスクロールすると、[認証ソース（Authentication Source）]、[Zero Trustアプリケーション（Zero Trust Application）]、および[Zero Trustアプリケーションポリシー（Zero Trust Application Policy）] が表示されます。

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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。