アイデンティティ ポリシー

アイデンティティ ポリシーを使用して、接続からユーザ アイデンティティ情報を収集できます。その後、ユーザアイデンティティに基づく使用状況をダッシュボードに表示し、ユーザまたはユーザ グループに基づくアクセス制御を設定できます。

アイデンティティ ポリシーの概要

アイデンティティポリシーを使って、接続に関連付けられたユーザを検出できます。ユーザを特定することにより、脅威、エンドポイント、ネットワーク インテリジェンスとユーザ アイデンティティ情報を関連付けることができます。ネットワーク動作、トラフィック、イベントを個別のユーザに直接リンクすることにより、ポリシー違反、攻撃、またはネットワークの脆弱性の発生源の特定に役立てることができます。

たとえば、侵入イベントのターゲットになっているホストの所有者や内部攻撃またはポート スキャンを開始した人物を特定できます。高帯域幅ユーザや望ましくない Web サイトまたはアプリケーションにアクセスしているユーザを特定することもできます。

ユーザ検出には、分析のためのデータ収集以上のメリットがあります。ユーザ アイデンティティに基づいてリソースへのアクセスを選択的に許可またはブロックできるようユーザ名やユーザ グループ名に基づくアクセス ルールを作成することもできます。

ユーザ アイデンティティは、次の方法で取得できます。

- パッシブ認証：すべてのタイプの接続で、ユーザ名とパスワードを求められることなく、その他の認証サービスからユーザ アイデンティティを取得します。

- アクティブ認証：HTTP 接続でのみ、ユーザ名とパスワードの入力が求められ、送信元 IP アドレスのユーザ アイデンティティを取得するために指定のアイデンティティ ソースに対する認証が行われます。

ここでは、ユーザ アイデンティティについて詳しく説明します。

パッシブ認証経由のユーザ アイデンティティの確立

パッシブ認証では、ユーザにユーザ名とパスワードを求めることなくユーザアイデンティティを収集します。システムは、指定したアイデンティティ ソースからマッピングを取得します。

ユーザと IP アドレスのマッピングは次のソースから受動的に取得できます。

- リモート アクセス VPN ログイン。パッシブ アイデンティティについては次のユーザ タイプがサポートされています。
  - 外部認証サーバで定義されたユーザ アカウント。
  - Device Manager で定義されたローカルユーザーアカウント。
- Cisco Identity Services Engine（ISE）、Cisco Identity Services Engine Passive Identity Connector（ISE PIC）。

特定のユーザが複数のソースによって識別される場合は、RA VPN ID が優先されます。

アクティブ認証経由のユーザ アイデンティティの確立

認証は、ユーザのアイデンティティを確認する動作です。

アクティブ認証を使用すると、ユーザとアイデンティティのマッピングが存在しないシステムの IP アドレスから HTTP トラフィック フローが送られてきたときに、システム用に設定されたディレクトリに対してトラフィック フローを開始したユーザを認証するかどうかを判断できます。ユーザが正常に認証された場合、IP アドレスには、認証されたユーザのアイデンティティがあると見なされます。

認証に失敗しても、ユーザのネットワーク アクセスは阻止されません。最終的には、アクセス ルールがそのようなユーザへのアクセス権を決定します。

不明なユーザの処理

アイデンティティ ポリシーのためにディレクトリ サーバを設定する場合、システムはディレクトリ サーバからユーザおよびグループ メンバーシップ情報をダウンロードします。この情報は 24 時間ごとの真夜中に、またはディレクトリの設定を編集して保存するたびに（変更を何も加えていなくても）更新されます。

アクティブな認証用アイデンティティ ルールに求められた際に、ユーザが認証に成功しても、ユーザの名前がダウロードされたユーザのアイデンティティ情報にない場合、ユーザは「不

明」としてマークされます。アイデンティティ関連のダッシュボードにはユーザの ID は表示されず、ユーザはグループ ルールにも一致しません。

ただし、不明ユーザ用のアクセス制御ルールはすべて適用されます。例えば、不明ユーザに対して接続をブロックする場合、これらのユーザは認証に成功した場合（つまりディレクトリ サーバがユーザを認識し、パスワードが有効である場合）でもブロックされます。

ユーザの追加または削除やグループ メンバーシップの変更など、ディレクトリ サーバに変更を加えた場合、システムがその更新をディレクトリからダウンロードするまで、これらの変更はポリシーに反映されません。

真夜中の日次更新まで待てず、すぐに更新を適用させる必要がある場合は、ディレクトリのレルム情報を編集します（**[オブジェクト（Objects）]** > **[アイデンティティ ソース（Identity Sources）]** に移動し、レルムを編集する）。[保存（Save）] をクリックして、変更を展開します。システムはただちに更新情報をダウンロードします。

（注） システムに新しいユーザ情報や削除されたユーザ情報があるかを確認するには、**[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]** に移動し、[ルールの追加（+）（Add Rule (+)）] ボタンをクリックし、[ユーザ（Users）] タブにあるユーザのリストを確認します。新しいユーザが見つからない、もしくは、削除されたユーザが見つかる場合、システムの情報は古いままです。

アイデンティティ ポリシーを実装する方法

ユーザ アイデンティティの取得を有効にし、IP アドレスに関連付けられているユーザを認識させるには、いくつかの項目を設定する必要があります。正しく設定されている場合、監視ダッシュボードおよびイベントでユーザ名を確認できます。ユーザアイデンティティは、アクセス制御ルールや SSL 復号ルールでもトラフィック一致基準として使用できます。

次の手順では、アイデンティティ ポリシーを機能させるために設定する必要がある内容の概要を示します。

手順

ステップ 1 AD アイデンティティ レルムを設定します。

（ユーザ認証を要求して）ユーザアイデンティティをアクティブに収集するか、またはパッシブに収集して、ユーザ アイデンティティ情報を含む Active Directory（AD）サーバを設定する必要があります。AD アイデンティティ レルムの設定を参照してください。

パッシブ ID を設定すると、複数の AD レルムの ID からシステムがプルできる AD レルムシーケンスを作成できます。この機能は、ネットワーク内に複数の AD ドメインがある場合に役立ちます。

ステップ 2 パッシブ認証アイデンティティ ルールを使用する場合は、パッシブ アイデンティティ ソースを設定します。

デバイスに実装しているサービスおよびネットワークで使用可能なサービスに基づき、次のいずれかを設定できます。

- リモートアクセス VPN：デバイスへのリモートアクセス VPN 接続をサポートする場合は、AD サーバーまたは（Device Manager に定義されている）ローカルユーザーに基づいて、ユーザーログイン時にアイデンティティを提供できます。RA VPN の設定方法については、リモート アクセス VPN の設定を参照してください。
- Cisco Identity Services Engine（ISE）または Cisco Identity Services Engine Passive Identity Connector（ISE PIC）：これらの製品を使用する場合は、デバイスを pxGrid サブスクライバとして設定し、ISE からユーザ アイデンティティを取得できます。「Identity Services Engine の設定」を参照してください。

ステップ 3 **[ポリシー（Policies）]>[アイデンティティ（Identity）]** を選択し、アイデンティティ ポリシーを有効にします。「アイデンティティ ポリシーの設定 （6 ページ）」を参照してください。

ステップ 4 アイデンティティ ポリシーの設定 （7 ページ）。

システムに設定しているソースに基づいて、パッシブ アイデンティティ ソースが自動的に選択されます。アクティブ認証を設定する場合は、キャプティブ ポータルおよび（SSL 復号ポリシーをまだ有効にしていない場合の）SSL 再署名復号用の証明書を設定する必要があります

ステップ 5 アイデンティティ ポリシーのデフォルト アクションの設定 （9 ページ）を確認してください。

パッシブ認証だけを使用する場合は、パッシブ認証に対するデフォルト アクションを設定でき、特定のルールを作成する必要はありません

ステップ 6 アイデンティティ ルールの設定 （9 ページ）を確認してください。

関連するネットワークからパッシブまたはアクティブユーザ アイデンティティを収集するルールを作成します。

アクティブ認証のベストプラクティス

アイデンティティ ルールによりユーザのアクティブ認証が要求されると、そのユーザを接続するために使用されているインターフェイス上のキャプティブ ポータル ポートにユーザがリダイレクトされ、ユーザに認証が求められます。

このリダイレクションはインターフェイス IP アドレスに対するものなので、ID ポリシー証明書は正確には一致せず、ユーザは信頼できない証明書エラーを受け取ります。続行してデバイスに対して認証されるには、ユーザは証明書を受け入れる必要があります。この動作は中間者攻撃に似ているため、ユーザは信頼できない証明書を受け入れることに消極的です。

この問題を回避するために、デバイス上の1インターフェイスの完全修飾ドメイン名（FQDN）を使用するようにアクティブ認証を設定できます。適切に設定された証明書を使用すると、ユーザは信頼できない証明書エラーを受け取ることがなくなり、認証がよりシームレスになり、安全性が向上します。

始める前に

アクティブ認証はHTTPトラフィックに対してのみ行われ、ユーザのワークステーションや他のクライアントデバイスに対する最新のユーザマッピングがデバイスにない場合は常に、エンドユーザの作業が中断されます。代わりにパッシブ認証を実装することで、中断を回避できます。

手順

ステップ1 DNSサーバで、アクティブ認証を収集するために使用するインターフェイスのインターフェイスIPアドレスの完全修飾ドメイン名（FQDN）を定義します。

これはキャプティブポータルとも呼ばれ、ルーテッドインターフェイスである必要があります。

ステップ2 認証局（CA）を使用して、このFQDNの証明書を取得します。

ftd1.captive-port.example.comなど、特定のFQDNの証明書を作成できます。（任意）以下を実行できます。

- *.captive-port.example.comなど、さまざまなデバイス上のキャプティブ ポータル インターフェイスに適用できるワイルドカード証明書を取得します。ワイルドカードの範囲を広くして、*.eng.example.comや*.example.comなどの幅広いエンドポイントに適用できます。
- 証明書に複数のサブジェクト代替名（SAN）を含めます。

ステップ3 **[オブジェクト（Objects）]** > **[証明書（Certificates）]** を選択し、証明書をアップロードします。

ステップ4 **[オブジェクト（Objects）]** > **[ネットワーク（Network）]** を選択し、DNS名のFQDNネットワークオブジェクトを作成します。

ステップ5 **[ポリシー（Policies）]** > **[アイデンティティ（Identity）]** ページで、証明書とFQDNオブジェクトを使用してIDポリシー設定を更新します。

ステップ6 アクティブ認証を使用するIDポリシーのルールを作成します。

アイデンティティ ポリシーの設定

アイデンティティ ポリシーを使用して、接続からユーザ アイデンティティ情報を収集できます。その後、ユーザアイデンティティに基づく使用状況をダッシュボードに表示し、ユーザまたはユーザ グループに基づくアクセス制御を設定できます。

次に、アイデンティティ ポリシーを介してユーザ アイデンティティを取得するための設定について説明します。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アイデンティティ（Identity）]** の順に選択します。

アイデンティティ ポリシーをまだ定義していない場合には、[アイデンティティポリシーを有効にする（Enable Identity Policy）] をクリックして、アイデンティティ ポリシーの設定 （7 ページ）の説明のとおりに設定します。

ステップ 2 アイデンティティ ポリシーを管理します。

アイデンティティを設定した後、このページにすべてのルールが順番に一覧表示されます。ルールは上から下の順にトラフィックと照合され、最初に一致したルールが、適用するアクションを決定します。このページで、次を実行できます。

- アイデンティティ ポリシーを有効または無効にするには、[アイデンティティポリシー（Identity Policy）] トグルをクリックします。
- アイデンティティポリシー設定を変更するには、[アイデンティティポリシー設定（Identity Policy Configuration）] ボタン（）をクリックします。
- [デフォルトアクション（Default Action）] を変更するには、アクションをクリックして、希望のアクションを選択します。アイデンティティ ポリシーのデフォルト アクションの設定 （9 ページ）を参照してください。
- ルールを移動するには、編集して [順序（Order）] ドロップダウン リストから新しい場所を選択します。
- ルールを設定するには、次の手順を実行します。
  - 新しいルールを作成するには、[+] ボタンをクリックします。
  - 既存のルールを編集する場合は、（[操作（Actions）]列の）対象のルールの編集アイコン（  ）をクリックします。また、テーブル内の特定のルールプロパティをクリックして、そのプロパティを選択的に編集することもできます。
  - 不要になったルールを削除する場合は、（[操作（Actions）]列の）対象のルールの削除アイコン（  ）をクリックします。

アイデンティティ ルールの作成と編集の詳細については、アイデンティティ ルールの設定（9 ページ）を参照してください。

アイデンティティ ポリシーの設定

アイデンティティ ポリシーを機能させるには、ユーザ アイデンティティ情報を提供する送信元を設定する必要があります。必要な設定は、設定するルールのタイプ（パッシブ、アクティブ、または両方）によって異なります。

別のセクションで、設定ダイアログボックスにこれらの設定が表示されます。ダイアログボックスにアクセスする方法に応じて、両方のセクションが表示されるか、または片方のセクションだけが表示されます。構成済みの必要な設定を使用せずに認証タイプのルールを作成しようとすると、自動的にダイアログボックスが表示されます。

次の手順で、すべてのダイアログボックスについて説明します。

始める前に

ディレクトリ サーバ、Threat Defense デバイス、およびクライアント間で時刻設定が一致していることを確認します。これらのデバイス間で時刻にずれがあると、ユーザ認証が成功しない場合があります。「一致」とは、別のタイム ゾーンを使用できるが、たとえば、10 AM PST = 1 PM EST など、それらのゾーンに対して相対的に同じになっている必要があることを意味しています。

手順

ステップ 1 **[ポリシー（Policies）] > [アイデンティティ（Identity）]** を選択します。

ステップ 2 [アイデンティティポリシー設定（Identity Policy Configuration）] ボタン（  ）をクリックします。

ステップ 3 [パッシブ認証（Passive Authentication）] オプションを設定します。

ダイアログボックスに、設定済みのパッシブ認証ソースが表示されます。

必要に応じて、このダイアログボックスで ISE を設定できます。ISE オブジェクトを設定していない場合は、[ISEの統合（Integrate ISE）] リンクをクリックしてすぐに作成することができます。オブジェクトが存在する場合は、状態（[有効（Enabled）] または [無効（Disabled）]）とともに表示されます。

パッシブ認証ルールを作成するには、少なくとも 1 つの有効なパッシブ アイデンティティ ソースを設定している必要があります。

ステップ 4 [アクティブ認証（Active Authentication）] オプションを設定します。

アイデンティティルールによりユーザのアクティブ認証が要求されると、そのユーザはキャプティブポータルポートにリダイレクトされ、認証を求められます。これらの設定を設定する前に、アクティブ認証のベストプラクティス （4 ページ）を読んでください。

- [サーバ証明書（Server Certificate）]：アクティブ認証時にユーザに提示する内部証明書を選択します。必要な証明書をまだ作成していない場合は、ドロップダウンリストの一番下にある [新しい内部証明書の作成（Create New Internal Certificate）] をクリックします。

  ユーザのブラウザが信頼済みの証明書をアップロードしない場合、ユーザは証明書を承認するよう要求されることになります。

- [ホスト名にリダイレクト（Redirect to Host Name）]（Snort 3.0 のみ）：アクティブな認証要求のキャプティブポータルとして使用するインターフェイスの完全修飾ホスト名を定義するネットワークオブジェクトを選択します。オブジェクトが存在しない場合は、[新しいネットワークの作成（Create New Network）] をクリックします。

  FQDN は、デバイス上のいずれかのインターフェイスの IP アドレスに解決される必要があります。FQDN を使用すると、クライアントが認識するアクティブ認証用の証明書を割り当てることができます。これにより、IP アドレスにリダイレクトされたときにユーザに表示される信頼できない証明書の警告を回避できます。証明書では、FQDN、ワイルドカード FQDN、または複数の FQDN をサブジェクト代替名（SAN）に指定できます。

  アイデンティティルールによりユーザのアクティブ認証が要求されているが、リダイレクト FQDN を指定していない場合、ユーザは、接続されているインターフェイス上のキャプティブポータルポートにリダイレクトされます。

- [ポート（Port）]：キャプティブ ポータル ポート。デフォルトは 885（TCP）です。別のポートを設定する場合は、1025 ～ 65535 の範囲にする必要があります。

  （注）
  [ホスト名にリダイレクト（Redirect to Host Name）] FQDN を指定しない場合、HTTP 基本、HTTP 応答ページ、および NTLM 認証方式では、インターフェイスの IP アドレスを使用してユーザがキャプティブポータルにリダイレクトされます。ただし、HTTP ネゴシエートでは、完全修飾 DNS 名 *firewall-hostname.AD-domain-name* を使用してユーザがリダイレクトされます。[ホスト名にリダイレクト（Redirect to Host Name）] FQDN を指定せずに HTTP ネゴシエートを使用する場合は、アクティブ認証が必要なすべての内部インターフェイスの IP アドレスにこの名前をマッピングするように DNS サーバを更新する必要もあります。そうでない場合は、リダイレクションが完了せず、ユーザは認証できません。認証方式に関係なく一貫した動作を確保するために、[ホスト名にリダイレクト（Redirect to Host Name）] FQDN を常に指定することを推奨します。

ステップ 5 （アクティブ認証のみ）。[再署名証明書の復号（Decrypt Re-Sign Certificate）] で、再署名証明書での復号を実装するルールに使用するために内部 CA 証明書を選択します。

事前定義済みの NGFW-Default-InternalCA 証明書か、作成またはアップロードしたものを使用できます。証明書がまだ存在しない場合は、[内部CAを作成（Create Internal CA）] をクリックして作成します。

クライアントのブラウザに証明書をまだインストールしていない場合は、ダウンロードボタン（）をクリックしてコピーを入手します。証明書をインストールする方法については、各ブラウザのマニュアルを参照してください。再署名の復号ルールの CA 証明書のダウンロードも参照してください。

（注）
SSL 復号ポリシーをまだ構成していない場合にのみ SSL 復号の設定が求められます。ID ポリシーを有効にした後、これらの設定を変更するには、SSL 復号ポリシー設定を編集します。

ステップ 6 **[保存（Save）]** をクリックします。

アイデンティティ ポリシーのデフォルト アクションの設定

アイデンティティ ポリシーにはデフォルト アクションがあり、これは個別のアイデンティティ ルールに一致しない接続に実行されます。

実際には、ルールがないことがポリシーの有効な設定になります。すべてのトラフィックの送信元でパッシブ認証を使用する予定の場合は、単純にパッシブ認証をデフォルト アクションとして設定します。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アイデンティティ（Identity）]** の順に選択します。

ステップ 2 [デフォルトアクション（Default Action）] をクリックして、次のいずれかを選択します。

- [パッシブ認証（任意のアイデンティティソース）（Passive Auth (Any Identity Source)）]：ユーザ アイデンティティは、任意のアイデンティティ ルールに一致しない接続に対して設定されたすべてのパッシブ アイデンティティ ソースを使用して特定されます。パッシブ アイデンティティ ソースを設定しない場合は、パッシブ認証をデフォルトとして使用すると [認証なし（No Auth）] を使用することと同じになります。
- [認証なし（認証不要）（No Auth (No Authentication Required)]：ユーザ アイデンティティは、任意のアイデンティティ ルールに一致しない接続について特定されません。

アイデンティティ ルールの設定

アイデンティティ ルールにより、一致するトラフィックでユーザ アイデンティティ情報を収集するかどうかが決まります。一致するトラフィックのユーザアイデンティティ情報を収集しない場合は、[認証なし（No Authentication）] を設定できます。

注意する点として、ルールの設定に関わらず、アクティブ認証はHTTP トラフィックに対してのみ行われます。したがって、HTTP 以外のトラフィックをアクティブ認証から除外するため

のルールを作成する必要はありません。アクティブ認証ルールをすべての送信元および宛先に適用するだけで、すべての HTTP トラフィックのユーザ アイデンティティ情報を取得できます。

（注） また、認証が失敗してもネットワーク アクセスには影響がないことに注意してください。アイデンティティ ポリシーが収集するのはユーザ アイデンティティ情報のみです。認証に失敗したユーザがネットワークにアクセスできないようにするには、アクセス ルールを使用する必要があります。

始める前に

ルールは、トップダウン方式で評価されます。特定のルールの指定されたネットワーク基準に一致する接続の場合、ユーザーは、ルールで指定されたアイデンティティ レルムに対して評価されます。そのレルムの一部ではない場合、そのユーザーは不明としてマークされ、アイデンティティ ポリシー内のそれ以上のルールは評価されません。そのため、評価する必要があるレルムが複数ある場合は、単一のレルムではなく、必ずレルム シーケンスを使用してください。

手順

ステップ 1 **[ポリシー（Policies）] > [アイデンティティ（Identity）]** の順に選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成する場合は、[+] ボタンをクリックします。
- 既存のルールを編集する場合は、対象のルールの編集アイコン（）をクリックします。

不要になったルールを削除する場合は、対象のルールの削除アイコン（）をクリックします。

ステップ 3 [順序（Order）] で、ルールの番号付きリストのどこにルールを挿入するかを選択します。

ルールは最初に一致したものから順に適用されるため、限定的なトラフィック一致基準を持つルールは、同じトラフィックに適用され、汎用的な基準を持つルールよりも上に置く必要があります。

デフォルトでは、ルールはリストの最後に追加されます。ルールの配置を後で変更する場合は、このオプションを編集して配置を変更します。

ステップ 4 [タイトル（Title）] にルールの名前を入力します。

ステップ 5 [Action] を選択し、必要に応じて [AD Identity Source] を選択します。

パッシブおよびアクティブ認証ルールのユーザ アカウントが含まれる AD アイデンティティ レルムを選択する必要があります。必要なレルムがまだ存在しない場合、[新規アイデンティティ レルムの作成（Create New Identity Realm）] をクリックして作成します。パッシブ認証では、単一の AD レルム オブジェクトではなく、AD レルム シーケンスを選択できます。

- [パッシブ認証（Passive Auth）]：パッシブ認証を使用して、ユーザ アイデンティティを判断します。設定されたすべてのアイデンティティ ソースが表示されます。ルールでは、設定されたすべてのソースが自動的に使用されます。
- [アクティブ認証（Active Auth）]：アクティブ認証を使用して、ユーザ アイデンティティを判断します。アクティブ認証はHTTP トラフィックのみに適用されます。他のタイプのトラフィックが、アクティブ認証を要求または許可するアイデンティティ ポリシーに適合した場合、アクティブ認証は試行されません。
- [認証なし（No Auth）]：ユーザ アイデンティティ情報を取得しません。該当するトラフィックにアイデンティティ ベースのアクセス ルールは適用されません。このようなユーザは [認証不要（No Authentication Required）] としてマークされます。

ステップ 6 （アクティブ認証のみ）ディレクトリ サーバでサポートされる認証方式（[タイプ（Type）]）を選択します。

- [HTTP Basic]：暗号化されていないHTTP 基本認証（BA）接続を使用してユーザを認証します。ユーザはブラウザのデフォルト認証ポップアップ ウィンドウを使用してネットワークにログインします。これはデフォルトです。
- [NTLM]：NT LAN Manager（NTLM）接続を使用してユーザを認証します。この選択項目は、AD レルムを選択した場合にのみ有効になります。ユーザはブラウザのデフォルト認証ポップアップ ウィンドウを使用してネットワークにログインしますが、IE およびFirefox ブラウザでは、それぞれの Windows ドメイン ログインを使用して透過的に認証が行われるように設定することができます（透過的なユーザ認証のイネーブル化 （14 ページ）を参照）。
- [HTTP ネゴシエート（HTTP Negotiate）]：このオプションを選択すると、ユーザ エージェント（トラフィック フローを開始するためにユーザが使用しているアプリケーション）とActive Directory サーバの間でデバイスが方式をネゴシエートできるようになります。ネゴシエーションの結果は、一般的にサポートされている方式のうち最も強力な方式（NTLM、基本の順）になります。ユーザはブラウザのデフォルト認証ポップアップ ウィンドウを使用してネットワークにログインします。
- [HTTP 応答ページ（HTTP Response Page）]：システムで提供する Web ページを使用してユーザに認証を求めます。これは、HTTP 基本認証の一種です。

（注）
[ホスト名にリダイレクト（Redirect to Host Name）] FQDN を指定しない場合、HTTP 基本、HTTP 応答ページ、および NTLM 認証方式では、インターフェイスの IP アドレスを使用してユーザがキャプティブポータルにリダイレクトされます。ただし、HTTP ネゴシエートでは、完全修飾 DNS 名 *firewall-hostname.AD-domain-name* を使用してユーザがリダイレクトされます。[ホスト名にリダイレクト（Redirect to Host Name）] FQDN を指定せずに HTTP ネゴシエートを使用する場合は、アクティブ認証が必要なすべての内部インターフェイスの IP アドレスにこの名前をマッピングするように DNS サーバを更新する必要もあります。そうでない場合は、リダイレクションが完了せず、ユーザは認証できません。認証方式に関係なく一貫した動作を確保するために、[ホスト名にリダイレクト（Redirect to Host Name）] FQDN を常に指定することを推奨します。

ステップ 7 （アクティブ認証のみ）**[ゲストとしてフォールバック（Fall Back as Guest）]** > **[オン/オフ（On/Off）]** の順に選択し、アクティブ認証に失敗したユーザに[ゲスト（Guest）]ユーザのラベルを付けるかどうかを指定します。

ユーザは、正常に認証する 3 つの機会が得られます。3 回とも失敗した場合にユーザがどのようにマークされるかは、このオプションによって決まります。これらの値に基づき、アクセスルールを書き込みできます。

- **[ゲストとしてフォールバック（Fall Back as Guest）]** > **[オン（On）]**：ユーザは [ゲスト（Guest）] としてマークされます。
- **[ゲストとしてフォールバック（Fall Back as Guest）]** > **[オフ（Off）]**：ユーザは [失敗した認証（Failed Authentication）] としてマークされます。

ステップ 8 [送信元/宛先（Source/Destination）] タブで、トラフィック一致基準を定義します。

注意する点として、アクティブ認証はHTTP トラフィックでのみ試行されます。したがって、HTTP 以外のトラフィックに対して 「認証なし」のルールを設定は不要で、HTTP 以外のトラフィックに対してアクティブ認証ルールを作成するポイントもありません。ただし、パッシブ認証は任意のタイプのトラフィックに有効です。

アイデンティティ ルールの送信元/宛先基準は、トラフィックが通過するセキュリティ ゾーン（インターフェイス）、IP アドレス、または IP アドレスの国または大陸（地理的位置）、またはトラフィックで使用されるプロトコルおよびポートを定義します。デフォルトでは、すべてのゾーン、アドレス、地理的ロケーション、プロトコル、ポートが対象になります。

条件を変更するには、条件内の [+] ボタンをクリックし、希望するオブジェクトまたは要素を選択し、ポップアップ ダイアログボックスの [OK] をクリックします。基準にオブジェクトが必要で、そのオブジェクトが存在しない場合、[新規オブジェクトの作成（Create New Object）] をクリックします。オブジェクトまたは要素をポリシーから削除するには、そのオブジェクトまたは要素の [x] をクリックします。

以下のトラフィック一致基準を設定できます。

送信元ゾーン、送信先ゾーン

トラフィックが経由するインターフェイスを定義するセキュリティ ゾーン オブジェクト。どのインターフェイスのトラフィックでも適用するものとして、いずれか、または両方の基準を定義することも、両方とも未定義にすることもできます。

- ゾーン内のインターフェイスからデバイスを発信するトラフィックと一致させるには、そのゾーンを [送信先ゾーン（Destination Zones）] に追加します。
- ゾーン内のインターフェイスからデバイスに着信するトラフィックと一致させるには、そのゾーンを [送信元ゾーン（Source Zones）] に追加します。
- 送信元ゾーンと送信先ゾーンの条件を両方ともルールに追加した場合、指定した送信元ゾーンのいずれかから発信されて、指定した送信先ゾーンのいずれかを経由するトラフィックが一致することになります。

トラフィックがデバイスに出入りする場所に基づいてルールを適用する必要がある場合は、この基準を使用します。たとえば、ネットワーク内から発信されるすべてのトラフィックからユーザ アイデンティティが収集されるようにするには、内部ゾーンを [送信元ゾーン（Source Zones）] として選択し、送信先ゾーンを空のままにします。

（注）
1 つのルールにパッシブ セキュリティ ゾーンとルーテッド セキュリティ ゾーンを混在させることはできません。さらに、パッシブセキュリティゾーンは送信元ゾーンとしてのみ指定でき、宛先ゾーンとして指定することはできません。

送信元ネットワーク、宛先ネットワーク

ネットワーク アドレスまたはトラフィックの場所を定義するネットワーク オブジェクトまたは地理的位置です。

- IP アドレスまたは地理的位置からのトラフィックを一致させるには、[送信元ネットワーク（Source Networks）] を設定します。
- IP アドレスまたは地理的位置へのトラフィックを一致させるには、[送信先ネットワーク（Destination Networks）] を設定します。
- 送信元と送信先ネットワークの両方の条件をルールに追加すると、一致するトラフィックは指定した IP アドレスのいずれかから送信され、送信先 IP アドレスのいずれかを通って出力されなければなりません。

この条件を追加するには、次のタブから選択します。

- [ネットワーク（Network）]：制御するトラフィックの送信元または宛先 IP アドレスを定義するネットワーク オブジェクトまたはグループを選択します。
- [地理位置情報（Geolocation）]：位置情報機能を選択して、その送信元または宛先の国や大陸に基づいてトラフィックを制御できます。大陸を選択すると、その大陸内のすべての国が選択されます。地理的位置を直接ルールで選択するほかに、作成した位置情報オブジェクトを選択して場所を定義することもできます。地理的位置を使用すると、特定の国で使用されているすべての潜在的な IP アドレスを知る必要なく、その国へのアクセスを簡単に制限できます。

  （注）
  最新の地理的ロケーションデータを使用してトラフィックがフィルタリングされるようにするために、定期的に地理位置情報データベース（GeoDB）を更新することを強く推奨します。

送信元ポート、宛先ポート/プロトコル

トラフィックで使用されるプロトコルを定義するポート オブジェクト。TCP/UDP の場合、ポートが含まれます。

- 特定のプロトコルまたはポートからのトラフィックと一致させるには、[送信元ポート（Source Ports）] を設定します。送信元ポートに設定できるのは、TCP/UDP のみです。

- プロトコルまたはポートからのトラフィックを一致させるには、[宛先ポート/プロトコル（Destination Ports/Protocols）] を設定します。
- 特定の TCP/UDP ポートから特定の TCP/UDP ポートへ発信されるトラフィックを一致させるには、両方のポートを設定します。送信元および宛先ポートの両方を条件に追加する場合は、単一のトランスポート プロトコル（TCP または UDP）を共有するポートのみを追加できます。たとえば、TCP/80 ポートから TCP/8080 ポートへのトラフィックをターゲットにすることができます。

ステップ 9 **[OK]** をクリックします。

透過的なユーザ認証のイネーブル化

アクティブ認証を許可するようにアイデンティティ ポリシーを設定した場合は、次の認証方式を使用してユーザ アイデンティティを取得できます。

HTTP 基本認証

HTTP 基本認証では、ユーザは常に自分のディレクトリ ユーザ名とパスワードで認証を行うよう要求されます。パスワードはクリア テキストで送信されます。そのため、基本認証はセキュアな認証形式とは見なされません。

基本認証は、デフォルトの認証メカニズムです。

HTTP レスポンス ページ

これは、HTTP 基本認証の一種であり、ユーザにログイン ブラウザ ページが表示されます。

NTLM、HTTP ネゴシエート（Active Directory 用の統合 Windows 認証）

統合 Windows 認証では、ユーザがドメインにログインしてワークステーションを使用するという事実が利用されます。ブラウザは、アクティブ認証中の 脅威に対する防御 キャプティブ ポータルを含め、サーバへのアクセス時にこのドメイン ログインの使用を試みます。パスワードは送信されません。認証が成功すると、ユーザは透過的に認証されるため、認証チャレンジが実行されたのを意識することはありません。

ブラウザがドメイン ログイン クレデンシャルを使用して認証要求を満足できない場合、ユーザは、ユーザ名とパスワードの入力を要求されますが、これは基本認証と同じユーザ エクスペリエンスとなります。つまり、統合 Windows 認証を設定した場合は、同じドメイン内のネットワークまたはサーバにアクセスする際、ユーザがクレデンシャルを入力する必要がなくなります。

HTTP ネゴシエートでは、アクティブ ディレクトリ サーバとユーザ エージェントの両方でサポートされる最も強力な方式が選択されます。ネゴシエーションの認証方式で HTTP Basic が選択された場合は、トランスペアレント認証が行われません。強度の順位はNTLM、基本の順番です。トランスペアレント認証を可能にするためには、ネゴシエーションで NTLM を選択する必要があります。

トランスペアレント認証を有効にするには、統合 Windows 認証をサポートするようにクライアントブラウザを設定する必要があります。以降のセクションでは、広く利用されているブラウザがサポートしている統合 Windows 認証の一般的な要件と基本的な設定について説明します。詳細についてはブラウザ（またはその他のユーザエージェント）のヘルプを参照してください。これは、ソフトウェアのリリースによって方法が異なるためです。

ヒント Chrome や Safari など、すべてのブラウザが統合 Windows 認証をサポートしているとは限りません（本書の執筆時点で入手可能なバージョンに基づきます）。ユーザはユーザ名とパスワードの入力を要求されます。使用しているバージョンがサポートされているかを確認するには、ブラウザのマニュアルを参照してください。

トランスペアレント認証の要件

トランスペアレント認証を実装するには、ユーザ ブラウザまたはユーザ エージェントを設定する必要があります。これは、個別に実行することも、そのための設定を作成し、ソフトウェア配布ツールを使用してその設定をクライアントワークステーションにプッシュすることもできます。この作業をユーザが自分で実行する場合は、ネットワークの具体的な設定パラメータを提供する必要があります。

ブラウザまたはユーザ エージェントに関係なく、次の一般的な設定を実装する必要があります。

- 脅威に対する防御 リダイレクトホスト名、またはユーザがネットワークへの接続に使用するインターフェイスを [信頼済みサイト（Trusted Sites）] リストに追加します。リダイレクトホスト名を使用しない場合、IPアドレスか、使用可能な場合は完全修飾ドメイン名（inside.example.comなど）を使用できます。また、ワイルドカードやアドレスの一部を使用して、汎用化された信頼済みサイトを作成できます。たとえば、*.example.com または単に example.com を使用してすべての内部サイトを網羅し、自社ネットワーク内（example.com 部分は自社ドメイン名）のすべてのサイトを信頼することができます。インターフェイスの特定アドレスを追加する場合には、信頼済みサイトに複数のアドレスを追加して、ネットワークへのすべてのユーザ アクセス ポイントに対処することが必要な場合があります。
- 統合Windows認証は、プロキシサーバ経由で機能しません。したがって、プロキシを使用しないか、脅威に対する防御リダイレクトホスト名を追加するか、またはプロキシを経由しないアドレスにインターフェイスを追加する必要があります。プロキシを使用する必要がある場合、ユーザは NTLM を使用していても認証を要求されます。

ヒント トランスペアレント認証の設定は必須ではありませんが、エンドユーザにとって便利です。トランスペアレント認証を設定しなかった場合、ユーザはすべての認証方式に対するログインチャレンジを提示されます。

トランスペアレント認証用の Internet Explorer の設定

NTLM トランスペアレント認証用に Internet Explorer を設定するには次の手順に従います。

手順

ステップ 1 [ツール（Tools）] > [インターネット オプション（Internet Options）] を選択します。

ステップ 2 [セキュリティ（Security）] タブを選択し、[ローカル イントラネット（Local Intranet）] ゾーンを選択した後、次の手順を実行します。

a) [サイト（Sites）] ボタンをクリックして、信頼済みサイトのリストを開きます。

b) 少なくとも次のオプションの 1 つが選択されていることを確認します。

- [イントラネット ネットワークの自動検出（Automatically detect intranet network）]。このオプションを選択すると、他のすべてのオプションがディセーブルになります。
- [プロキシをバイパスするすべてのサイトを含める（Include all sites that bypass the proxy）]。

c) [詳細（Advanced）] をクリックして [ローカル イントラネット サイト（Local Intranet Sites）] ダイアログボックスを開いた後、信頼する URL を [サイトの追加（Add Site）] ボックスに貼り付けて [追加（Add）] をクリックします。

複数の URL が存在する場合は、このステップを繰り返します。ワイルドカードを使用して、**`http://*.example.com`** のように URL の一部を指定するか、または単に **`*.example.com`** と指定します。

このダイアログボックスを閉じて、[インターネット オプション（Internet Options）] ダイアログボックスに戻ります。

d) [ローカルイントラネット（Local Intranet）] が選択されたままの状態で、[カスタムレベル（Custom Level）] をクリックして [セキュリティ設定（Security Settings）] ダイアログボックスを開きます。**[ユーザ認証（User Authentication）]** > **[ログオン（Logon）]** 設定を探して、[イントラネット ゾーンのみ自動ログオン（Automatic logon only in Intranet zone）] を選択します。[OK]をクリックします。

ステップ 3 [インターネット オプション（Internet Options）] ダイアログボックスで [接続（Connections）] タブをクリックし、次に [LAN 設定（LAN Settings）] をクリックします。

[LANにプロキシサーバを使用する（Use a proxy server for your LAN）] が選択されている場合、脅威に対する防御 インターフェイスがプロキシをバイパスすることを確認する必要があります。必要に応じて、次のいずれかを実行します。

- [ローカルアドレスのプロキシサーバをバイパス]を選択します。

- [詳細（Advanced）] をクリックして、アドレスを [次で始まるアドレスにはプロキシ サーバを使用しない（Do not use proxy server for addresses beginning with）] ボックスに入力します。たとえば、**`*.example.com`** のようにワイルドカードを使用できます。

トランスペアレント認証用の Firefox の設定

NTLM トランスペアレント認証用に Firefox を設定するには、次の手順に従います。

手順

ステップ 1 [about:config] を開きます。フィルタ バーを使用して、変更する必要のあるプリファレンスを検索します。

ステップ 2 NTLM をサポートするには、次のプリファレンスを変更します（network.automatic でフィルタリング）。

- [network.automatic-ntlm-auth.trusted-uris]：プリファレンスをダブルクリックし、URL を入力して [OK] をクリックします。カンマで区切って複数の URL を入力できます。プロトコルを含めるかどうかは任意です。例：

  ```
  http://host.example.com, http://hostname, myhost.example.com
  ```

  URL の一部を使用することもできます。Firefox は、ランダムに部分文字列と照合するのではなく、文字列の末尾と照合します。したがって、ドメイン名のみ指定することにより、内部ネットワーク全体を包含することができます。例：

  ```
  example.com
  ```

- [network.automatic-ntlm-auth.allow-proxies]：値が、デフォルトの [true] であることを確認します。値が [false] になっている場合は、ダブルクリックして変更します。

ステップ 3 HTTP プロキシ設定を確認します。これを確認するには、**[ツール（Tools）]** > **[オプション（Options）]** を選択し、次に [オプション（Options）] ダイアログボックスで [ネットワーク（Network）] タブをクリックします。[接続（Connection）] グループで、[設定（Settings）] ボタンをクリックします。

- [プロキシなし（No Proxy）] が選択されている場合は、何も設定する必要がありません。
- [システム プロキシ設定を使用（Use System Proxy Settings）] が選択されている場合、[about:config] 内の [network.proxy.no_proxies_on] プロパティを変更して、[network.automatic-ntlm-auth.trusted-uris] に含めた信頼済み URI を追加する必要があります。
- [手動プロキシ設定（Manual Proxy Configuration）] が選択されている場合、これらの信頼済み URI を包含するように [プロキシなし（No Proxy For）] リストを更新します。

- 他のオプションの1つが選択されている場合、これらの設定で使用するプロパティから同一の信頼済み URI が除外されていることを確認します。

アイデンティティ ポリシーのモニタリング

認証が必要なアイデンティティ ポリシーが正しく機能している場合、ユーザ情報は **[モニタリング（Monitoring）]** > **[ユーザ（Users）]** ダッシュボードやその他のダッシュボード（ユーザ情報を含む）に表示されます。

さらに、**[モニタリング（Monitoring）]** > **[イベント（Events）]** に表示されるイベントにユーザ情報が含まれます。

ユーザ情報がまったく表示されない場合は、ディレクトリ サーバが正しく機能していることを確認してください。[ディレクトリ サーバ設定（directory server configuration）] ダイアログボックスの [テスト（Test）] ボタンを使用して接続を確認します。

ディレクトリ サーバが機能し、使用可能である場合、アクティブ認証を必要とするアイデンティティ ルールのトラフィック一致条件が、ユーザを照合するように書かれていることを確認します。たとえば、ユーザ トラフィックがデバイスを通過する際のインターフェイスが、ソース ゾーンに含まれていることを確認します。アクティブ認証アイデンティティ ルールは HTTP トラフィックのみを照合するため、ユーザはデバイスを通じてそのタイプのトラフィックを送信している必要があります。

パッシブ認証の場合、そのソースを使用しているときは、ISE オブジェクトの [テスト（Test）] ボタンを使用します。リモート アクセス VPN を使用している場合は、サービスが正常に機能していることと、ユーザが VPN 接続を確立できることを確認します。問題の特定と解決の詳細については、これらの機能に関するトラブルシューティングのトピックを参照してください。

アイデンティティ ポリシーの例

使用例の章には、アイデンティティ ポリシーの実装例が含まれています。ネットワーク トラフィックを調べる方法を参照してください。

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。