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、接続からユーザーアイデンティティ情報を収集できます。その後で、ダッシュボードにユーザーアイデンティティに基づく使用状況を表示し、ユーザーまたはユーザー グループに基づくアクセス コントロールを設定できます。

アイデンティティ ポリシーの概要

接続に関連付けられているユーザーを検出するためにアイデンティティ ポリシーを使用できます。ユーザーを識別することで、脅威、エンドポイント、およびネットワーク インテリジェンスをユーザー ID 情報に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、およびイベントを個別のユーザーに直接リンクすることによって、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とされたホストを誰が所有し、誰が内部攻撃やポート スキャンを開始したかを確認できます。また、高帯域幅のユーザーや、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ーを確認することもできます。

ユーザーの検出は、分析用のデータを収集するだけではありません。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、ユーザー アイデンティティについて詳しく説明します。

パッシブ認証によるユーザー アイデンティティの確立

パッシブ認証では、ユーザーにユーザー名とパスワードを求めることなくユーザー ID 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）。

特定のユーザー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。

アクティブ認証によるユーザー ID 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、HTTP トラフィック フローがユーザー ID のマッピングがないシステムの IP アドレスから送られてきたときに、ネットワークに設定されたディレクトリを使用して、トラフィック フローを開始したユーザーを認証するかどうかを決定できます。ユーザーが正常に認証された場合、IP アドレスは認証されたユーザーの識別情報を保持していると見なされます。

認証が失敗しても、ユーザーのネットワーク アクセスは妨げられません。アクセス ルールは最終的に、これらのユーザーにどのアクセスを提供するか決定します。

不明なユーザーの対処

アイデンティティ ポリシーのディレクトリ サーバーを設定すると、システムはディレクトリ サーバーからユーザーおよびグループ 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 時間ごとに夜中に更新されるか、またはディレクトリ設定を編集して保存するたびに（変更がなくても）更新されます。

アクティブな認証アイデンティティ ルールによって求められた認証に成功したにも関わらず、ユーザー名がダウンロードしたユーザー ID 情報の中に存在しない場合、不明なユーザーとし

てマークされます。ID 関連のダッシュボードにそのユーザーの ID は表示されず、ユーザー一致グループ ルールにも検出されません。

ただし、不明なユーザーに対するアクセス コントロール ルールが適用されます。たとえば、不明なユーザーの接続をブロックすると、これらのユーザーは、たとえ認証に成功（ディレクトリ サーバーがユーザーとパスワードが有効であると認識したことを意味する）してもブロックされます。

そのため、ユーザーの追加や削除、グループ メンバーシップの変更などをディレクトリ サーバーに加えた場合、システムがディレクトリから更新情報をダウンロードするまで、これらの変更はポリシーの適用に反映されません。

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） 新規に追加したユーザー、または削除したユーザーの情報がシステムに反映されているかどうかを確認するには、**[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]** を選択して、[ルールの追加(+)（Add Rule (+)）] ボタンをクリックします。[ユーザー（Users）] タブに表示されたユーザーのリストを確認してください。新規ユーザーを検出できないか、または削除されたユーザーが検出される場合、システムには古い情報があります。

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 復号化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 （5 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 ポリシー設定の構成 （6 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）。

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）。

関連するネットワークからパッシブまたはアクティブ ユーザー 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 ルールにユーザのアクティブ認証が必要な場合、ユーザは接続されているインターフェイスのキャプティブ ポータル ポートにリダイレクトされ、その後、認証を要求されます。

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、ユーザー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、ユーザー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、ユーザー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、

ユーザー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、ユーザー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ーマッピングがデバイスにない場合は常に、エンドユーザー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サーバーで、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、接続からユーザーアイデンティティ情報を収集できます。その後で、ダッシュボードにユーザーアイデンティティに基づく使用状況を表示し、ユーザーまたはユーザー グループに基づくアクセス コントロールを設定できます。

次に、アイデンティティ ポリシーでユーザー アイデンティティを取得するために必要な要素を設定する方法の概要を示します。

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。

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 ポリシー設定の構成（6 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。

アイデンティティ設定を行うと、このページにすべてのルールが順番にリストアップされます。上から下に向かってルールがトラフィックと照合され、最初に適合したルールによって、適用されるアクションが決定されます。このページで次の操作を実行できます。

- 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。テーブルでプロパティをクリックして、選択的にルールのプロパティを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（delete）] アイコン（  ）をクリックします。

アイデンティティ ルールの作成と変更の詳細については、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 ポリシー設定の構成

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 サーバー、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ますが、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ーのアクティブ認証が要求されると、そのユーザー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。

  ブラウザが信頼している証明書をアップロードしない場合、ユーザは証明書を許可する必要があります。

- [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ー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、ユーザーは、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ー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、ユーザは完全修飾 DNS 名 *firewall-hostname.AD-domain-name* を使用して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 サーバーを更新する必要もあります。そうしないと、リダイレクトは実行できず、ユーザを認証できません。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）]** を選択します。

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)]：ユーザー 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 ルールは、一致するトラフィックに対してユーザ識別情報を収集する必要があるかどうかを定義します。一致するトラフィックのユーザ識別情報を取得しない場合は、「認証なし」を設定します。

ルール設定に関係なく、アクティブ認証はHTTPトラフィックに対してのみ実行されることに注意してください。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ルールを作成する必要はありません。すべてのHTTPトラフィックに対してユーザ識別情報を取得する場合は、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済みます。

（注） また、認証に失敗してもネットワーク アクセスには影響しません。アイデンティティ ポリシーは、ユーザ識別情報のみを収集します。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。

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 次のいずれかを実行します。

- 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には、ルールの [編集（edit）] 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には、ルールの [削除（delete）] 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。ルールの順序を後で変更する場合、このオプションを編集します。

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）]：ユーザ識別情報を取得しません。このトラフィックに、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。これらのユーザは、[認証不要（No Authentication Required）] とマークが付けられます。

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

- [HTTP基本（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の認証ポップアップ ウィンドウを使用してネットワークにログインします。これがデフォルトです。
- [NTLM]：NT LAN マネージャ（NTLM）接続を使用して、ユーザを認証します。この選択は AD レルムを選択するときにのみ使用できます。Windows ドメインのログインを使ってトランスペアレント認証が行われるよう、IE と Firefox ブラウザを設定することはできますが、ユーザはブラウザのデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします（トランスペアレント ユーザ認証の有効化 （13 ページ）を参照してください）。

- [HTTPネゴシエート（HTTP Negotiate）]：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）方式とActive Directoryサーバ方式の間でデバイスがネゴシエーションできるようになります。ネゴシエーションの結果は、NTLM、ベーシックの順に、共通にサポートされ、使用されている最も強力な方式になります。ユーザはブラウザのデフォルトの認証ポップアップ 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）]：システムが提供するWebページを使用して、ユーザに認証を求めるプロンプトを表示します。これは、HTTP 基本認証の 1 つの形式です。

（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ー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、ユーザは完全修飾 DNS 名 *firewall-hostname.AD-domain-name* を使用して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 サーバーを更新する必要もあります。そうしないと、リダイレクトは実行できず、ユーザを認証できません。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）アクティブ認証に失敗したユーザをゲストユーザとしてラベル付けするかどうかを決めるには、**[ゲストとしてフォールバック（Fall Back as Guest）]** > **[オン/オフ（On/Off）]** を選択します。

ユーザは、正常に認証する3つの機会が得られます。失敗した場合、このオプションの選択により、ユーザがどのようにマーク付けされるかが決まります。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。

アクティブ認証は、HTTP トラフィックに対してのみ試されることに注意してください。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。デフォルトは、すべてのゾーン、アドレス、地理的位置、プロトコル、およびポートです。

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。

次のトラフィック一致基準を設定できます。

送信元ゾーン、宛先ゾーン

トラフィックが通過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。1つの基準を定義する 、両方の基準を定義する、またはどちらの基準も定義しないことができます。指定しない基準は、すべてのインターフェイスのトラフィックに適用されます。

- ゾーン内のインターフェイスからデバイスを離れるトラフィックを照合するには、そのゾーンを [宛先ゾーン（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入るトラフィックを照合するには、そのゾーンを [送信元ゾーン（Source Zones）] に追加します。
- 送信元ゾーン条件と宛先ゾーン条件の両方をルールに追加する場合、一致するトラフィックは指定された送信元ゾーンの 1 つから発生し、宛先ゾーンの 1 つを通って出力する必要があります。

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、内部ネットワークから発信されるすべてのトラフィックからユーザ識別情報を収集する場合、内部ゾーンを [送信元ゾーン（Source Zones）] として選択し、宛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

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

- IP アドレスまたは地理的位置からのトラフィックを照合するには、[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照合するには、[宛先ネットワーク（Destination Networks）] を設定します。
- 送信元（Source）ネットワーク条件と宛先（Destination）ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信されかつ宛先 IP アドレスに送信されるトラフィックの照合を行う必要があります。

この条件を追加する場合、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、大陸内のすべての国が選択されます。ルール内で地理的位置を直接選択する以外に、作成した地理位置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） 最新の地理的位置データを使用してトラフィックをフィルタ処理できるように、地理位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします。

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 では、これにポートを含めることができます。

- プロトコルまたはポートからのトラフィックを照合するには、[送信元ポート（Source Ports）] を設定します。送信元ポートを使用できるのは、TCP/UDP のみです。
- プロトコルまたはポートへのトラフィックを照合するには、[宛先ポート/プロトコル（Destination Ports/Protocols）] を設定します。
- 特定の TCP/UDP ポートから発生し、特定の TCP/UDP ポートに向かうトラフィックを照合するには、両方設定します。送信元ポートと宛先ポートの両方を条件に追加する場合、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、ポート TCP/80 からポート TCP/8080 へのトラフィックを対象にできます。

ステップ 9 [OK] をクリックします。

トランスペアレント ユーザ認証の有効化

アクティブ認証を有効にするためにアイデンティティ ポリシーを設定する場合、ユーザ ID を取得するために次の認証方式を使用できます。

HTTP Basic

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を認証するように要求されます。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 応答ページ

これは、HTTP 基本認証の一種であり、ユーザのログイン ブラウザ ページに表示されます。

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

統合 Windows 認証は、実際に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ために利用されます。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、ユーザは何らかの認証チャレンジが実行されたことを意識せずに、トランスペアレント認証が行われます。

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たせない場合、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 エクスペリエンスです。したがって、統合 Windows 認証を設定した場合、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ときに、ユーザがクレデンシャルを入力する必要性を減らすことができます。

なお、HTTP ネゴシエートは、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がサポートする、最も強力な方式を選択することに注意してください。ネゴシエーションが認証方式としてHTTP基本認証を選択した場合、トランスペアレント認証は行われません。強度の順序は、NTLM、次に基本認証です。トランスペアレント認証を可能にするには、ネゴシエーションが 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。以下に、統合 Windows 認証をサポートする、広く使用されている一部のブラウザに関して、一般的な要件と基本設定について説明します。ソフトウェア リリースごとに技術が変更される場合があるため、詳細情報についてはブラウザ（または他のユーザ エージェント）のヘルプを参照してください。

ヒント　Chrome および Safari など、すべてのブラウザが統合 Windows 認証をサポートするとは限りません（このガイドのリリース時に使用可能だった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でサポートが使用可能かどうかを確認するには、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、ブラウザまたはユーザー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。この作業をユーザーが自分で実行する場合は、ネットワークで機能する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、またはユーザー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、ワイルドカードまたはアドレスの一部

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、一般的には *.example.com または単に example.com を使用してすべて内部サイトを網羅し、ネットワーク内のすべてのサイトを信頼できます（自身のドメイン名を使用）。インターフェイスの特定アドレスを追加する場合は、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ー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、ユーザーは NTLM を使用する場合で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、ユーザー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を有効にするよう Internet Explorer を設定するには、次の手順を実行します。

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、信頼できる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を自動的に検出する（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無効になります。
- [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き、次に信頼する 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。**[ユーザー認証（User Authentication）] > [ログオン（Logon）]** 設定を探して、[自動ログオンをイントラネットゾーンのみで有効にする（Automatic logon only in Intranet zone）] を選択します。[OK] をクリック

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でプロキシ サーバーを使用する（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。

- [ローカルアドレスにはプロキシサーバを使用しない（Bypass proxy server for local addresses）] 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ーを使用しない（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を有効にするよう Firefox を設定するには、次の手順を実行します。

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、修正する必要のある設定を検索します。

ステップ 2 NTLM をサポートするには、次の設定を修正します（network.automatic でフィルタリング）。

- [network.automatic-ntlm-auth.trusted-uris] ：設定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。次に例を示します。

```
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。次に例を示します。

```
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）] タブをクリックすると見つかります。[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。
- [システムの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] プロパティを修正して、[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

認証を必要とするアイデンティティ ポリシーが正常に動作している場合は、**[モニタリング（Monitoring）]**>**[ユーザー（Users）]** ダッシュボードやユーザー情報を含むその他のダッシュボードにユーザー情報が表示されます。

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もユーザー情報が含まれています。

ユーザー情報が表示されない場合は、ディレクトリ サーバーが正常に機能していることを確認します。接続を確認するには、ディレクトリ サーバーの設定ダイアログ ボックスの [テスト（Test）] ボタンを使用します。

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、送信元ゾーンに、ユーザー トラフィックがデバイスに入力するために経由するインターフェイスが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。