アイデンティティ ポリシー

次のトピックでは、アイデンティティ ルールとアイデンティティ ポリシーの作成方法と管理方法について説明します。

アイデンティティ ポリシーについて

アイデンティティ ポリシーには、アイデンティティ ルールが含まれます。アイデンティティ ルールでは、トラフィックのセットを、レルムおよび認証方式（パッシブ認証、アクティブ認証、または認証なし）と関連付けます。

次の段落の最後に記載されている例外を除き、使用する予定のレルムと認証方式は、アイデンティティ ルールで起動する前に設定する必要があります。

- **Integration** > **Other Integrations** > **Realms** > **Realms** で、アイデンティティ ポリシー外のレルムを構成します。詳細については、LDAP レルムまたは Active Directory（AD）レルムおよびレルムディレクトリを作成する を参照してください。
- **Integration** > **Other Integrations** > **Identity Sources** で、パッシブ認証 ID ソースである ISE/ISE-PIC を構成します。詳細については、Cisco Identity Services Engine (Cisco ISE) アイデンティティ ソースの構成方法を参照してください。

- パッシブ認証のアイデンティティ ソースである TS エージェントについては、システムの外で構成します。詳細については、『*Cisco Terminal Services (TS) Agent Guide*』を参照してください。
- アクティブ認証のアイデンティティ ソースであるキャプティブ ポータルについては、アイデンティティ ポリシー内で設定します。詳細については、ユーザー制御のためのキャプティブ ポータルの構成方法を参照してください。
- リモート アクセス VPN ポリシー内では、アクティブな認証アイデンティティ ソースであるリモート アクセス VPN を設定します。詳細については、リモート アクセス VPN 認証を参照してください。

単一のアイデンティティ ポリシーに複数のアイデンティティ ルールを追加した後、ルールの順番を決めます。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。トラフィックが一致する最初のルールがそのトラフィックを処理するルールです。

ネットワーク オブジェクトでトラフィックをフィルタ処理することもできます。これにより、デバイスがメモリ制限に達しているか、または制限に近い状態の場合に、各デバイスがモニターするネットワークが制限されます。

1 つ以上のアイデンティティ ポリシーを設定した後、1 つのアイデンティティ ポリシーをアクセス コントロール ポリシーに関連付ける必要があります。ネットワークのトラフィックがアイデンティティ ルールの条件と一致する場合、システムはトラフィックを指定されたレルムと関連付け、指定されたアイデンティティ ソースを使用してトラフィックのユーザーを認証します。

アイデンティティ ポリシーを構成しない場合、システムはユーザー認証を実行しません。

アイデンティティ ポリシーの作成に関する例外

次のすべてに該当する場合、アイデンティティ ポリシーは必要ありません。

- ISE/ISE-PIC アイデンティティ ソースを使用できます。
- アクセス コントロール ポリシーのユーザまたはグループは使用しません。
- アクセス コントロール ポリシーのセキュリティ グループ タグ（SGT）を使用します。詳細については、「ISE SGT とカスタム SGT ルール条件との比較」を参照してください。

関連トピック

アイデンティティ ポリシーのセットアップ方法

アイデンティティ ポリシーのライセンス要件

Threat Defense License

任意

アイデンティティ ポリシーの要件と前提条件

Model support

任意

Supported domains

Any

User roles

- Admin
- Access Admin
- Network Admin

アイデンティティ ポリシーの作成

このタスクでは、アイデンティティポリシーの作成方法について説明します。

始める前に

アイデンティティ ポリシーは、アクセス コントロール ポリシーのレルムでユーザやグループを使用するために必要です。LDAP レルムまたは Active Directory（AD）レルムおよびレルムディレクトリを作成するの説明に従って 1 つ以上のレルムを作成し、有効にします。

（オプション）多数のユーザーグループをモニターする特定の管理対象デバイスの場合、管理対象デバイスのメモリ制限のためにグループに基づいてユーザーマッピングがドロップされることがあります。その結果、レルムまたはユーザー条件を使用するルールが想定どおりに実行されない可能性があります。デバイスがバージョン6.7以降を実行している場合は、1つのネットワークまたはネットワーク グループ オブジェクトのみによってトラフィックをモニターするアイデンティティルールを設定できます。ネットワークオブジェクトの作成については、ネットワーク オブジェクトの作成を参照してください。

次のすべてに該当する場合、アイデンティティ ポリシーは必要ありません。

- ISE/ISE-PIC アイデンティティ ソースを使用できます。
- アクセス コントロール ポリシーのユーザまたはグループは使用しません。
- アクセス コントロール ポリシーのセキュリティ グループ タグ（SGT）を使用します。詳細については、「ISE SGT とカスタム SGT ルール条件との比較」を参照してください。

手順

ステップ 1 Firewall Management Center にログインします。

ステップ 2 **Policies** > **Access Control heading** > **Identity** をクリックし、[新しいポリシー（New Policy）] をクリックします。

ステップ 3 [名前（Name）] を入力し、必要に応じて [説明（Description）] を入力します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 ポリシーにルールを追加するには、アイデンティティ ルールの作成 （14 ページ）で説明されているように、[ルールの追加（Add Rule）] をクリックします。

ステップ 6 ルール カテゴリを作成するには、[カテゴリの追加（Add Category）] をクリックします。

ステップ 7 キャプティブポータルのアクティブ認証を設定するには、[アクティブ認証（Active Authentication）] をクリックし、アクティブ認証ルールを含むアイデンティティ ポリシーを作成します。 を参照します。

ステップ 8 （オプション）ネットワークオブジェクトでトラフィックをフィルタ処理するには、[Identity Source] タブをクリックします。リストから、この ID ポリシーのトラフィックのフィルタ処理に使用するネットワークオブジェクトをクリックします。新しいネットワークオブジェクトを作成するには、**Add** (＋) をクリックします。

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

次のタスク

- 照合するユーザーおよび他のオプションを指定するルールを、アイデンティティ ポリシーに追加します（アイデンティティ ルールの作成 （14 ページ）を参照）。
- 指定したリソースへのアクセスを特定のユーザーに許可またはブロックするには、このアイデンティティ ポリシーをアクセス コントロール ポリシーに関連付けます（アクセス制御への他のポリシーの関連付けを参照）。
- （Microsoft Azure AD レルムの場合は不要です）。設定変更を管理対象デバイスに展開します（設定変更の展開を参照）。

問題が発生した場合は、ユーザー制御のトラブルシューティング （27 ページ）を参照してください。

関連トピック

アクティブ認証ルールを含むアイデンティティ ポリシーを作成します。
キャプティブ ポータル フィールド
ユーザー制御のトラブルシューティング （27 ページ）
アイデンティティ マッピング フィルタの作成 （5 ページ）

アイデンティティ マッピング フィルタの作成

アイデンティティ マッピング フィルタを使用して、アイデンティティ ルールが適用されるネットワークを制限できます。たとえば、Firewall Management Center がメモリ量の限られた FTD を管理している場合、モニターするネットワークを制限できます。

IPv4 アドレスと IPv6 アドレスに対して個別のアイデンティティ マッピング フィルタを作成する必要があります。

必要に応じて、以下からサブネットを除外することもできます。

- ユーザーから IP へ、およびセキュリティ グループ タグ（SGT）から IP へのマッピングを ISE から受信する。
- passive identity agent から、ユーザーから IP へのマッピングを受信する。

通常は、Snort アイデンティティ正常性モニターのメモリエラーを防ぐために、メモリの少ない管理対象デバイスに対してこれを行う必要があります。

始める前に

次の作業を実行します。

1. アイデンティティ ポリシーに必要なレルムを作成します。LDAP レルムまたは Active Directory（AD）レルムおよびレルム ディレクトリを作成するを参照してください。
2. アイデンティティ ポリシーを作成します。アイデンティティ ポリシーの作成 （3 ページ）を参照してください。
3. ネットワーク オブジェクトの作成の説明に従って、ネットワーク オブジェクトまたはネットワーク グループ オブジェクトを作成します。作成するネットワーク オブジェクトまたはグループでは、管理対象デバイスがアイデンティティ ポリシーでモニターするネットワークを定義する必要があります。

手順

ステップ 1 Firewall Management Center にログインします。

ステップ 2 **Policies** > **Access Control heading** > **Identity** をクリックします。

ステップ 3 **Edit** (✎) をクリックします。

ステップ 4 [アイデンティティの送信元（Identity Source）] タブをクリックします。

ステップ 5 [アイデンティティ マッピング フィルタ（Identity Mapping Filter）] リストから、フィルタとして使用するネットワーク オブジェクトの名前をクリックする。

新しいネットワーク オブジェクトを作成するには、ネットワーク オブジェクトの作成を参照してください。

（注）

トラフィックを IPv6 アドレスに制限するには、少なくとも 1 つのアドレス、ネットワーク、またはグループをフィルタに追加する必要があります。

ステップ 6 **[Save（保存）]** をクリックします。

ステップ 7 （Microsoft Azure AD レルムの場合は不要です）。設定変更を管理対象デバイスに展開します（設定変更の展開を参照）。

次のタスク

（Microsoft Azure AD レルムの場合は不要です）。アイデンティティ ポリシーをアクセス コントロール ポリシーに関連付けます（アクセス制御への他のポリシーの関連付け を参照）。

ISEアイデンティティマッピングフィルタ（サブネットフィルタとも呼ばれる）を確認または変更するには、以下のコマンドを使用します。

```
show identity-subnet-filter
configure identity-subnet-filter { add | remove } subnet
```

アイデンティティ ルールの条件

ルール条件を使用すると、アイデンティティポリシーを微調整して、制御するユーザーとネットワークをターゲットにすることができます。詳細については、次の項を参照してください。

関連トピック

セキュリティ ゾーン ルール条件
ネットワークルールの条件
VLAN タグ ルールの条件
ポートルールの条件
レルムと設定のルール条件 （11 ページ）

セキュリティ ゾーン ルール条件

セキュリティゾーンはネットワークをセグメント化して複数のデバイス間でインターフェイスをグループ化することで、トラフィックフローを管理、分類、および復号しやすくします。

セキュリティゾーンは、トラフィックをその送信元と宛先のセキュリティゾーンで制御または復号します。送信元ゾーンと宛先ゾーンの両方をゾーン条件に追加すると、送信元ゾーンのいずれかにあるインターフェイスから発信され、宛先ゾーンのいずれかにあるインターフェイスを通過するトラフィックだけが一致することになります。

ゾーン内のすべてのインターフェイスは同じタイプ（すべてインライン、パッシブ、スイッチド、またはルーテッド）である必要があるのと同じく、ゾーン条件で使用するすべてのゾーンも同じタイプである必要があります。パッシブに展開されたデバイスはトラフィックを送信しないため、パッシブインターフェイスのあるゾーンを宛先ゾーンとして使用することはできません。

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

ヒント　ゾーンによってルールを制限することは、システムのパフォーマンスを向上させる最適な手段の 1 つです。ルールがデバイスのインターフェイスを通過するトラフィックに適用しなければ、ルールがそのデバイスのパフォーマンスに影響することはありません。

セキュリティ ゾーン条件とマルチテナンシー

マルチドメイン導入では、先祖ドメイン内に作成されるゾーンに、別のドメイン内にあるデバイス上のインターフェイスを含めることができます。子孫ドメイン内のゾーン条件を設定すると、その設定は表示可能なインターフェイスだけに適用されます。

ネットワークルールの条件

ネットワークは、内部ヘッダーを使用して、送信元と宛先の IP アドレスを基準にトラフィックを制御するか、復号します。外部ヘッダーを使用するトンネルルールでは、ネットワーク条件の代わりにトンネル エンドポイント条件を使用します。

事前定義されたオブジェクトを使用してネットワーク条件を作成することも、個々の IP アドレスまたはアドレスブロックを手動で指定することもできます。

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

（注）　アイデンティティルールで FDQN ネットワークオブジェクトを使用することはできません。

ホスト名ネットワーク ルール条件へのリダイレクト

（Snort 3.0 のみ）キャプティブポータルがアクティブな認証要求に使用できるインターフェイスの完全修飾ホスト名（FQDN）を含むネットワークオブジェクトを使用できます。

FQDN は、管理対象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、管理対象デバイスの IP アドレスにリダイレクトされたときにユーザー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、1 つの 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、接続されている管理対象デバイスの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。

[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、ユーザーは完全修飾 DNS 名 *firewall-hostname.directory-server-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には、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。

VLAN タグ ルールの条件

（注） アクセス ルールの VLAN タグは、インラインセットにのみ適用されます。VLAN タグを持つアクセスルールは、ファイアウォール インターフェイス上のトラフィックを照合しません。

VLAN ルール条件によって、Q-in-Q（スタック VLAN）など、VLAN タグ付きトラフィックが制御されます。システムでは、プレフィルタ ポリシー（そのルールで最も外側の VLAN タグを使用する）を除き、最も内側の VLAN タグを使用して VLAN トラフィックをフィルタ処理します。

次の Q-in-Q サポートに注意してください。

- Firepower 4100/9300 上の Firewall Threat Defense：Q-in-Q をサポートしません（1 つの VLAN タグのみをサポート）。
- 他のすべてのモデルの Firewall Threat Defense
  - インラインセットおよびパッシブインターフェイス：Q-in-Q をサポートします（最大 2 つの VLAN タグをサポート）。
  - ファイアウォール インターフェイス：Q-in-Q をサポートしません（1 つの VLAN タグのみをサポート）。

事前定義のオブジェクトを使用して VLAN 条件を作成でき、また 1 ～ 4094 の VLAN タグを手動で入力することもできます。VLAN タグの範囲を指定するには、ハイフンを使用します。

クラスタで VLAN マッチングに問題が発生した場合は、アクセス コントロール ポリシーの詳細オプションである [トランスポート/ネットワークリプロセッサ設定（Transport/Network Preprocessor Settings）] を編集し、[接続の追跡時にVLAN ヘッダーを無視する（Ignore the VLAN header when tracking connections）] オプションを選択します。

ポートルールの条件

ポート条件を使用することで、トラフィックの送信元および宛先のポートに応じてそのトラフィックを制御できます。

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

ポートベースのルールのベストプラクティス

ポートの指定は、アプリケーションをターゲット指定するための従来の方法です。ただし、アプリケーションは、固有のポートを使用してアクセス コントロール ブロックをバイパスするように設定することが可能です。そのため、可能な場合は常に、ポート基準ではなくアプリケーション フィルタリング基準を使用してトラフィックをターゲット指定します。

アプリケーションフィルタリングは、制御フローとデータフローのために個別のチャネルを動的に開くアプリケーション（Firewall Threat Defense など）にも推奨されます。ポートベースのアクセス コントロール ルールを使用すると、これらの種類のアプリケーションが正しく動作しなくなり、望ましい接続がブロックされる可能性があります。

送信元と宛先ポートの制約の使用

送信元ポートと宛先ポートの両方を制約に追加する場合、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、送信元ポートとして DNS over TCP を追加する場合は、宛先ポートとして Yahoo Messenger Voice Chat（TCP）を追加できますが、Yahoo Messenger Voice Chat（UDP）は追加できません。

送信元ポートのみ、あるいは宛先ポートのみを追加する場合は、異なるトランスポートプロトコルを使用するポートを追加できます。たとえば、DNS over TCP および DNS over UDP の両方を 1 つのアクセス コントロール ルールの送信元ポート条件として追加できます。

ポート、プロトコル、および ICMP コード ルールの条件

ポート条件により、送信元ポートと宛先ポートに基づいてトラフィックが照合されます。ルールのタイプによって、「ポート」は次のいずれかを表します。

- TCP と UDP：TCP と UDP のトラフィックは、ポートに基づいて制御できます。システムは、カッコ内に記載されたプロトコル番号+オプションの関連ポートまたはポート範囲を使用してこの設定を表します。例：TCP(6)/22。
- ICMP：ICMP および ICMPv6（IPv6 ICMP）トラフィックは、そのインターネット層プロトコルと、オプションでタイプおよびコードに基づいて制御できます。例：ICMP(1):3:3
- プロトコル：ポートを使用しないその他のプロトコルを使用してトラフィックを制御できます。

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

ポートベースのルールのベスト プラクティス

ポートの指定は、アプリケーションをターゲット指定するための従来の方法です。ただし、アプリケーションは、固有のポートを使用してアクセス コントロール ブロックをバイパスするように設定することが可能です。そのため、可能な場合は常に、ポート基準ではなくアプリケーション フィルタリング基準を使用してトラフィックをターゲット指定します。なお、プレフィルタルールではアプリケーション フィルタリングを使用できません。

アプリケーション フィルタリングは、制御フローとデータフローのために個別のチャネルを動的に開くアプリケーション（FTP など）にも推奨されます。ポートベースのアクセス コントロール ルールを使用すると、これらの種類のアプリケーションが正しく動作しなくなり、望ましい接続がブロックされる可能性があります。

送信元と宛先ポートの制約の使用

送信元ポートと宛先ポートの両方を制約に追加する場合、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、送信元ポートとして DNS over TCP を追加する場合は、宛先ポートとして Yahoo Messenger Voice Chat（TCP）を追加できますが、Yahoo Messenger Voice Chat（UDP）は追加できません。

送信元ポートのみ、あるいは宛先ポートのみを追加する場合は、異なるトランスポートプロトコルを使用するポートを追加できます。たとえば、DNS over TCP と DNS over UDP の両方を 1 つのアクセスコントロールルールの宛先ポート条件として追加できます。

ポート条件を使用した非 TCP トラフィックの照合

ポートベースではないプロトコルを照合できます。デフォルトでは、ポート条件を指定しない場合は IP トラフィックを照合します。非 TCP トラフィックを照合するためのポート条件を設定することはできますが、いくつかの制約事項があります。

- アクセス コントロール ルール：クラシック デバイスの場合、GRE でカプセル化されたトラフィックをアクセス コントロール ルールに照合するには、宛先ポート条件として GRE（47）プロトコルを使用します。GRE 制約ルールには、ネットワーク ベースの条件（ゾーン、IP アドレス、ポート、VLAN タグ）のみを追加できます。また、GRE 制約ルールが設定されたアクセス コントロール ポリシーでは、システムが外側のヘッダーを使用して**すべての**トラフィックを照合します。Firewall Threat Defense デバイスの場合、GRE でカプセル化されたトラフィックを制御するには、プレフィルタ ポリシーでトンネル ルールを使用します。
- 復号ルール：これらのルールは TCP ポート条件のみをサポートします。
- IMCP エコー：タイプ 0 が設定された宛先 ICMP ポート、またはタイプ 129 が設定された宛先 ICMPv6 ポートは、要求されていないエコー応答だけと照合されます。ICMP エコー要求への応答として送信される ICMP エコー応答は無視されます。ルールですべての ICMP エコーに一致させるには、ICMP タイプ 8 または ICMPv6 タイプ 128 を使用してください。

レルムと設定のルール条件

[レルムと設定（Realm & Settings）] タブページでは、アイデンティティルールを適用するレルムまたはレルムシーケンスを選択できます。キャプティブポータルを使用している場合は、追加のオプションがあります。

認証レルム（Authentication Realm）

[レルム（Realm）] リストから、レルムまたはレルムシーケンスをクリックします。

[アクション（Action）] で指定されたアクションの実行対象になるユーザーが含まれるレルムまたはレルムシーケンス。アイデンティティルールのレルムまたはレルムシーケンスとして選択する前に、これを完全に設定する必要があります。

（注） リモート アクセス VPN が有効で、展開で VPN 認証に RADIUS サーバー グループを使用している場合は、この RADIUS サーバー グループに関連付けられているレルムを指定してください。

アクティブ認証のみ：その他のオプション

認証タイプとして [アクティブ認証（Active Authentication）] を選択するか、[パッシブまたはVPN IDを確立できない場合はアクティブ認証を使用（Use active authentication if passive or VPN identity cannot be established）] チェックボックスをオンにした場合、次のオプションがあります。

パッシブまたはVPN IDを確立できない場合はアクティブ認証を使用

（パッシブ認証ルールのみ）このオプションを選択すると、パッシブまたは VPN 認証でユーザーを識別できない場合にキャプティブ ポータル アクティブ認証を使用してユーザーが認証されます。このオプションを選択するには、アイデンティティポリシーでアクティブ認証ルールを設定する必要があります。（つまり、ユーザーはキャプティブポータルを使用して認証する必要があります）

このオプションを無効にすると、VPN ID を持たないユーザまたはパッシブ認証では識別できないユーザは、「不明（Unknown）」と識別されます。

このトピックで後述する**認証レルム**リストの説明も参照してください。

認証でユーザーを識別できない場合は特別 ID/ゲストとして識別する（Identify as Special Identities/Guest if authentication cannot identify user）

このオプションを選択すると、キャプティブ ポータル アクティブ認証に指定された回数失敗したユーザーがゲストとしてネットワークにアクセスできます。これらのユーザーは、Firewall Management Center 上ではユーザー名（ユーザー名が AD または LDAP サーバーに存在する場合）または[ゲスト（Guest）]（ユーザー名が不明の場合）で表示されます。これらのユーザーのレルムは、アイデンティティ ルールで指定されたレルムです。（デフォルトでは、失敗したログインの数は 3 回です。）

ルール アクションとして [アクティブ認証（Active Authentication）]（つまり、キャプティブ ポータル認証）を設定している場合にのみ、このフィールドが表示されます。

認証プロトコル（Authentication Protocol）

キャプティブ ポータル アクティブ認証を実行するために使用する方法です。応答ページでログインしたときにユーザーに表示される内容の例をアクティブ認証ルールによるサンプル アイデンティティ ポリシーの作成 （20 ページ） に示します。

選択は、レルム、LDAP、または AD のタイプによって異なります。

- 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ーを認証するには、[HTTP 基本（HTTP Basic）] を選択します。ユーザー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。

  ほとんどの Web ブラウザは、**HTTP 基本**ログインからクレデンシャルをキャッシュし、古いセッションがタイムアウトした後にシームレスに新しいセッションを開始するためにそのクレデンシャルを使用します。

- NT LAN Manager（NTLM）接続を使用してユーザーを認証するには **NTLM** を選択します。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。透過的な認証がユーザーのブラウザで設定されている場合、ユーザーは自動的にログインします。透過的な認証が設定されていない場合、ユーザーは各自のブラウザで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。

- Kerberos 接続を使用してユーザーを認証する場合は、[Kerberos] を選択します。この選択は、セキュア LDAP（LDAPS）が有効になっているサーバーに対して AD レルムを選択する場合にのみ可能です。透過的な認証がユーザーのブラウザで設定されている場合、ユーザーは自動的にログインします。透過的な認証が設定されていない場合、ユーザーは各自のブラウザで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。

（注） 選択する [レルム（Realm）] は、Kerberos キャプティブ ポータル アクティブ認証を実行するために、[AD 参加ユーザー名（AD Join Username）] および [AD 参加パスワード（AD Join Password）] を使用して設定する必要があります。

（注） Kerberos キャプティブ ポータルを実行するアイデンティティ ルールを作成しようとしており、DNS 解決は設定済みである場合は、キャプティブ ポータル デバイスの完全修飾ドメイン名（FQDN）を解決する DNS サーバーを設定する必要があります。FQDN は、DNS の設定時に指定したホスト名と一致する必要があります。

Firewall Threat Defense デバイスの場合、FQDN は、キャプティブ ポータルに使用されるルーテッド 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。

- キャプティブ ポータル サーバーが認証接続に HTTP 基本認証、Kerberos、または NTLM を選択できるようにするには、[HTTP ネゴシエート（HTTP Negotiate）] を選択します。このタイプは AD レルムを選択するときにのみ使用できます。

（注） 選択する [レルム（Realm）] は、[HTTP ネゴシエート（HTTP Negotiate）] で Kerberos キャプティブ ポータル アクティブ認証を選択するために、[AD 参加ユーザー名（AD Join Username）] および [AD 参加パスワード（AD Join Password）] を使用して設定する必要があります。

（注） [HTTP ネゴシエート（HTTP Negotiate）] キャプティブ ポータルを実行するアイデンティティ ルールを作成しようとしており、DNS 解決は設定済みである場合は、キャプティブ ポータル デバイスの完全修飾ドメイン名（FQDN）を解決する DNS サーバーを設定する必要があります。キャプティブ ポータルに使用するデバイスの FQDN は、DNS の設定時に入力したホスト名と一致している必要があります。

- ユーザーがログインするレルムを選択できるようにするには、[HTTP 応答ページ（HTTP Response Page）] を選択します。

  必要に応じて、応答ページをカスタマイズできます。たとえば、会社のスタイル標準に準拠できます。

アクティブ認証レルム

（パッシブ認証ルールのみ）[パッシブまたはVPNアイデンティティを確立できない場合にアクティブ認証を使用する（Use active authentication if passive or VPN identity cannot be established）] をクリックした場合は、レルムまたはレルムシーケンスの名前をクリックする必要があります。レルムまたはレルムシーケンスの可用性は、認証プロトコルの選択によって以下のように決定されます。

- **HTTP 基本**または**HTTP 応答ページ**認証プロトコル：レルムまたはレルムシーケンスのいずれかを選択できます。
- **NTLM**、**Kerberos**、または**HTTP ネゴシエート**認証プロトコル：レルムのみを選択できます。レルムシーケンスは選択できません。

アイデンティティ ルールの作成

アイデンティティ ルールの設定オプションに関する詳細については、アイデンティティ ルール フィールド （16 ページ）を参照してください。

始める前に

レルムまたはレルムシーケンスを作成して有効にする必要があります。

- LDAP レルムまたは Active Directory（AD）レルムおよびレルムディレクトリを作成するの説明に従って、Microsoft Azure Active Directory レルムおよびレルムディレクトリを作成します。
- （Microsoft AD レルムのみ）。ユーザーおよびグループをダウンロードし、ユーザーとグループを同期するで説明したようにレルムを有効にします。
- Microsoft Azure AD (SAML) レルムを作成するの説明に従って、Microsoft Azure AD（SAML）レルムを作成します。
- （オプション）レルムシーケンスを作成するの説明に従って、レルムシーケンスを作成します。
- 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。

注意 TLS/SSL 復号が無効の場合（つまりアクセス コントロール ポリシーに a decryption policyが含まれない場合）に、アクティブな最初の認証ルールを追加するか、アクティブな最後の認証ルールを削除すると設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、割り当てられたデバイスがトラフィックを処理する方法に応じて異なります。詳細については、Snort の再起動によるトラフィックの動作を参照してください。

アクティブな認証ルールに [アクティブ認証（Active Authentication）] ルールアクションが含まれるか、[パッシブ/VPNアイデンティティを確立できない場合にアクティブ認証を使用（Use active authentication if passive or VPN identity cannot be established）] が選択された [パッシブ認証（Passive Authentication）] ルールアクションが含まれることに注意してください。

手順

ステップ 1 Firewall Management Center にログインします。

ステップ 2 **Policies** > **Access Control heading** > **Identity** をクリックします。

ステップ 3 アイデンティティルールの追加先となるアイデンティティポリシーの横にある **Edit** () をクリックします。

代わりに **View** () 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [ルールの追加（Add Rule）] をクリックします。

ステップ 5 名前を入力します。

ステップ 6 指定されたルールを適用する場合は、[有効（Enabled）] チェックボックスをオンにします。

ステップ 7 既存のカテゴリにルールを追加するには、ルールを [挿入（Insert）] する場所を指定します。新しいカテゴリを追加するには、[カテゴリの追加（Add Category）] をクリックします。

ステップ 8 一覧からルール [アクション（Action）] を選択します。

ステップ 9 キャプティブ ポータルを設定する場合は、ユーザー制御のためのキャプティブ ポータルの構成方法を参照してください。

ステップ 10 （オプション）アイデンティティ ルールに条件を追加するには、アイデンティティ ルールの条件 （6 ページ）を参照してください。

ステップ 11 [追加（Add）] をクリックします。

ステップ 12 ポリシーエディタで、ルールの位置を設定します。クリックしてドラッグするか、または右クリックメニューを使用してカットアンドペーストを実行します。ルールには1から番号が付けられます。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。トラフィックが一致する最初のルールは、そのトラフィックを処理するルールです。適切なルールの順序を指定することで、ネットワークトラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。

ステップ 13 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開を参照してください。

アイデンティティ ルール フィールド

次のフィールドを使用して、アイデンティティ ルールを構成します。

Enabled

このオプションを有効にすると、ID ポリシーのアイデンティティルールが有効になります。このオプションの選択を解除すると、アイデンティティ ルールが無効になります。

Action

指定したレルムでユーザーに対して実行する認証のタイプを指定します。これには、[パッシブ認証（Passive Authentication）]（デフォルト）、[アクティブ認証（Active Authentication）]、または [認証なし（No Authentication）] があります。アイデンティティルールのアクションとして選択する前に、認証方式、またはアイデンティティ ソースを完全に設定する必要があります。

さらに、VPN が有効になっている場合（少なくとも 1 つの管理対象デバイスで構成されている場合）、リモート アクセス VPN セッションは VPN によってアクティブに認証されます。他のセッションはルール アクションを使用します。つまり、VPN が有効になっている場合は、選択したアクションに関係なく、すべてのセッションで VPN ID の判別が最初に行われます。指定されたレルム上に VPN ID が見つかった場合、これは使用されるアイデンティティ ソースになります。選択されていても、追加のキャプティブ ポータル アクティブ認証は実行されません。

VPN アイデンティティ ソースが見つからない場合は、指定されたアクションに従ってプロセスが続行されます。アイデンティティ ポリシーを VPN 認証のみに制限することはできません。VPN ID が見つからない場合は、選択されたアクションに従ってルールが適用されるためです。

注意 TLS/SSL 復号が無効の場合（つまりアクセス コントロール ポリシーに SSL ポリシーが含まれない場合）に、アクティブな最初の認証ルールを追加するか、アクティブな最後の認証ルールを削除すると 設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、割り当てられたデバイスがトラフィックを処理する方法に応じて異なります。詳細については、Snort の再起動によるトラフィックの動作を参照してください。

アクティブな認証ルールに **[アクティブ認証（Active Authentication）]** ルール アクションが含まれるか、[パッシブ/VPNアイデンティティを確立できない場合にアクティブ認証を使用（Use active authentication if passive or VPN identity cannot be established）] が選択された **[パッシブ認証（Passive Authentication）]** ルールアクションが含まれることに注意してください。

使用中のシステムのバージョンでサポートされるパッシブおよびアクティブ認証方式の詳細については、ユーザー アイデンティティ ソースについてを参照してください。

ID ポリシーおよびルールの例

以下のセクションでは、パッシブ認証ルールまたはアクティブ認証ルールを使用して ID ポリシーを設定する例を示します。さらに、レルムまたはレルムシーケンスのいずれかを使用してアクティブ認証でユーザーを認証できるため、別の例を示します。

アクティブ認証とは、キャプティブポータルを使用してユーザーを認証することを意味します。ユーザーは、許可されたリソースにアクセスするためにネットワークログイン情報を入力します。（RA-VPN は別のタイプのアクティブ認証ですが、キャプティブポータル認証と一緒に使用することはできません。詳細については、リモート アクセス VPN アイデンティティ ソースを参照してください）。

パッシブ認証は、他のすべてのタイプを指します。パッシブ認証には、Microsoft Active Directory レルム、Microsoft Azure Active Directory レルム、Cisco Identity Services Engine などの使用が含まれます。

Microsoft Azure Active Directory レルムを使用して、ここでは説明していない別の方法でユーザーを認証できます。詳細については、「Microsoft Azure AD (SAML) レルムを作成する」を参照してください。

前提条件

例では以下の前提条件を使用しています。

- 信頼関係で設定された 2 つの子ドメインを持つ、「forest.example.com」という名前の Microsoft Active Directory（AD）レルム：
  - 米国西部

- 米国東部

- 両方のレルムを含む「US」という名前のレルムシーケンス
- レルムシーケンスを使用してユーザーを認証するパッシブ認証ルール
- 2 つのアクティブな認証ルール：
  - レルムでユーザーを認証し、NTLM 認証プロトコルを使用する 1 つのルール
  - レルムシーケンスでユーザーを認証し、HTTP 応答ページ認証プロトコルを使用する 1 つのルール
- 各 ID ルールの例は、異なる ID ポリシーに関連付けられています。

パッシブ認証 ID ルール

パッシブ認証 ID ルールを設定する場合、LDAP、Microsoft Active Directory レルム、または Microsoft AD レルムシーケンスのいずれかを使用してユーザーを認証することを選択できます。レルムを使用して、任意の認証タイプで認証できます。レルムシーケンスでは、使用できる認証タイプが制限されます。例については、パッシブな認証ルールによるアイデンティティポリシーの作成 （18 ページ）を参照してください。

アクティブ認証 ID ルール。

アクティブ認証 ID ルールを設定する場合、LDAP、Microsoft Active Directory レルム、または Microsoft AD レルムシーケンスのいずれかを使用してユーザーを認証することを選択できます。レルムを使用して、任意の認証タイプで認証できます。レルムシーケンスでは、使用できる認証タイプが制限されます。

以下の認証タイプを除き、Microsoft Active Directory レルムシーケンスを使用してユーザーを認証することもできます。

- NTLM
- Kerberos
- HTTP ネゴシエート

例については、アクティブ認証ルールによるサンプル アイデンティティ ポリシーの作成 （20 ページ）を参照してください。

パッシブな認証ルールによるアイデンティティポリシーの作成

このタスクでは、US レルムシーケンスを使用してユーザーを認証するパッシブ認証ルールを使用してアイデンティティポリシーを作成する方法について説明します。シーケンス内の最初のレルムでユーザーが見つからない場合、システムは、レルムシーケンスにリストされている順序で、シーケンス内の他のレルムを検索します。それでもレルムまたはレルムシーケンス内でユーザーが見つからない場合、そのユーザーは [不明（Unknown）] として識別されます。

ユーザーがシーケンスのどのレルムにも見つからない場合は、キャプティブポータル（アクティブ認証）でユーザーを認証することもできます。詳細については、「キャプティブ ポータルのガイドラインと制限事項」を参照してください。

手順

ステップ 1 Firewall Management Center にログインします。

ステップ 2 **Policies** > **Access Control heading** > **Identity** をクリックします。

ステップ 3 [新しいポリシー（New Policy）] をクリックします。

ステップ 4 ポリシーの [名前（Name）] と、必要に応じて [説明（Description）] を入力します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 [ルールの追加（Add Rule）] をクリックします。

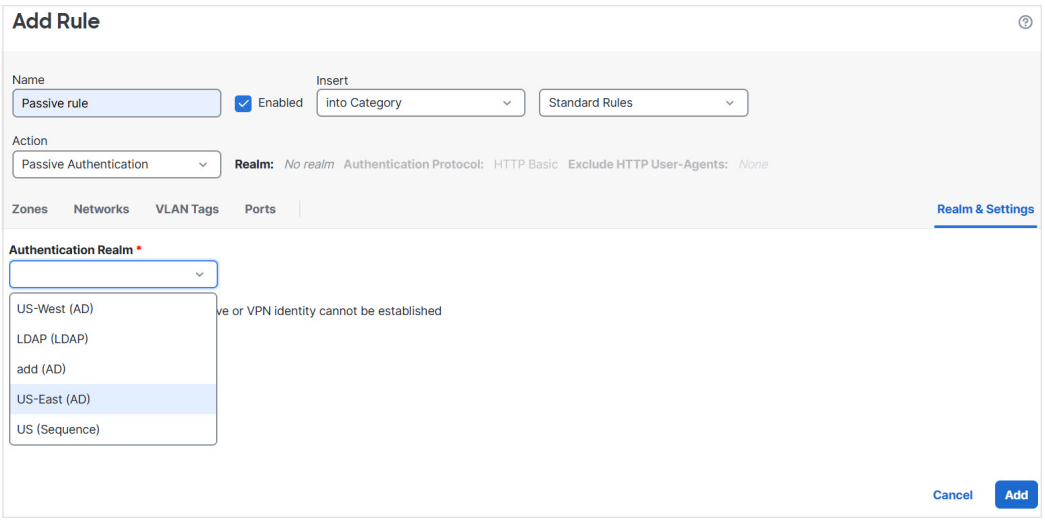
ステップ 7 ルールの [名前（Name）] を入力します。

ステップ 8 リストから [パッシブ認証（Passive Authentication）] をクリックします。

ステップ 9 [レルムおよび設定（Realms & Settings）] タブページをクリックします。

ステップ 10 リストから、レルムまたはレルムシーケンスの名前をクリックします。

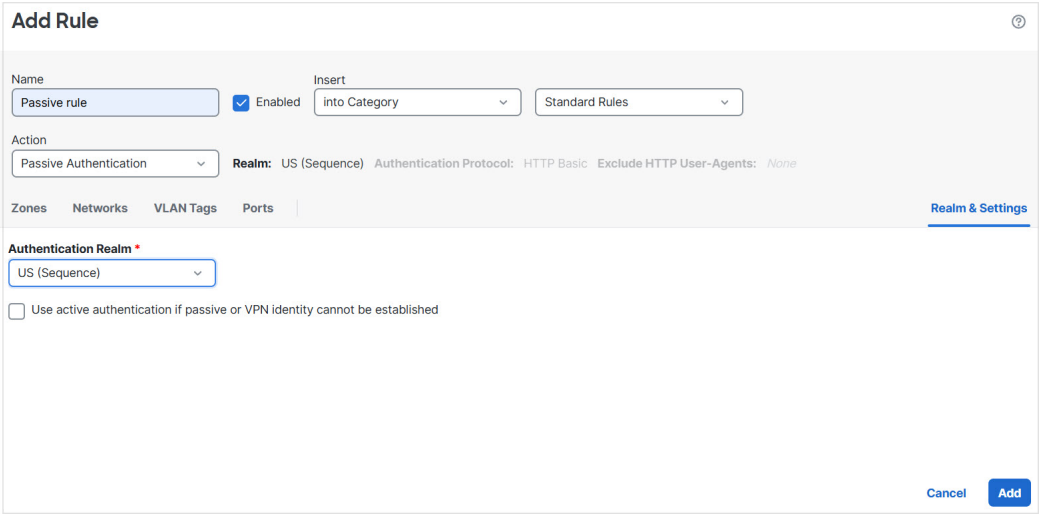
次の図は例を示しています。



- レルムを選択すると（例のように **US-East** など）、システムは、ルールに一致するユーザーをそのレルムで検索します。ユーザーが見つからない場合、そのユーザーは [不明（Unknown）] として識別されます。
- レルムシーケンスを選択した場合（例のように **US (Sequence)** など）、レルムシーケンスで指定された順序でシーケンス内のすべてのレルムでユーザーが検索されます。ユーザーが見つからない場合、そのユーザーは [不明（Unknown）] として識別されます。
- LDAP レルムを選択することもできます。

- ユーザーを認証する他の方法については、「**パッシブまたは VPN ID を確立できない場合はアクティブ認証を使用**」をご確認ください。詳細については、「キャプティブ ポータルのガイドラインと制限事項」を参照してください。

以下の図は、US レルムシーケンスでユーザーを検索するように設定されたパッシブ アイデンティティ ポリシーの例を示しています。



ステップ 11 （オプション）ネットワークオブジェクトでトラフィックをフィルタ処理するには、[Identity Source] タブをクリックします。リストから、この ID ポリシーのトラフィックのフィルタ処理に使用するネットワークオブジェクトをクリックします。新しいネットワークオブジェクトを作成するには、**Add** (＋) をクリックします。

ステップ 12 アイデンティティ条件を設定します（アイデンティティ ルールの条件（6 ページ）を参照）。

ステップ 13 アイデンティティルールをアクセス制御ルールに関連付けます（アクセス制御への他のポリシーの関連付けを参照）。

ステップ 14 設定変更を管理対象デバイスに展開します（設定変更の展開を参照）。

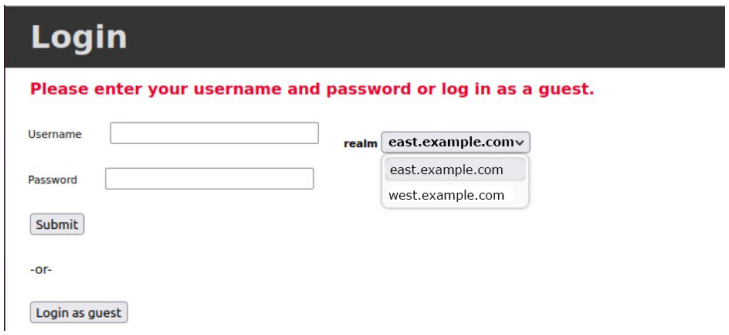
アクティブ認証ルールによるサンプル アイデンティティ ポリシーの作成

この関連タスクでは、レルムまたはレルムシーケンスのいずれかを使用して認証が実行される「アクティブ認証」ルールによってアイデンティティポリシーを設定する例を示します。

違いは次のとおりです。

- レルムでは、サポートされている任意の認証タイプ（現時点では、**HTTP 基本**、**NTLM**、**Kerberos**、**HTTP ネゴシエート**、または **HTTP 応答ページ**）を使用できます。
- レルムシーケンスでは、認証タイプが **HTTP 基本**と **HTTP 応答ページ**のみに制限されます。

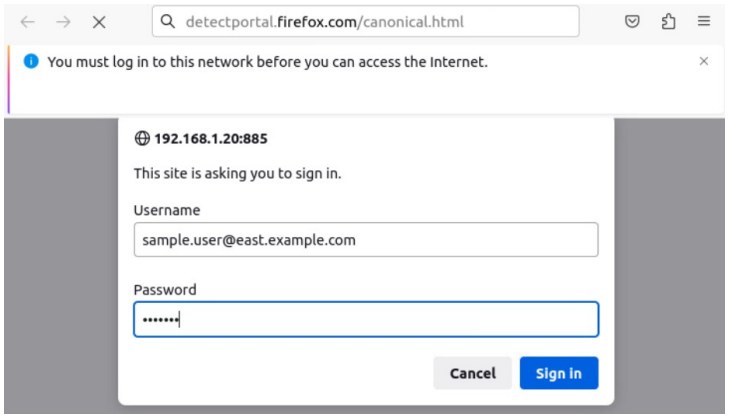
レルムシーケンスとHTTP応答ページ認証タイプで認証されたユーザーには、デフォルトで次のように表示されます。



ユーザーは、次のいずれかの方法で認証できます。

- レルムシーケンスに含まれるレルムのリストが表示される場合（図を参照）、ユーザーは、表示されたフィールドにユーザー名とパスワードを入力し、リストにあるユーザーのレルムの名前をクリックする必要があります。
- レルムがリストに表示されない場合、ユーザーはログイン情報を `username@domain` 形式で入力できます。

レルムと HTTP 基本認証ページで認証されるユーザーには、次の情報が表示されます。



ユーザーは、`username@domain` の形式でユーザー名を入力する必要があります。

手順

ステップ 1 Firewall Management Center にログインします。

ステップ 2 **Policies** > **Access Control heading** > **Identity** をクリックします。

ステップ 3 [新しいポリシー（New Policy）] をクリックします。

ステップ 4 ポリシーの [名前（Name）] と、必要に応じて [説明（Description）] を入力します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 [アクティブ認証（Active Authentication）] タブをクリックします。

ステップ 7 次の情報を入力します。

- [サーバー証明書（Server Certificate）]：リストから、Firewall Threat Defense デバイスへのセキュアな接続に使用する内部証明書オブジェクトをクリックするか、**Add**(＋)をクリックしてオブジェクトを追加します。
- [ホスト名へのリダイレクト（Redirect to Host Name）]：（オプション）リストから、キャプティブポータル要求のリダイレクト先のネットワークオブジェクトをクリックします。この値を省略すると、要求は管理対象デバイスの IP アドレスにリダイレクトされます。

  Add(＋)をクリックして新しいネットワークオブジェクトを作成することができます。詳細については、ホスト名ネットワーク ルール条件へのリダイレクト （7 ページ）を参照してください。

  このオプションを使用するには、管理対象デバイスで Snort 3 が有効になっている必要があります。
- [ポート（Port）]：使用するキャプティブポータルのポートを入力します。このポートは、キャプティブポータルに対して一意であり、設定したアクセス制御ルールと一致する必要があります（TCP ポート アクセス コントロール ルールの作成を参照）（デフォルトは 885）。
- [最大ログイン試行回数（Maximum login attempts）]：ログインが失敗するまでの最大ログイン試行回数を入力します（デフォルトは 3）。
- [ファイアウォール全体でアクティブ認証セッションを共有（Share active authentication sessions across firewalls）]：オフにして Firewall Management Center を有効にすると、ユーザーが前回とは異なる管理対象デバイスを使用してネットワークにアクセスするたびに再認証が強制されます。

  このオプションの詳細については、キャプティブ ポータル フィールドを参照してください。
- [アクティブ認証応答ページ（Active Authentication Response Page）]：キャプティブ ポータル ユーザー用のシステム提供ログインページまたはカスタムログインページを選択します。オプションの詳細については、キャプティブ ポータル フィールドを参照してください。

ステップ 8 [保存（Save）] をクリックしてアイデンティティポリシーの変更内容を保存します。

ステップ 9 [ルール（Rules）] タブをクリックします。

ステップ 10 [ルールの追加（Add Rule）] をクリックします。

ステップ 11 ルールの [名前（Name）] を入力します。

ステップ 12 リストから [アクティブ認証（Active Authentication）] をクリックします。

ステップ 13 [レルムおよび設定（Realms & Settings）] タブページをクリックし、次のいずれかのセクションに進みます。

次のタスク

次のいずれかのセクションに進みます。

- レルムを使用したアクティブ認証 （23 ページ）
- レルムシーケンスを使用したアクティブ認証 （24 ページ）

レルムを使用したアクティブ認証

このタスクでは、レルムと使用可能な認証プロトコル（現時点では、**HTTP 基本**、**NTLM**、**Kerberos**、**HTTP ネゴシエート**、または **HTTP 応答ページ**）を使用してキャプティブ ポータル ユーザーを認証する方法について説明します。

始める前に

アクティブ認証ルールによるサンプル アイデンティティ ポリシーの作成 （20 ページ）で説明されているタスクを完了します。

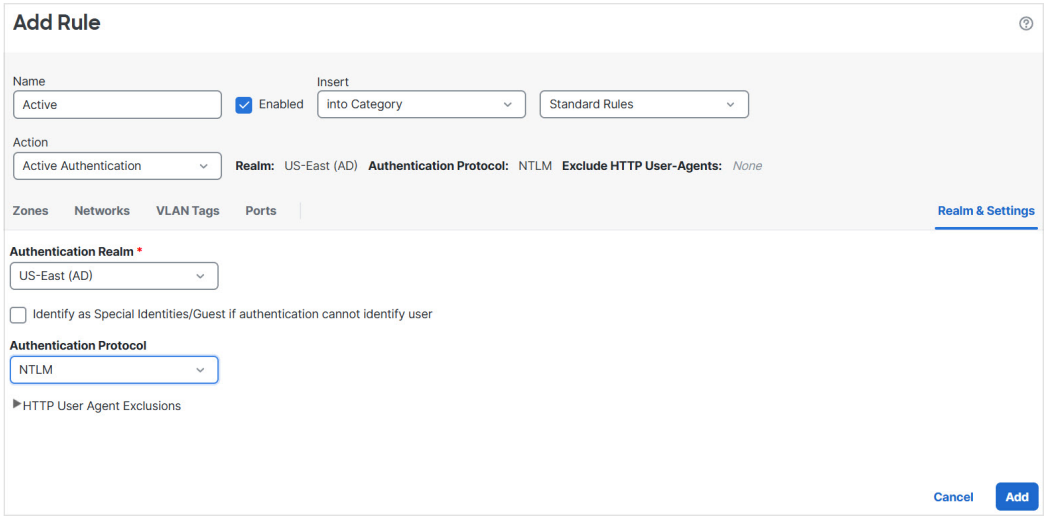
手順

ステップ 1 アクティブ認証ルールによるサンプル アイデンティティ ポリシーの作成 （20 ページ）から続行します。

ステップ 2 [レルムおよび設定（Realms & Settings）] タブページで、[米国東部（US-East）] をクリックします。

ステップ 3 [認証プロトコル（Authentication Protocol）] リストから、[NTLM] をクリックします。

次の図は例を示しています。



レルムを選択すると（例のように）、システムは、ルールに一致するユーザーを、そのレルムで検索します。ユーザーが見つからない場合、そのユーザーは[不明（Unknown）]として識別されます。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 （オプション）ネットワークオブジェクトでトラフィックをフィルタ処理するには、[Identity Source] タブをクリックします。リストから、この ID ポリシーのトラフィックのフィルタ処理に使用するネットワークオブジェクトをクリックします。新しいネットワークオブジェクトを作成するには、**Add** (＋) をクリックします。

ステップ 6 アイデンティティ条件を設定します（アイデンティティ ルールの条件（6 ページ）を参照）。

ステップ 7 アイデンティティルールをアクセス制御ルールに関連付けます（アクセス制御への他のポリシーの関連付けを参照）。

ステップ 8 設定変更を管理対象デバイスに展開します（設定変更の展開を参照）。

レルムシーケンスを使用したアクティブ認証

このタスクでは、レルムシーケンスを使用してキャプティブ ポータル ユーザーを認証する方法について説明します。この認証では、「HTTP 基本」または「HTTP 応答ページ」認証プロトコルに制限されます。

始める前に

アクティブ認証ルールによるサンプル アイデンティティ ポリシーの作成（20 ページ）で説明されているタスクを完了します。

手順

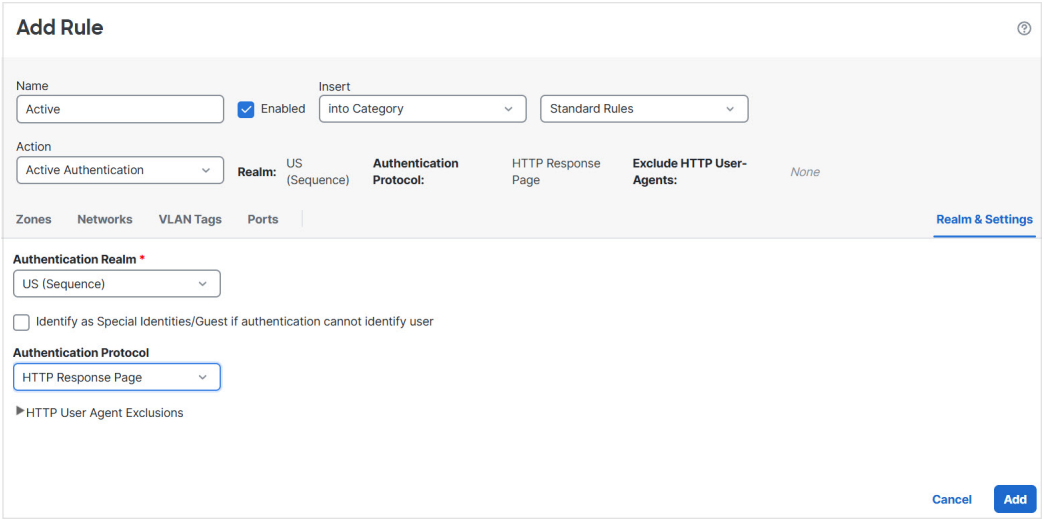
ステップ 1 アクティブ認証ルールによるサンプル アイデンティティ ポリシーの作成（20 ページ）から続行します。

ステップ 2 [レルムおよび設定（Realms & Settings）] タブページで、リストからレルムの名前をクリックします。

ステップ 3 リストの [US-East] をクリックします。

ステップ 4 [プロトコル（Protocol）] リストから、[HTTP応答ページ（HTTP Response Page）] をクリックします。

次の図は例を示しています。



レルムシーケンスを選択した場合（例のように）、システムは、レルムシーケンスで指定された順序でシーケンス内のレルムを検索します。シーケンスの最初のレルムは、「デフォルト」レルムと呼ばれます。これは、ユーザーが変更しない場合に使用されるレルムです。ユーザーが見つからない場合、そのユーザーは [不明（Unknown）] として識別されます。

（以前のバージョンからバージョン 7.4.1 にアップグレードした場合のみ）。カスタム認証フォームの更新で説明されているシーケンスでレルムのリストが表示されるように、HTTP 応答ページを編集します。

ステップ 5 [追加（Add）] をクリックします。

ステップ 6 （オプション）ネットワークオブジェクトでトラフィックをフィルタ処理するには、[Identity Source] タブをクリックします。リストから、この ID ポリシーのトラフィックのフィルタ処理に使用するネットワークオブジェクトをクリックします。新しいネットワークオブジェクトを作成するには、**Add** (+) をクリックします。

ステップ 7 アイデンティティ条件を設定します（アイデンティティ ルールの条件（6ページ）を参照）。

ステップ 8 アイデンティティ ルールをアクセス制御ルールに関連付けます（アクセス制御への他のポリシーの関連付けを参照）。

ステップ 9 設定変更を管理対象デバイスに展開します（設定変更の展開を参照）。

アイデンティティ ポリシーの管理

手順

ステップ 1 Firewall Management Center にログインします。

ステップ 2 **Policies** > **Access Control heading** > **Identity** をクリックします。

ステップ 3 ポリシーを削除するには、**Delete** ( ) をクリックします。 コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ポリシーを編集するには、ポリシーの横にある **Edit** ( ) をクリックし、アイデンティティ ポリシーの作成 （3 ページ）の説明に従って変更を行います。 代わりに **View** ( ) 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 5 ポリシーをコピーするには、**Copy** ( ) をクリックします。

ステップ 6 ポリシーのレポートを生成するには、現在のポリシーレポートの生成の説明に従って **Report** ( ) をクリックします。

ステップ 7 ポリシーを比較する方法については、ポリシーの比較を参照してください。

ステップ 8 ポリシーを整理するフォルダを作成するには、[カテゴリの追加（Add Category）] をクリックします。

次のタスク

設定変更を展開します設定変更の展開を参照してください。

アイデンティティ ルールの管理

手順

ステップ 1 Firewall Management Center にログインします。

ステップ 2 **Policies** > **Access Control heading** > **Identity** をクリックします。

ステップ 3 編集するポリシーの横にある **Edit** ( ) をクリックします。 代わりに **View** ( ) 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 アイデンティティルールを編集する場合は、**Edit** ( ) をクリックし、アイデンティティ ポリシーの作成 （3 ページ）の説明に従って変更を行います。

ステップ 5 アイデンティティルールを削除するには、**Delete** ( ) をクリックします。

ステップ 6 ルール カテゴリを作成するには、[カテゴリの追加（Add Category）] をクリックし、位置とルールを選択します。

ステップ 7 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開を参照してください。

ユーザー制御のトラブルシューティング

ユーザー ルールの予期しない動作に気付いたら、ルール、アイデンティティ ソース、またはレルムの設定を調整することを検討してください。その他の関連するトラブルシューティング情報については、以下を参照してください。

- Cisco ISE/ISE-PIC または Cisco TrustSec の問題のトラブルシューティング
- TS エージェント アイデンティティ ソースのトラブルシューティング
- キャプティブ ポータルのアイデンティティ ソースのトラブルシューティング
- レルムとユーザーのダウンロードをトラブルシュートする

レルム、ユーザー、またはユーザー グループを対象とするルールがトラフィックと一致しない

TS エージェントまたは ISE/ISE-PIC デバイスのモニター対象に多くのユーザー グループを設定した場合、またはネットワークでホストにマップされるユーザー数が非常に多い場合、Firewall Management Center のユーザー制限が原因で、システムがユーザー レコードをドロップすることがあります。その結果、ユーザー条件のルールが、一致することが想定されているトラフィックと一致しない可能性があります。

ユーザー グループまたはユーザー グループ内のユーザーを対象とするルールが、一致することが想定されているトラフィックと一致しない

ユーザー グループ条件を含むルールを設定する場合は、LDAP または Active Directory サーバーでユーザー グループを設定している必要があります。サーバーが基本的なオブジェクト階層でユーザーを整理している場合、システムはユーザー グループ制御を実行できません。

セカンダリ グループ内のユーザーを対象とするルールが、一致することが想定されているトラフィックと一致しない

Active Directory サーバーのセカンダリ グループのメンバーであるユーザーを含めるか除外するユーザー グループ条件を含むルールを設定する場合、サーバーは報告するユーザーの数を制限していることがあります。

デフォルトでは、Active Directory サーバーはセカンダリ グループから報告するユーザーの数を制限します。この制限は、セカンダリ グループ内のすべてのユーザーが Firewall Management Center に報告され、ユーザー条件を含むルールでの使用に適するようにカスタマイズする必要があります。

ルールが、初めて表示されたユーザーと一致しない

システムは、以前に表示されていないユーザーからのアクティビティを検出すると、サーバーからそれらのユーザーに関する情報を取得します。システムがこの情報を正常に取得するまで、このユーザーに表示されるアクティビティは、一致するルールによって処理されません。代わりに、ユーザー セッションが、一致する次のルール（または該当する場合はポリシーのデフォルト アクション）によって処理されます。

たとえば、次のような状況が考えられます。

- ユーザー グループのメンバーであるユーザーが、ユーザー グループ条件を含むルールに一致しない。
- ユーザーデータの取得に使用されたサーバーが Active Directory サーバーである場合、TS エージェントまたは ISE デバイスによって報告されたユーザーがルールと一致しない。

これにより、システムがユーザー データをイベント ビューおよび分析ツールに表示するのが遅れる可能性があることに注意してください。

ルールがすべての ISE/ISE-PIC ユーザーと一致しない

これは想定されている動作です。Active Directory ドメイン コントローラで認証された ISE/ISE-PIC ユーザーに対してユーザー制御を実行することができます。LDAP、RADIUS、または RSA ドメイン コントローラで認証された ISE/ISE-PIC ユーザーに対するユーザー制御は実行できません。

ユーザーとグループによる大量のメモリの使用

ユーザーとグループの処理によって大量のメモリが使用されている場合、ヘルスアラートが表示されます。すべてのユーザーセッションが Firewall Management Center のすべての管理対象デバイスに伝達されることに注意してください。Firewall Management Center がメモリ容量の異なるデバイスを管理している場合、メモリ容量が最も小さいデバイスによって、システムがエラーなしで処理できるユーザーセッションの数が決まります。

アイデンティティプロセスに割り当てられたメモリを調整することはできません。デバイスに使用可能なメモリがある場合でも、メモリ不足の問題を報告することがあります。問題が解決しない場合、次の選択肢があります。

- 容量の小さい管理対象デバイスをサブネットに分離し、パッシブ認証データをそれらのサブネットに報告しないように ISE/ISE-PIC を設定します。

  『*Cisco Identity Services Engine Administrator Guide*』のネットワークデバイスの管理に関する章を参照してください。

- セキュリティグループタグ（SGT）の登録を解除します。

  詳細については、Cisco Identity Services Engine (Cisco ISE) アイデンティティソースの構成方法を参照してください。

- 管理対象デバイスをメモリが大きなモデルにアップグレードします。

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。