ユーザー 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。

- **[システム（System）] > [統合（Integration）] > [レルム（Realms）]** でアイデンティティ ポリシー外のレルムを設定します。詳細については、LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成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 ISE/ISE-PIC は、**[システム（System）] > [統合（Integration）] > [アイデンティティ ソース（Identity Sources）]**で設定します。
- 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、システムの外で設定します。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 ポータルの設定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 ポリシーを設定しない場合、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 ポリシーの設定方法

アイデンティティポリシーのライセンス要件

Threat Defense ライセンス

いずれか（Any）

従来のライセンス

Control

アイデンティティポリシーの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

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 レルムおよびレルムディレクトリの作成の説明に従って 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 Management Center にログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アイデンティティ（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 （13 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、キャプティブポータルの設定パート 2：アイデンティティポリシーおよびアクティブ認証ルールの作成 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、[追加（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 （13 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）。
- 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 （17 ページ）を参照してください。

関連トピック

キャプティブポータルの設定パート 2：アイデンティティポリシーおよびアクティブ認証ルールの作成
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 （17 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、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。

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 レルムおよびレルム ディレクトリの作成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 Management Center にログインします。

ステップ 2 **[ポリシー（Policies）]** > **[アイデンティティ（Identity）]** をクリックします。

ステップ 3 [編集（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 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

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条件
VLAN タグルール条件
ポートルールの条件
レルムと設定のルール条件 （10 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にリダイレクト

（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（FTD 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。。

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 （15 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 レルムおよびレルムディレクトリの作成の説明に従って、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。
- 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の同期で説明したようにレルムを有効にします。
- （オプション）レルムシーケンスの作成の説明に従って、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 復号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、ターゲット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 Management Center にログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アイデンティティ（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 [編集（Edit）]（） をクリックします。

代わりに [表示（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 ポータルの設定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 ルールを設定します。

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設定されている場合）、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、ターゲット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。

アイデンティティ ポリシーの管理

手順

ステップ 1 Management Center にログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アイデンティティ（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、[削除（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 [編集（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 [表示（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、[コピー（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 **[レポート（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 Management Center にログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アイデンティティ（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 [編集（Edit）]（）をクリックします。代わりに [表示（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、[編集（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、[削除（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。

- 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のトラブルシュート

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。
- 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。