アイデンティティ ポリシーの作成および管理

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。

アイデンティティ ルールで呼び出す前に、使用するレルムおよび認証方式を完全に設定しておく必要があります。

- **[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、レルム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 ソースであるユーザ エージェントと 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。詳細については、ユーザ制御のためのユーザ エージェントの設定およびユーザ制御用 ISE/ISE-PIC の設定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、Firepower 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 の AAA の設定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。

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、システムはユーザ認証を実行しません。

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 ルールの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator/Access Admin/Network Admin

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 （3 ページ）を参照してください。

手順

ステップ 1 まだ Firepower Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [ID（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。

代わりに表示アイコン（  ）が表示される場合、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 ルールを**有効**にするかどうかを指定します。

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 [レルムおよび設定（Realms & Settings）] タブをクリックします。

ステップ 10 [レルム（Realms）] 一覧から、アイデンティティ ルールのレルムを選択します。各アイデンティティ ルールにレルムを関連付ける必要があります。

レルム要件の唯一の例外は、ISE SGT 属性タグのみを使用してユーザ制御を実装する場合です。この場合は、ISE サーバのレルムを設定する必要はありません。ISE SGT 属性条件は、関連するアイデンティティ ポリシーの有無にかかわらずポリシーで設定できます。

ステップ 11 キャプティブ ポータルを設定する場合は、ユーザ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 12 （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、ルール条件タイプを参照してください。

ステップ 13 [追加（Add）] をクリックします。

ステップ 14 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 15 [保存（Save）] をクリックします。

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。

[有効（Enabled）]

このオプションを選択すると、アイデンティティ 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。

アクション（Action）

指定したレルムでユーザ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 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と 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。

アクティブ認証ルールには [アクティブ認証（Active Authentication）] ルール アクションが含まれているか、または **[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する（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ています。

Firepower 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 アイデンティティ ソースについてを参照してください。

レルム

指定された**アクション**を実行するユーザが含まれるレルム。アイデンティティ ルールのレルムとして選択する前に、レルム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 グループを使用している場合は、この RADIUS サーバ 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。

（注） [Kerberos]（または [Kerberos] をオプションとする場合は [HTTP ネゴシエート（HTTP Negotiate）]）を、アイデンティティ ルールの [認証プロトコル（Authentication Protocol）] として選択する場合、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できるように、[AD 参加ユーザ名（AD Join Username）] と [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。

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します。

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 ポリシーでキャプティブ ポータル アクティブ認証を設定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。

認証でユーザ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。これらのユーザは、Firepower Management Console ではユーザ名（ユーザ名が AD または LDAP サーバに存在する場合）または [ゲスト（Guest）]（ユーザ名が不明の場合）で表示されます。これらのユーザのレルムは、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

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

  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のブラウザで設定されている場合、ユーザ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のブラウザで設定されている場合、ユーザ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。

ASA with FirePOWER Services および Firepower 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。

ASA with FirePOWER Services デバイスの場合、FQDN は ASA FirePOWER モジュールの FQDN です。

アイデンティティ ポリシーの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator/Access Admin/Network Admin

始める前に

- レルム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。

手順

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

ステップ 2 **[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [ID（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 （2 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、ユーザ制御のためのキャプティブ ポータルの設定方法で説明されているように、[アクティブ認証（Active Authentication）] タブをクリックします。

ステップ 8 [保存（Save）] をクリックして、アイデンティティ ポリシーを保存します。

次のタスク

- 照合するユーザ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 （2 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）。

アイデンティティ ルールの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator/Access Admin/Network Admin

手順

ステップ 1 まだ Firepower Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [ID（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アイコン（  ）をクリックします。代わりに表示アイコン（  ）が表示される場合、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 ルールを編集するには、編集アイコン（  ）をクリックし、アイデンティティ ポリシーの作成 （7 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、削除アイコン（  ）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。

アイデンティティ ポリシーの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator/Access Admin/Network Admin

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 まだ Firepower Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [ID（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（）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（）をクリックし、アイデンティティ ポリシーの作成 （7 ページ） の説明に従って変更を行います。代わりに表示アイコン（）が表示される場合、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 アイコン（）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 アイコン（）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。