ユーザ アイデンティティ ソース

以下のトピックでは、Firepower システムのユーザ アイデンティティ ソースについて説明します。

- ユーザ アイデンティティ ソースについて，1 ページ
- ユーザ エージェントのアイデンティティ ソース，3 ページ
- ISE アイデンティティ ソース，5 ページ
- キャプティブ ポータルのアイデンティティ ソース，10 ページ
- トラフィック ベース検出のアイデンティティ ソース，16 ページ

ユーザ アイデンティティ ソースについて

次の表に、Firepower システムでサポートされているユーザ アイデンティティ ソースの概要を示します。

ユーザ アイデンティティ ソース	ポリシー	サーバ要件	ソース タイプ	認証タイプ（Authentication Type）	ユーザ認識	ユーザ制御	詳細
ユーザ エージェント	ID	Microsoft Active Directory	権限のあるログイン	パッシブ	Yes	Yes	ユーザ エージェントのアイデンティティ ソース，（3 ページ）

ユーザ アイデンティティ ソース	ポリシー	サーバ要件	ソース タイプ	認証タイプ（Authentication Type）	ユーザ認識	ユーザ制御	詳細
ISE	ID	Microsoft Active Directory	権限のあるログイン	パッシブ	Yes	Yes	ISE アイデンティティ ソース, （5 ページ）
キャプティブ ポータル	ID	LDAP または Microsoft Active Directory	権限のあるログイン	active	Yes	Yes	キャプティブ ポータルのアイデンティティ ソース, （10 ページ）
トラフィック ベースの検出	ネットワーク検出	適用対象外	権限のないログイン	適用対象外	Yes	No	トラフィック ベース検出のアイデンティティ ソース, （16 ページ）

展開するアイデンティティ ソースを選択する際には、以下を検討してください。

- 非 LDAP ユーザ ログインを検出するにはトラフィック ベースの検出を使用する必要があります。たとえば、ユーザ エージェントのみを使用してユーザ アクティビティを検出している場合は、非 LDAP ログインを制限しても効果はありません。
- 失敗したログインまたは認証アクティビティを記録するには、トラフィック ベースの検出またはキャプティブ ポータルを使用する必要があります。失敗したログインまたは認証試行で新しいユーザがデータベース内のユーザのリストに追加されることはありません。
- キャプティブ ポータルを使用するには、センシング インターフェイス（仮想ルータなど）に IP アドレスがあるアプライアンスを展開する必要があります。

これらのアイデンティティ ソースからのデータは、Firepower Management Center のユーザ データベースとユーザ アクティビティ データベースに格納されます。Firepower Management Center サーバ ユーザ ダウンロードを設定して、新しいユーザ データがデータベースに自動的かつ定期的にダウンロードされるようにできます。

Firepower システムでのユーザ検出の詳細については、ユーザ検出の基本を参照してください。

ユーザ エージェントのアイデンティティ ソース

ユーザエージェントは、パッシブ認証方法で、信頼できるアイデンティティ ソース（つまり、信頼された Active Directory サーバでユーザ情報が提供されます）でもあります。ユーザ エージェントは、Firepower システムと統合されると、ユーザが Active Directory クレデンシャルでホストにログインする、またはホストからログアウトするときに、そのユーザをモニタします。ユーザ エージェントから取得されたデータは、ユーザ認識とユーザ制御に使用できます。

ユーザエージェントは、各ユーザを IP アドレスと関連付けます。これにより、ユーザ条件を使用するアクセス コントロール ルールをトリガーすることができます。1 つのユーザ エージェントを使用して、最大 5 つの Active Directory サーバでユーザ アクティビティをモニタでき、最大 5 つの Firepower Management Center に暗号化データを送信できます。

ユーザ エージェントは失敗したログイン試行を報告しません。

ユーザ エージェントは、以下を含む段階的な設定が必要です。

- ユーザ エージェントがインストールされている少なくとも 1 台のコンピュータ 。
- ユーザ エージェントがインストールされたコンピュータまたは Active Directory サーバと Firepower Management Center との間の接続。
- ユーザ エージェントからユーザ データを受け取る各 Firepower Management Center で設定されたアイデンティティ レルム。

段階的なユーザ エージェントの設定とサーバの要件の詳細については、『*Firepower* ユーザ エージェント構成ガイド』を参照してください。

（注） コンピュータまたは Active Directory サーバの時間が Firepower Management Center の時間と同期されていることを確認します。アプライアンスが同期されていないと、予想外の間隔でユーザのタイムアウトが実行される可能性があります。

Firepower Management Center接続は、ログインとログオフがユーザ エージェントによって検出されたユーザのメタデータを取得可能にするだけでなく、アクセス コントロール ルール内で使用するユーザとグループを指定するためにも使用されます。ユーザ エージェントが特定のユーザ名を除外するように設定されている場合は、そのようなユーザ名のログイン データは Firepower Management Center に報告されません。ユーザ エージェントのデータは、Firepower Management Center のユーザ データベースとユーザ アクティビティ データベースに保存されます。

（注） ユーザ エージェントは $ 記号で終わる Active Directory ユーザ名を Firepower Management Center に送信できません。これらのユーザをモニタする場合は、最後の $ の文字を削除する必要があります。

複数のユーザがリモート セッションを使用してホストにログインしている場合は、エージェントがそのホストからのログインを正確に検出しない場合があります。これを防ぐ方法の詳細については、『*Firepower* ユーザ エージェント構成ガイド』を参照してください。

ユーザ エージェント接続の設定

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）	任意（Any）	任意（Any）	グローバルだけ	Admin/Access Admin/Network Admin

ユーザ エージェントの詳細については、ユーザ エージェントのアイデンティティ ソース, （3 ページ） を参照してください。

はじめる前に

- ユーザ エージェント データを使用してユーザ制御を実行する場合は、レルムの作成の説明に従ってユーザ エージェント接続用の Active Directory レルムを設定して有効にします。

手順

ステップ 1 [システム（System）] > [統合（Integration）] をクリックします。

ステップ 2 [アイデンティティの送信元（Identity Sources）] タブをクリックします。

ステップ 3 [サービス タイプ（Service Type）] に [ユーザ エージェント（User Agent）] をクリックし、ユーザ エージェント接続を有効にします。

（注） 接続を無効にするには、[なし（None）] をクリックします。

ステップ 4 [新規エージェント（New Agent）] をクリックして新しいエージェントを追加します。

ステップ 5 エージェントをインストールするコンピュータの [ホスト名（Hostname）] または [アドレス（Address）] を入力します。IPv4 アドレスを使用する必要があります。IPv6 アドレスを使用してユーザ エージェントに接続するように Firepower Management Center を設定することはできません。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 接続を削除するには、削除アイコン（  ）をクリックして、その削除を確認します。

次の作業

- *Firepower* ユーザ エージェント構成ガイド の説明に従って、ユーザ エージェントの設定を続けます。

- アイデンティティ ルールの作成の説明に従ってアイデンティティ ルールを設定します。
- 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）。

関連トピック

ユーザ 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, （5 ページ）
アクセス コントロール ポリシーの開始

ユーザ 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

ユーザエージェント接続に問題が起こった場合は、*Firepower* ユーザ エージェント構成ガイド を確認してください。

このガイドの関連するトラブルシューティング情報については、レルムとユーザのダウンロードのトラブルシューティングとユーザ制御のトラブルシューティングを参照してください。

ユーザエージェントによって報告されるユーザデータに関する問題が発生した場合は、次の点に注意してください。

- システムはデータがまだデータベースにないユーザ エージェント ユーザのアクティビティを検出すると、サーバからそれらに関する情報を取得します。ユーザのアクティビティは、システムがユーザのダウンロードでユーザに関する情報の取得に成功するまでルールで処理されず、Web インターフェイスに表示されません。

ISE アイデンティティ ソース

Cisco Identity Services Engine（ISE）の展開を Firepower システムと統合して、ISE をパッシブ認証に使用できます。

ISE は、信頼できるアイデンティティ ソースで、Active Directory（AD）、LDAP、RADIUS、または RSA を使用して認証するユーザに関するユーザ認識データを提供します。さらに、Active Directory ユーザのユーザ制御を行えます。ISE は、ISE ゲスト サービス ユーザの失敗したログイン試行またはアクティビティは報告しません。

（注） Firepower は、マシンの認証をユーザと関連付けないため、AD 認証と同時に 802.1x マシン認証を使用することはできません。802.1x アクティブ ログインを使用する場合は、802.1x アクティブ ログイン（マシンとユーザの両方）だけを報告するように ISE を設定します。このように設定すれば、マシン ログインはシステムに 1 回だけ報告されます。

Cisco ISE の詳細については、*Cisco Identity Services Engine Administrator Guide*を参照してください。

ISE バージョンと設定の互換性

ご使用の ISE バージョンと設定は、次のように Firepower との統合や相互作用に影響を与えます。

- ISE サーバと Firepower Management Center の時刻を同期します。そうしないと、システムが予期しない間隔でユーザのタイムアウトを実行する可能性があります。
- 多数のユーザ グループをモニタするように ISE を設定した場合、システムはメモリ制限のためにグループに基づいてユーザ マッピングをドロップすることがあります。その結果、レルムまたはユーザ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。
- ISE のバージョン 1.3 には、IPv6 対応エンドポイントのサポートが含まれていません。ISE のこのバージョンを実行している場合、ユーザ アイデンティティ データを収集したり、IPv6 対応エンドポイント上で修正を実行したりすることはできません。

システムのこのバージョンと互換性がある特定のバージョンの ISE については、『*Cisco Firepower Compatibility Guide*』を参照してください。

ISE 属性

ISE 接続を設定すると、ISE 属性データが Firepower Management Center データベースに入力されます。ユーザ認識とユーザ制御に使用できる ISE 属性は、次のとおりです。

セキュリティ グループ タグ（SGT）（Security Group Tag (SGT)）

セキュリティ グループ タグ（SGT）は、信頼ネットワーク内のトラフィックの送信元の権限を指定します。Cisco ISE および Cisco TrustSec は、ネットワークに入るときに、セキュリティ グループ アクセス（SGA）と呼ばれる機能を使用して、パケットに SGT 属性を適用します。これらの SGT は、ISE または TrustSec 内のユーザの割り当てられたセキュリティ グループに対応します。ID ソースとして ISE を設定すると、Firepower システムは、これらの SGT を使用してトラフィックをフィルタリングできます。

エンドポイント ロケーション（Endpoint Location）（またはロケーション IP（Location IP））

[エンドポイント ロケーション（Endpoint Location）] 属性は、ISE によって識別される、ユーザの認証に ISE を使用したネットワーク デバイスの IP アドレスです。

エンドポイント プロファイル（Endpoint Profile）（またはデバイス タイプ（Device Type））

[エンドポイント プロファイル（Endpoint Profile）] 属性は、ISE によって識別されるユーザのエンドポイント デバイス タイプです。

ISE 接続の設定

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）	任意（Any）	任意（Any）	グローバルだけ	Admin/Access Admin/Network Admin

詳細については、ISE アイデンティティ ソース, （5 ページ）およびISE 設定フィールド, （8 ページ）を参照してください。

はじめる前に

- Firepower Management Center のアクセス元となるマシンで証明書を作成するか、証明書データとキーを利用可能にします。
- ISE データを使用してユーザ制御を実装する予定の場合、レルムの作成の説明に従って、pxGrid のペルソナを想定して ISE サーバのレルムを設定し有効にします。

手順

ステップ 1 [システム（System）] > [統合（Integration）] をクリックします。

ステップ 2 [アイデンティティの送信元（Identity Sources）] タブをクリックします。

ステップ 3 [サービス タイプ（Service Type）] で [Identity Services Engine] をクリックし、ISE 接続を有効にします。

（注） 接続を無効にするには、[なし（None）] をクリックします。

ステップ 4 [プライマリ ホスト名/IP アドレス（Primary Host Name/IP Address）]、およびオプションで [セカンダリ ホスト名/IP アドレス（Secondary Host Name/IP Address）] を入力します。

ステップ 5 [pxGrid サーバ CA（pxGrid Server CA）] および [MNT サーバ CA（MNT Server CA）] リストから該当する認証局を、[FMC サーバ証明書（FMC Server Certificate）] リストから適切な証明書をそれぞれクリックします。また、追加アイコン（  ）をクリックして証明書を追加することもできます。

（注） [FMC サーバ証明書（FMC Server Certificate）] には、clientAuth 拡張キー使用値が含まれている必要があります。そうでない場合、拡張キー使用値は含まれていてはなりません。

ステップ 6 （オプション）CIDR ブロック表記を使用して [ISE ネットワーク フィルタ（ISE Network Filter）] を入力します。

ステップ 7 接続をテストするには、[テスト（Test）] をクリックします。

次の作業

- アイデンティティ ルールを作成します（アイデンティティ ルールの作成 を参照）。
- 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）。

関連トピック

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, （16 ページ）
信頼できる認証局オブジェクト
内部証明書オブジェクト

ISE 設定フィールド

次のフィールドを使用して ISE への接続を設定します。

プライマリおよびセカンダリ ホスト名/IP アドレス（Primary and Secondary Host Name/IP Address）

プライマリ（およびオプションでセカンダリ）ISE サーバのホスト名または IP アドレス。

pxGrid サーバ CA（pxGrid Server CA）

pxGrid フレームワークの認証局。展開にプライマリとセカンダリの pxGrid ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

MNT サーバ CA（MNT Server CA）

一括ダウンロード実行時の ISE 証明書の認証局。展開にプライマリとセカンダリの MNT ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

FMC サーバ証明書（FMC Server Certificate）

ISE への接続時、または一括ダウンロードの実行時に Firepower Management Center が ISE に提供する必要がある証明書およびキー。

（注） [FMC サーバ証明書（FMC Server Certificate）] には、clientAuth 拡張キー使用値が含まれている必要があります。そうでない場合、拡張キー使用値は含まれていてはなりません。

ISE ネットワーク フィルタ（ISE Network Filter）

オプションのフィルタで、ISE が Firepower Management Center にレポートするデータを制限するために設定できます。ネットワーク フィルタを指定する場合、ISE はそのフィルタ内のネットワークからデータをレポートします。次の方法でフィルタを指定できます。

- 任意（Any）のフィルタを指定する場合はフィールドを空白のままにします。
- CIDR 表記を使用して単一の IPv4 アドレス ブロックを入力します。
- CIDR 表記を使用して IPv4 アドレス ブロックのリストをカンマで区切って入力します。

（注） このバージョンの FirePOWER システムは、ISE のバージョンに関係なく、IPv6 アドレスを使用したフィルタリングをサポートしません。

関連トピック

信頼できる認証局オブジェクト
内部証明書オブジェクト

ISE アイデンティティ ソースのトラブルシューティング

関連の他のトラブルシューティングについては、レルムとユーザのダウンロードのトラブルシューティングおよびユーザ制御のトラブルシューティングを参照してください。

ISE 接続に問題が起こった場合は、次のことを確認してください。

- ISE と Firepower システムを正常に統合するには、ISE 内の pxGrid アイデンティティ マッピング機能を有効にする必要があります。
- [FMC サーバ証明書（FMC Server Certificate）] には、[clientAuth] 拡張キー使用値が含まれている必要があります。そうでない場合、拡張キー使用値は含まれていてはなりません。
- ISE サーバの時刻は、Firepower Management Center の時刻と同期している必要があります。アプライアンスが同期されていないと、予想外の間隔でユーザのタイムアウトが実行される可能性があります。
- 展開にプライマリとセカンダリの pxGrid ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。
- 展開にプライマリとセカンダリの MNT ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

ISE によって報告されるユーザ データに関する問題が発生した場合は、次の点に注意してください。

- システムはデータがまだデータベースにない ISE ユーザのアクティビティを検出すると、サーバからそれらに関する情報を取得します。ISE ユーザから見えるアクティビティは、シ

ステムがユーザのダウンロードで情報の取得に成功するまでアクセス コントロール ルールで**処理されず**、Web インターフェイスに**表示されません**。

- LDAP、RADIUS、または RSA ドメイン コントローラで認証された ISE ユーザに対するユーザ制御は実行できません。
- Firepower Management Center は、ISE ゲスト サービス ユーザのユーザ データを受信できません。
- 使用する ISE バージョンと構成は、Firepower システムでの ISE の使用方法に影響を与えます。詳細については、ISE アイデンティティ ソース, （5 ページ）を参照してください。
-

サポートされている機能に問題がある場合は、ISE アイデンティティ ソース, （5 ページ）で詳細を参照してバージョンの互換性を確認してください。

キャプティブ ポータルのアイデンティティ ソース

キャプティブ ポータルは、Firepower システムでサポートされる権限のあるアイデンティティ ソースの 1 つです。これは Firepower システムでサポートされる唯一のアクティブな認証方式であり、ユーザは管理対象デバイスを使用してネットワークに対する認証を行うことができます。

通常、キャプティブ ポータルを使用して、インターネットにアクセスするため、または制限されている内部リソースにアクセスするための認証を要求します。必要に応じて、リソースへのゲスト アクセスを設定することができます。システムはキャプティブ ポータル ユーザを認証した後、それらのユーザのトラフィックをアクセス制御ルールに従って処理します。キャプティブ ポータルは、HTTP および HTTPS のトラフィックのみで認証を行います。

（注） キャプティブ ポータルが認証を実行する前に、HTTPS トラフィックを復号化する必要があります。

キャプティブ ポータルはまた、失敗した認証の試行を記録します。失敗した試行で新しいユーザがデータベース内のユーザのリストに追加されることはありません。キャプティブ ポータルで報告される失敗した認証アクティビティのユーザ アクティビティ タイプは [認証失敗ユーザ（Failed Auth User）] です。

キャプティブ ポータルから取得された認証データはユーザ認識とユーザ制御に使用できます。

アイデンティティ ポリシーでキャプティブ ポータルを設定して展開すると、指定されたレルムのユーザは以下のデバイスを介して認証を行ってからネットワークにアクセスします。

- 7000 および 8000 シリーズ デバイス上の仮想ルータ
- バージョン 9.5(2) 以降で稼働するルーテッド モードの ASA FirePOWER デバイス

アイデンティティ ポリシーのキャプティブ ポータルを設定し、アイデンティティ ルールのアクティブ認証を呼び出します。アイデンティティ ポリシーはアクセス コントロール ポリシーで呼

び出されます。詳細については、キャプティブ ポータル アイデンティティ ルールの設定, （11 ページ）を参照してください。

キャプティブ ポータル アクティブ認証を実行できるのは、ルーテッド インターフェイスが設定されているデバイスのみです。アクセス コントロール ポリシーで参照されているアイデンティティ ポリシーに 1 つ以上のキャプティブ ポータルのアイデンティティ ルールが含まれ、以下を管理する Firepower Management Centerにポリシーを展開する場合、次のようになります。

- ルーテッドインターフェイスが設定されている 1 つ以上のデバイスの場合、ポリシー導入は成功し、ルーテッド インターフェイスがアクティブ認証を実行します。

  システムは ASA with FirePOWER デバイスでインターフェイス タイプを検証しません。ASA with FirePOWER デバイス上でインライン（タップ モード）インターフェイスにキャプティブ ポータル ポリシーを適用すると、ポリシーは正常に展開されますが、これらのルールに一致するトラフィック内のユーザは「不明」と識別されます。

- 1 つ以上の NGIPSv デバイスの場合、ポリシー導入は失敗します。

以下の要件と制約事項に注意してください。

- システムがサポートするキャプティブ ポータル ログインの数は 1 秒あたり最大 20 です。
- キャプティブ ポータルに使用する予定のデバイスの IP アドレスおよびポートを宛先とするトラフィックを許可する必要があります。アクセス制御で宛先が許可されない場合、キャプティブ ポータルを使用してトラフィックを認証することはできません。
- キャプティブ ポータル アクティブ認証を HTTPS トラフィックで行う場合、SSL ポリシーを使用して、認証対象のユーザからのトラフィックを復号する必要があります。キャプティブ ポータル ユーザの Web ブラウザと管理対象デバイス上のキャプティブ ポータル デーモンとの間の接続では、トラフィックを復号できません。この接続は、キャプティブ ポータル ユーザの認証に使用されます。

関連トピック

キャプティブ ポータル アイデンティティ ルールの設定, （11 ページ）

キャプティブ ポータル アイデンティティ ルールの設定

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（NGIPSv を除く）	任意（Any）	Administrator/Access Admin/Network Admin

キャプティブ ポータルのいくつかのアイデンティティ ポリシー設定はアクセス コントロール ポリシーの [アクティブ認証（Active Authentication）] タブページで行い、残りの設定はアクセス コントロール ポリシーに関連付けられたアイデンティティ ルールで行います。

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、[パッシブ認証でユーザを識別できない場合にアクティブ認証を使用（Use active authentication if passive authentication cannot identify user）] 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ます。それぞれのケースで、システムは SSL 復号を透過的に有効化/無効化し、これにより Snort プロセスが再起動します。

キャプティブ ポータルの詳細については、キャプティブ ポータルのアイデンティティ ソース，（10 ページ）およびキャプティブ ポータル フィールド，（14 ページ）を参照してください。

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、管理対象デバイスのモデルおよびトラフィックの処理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。

はじめる前に

- ルーテッド インターフェイスが設定された 1 つ以上のデバイスが、 Firepower Management Center によって管理されていることを確認します。

  Firepower Management Center で ASA with FirePOWER デバイスを管理している場合には、キャプティブ ポータルのアイデンティティ ソース，（10 ページ） を参照してください。

- Firepower Management Center のアクセス元となるマシンで証明書を作成するか、証明書データとキーを利用可能にします。

- HTTPS トラフィックでキャプティブ ポータルのアクティブ認証を実行するには、キャプティブ ポータルを使用して認証対象のユーザから送信されたトラフィックを復号する SSL ルールを作成する必要があります。

- （ルーテッド モードで ASA バージョン 9.5(2) 以降を実行する）ASA FirePOWER デバイスをキャプティブ ポータルに使用するには、**captive-portal** ASA CLI コマンドを使用してキャプティブ ポータルでのアクティブ認証を有効にし、『*ASA* ファイアウォール設定ガイド（バージョン 9.5(2) 以降）』（http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html [英語]）の説明に従ってポートを定義します。

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、アイデンティティ ポリシーを作成または編集します。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 3 新しいアクセス コントロール ポリシーを作成する場合は、[保存（Save）] をクリックします。

ステップ 4 [ルールの追加（Add Rule）] をクリックして新しいキャプティブ ポータル アイデンティティ ポリシー ルールを追加するか、編集アイコン（  ）をクリックして既存のルールを編集します。

ステップ 5 [アクティブ認証（Active Authentication）] タブをクリックします。

ステップ 6 リストから適切な [サーバ証明書（Server Certificate）] を選択するか、追加アイコン（  ）をクリックして証明書を追加します。

ステップ 7 [ポート（Port）] を入力して、[最大ログイン試行回数（Maximum login attempts）] を指定します。（デフォルトで、キャプティブ ポータルはポート 885 を使用します。）

ステップ 8 （オプション）キャプティブ ポータル応答ページの設定, （15 ページ） の説明に従って、[アクティブ認証応答ページ（Active Authentication Response Page）] を選択します。

ステップ 9 [ルール（Rules）] タブをクリックします。

ステップ 10 [レルムおよび設定（Realm & Settings）] タブをクリックします。

ステップ 11 （オプション）[認証でユーザを識別できない場合はゲストとして識別する（Identify as Guest if authentication cannot identify user）] をオンにします。詳細については、キャプティブ ポータル フィールド, （14 ページ）を参照してください。

ステップ 12 リストから [認証タイプ（Authentication Type）] を 1 つクリックします。

ステップ 13 （オプション）[HTTP ユーザ エージェントの除外（Exclude HTTP User-Agents）] をクリックし、キャプティブ ポータルからのアプリケーションの除外 の説明に従って特定のアプリケーション トラフィックをキャプティブ ポータルから除外します。

ステップ 14 [追加（Add）] をクリックするか、ルールの編集を続けます。

ステップ 15 [保存（Save）] をクリックします。

次の作業

- ユーザ認証のためにキャプティブ ポータルで使用する SSL トラフィックを複合して再署名する SSL アクセス制御ルールを作成します。ルールのターゲットを [不明な（Unknown）] ユーザに設定し、ルールをアクセス コントロール ポリシーに関連付けます。詳細については、SSL ルールの使用を開始するには を参照してください。
- キャプティブ ポータル ポート（デフォルトでは TCP ポート 885）経由でトラフィックを許可するアクセス制御ルールを作成します。詳細については、次を参照してください。アクセス コントロール ルールの作成および編集

- 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）。

関連トピック

キャプティブ ポータルからのアプリケーションの除外
内部証明書オブジェクト
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，（16 ページ）
Snort® の再起動シナリオ

キャプティブ ポータル 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 ポリシーの[アクティブ認証（Active Authentication）]タブでキャプティブ ポータルを設定します。アイデンティティ ルール フィールドも参照してください。

サーバ証明書（Server Certificate）

キャプティブ ポータル デーモンが示すサーバ証明書。

[ポート（Port）]

キャプティブ ポータル接続のために使用するポート番号。ASA FirePOWER デバイスをキャプティブ ポータルに使用しようとする場合は、このフィールドのポート番号が、**captive-portal** CLI コマンドを使用して ASA FirePOWER デバイスで設定したポート番号と一致していなければなりません。

最大ログイン試行回数（Maximum login attempts）

ユーザのログイン要求がシステムによって拒否されるまでに許容されるログイン試行失敗の最大数。

アクティブ認証回答ページ（Active Authentication Response Page）

キャプティブ ポータル ユーザに対して表示される、システム提供またはカスタムの HTTP 応答ページ。アイデンティティ ポリシーのアクティブ認証設定で[アクティブ認証応答ページ（Active Authentication Response Page）] を選択したら、[HTTP 応答ページ（TTP Response Page）] で 1 つ以上のアイデンティティ ルールを [認証タイプ（Authentication Type）] として設定する必要があります。

関連トピック

内部証明書オブジェクト

キャプティブ ポータル応答ページの設定

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（NGIPSv を除く）	任意（Any）	Administrator/Access Admin/Network Admin

キャプティブ ポータルユーザを表示するために、システム提供またはカスタムのいずれかのHTTP応答ページを選択できます。

キャプティブ ポータルの詳細については、キャプティブ ポータルのアイデンティティ ソース，（10 ページ）およびキャプティブ ポータル フィールド，（14 ページ）を参照してください。

はじめる前に

- キャプティブ ポータル アイデンティティ ルールの設定，（11 ページ）の説明に従ってキャプティブ ポータルの設定を開始します。

手順

ステップ 1 アイデンティティ ポリシーの [アクティブ認証（Active Authentication）] タブで、ドロップダウンメニューから [アクティブ認証応答ページ（Active Authentication Response Page）] を選択します。

- 汎用的な応答を使用する場合は、[システム提供（System-provided）] を選択します。表示アイコン（  ）をクリックすると、このページの HTML コードが表示されます。
- カスタム応答を作成する場合は、[カスタム...（Custom...）] を選択します。ポップアップ ウィンドウが表示されます。このウィンドウに事前入力されているシステムによって提供されるコードを置換または変更できます。完了したら、変更を保存します。カスタムページは、編集アイコン（）をクリックすると編集できます。

ステップ 2 [保存（Save）] をクリックします。

次の作業

- キャプティブ ポータル アイデンティティ ルールの設定，（11 ページ）の説明に従ってキャプティブ ポータルの設定を続けます。

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

関連の他のトラブルシューティングについては、レルムとユーザのダウンロードのトラブルシューティングおよびユーザ制御のトラブルシューティングを参照してください。

キャプティブ ポータルに関する問題が発生した場合は、次の点を確認してください。

- キャプティブ ポータル サーバの時刻は、Firepower Management Center の時刻と同期している必要があります。
-
- Firepower Management Center と管理対象デバイスとの間の接続に障害が発生した場合、ユーザが以前に認識され Firepower Management Center にダウンロードされた場合を除き、デバイスによって報告されたすべてのキャプティブ ポータル ログインはダウンタイム中に特定できません。識別されていないユーザは、Firepower Management Center で [不明（Unknown）] のユーザとして記録されます。ダウンタイム後、不明のユーザはアイデンティティ ポリシーのルールに従って再確認され、処理されます。
- キャプティブ ポータルに使用する予定のデバイスにインライン インターフェイスとルーテッド インターフェイスの両方が含まれる場合、キャプティブ ポータル デバイス上でルーテッド インターフェイスだけを対象とするようにキャプティブ ポータル アイデンティティ ルールでゾーン条件を設定する必要があります。
- システムは ASA with FirePOWER デバイスでインターフェイス タイプを検証しません。ASA with FirePOWER デバイス上でインライン（タップ モード）インターフェイスにキャプティブ ポータル ポリシーを適用すると、ポリシーは正常に展開されますが、これらのルールに一致するトラフィック内のユーザは「不明」と識別されます。

トラフィック ベース検出のアイデンティティ ソース

トラフィック ベース検出は、Firepower システムでサポートされている唯一の権限のないアイデンティティ ソースです。トラフィック ベース検出を設定すると、管理対象デバイスは、指定したネットワークでの LDAP、AIM、POP3、IMAP、Oracle、SIP（VoIP）、FTP、HTTP、MDNS、SMTP のログインを検出します。トラフィック ベースの検出から取得されたデータは、ユーザ認識にのみ使用できます。権威のあるアイデンティティ ソースとは異なり、トラフィック ベースの検出はネットワーク検出ポリシーで設定します。トラフィック ベースのユーザ検出の設定を参照してください。

次の制限事項に注意してください。

- トラフィック ベースの検出では、LDAP 接続に対する Kerberos ログインのみを LDAP 認証として解釈します。また、管理対象デバイスは、SSL や TLS などのプロトコルを使用して暗号化された LDAP 認証を検出できません。

- トラフィック ベースの検出では OSCAR プロトコルを使用した AIM ログインだけを検出します。TOC2 を使用する AIM ログインは検出できません。
- トラフィック ベースの検出では SMTP ロギングを制限することができません。これは、ユーザが SMTP ログインに基づいてデータベースに追加されていないためです。システムが SMTP ログインを検出しても、一致する電子メール アドレスのユーザがデータベース内に存在しなければ、そのログインは記録されません。

トラフィック ベースの検出は、失敗したログイン試行も記録します。失敗ログイン試行で新しいユーザがデータベース内のユーザのリストに追加されることはありません。トラフィック ベースの検出により検出された失敗ログイン アクティビティのユーザ アクティビティ タイプは [失敗したユーザ ログイン（Failed User Login）] です。

（注） システムは失敗した HTTP ログインと成功した HTTP ログインを区別できません。HTTP ユーザ情報を表示するには、トラフィック ベースの検出設定で [失敗したログイン試行の取得（Capture Failed Login Attempts）] を有効にする必要があります。

注意 ネットワーク検出ポリシーを使用して、HTTP、FTP、MDNS プロトコルを介した非権限、トラフィック ベースのユーザ検出を有効/無効にすると 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、管理対象デバイスのモデルおよびトラフィックの処理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。

トラフィック ベースの検出データ

デバイスがトラフィック ベースの検出を使用してログインを検出すると、次の情報をユーザアクティビティとして記録するために Firepower Management Centerに送信します。

- ログインで識別されたユーザ名
- ログインの時刻
- ログインに関係する IP アドレス。このアドレスは、ユーザのホスト（LDAP、POP3、IMAP、および AIM ログインの場合）、サーバ（HTTP、MDNS、FTP、SMTP および Oracle ログインの場合）、またはセッション発信元（SIP ログインの場合）の IP アドレスになります。
- ユーザの電子メール アドレス（POP3、IMAP、および SMTP ログインの場合）
- ログインを検出したデバイスの名前

ユーザがすでに検出されている場合、Firepower Management Centerはそのユーザのログイン履歴を更新します。Firepower Management Center は POP3 および IMAP ログイン内の電子メール アドレスを使用して LDAP ユーザに関連付ける場合があることに注意してください。これは、Firepower Management Center が新しい IMAP ログインを検出して、その IMAP ログイン内の電子メール アド

レスが既存の LDAP ユーザのアドレスと一致した場合は、IMAP ログインで新しいユーザが作成されるのではなく、LDAP ユーザの履歴が更新されることを意味します。

ユーザが以前に検出されなかった場合、Firepower Management Center はユーザ データベースにユーザを追加します。AIM、SIP、Oracle ログインでは、常に新しいユーザ レコードが作成されます。これは、それらのログイン イベントには Firepower Management Center が他のログイン タイプに関連付けることができるデータが含まれていないためです。

Firepower Management Center は、次の場合に、ユーザ アイデンティティまたはユーザ ID を記録しません。

- そのログイン タイプを無視するようにネットワーク検出ポリシーを設定した場合
- 管理対象デバイスが SMTP ログインを検出したものの、ユーザ データベースに電子メール アドレスが一致する、検出済みの LDAP、POP3、または IMAP ユーザが含まれていない場合

ユーザ データはユーザ テーブルに追加されます。

トラフィック ベースの検出戦略

ユーザ アクティビティを検出するプロトコルを制限して、検出するユーザの総数を削減することにより、ほぼ完全なユーザ情報を提供していると思われるユーザに焦点を絞ることができます。プロトコルの検出を制限すると、ユーザ名の散乱を最小限に抑え、Firepower Management Center 上の記憶域を節約することができます。

トラフィック ベースの検出プロトコルを選択する際には、以下を検討してください。

- AIM、POP3、IMAP などのプロトコル経由でユーザ名を取得すると、契約業者、訪問者、およびその他のゲストからのネットワーク アクセスによって組織に無関係なユーザ名が収集される可能性があります。
- AIM、Oracle、および SIP ログインは、無関係なユーザ レコードを作成する可能性があります。この現象は、このようなログイン タイプが、システムが LDAP サーバから取得するユーザ メタデータのいずれにも関連付けられていないうえ、管理対象デバイスが検出するその他のログイン タイプに含まれている情報のいずれにも関連付けられていないために発生します。そのため、Firepower Management Centerは、これらのユーザとその他のユーザ タイプを関連付けることができません。

関連トピック

トラフィック ベースのユーザ検出の設定