ユーザ アイデンティティ ソース

以下のトピックでは、ユーザ認識のソースである、Firepower システム ユーザのアイデンティティ ソースについて説明しています。これらのユーザは、アイデンティティおよびアクセス コントロール ポリシーで制御できます。

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。各アイデンティティ ソースは、ユーザ認識のためのユーザの記憶域を提供します。これらのユーザは、アイデンティティおよびアクセス コントロール ポリシーで制御できます。

ユーザ アイデンティティ ソース	ポリシー	サーバ要件	タイプ（Type）	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	アイデンティティ	Microsoft Active Directory	権限のあるログイン	パッシブ	○	○	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	タイプ（Type）	認証タイプ（Authentication Type）	ユーザ認識	ユーザ制御	詳細
ISE	アイデンティティ	Microsoft Active Directory	権限のあるログイン	パッシブ	○	○	ISE アイデンティティ ソース （6 ページ）
TS エージェント	アイデンティティ	Microsoft Windows Terminal Server	権限のあるログイン	パッシブ	○	○	ターミナル サービス（TS）エージェントのアイデンティティ ソース （12 ページ）
キャプティブ ポータル	アイデンティティ	LDAP または Microsoft Active Directory	権限のあるログイン	Active	○	○	キャプティブ ポータルのアイデンティティ ソース （14 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	[はい（Yes）]	[いいえ（No）]	トラフィック ベース検出のアイデンティティ ソース （32 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 ポータルのアイデンティティ ソースには、ルーテッド インターフェイスを備えた管理対象デバイスが必要です。キャプティブ ポータルでインライン（タップ モードとも呼ばれます）インターフェイスを使用することはできません。

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。

必要なアイデンティティ ソースを使用してアイデンティティ ルールを設定したら、各ルールにアクセス コントロール ポリシーを関連付け、ポリシーを有効にするために管理対象デバイスに展開する必要があります。アクセス コントロール ポリシーおよび展開の詳細については、ユーザ条件、レルム条件、および ISE 属性条件（ユーザ制御）を参照してください。

Firepower システムでのユーザ検出の一般情報については、ユーザ アイデンティティについて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 エージェントのガイドライン

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。

ユーザ制御のためのユーザ エージェントの設定

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
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。

始める前に

- #unique_508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、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 **[システム（System）] > [統合（Integration）]** をクリックします。

ステップ 3 [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 4 [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 5 [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 6 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 7 [追加（Add）] をクリックします。

ステップ 8 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。

次のタスク

- *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。
- #unique_455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）。
- 設定変更の展開の説明に従って、使用するアイデンティティ ポリシーとアクセス コントロール ポリシーを管理対象デバイスに展開します。

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ト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。

- Firepower Management Center のハイ アベイラビリティが設定されており、プライマリが失敗した場合、たとえ以前ユーザを確認できており、Firepower Management Center にダウンロード済みであっても、フェールオーバーダウンタイム中にユーザエージェントが報告したすべてのログインが特定不能となります。未確認のユーザは Firepower Management Center には不明なユーザとして記録されます。ダウンタイム後、[不明（Unknown）] 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び識別され、処理されます。
- ユーザ エージェントが TS エージェントと同じユーザをモニタした場合、システムは TS エージェントのデータを優先します。TS エージェントとユーザエージェントが同じ IP アドレスによる同一のアクティビティを報告した場合は、TS エージェントのデータのみがログに記録されます。
- アクティブ FTP セッションは、イベントの **Unknown** ユーザとして表示されます。これは正常な処理です。アクティブ FTP では、（クライアントではない）サーバが接続を開始し、FTP サーバには関連付けられているユーザ名がないはずだからです。アクティブ FTP の詳細については、RFC 959 を参照してください。

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 システムは、マシンの認証をユーザと関連付けないため、Active Directory 認証と同時に 802.1x マシン認証をサポート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 のガイドラインと制限事項

Firepower システムで ISE を構成する際に、このセクションで説明されているガイドラインを使用してください。

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。
- ISE データを使用してユーザ制御を実装するには、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。
- ISE サーバに接続する各 Firepower Management Center ホスト名は一意である必要があります。そうでない場合、Firepower Management Center のいずれかへの接続は廃棄されます。
- 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。
- ISE のバージョン 2.0 パッチ 4 以降には、IPv6 対応エンドポイントのサポートが含まれています。
- ISE の展開で ISE Endpoint Protection Service（EPS）が有効で設定されている場合は、ISE 接続を使用して、相関ポリシー違反に関与している送信元または宛先ホストに対する ISE EPS 修復を実行できます。
- ユーザの EPSStatus が変更された後でユーザの SGT を更新するように ISE の展開を設定した場合は、ISE EPS 修復により、Firepower Management Center 上の SGT も更新されます。

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 でのクライアントの認証

ISE サーバと Firepower Management Center の間の接続が成功するには、ISE でクライアントを手動で承認する必要があります。（通常、接続テスト用と ISE エージェント用の 2 つのクライアントがあります）。

『*Cisco Identity Services Engine Administrator Guide*』の「Managing users and external identity sources」の章で説明しているように、ISE で [新しいアカウントを自動的に承認（Automatically approve new accounts）] を有効にすることもできます。

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。

（注） 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、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。詳細については、ISE 属性条件の設定を参照してください。

（注） 一部のルールでは、カスタム SGT 条件が ISE によって割り当てられなかった SGT 属性にタグ付けされたトラフィックを照合できます。これはユーザ制御とみなされず、アイデンティティ ソースとして ISE を使用しない場合にのみ機能します。カスタム SGT 条件 を参照してください。

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 ロケーション（Endpoint Location）]（[ロケーション IP（Location IP）]）に基づいてトラフィックを制御するには、アイデンティティ ポリシーを設定し、展開する必要があります。

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。

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。

[エンドポイント プロファイル（Endpoint Profile）]（[デバイス タイプ（Device Type）]）に基づいてトラフィックを制御するには、アイデンティティ ポリシーを設定し、展開する必要があります。

ユーザ制御用 ISE 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
任意（Any）	任意（Any）	任意（Any）	グローバルだけ	Admin/Access Admin/Network Admin

始める前に

- レルムの作成の説明に従い、pxGrid 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。
- 暗号化接続を使用して ISE サーバで Firepower Management Center を認証するには、Firepower Management Center のアクセス元となるマシンで証明書データとキーを利用可能にするか、証明書を作成します。

手順

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

ステップ 2 **[システム（System）] > [統合（Integration）]** をクリックします。

ステップ 3 [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 4 [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 5 [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 6 [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 7 （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 8 接続をテストするには、[テスト（Test）] をクリックします。

テストが失敗した場合、接続障害に関する詳細については、[その他のログ（Additional Logs）] をクリックします。

次のタスク

- アイデンティティ ポリシーの作成の説明に従って、制御するユーザおよび他のオプションを、アイデンティティ ポリシーを使って指定します。

- アクセス制御への他のポリシーの関連付けの説明に従って、アイデンティティ 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。このポリシーは、トラフィックのフィルタリングと、必要に応じて検査を実行します。
- 設定変更の展開の説明に従って、使用するアイデンティティ ポリシーとアクセス コントロール ポリシーを管理対象デバイスに展開します。
- ワークフローの使用の説明に従って、ユーザ アクティビティをモニタします。

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 （27 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）pxGrid ISE サーバのホスト名または IP アドレス。

指定するホスト名により使用されるポートには、ISE と Firepower Management Center の両方から到達可能である必要があります。

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。
- ISE サーバと Firepower Management Center の間の接続が成功するには、ISE でクライアントを手動で承認する必要があります。（通常、接続テスト用と ISE エージェント用の 2 つのクライアントがあります）。

  『*Cisco Identity Services Engine Administrator Guide*』の「Managing users and external identity sources」の章で説明しているように、ISE で [新しいアカウントを自動的に承認（Automatically approve new accounts）] を有効にすることもできます。
- [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 ノードが含まれている場合は、
  - 両方のノードの証明書が、同じ認証局によって署名される必要があります。

- ホスト名により使用されるポートが、ISE サーバと Firepower Management Center の両方により到達可能である必要があります。

- 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。

- ISE が TS エージェントと同じユーザをモニタした場合、Firepower Management Center は TS エージェントのデータを優先します。TS エージェントと ISE が同じ IP アドレスによる同一のアクティビティを報告した場合は、TS エージェントのデータのみが Firepower Management Center に記録されます。

- 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 （6 ページ）を参照してください。

- アクティブ FTP セッションは、イベントの **Unknown** ユーザとして表示されます。これは正常な処理です。アクティブ FTP では、（クライアントではない）サーバが接続を開始し、FTP サーバには関連付けられているユーザ名がないはずだからです。アクティブ FTP の詳細については、RFC 959 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 （6 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。

ターミナルサービス（TS）エージェントのアイデンティティ ソース

TS エージェントはパッシブ認証方式で、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。Windows Terminal Server が認証を実行し、TS エージェントがスタンドアロンまたはハイ アベイラビリティの Firepower Management Center にその認証の実行を報告します。

TS エージェントは、Windows Terminal Server にインストールされると、個々のユーザがモニタ対象ネットワークにログインまたはログアウトする際にそのユーザに固有のポート範囲を割

り当てます。Firepower Management Center では、この固有のポートを使用して Firepower システムの個々のユーザを識別します。1 つの TS エージェントを使用して、1 つの Windows Terminal Server 上のユーザ アクティビティをモニタし、暗号化データを Firepower Management Center に送信できます。

TS エージェントは失敗したログイン試行を報告しません。TS 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。

TS エージェントのガイドライン

TS エージェントには段階的な設定が必要で、次のものがあります。

1. TS エージェントがインストールおよび設定された Windows Terminal Server。
2. サーバがモニタするユーザを対象とする 1 つ以上のアイデンティティ レルム。

TS エージェントは、Microsoft Windows Terminal Server にインストールします。段階的な TS エージェントのインストールと設定、およびサーバと Firepower システムの要件の詳細については、『*Cisco Terminal Services (TS) Agent Guide*』を参照してください。

TS エージェントのデータは [ユーザ（Users）] テーブル、[ユーザ アクティビティ（User Activity）] テーブル、および [接続イベント（Connection Event）] テーブルに表示され、ユーザ認識とユーザ制御に使用できます。

（注） TS エージェントが別のパッシブ認証のアイデンティティ ソース（ユーザ エージェントまたは ISE）と同じユーザをモニタする場合、Firepower Management Center では TS エージェントのデータを優先します。TS エージェントと別のパッシブのアイデンティティ ソースが同じ IP アドレスでアクティビティを報告した場合、TS エージェントのデータだけが Firepower Management Center に記録されます。

TS エージェントのユーザ制御の構成

TS エージェントをユーザ認識およびユーザ制御のアイデンティティ ソースとして使用するには、『*Cisco Terminal Services (TS) Agent Guide*』の説明に従って TS エージェント ソフトウェアをインストールして構成してください。

次に行う作業：

- アイデンティティ ポリシーの作成の説明に従い、アイデンティティ ポリシーを使用して、制御するユーザおよびその他のオプションを指定します。
- アクセス制御への他のポリシーの関連付けの説明に従って、アイデンティティ 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。このポリシーは、トラフィックのフィルタリングと、必要に応じて検査を実行します。
- 設定変更の展開の説明に従って、使用するアイデンティティ ポリシーとアクセス コントロール ポリシーを管理対象デバイスに展開します。

- ワークフローの使用の説明に従って、ユーザ アクティビティをモニタします。

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

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ト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。

TS エージェントと Firepower システムの統合に問題が起こった場合は、次のことを確認してください。

- TS エージェントサーバと Firepower Management Center の時計を同期させる必要があります。
- TS エージェントが別のパッシブ認証 ID ソース（ユーザ エージェントまたは ISE）と同じユーザをモニタしている場合、Firepower Management Center は TS エージェントのデータを優先します。TS エージェントとパッシブ ID ソースが同じ IP アドレスによるアクティビティを報告した場合は、TS エージェントのデータのみが Firepower Management Center に記録されます。
- アクティブ FTP セッションは、イベントの **Unknown** ユーザとして表示されます。これは正常な処理です。アクティブ FTP では、（クライアントではない）サーバが接続を開始し、FTP サーバには関連付けられているユーザ名がないはずだからです。アクティブ FTP の詳細については、RFC 959 を参照してください。

トラブルシューティングのすべての情報は、『*Cisco Terminal Services (TS) Agent Configuration Guide*』を参照してください。

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。

関連トピック

ユーザ制御のためのキャプティブ ポータルの設定方法 （17 ページ）

キャプティブ ポータルのガイドラインと制約事項

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
- ルーテッド モードの Firepower Threat Defense デバイス

必要なルーテッド インターフェイス

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。キャプティブ ポータルにルールを設定していて、キャプティブ ポータル デバイスにインライン インターフェイスとルーテッド インターフェイスが含まれている場合は、デバイス上のルーテッドインターフェイスのみを対象とするインターフェイス条件を設定する必要があります。

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。

キャプティブ ポータルとポリシー

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 ポリシーに関連付けられます。

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 **[パッシブ認証でユーザを識別できない場合はアクティブ認証を使用する（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ています。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。

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。

キャプティブ ポータルの要件と制約事項

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。
- （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）』（https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/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。
- 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。
- 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。

ユーザ制御のためのキャプティブ ポータルの設定方法

始める前に

アクティブ認証にキャプティブ ポータルを使用するには、アクセス コントロール ポリシー、アイデンティティ ポリシー、SSL ポリシーを設定して、アイデンティティおよびSSL ポリシーをアクセス コントロール ポリシーと関連付ける必要があります。最後にポリシーを管理対象デバイスに展開します。このトピックでは、このタスクのハイレベルな概要について説明します。

手順全体の例は、キャプティブ ポータルの設定パート 1：アイデンティティ ポリシーの作成（19 ページ）にあります。

最初に次のタスクを実行します。

- 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 ポータルのガイドラインと制約事項 （15 ページ） を参照してください。

- キャプティブ ポータルで暗号化認証を使用するには、Firepower Management Center のアクセス元となるマシンで証明書データとキーを利用可能にするか、PKI オブジェクトを作成します。PKI オブジェクトの作成方法については、PKI オブジェクト を参照してください。

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 ポータルを使用したユーザ アクティビティの制御方法のハイレベルな概要は次のとおりです。

手順

ステップ 1 次のトピックに記載されているようにレルムを作成し、有効化します。

- レルムの作成
- レルム ディレクトリの設定
- ユーザとグループのダウンロード

ステップ 2 キャプティブ ポータル用のアクティブ認証アイデンティティ ポリシーを作成します。アイデンティティ ポリシーによって、キャプティブ ポータルで認証後にレルム アクセス リソースで選択したユーザを有効にします。

詳細については、キャプティブ ポータルの設定パート 1：アイデンティティ ポリシーの作成（19 ページ）を参照してください。

ステップ 3 キャプティブ ポータル ポート（デフォルトでは TCP 885）上のトラフィックを許可するキャプティブ ポータルに関するアクセス コントロール ルールを設定します。
キャプティブ ポータルが使用可能な TCP ポートのいずれかを選択できます。どれを選択しても、そのポートでトラフィックを許可するルールを作成する必要があります。

詳細については、キャプティブ ポータルの設定パート 2：TCP ポートアクセス コントロール ルールの作成 （20 ページ）を参照してください。

ステップ 4 別のアクセス コントロール ルールを追加して、選択したレルムのユーザがキャプティブ ポータルを使用してリソースにアクセスできるようにします。
これにより、ユーザはキャプティブ ポータルで認証できます。 詳細については、キャプティブ ポータルの設定パート 3：ユーザ アクセス コントロール ルールの作成 （21 ページ）を参照してください。

ステップ 5 キャプティブ ポータル ユーザが HTTPS プロトコルを使用して Web ページにアクセスできるように、[不明（Unknown）] なユーザ用の SSL 復号 - 再署名ポリシーを設定します。
HTTPS トラフィックがキャプティブ ポータルへ送信される前に復号化される場合のみ、キャプティブ ポータルはユーザを認証できます。システムは、キャプティブ ポータルを [不明（Unknown）] ユーザと認識します。

詳細については、キャプティブ ポータルの設定パート 4：SSL 復号 - 再署名ポリシーの作成 （22 ページ）を参照してください。

ステップ 6 アイデンティティ ポリシーと SSL 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（ステップ 2）。
この最後の手順により、システムはキャプティブ ポータルを使用してユーザを認証します。

詳細については、キャプティブ ポータルの設定パート 5：アクセス コントロール ポリシーへのアイデンティティ ポリシーと SSL ポリシーの関連付け （24 ページ）を参照してください。

次のタスク

キャプティブ ポータルの設定パート 1：アイデンティティ ポリシーの作成 （19 ページ）を参照してください。

関連トピック

キャプティブ ポータルからのアプリケーションの除外 （26 ページ）
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 （27 ページ）
Snort® の再起動シナリオ

キャプティブ ポータルの設定パート 1：アイデンティティ ポリシーの作成

始める前に

5 つのパートに分かれたこの手順では、デフォルトの TCP ポート 885 を使用し、キャプティブ ポータルと SSL 復号の両方に Firepower Management Center サーバ証明書を使用して、キャプティブ ポータルを設定する方法を示します。この例の各パートでは、キャプティブ ポータルでアクティブ認証を実行できるようにするために必要なタスクについて説明します。

すべての手順を実行すると、ドメイン内のユーザ用に機能するようにキャプティブ ポータルを設定できます。必要に応じて、手順の各パートで説明されている追加のタスクを実行できます。

手順全体の概要については、ユーザ制御のためのキャプティブ ポータルの設定方法 （17 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）] > [アイデンティティ（Identity）]** の順にクリックして、アイデンティティ ポリシーを作成または編集します。

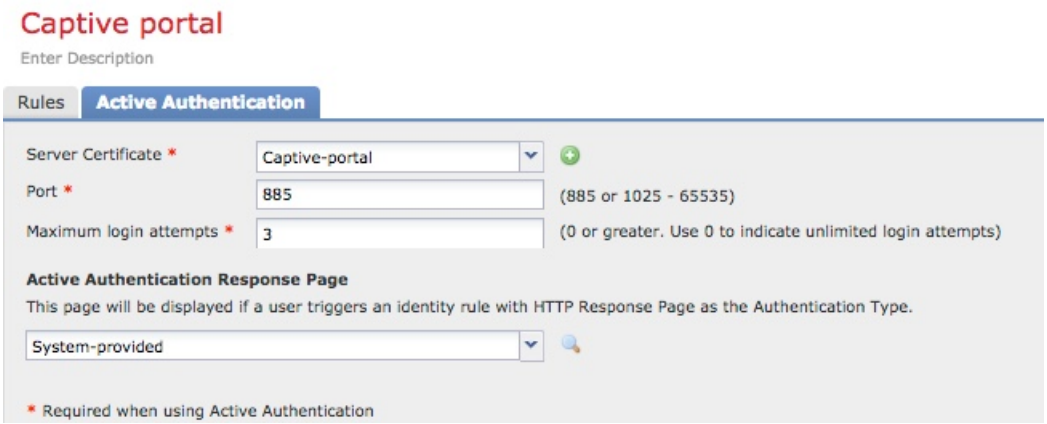
ステップ 3 （オプション）[カテゴリの追加（Add Category）] をクリックし、そのキャプティブ ポータル アイデンティティ ルール用にカテゴリを追加して、カテゴリの [名前（Name）] を入力します。

ステップ 4 [アクティブ認証（Active Authentication）] タブをクリックします。

ステップ 5 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 6 [ポート（Port）] フィールドに **885** と入力し、[最大ログイン試行回数（Maximum login attempts）] を指定します。

ステップ 7 （オプション）キャプティブ ポータル フィールド （25 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。
次の図は例を示しています。



ステップ 8 [保存（Save）] をクリックします。

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 11 ルールの [名前（Name）] を入力します。

ステップ 12 [アクション（Action）] リストから [アクティブ認証（Active Authentication）] を選択します。

システムは、TCP トラフィックにのみキャプティブ ポータルアクティブ認証を適用できます。アイデンティティ ルールの [アクション（Action）] が [アクティブ認証（Active Authentication）] である（つまりキャプティブ ポータルを使用している）場合、またはパッシブ認証を使用しており、[レルムおよび設定（Realms & Settings）] タブ ページのオプションで [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）] がオンに設定されている場合、TCP ポート制約のみを使用します。

ステップ 13 [レルムおよび設定（Realm & Settings）] タブをクリックします。

ステップ 14 [レルム（Realms）] 一覧から、ユーザ認証に使用するレルムを選択します。

ステップ 15 （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 （25 ページ）を参照してください。

ステップ 16 リストから [認証タイプ（Authentication Type）] を 1 つ選択します。

ステップ 17 （オプション）キャプティブ ポータルから特定のアプリケーション トラフィックを除外する方法については、キャプティブ ポータルからのアプリケーションの除外 （26 ページ）を参照してください。

ステップ 18 ルール条件タイプの説明に従って、ルールに条件を追加します（ポートやネットワークなど）。

ステップ 19 [追加（Add）] をクリックします。

ステップ 20 ページの上部にある [保存（Save）] をクリックします。

次のタスク

キャプティブ ポータルの設定パート 2：TCP ポートアクセス コントロール ルールの作成 （20 ページ）に進みます。

キャプティブ ポータルの設定パート 2：TCP ポートアクセス コントロール ルールの作成

この手順では、キャプティブ ポータルのデフォルト ポートである TCP ポート 885 を使用して、キャプティブポータルがクライアントと通信できるようにするアクセス コントロール ルールを作成する方法を示します。必要に応じて別のポートを選択できますが、キャプティブ ポータルの設定パート 1：アイデンティティ ポリシーの作成 （19 ページ）で選択したポートと一致している必要があります。

始める前に

キャプティブ ポータル設定全体の概要については、ユーザ制御のためのキャプティブ ポータルの設定方法 （17 ページ）を参照してください。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[ルールの追加（Add Rule）] をクリックします。

ステップ 2 ルールの [名前（Name）] を入力します。

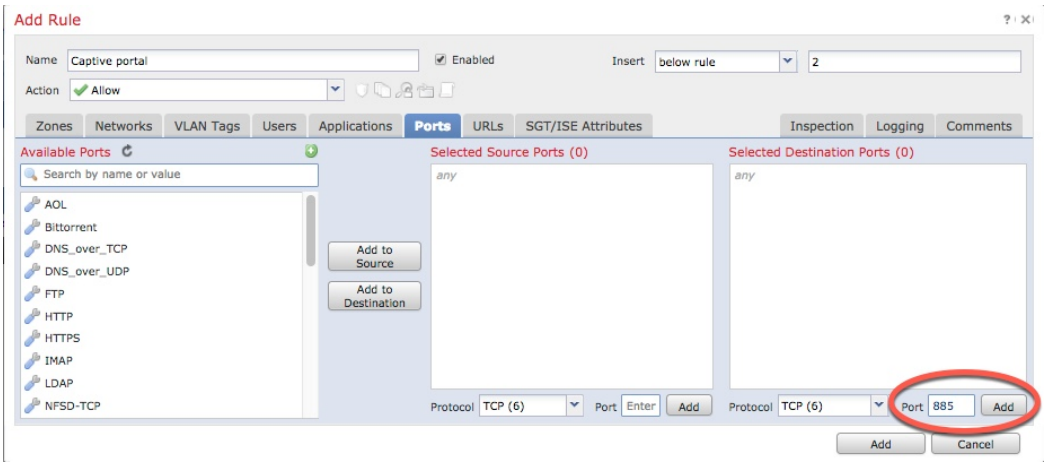
ステップ 3 [アクション（Action）] 一覧から、[許可（Allow）] を選択します。

ステップ 4 [ポート（Ports）] タブをクリックします。

ステップ 5 [選択した宛先ポート（Selected Destination Ports）] フィールドの [プロトコル（Protocol）] 一覧から、[TCP] を選択します。

ステップ 6 [ポート（Port）] フィールドに、「**885**」と入力します。

ステップ 7 [ポート（Port）] フィールドの横にある [追加（Add）] をクリックします。
次の図は例を示しています。



ステップ 8 ページ下部の [追加（Add）] をクリックします。

次のタスク

キャプティブ ポータルの設定パート 3：ユーザ アクセス コントロール ルールの作成 （21 ページ）に進みます。

キャプティブ ポータルの設定パート 3：ユーザ アクセス コントロール ルールの作成

この手順では、レルム内のユーザがキャプティブ ポータルを使用して認証できるようにするアクセス コントロール ルールを追加する方法について説明します。

始める前に

キャプティブ ポータル設定全体の概要については、ユーザ制御のためのキャプティブ ポータルの設定方法 （17 ページ）を参照してください。

手順

ステップ 1 ルール エディタで、[ルールの追加（Add Rule）] をクリックします。

ステップ 2 ルールの [名前（Name）] を入力します。

ステップ 3 [アクション（Action）] 一覧から、[許可（Allow）] を選択します。

ステップ 4 [ユーザ（Users）] タブをクリックします。

ステップ 5 [使用可能なレルム（Available Realms）] 一覧で、許可するレルムをクリックします。

ステップ 6 レルムが表示されない場合は、（更新）をクリックします。

ステップ 7 [使用可能なユーザ（Available Users）] 一覧で、ルールに追加するユーザを選択し、[ルールに追加（Add to Rule）] をクリックします。

ステップ 8 （オプション）ルール条件タイプの説明に従って、アクセス コントロール ポリシーに条件を追加します。

ステップ 9 [追加（Add）] をクリックします。

ステップ 10 [アクセス制御ルール（access control rule）] ページで、[保存（Save）] をクリックします。

ステップ 11 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。

次のタスク

キャプティブ ポータルの設定パート 4：SSL 復号 - 再署名ポリシーの作成 （22 ページ）に進みます。

キャプティブ ポータルの設定パート 4：SSL 復号 - 再署名ポリシーの作成

この手順では、トラフィックがキャプティブ ポータルに到達する前に、トラフィックを復号して再署名する SSL アクセス ポリシーを作成する方法について説明します。キャプティブ ポータルは、トラフィックが復号された後にのみトラフィックを認証できます。

始める前に

キャプティブ ポータル設定全体の概要については、ユーザ制御のためのキャプティブ ポータルの設定方法 （17 ページ）を参照してください。

手順

ステップ 1 PKI オブジェクトの説明に従って、SSL トラフィックを複合化するための証明書オブジェクトを作成します（まだ作成していない場合）。

ステップ 2 **[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [SSL]** の順にクリックします。

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）] を入力し、[デフォルトのアクション（Default Action）] を選択します。デフォルトのアクションについては、SSL ポリシーのデフォルト アクションを参照してください。

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 [アクション（Action）] 一覧から、[復号-再署名（Decrypt - Resign）] を選択します。

ステップ 9 [with] 一覧から、使用する PKI オブジェクトを選択します。

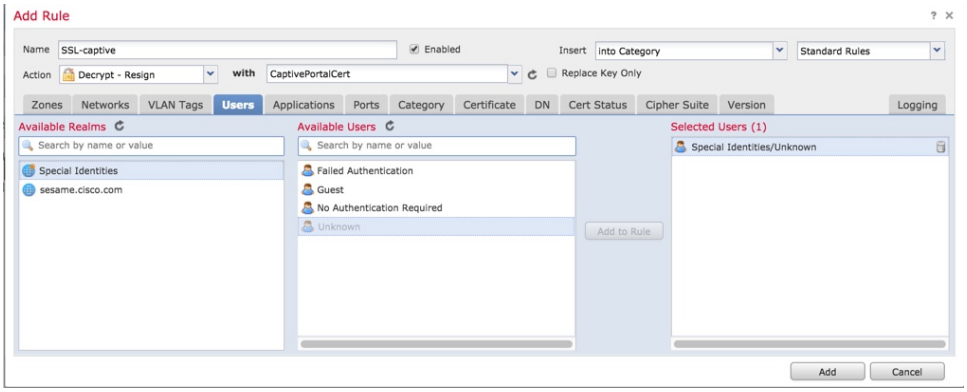
ステップ 10 [ユーザ（Users）] タブをクリックします。

ステップ 11 [使用可能なレルム（Available Realms）] 一覧の上にある （更新）をクリックします。

ステップ 12 [使用可能なレルム（Available Realms）] 一覧で、[特殊なアイデンティティ（Special Identities）] をクリックします。

ステップ 13 [使用可能なユーザ（Available Users）] 一覧で、[不明（Unknown）] をクリックします。

ステップ 14 [ルールに追加（Add to Rule）] をクリックします。
次の図は例を示しています。



ステップ 15 （オプション）SSL ルール条件の説明に従って、他のオプションを設定します。

ステップ 16 [追加（Add）] をクリックします。

ステップ 17 ページの上部にある [保存（Save）] をクリックします。

次のタスク

キャプティブ ポータルの設定パート 5：アクセス コントロール ポリシーへのアイデンティティ ポリシーと SSL ポリシーの関連付け （24 ページ）に進みます。

キャプティブ ポータルの設定パート 5：アクセス コントロール ポリシーへのアイデンティティ ポリシーと SSL ポリシーの関連付け

この手順では、アイデンティティ ポリシーと SSL [復号-再署名（Decrypt - Resign）] ルールを、以前に作成したアクセス コントロール ポリシーに関連付ける方法について説明します。この手順を実行すると、ユーザはキャプティブ ポータルを使用して認証できるようになります。

始める前に

キャプティブ ポータル設定全体の概要については、ユーザ制御のためのキャプティブ ポータルの設定方法 （17 ページ）を参照してください。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [アクセス コントロール（Access Control）]** をクリックして、キャプティブ ポータルの設定パート 2：TCP ポートアクセス コントロール ルールの作成 （20 ページ）の説明に従い作成したアクセス コントロール ポリシーを編集します。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 2 新しいアクセス コントロール ポリシーを作成するか、既存のポリシーを編集します。

ステップ 3 ページ上部の [アイデンティティ ポリシー（Identity Policy）] の横にあるリンクをクリックします。

ステップ 4 一覧から、使用するアイデンティティ ポリシーの名前を選択し、ページ上部にある [保存（Save）] をクリックします。

ステップ 5 上記の手順を繰り返して、使用するキャプティブ ポータル SSL 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。

ステップ 6 アクセス コントロール ポリシーのターゲット デバイスの設定の説明に従って、管理対象デバイスでそのポリシーをターゲットにします（この手順をまだ行っていない場合）。

次のタスク

- 設定変更の展開の説明に従って、使用するアイデンティティ ポリシーとアクセス コントロール ポリシーを管理対象デバイスに展開します。
- ワークフローの使用の説明に従って、ユーザ アクティビティをモニタします。

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）][認証プロトコル（Authentication Protocol）] として設定する必要があります。

システム提供の HTTP 応答ページには、[ユーザ名（Username）] と [パスワード（Password）] フィールドに加え、[ゲストとしてログイン（Login as guest）] ボタンがあり、ユーザはゲストとしてネットワークにアクセスできます。単一のログイン方法を表示するには、カスタム HTTP 応答ページを設定します。

次のオプションから選択します。

- 汎用的な応答を使用する場合は、[システム提供（System-provided）] をクリックします。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）] をクリックします。システム提供コードを示すウィンドウが表示され、これ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。

関連トピック

内部証明書オブジェクト

キャプティブ ポータルからのアプリケーションの除外

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
任意（Any）	Control	任意（NGIPSv を除く）	任意（Any）	Administrator、Access Admin、Network Admin

アプリケーション（HTTPユーザエージェント文字列によって指定される）を選択し、キャプティブポータルのアクティブ認証から除外することができます。これにより、選択されたアプリケーションからのトラフィックが認証を受けずにアイデンティティポリシーを通過できるようになります。

（注） このリストに表示されるのは、**User-Agent Exclusion タグ**が付けられたアプリケーションのみです。

手順

ステップ 1 アイデンティティ ルール エディタ ページの [レルムおよび設定（Realm & Settings）] タブで、[アプリケーション フィルタ（Application Filters）] リストのシスコ提供のフィルタを使用して、フィルタに追加するアプリケーションのリストを絞り込みます。

- リストを展開および縮小するには、各フィルタ タイプの横にある矢印をクリックします。
- フィルタ タイプを右クリックし、[すべて選択（Check All）] または [すべて選択解除（Uncheck All）] をクリックします。このリストには、各タイプで選択したフィルタ数が示されることに注意してください。
- 表示されるフィルタを絞り込むには、[名前で検索（Search by name）] フィールドに検索文字列を入力します。これは、カテゴリとタグの場合に特に有効です。検索をクリアするには、クリア アイコン（ ）をクリックします。
- フィルタのリストを更新し、選択したフィルタをすべてクリアするには、リロードアイコン（ ）をクリックします。
- すべてのフィルタと検索フィールドをクリアするには、[すべてのフィルタをクリア（Clear All Filters）] をクリックします。

（注） リストには一度に 100 のアプリケーションが表示されます。

ステップ 2 [使用可能なアプリケーション（Available Applications）] リストから、フィルタに追加するアプリケーションを選択します。

- 表示される個別のアプリケーションを絞り込むには、[名前で検索（Search by name）] フィールドに検索文字列を入力します。検索をクリアするには、クリア アイコン（✖）をクリックします。
- 使用可能な個別のアプリケーションのリストを参照するには、リストの下部にあるページング アイコンを使用します。
- アプリケーションのリストを更新し、選択したアプリケーションをすべてクリアするには、リロード アイコン（↻）をクリックします。

ステップ 3 外部認証から除外する、選択したアプリケーションを追加します。クリックしてドラッグするか、[ルールに追加（Add to Rule）] をクリックできます。結果は、選択したアプリケーション フィルタの組み合わせになります。

次のタスク

- 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。
- 設定済みの DNS 解決があり、**Kerberos**（または Kerberos をオプションとする場合は **HTTP ネゴシエート**）キャプティブ ポータルを実行するアイデンティティ ルールを作成する場合は、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）を解決するように DNS サーバを設定する必要があります。FQDN は、DNS 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。

- **Kerberos**（または Kerberos をオプションとする場合に **HTTP ネゴシエート**）を、アイデンティティ ルールの [認証タイプ（Authentication Type）] 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、[アクティブディレクトリ参加ユーザ名（AD Join Username）] と [アクティブディレクトリ参加パスワード（AD Join Password）] を使用して設定する必要があります。

- アイデンティティ ルールの [認証タイプ（Authentication Type）] として [HTTP 基本（HTTP Basic）] を選択した場合、ネットワーク上のユーザはセッションがタイムアウトしたことを認識しない場合があります。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。
- 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。
- アクティブ FTP セッションは、イベントの **Unknown** ユーザとして表示されます。これは正常な処理です。アクティブ FTP では、（クライアントではない）サーバが接続を開始し、FTP サーバには関連付けられているユーザ名がないはずだからです。アクティブ FTP の詳細については、RFC 959 を参照してください。

リモート アクセス VPN アイデンティティ ソース

Firepower Threat Defense は、リモート アクセス SSL と IPsec IKEv2 VPN をサポートするセキュアなゲートウェイ機能を提供します。完全なトンネル クライアントである AnyConnect Secure Mobility Client[AnyConnectSecureMobilityClient] は、セキュリティ ゲートウェイへのセキュアな SSL および IKEv2 IPsec 接続をリモート ユーザに提供します。これはエンドポイント デバイスでサポートされている唯一のクライアントで、Firepower Threat Defense デバイスへのリモート VPN 接続が可能です。

Firepower Threat Defense のリモート アクセス VPN の管理の説明に従って安全な VPN ゲートウェイを設定する場合、ユーザが Active Directory リポジトリ内にいる場合は、それらのユーザのアイデンティティ ポリシーを設定して、アクセス コントロール ポリシーにアイデンティティ ポリシーを関連付けることができます。

リモート ユーザから提供されるログイン情報は、LDAP/AD レルムまたは RADIUS サーバ グループによって検証されます。これらのエンティティは、Firepower Threat Defense セキュア ゲートウェイと統合されます。

（注） ユーザが認証ソースとして Active Directory を使用して RA VPN で認証を受ける場合、ユーザは自分のユーザ名を使用してログインする必要があります。`domain\username` または `username@domain` という形式でのログインは失敗します。（Active Directory はこのユーザ名をログオン名または場合によっては `sAMAccountName` として参照します）。詳細については、MSDN でユーザの命名属性 [英語] を参照してください。

認証に RADIUS を使用する場合、ユーザは前述のどの形式でもログインできます。

VPN 接続を介して一度認証されると、リモートユーザは *VPN の ID* を引き受けます。この VPN ID は、Firepower Threat Defense セキュア ゲートウェイ上のアイデンティティ ポリシーによって、そのリモート ユーザに属するネットワーク トラフィックを認識してフィルタリングするために使用されます。

アイデンティティ ポリシーはアクセス コントロール ポリシーと関連付けられ、これにより、誰がネットワーク リソースにアクセスできるかが決まります。リモート ユーザがネットワーク リソースからブロックされるか、ネットワーク リソースにアクセスできるかはこのようにして決まります。

関連トピック

VPN の概要
Firepower Threat Defense リモート アクセス VPN について
VPN の基本
Firepower Threat Defense リモート アクセス VPN の機能
Firepower Threat Defense リモート アクセス VPN に関するガイドラインと制限事項
Firepower Threat Defense のリモート アクセス VPN の管理

Firepower Threat Defense ダイナミック認証

Firepower Threat Defense は、RADIUS サーバを使用して、ダイナミック ACL またはユーザごとの ACL 名を使用する VPN リモート アクセスおよびファイアウォール カットスルー プロキシ セッションのユーザ許可を実行できます。ダイナミック ACL を実装するには、これをサポートするように RADIUS サーバを設定する必要があります。ユーザが認証を試みる場合、RADIUS サーバによってダウンロード可能 ACL、または ACL 名が Firepower Threat Defense に送信されます。所定のサービスへのアクセスが ACL によって許可または拒否されます。認証セッションの有効期限が切れると、Firepower Threat Defense によって ACL が削除されます。

関連トピック

RADIUS サーバ グループ
インターフェイス オブジェクト：インターフェイスグループとセキュリティ ゾーン
RADIUS ダイナミック認証の設定 （31 ページ）

ユーザ制御用 RA VPN 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

始める前に

- レルムの作成の説明に従って、レルムを作成します。
- 認証、認可、および監査（AAA）を使用するには、RADIUS サーバ グループの説明に従って RADIUS サーバ グループを設定します。

手順

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

ステップ 2 **[デバイス（Devices）] > [VPN] > [リモートアクセス（Remote Access）]** の順にクリックします。

ステップ 3 Firepower Threat Defense のリモート アクセス VPN の管理を参照してください。

次のタスク

- アイデンティティ ポリシーの作成の説明に従って、制御するユーザおよび他のオプションを、アイデンティティ ポリシーを使って指定します。
- アクセス制御への他のポリシーの関連付けの説明に従って、アイデンティティ 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。このポリシーは、トラフィックのフィルタリングと、必要に応じて検査を実行します。
- 設定変更の展開の説明に従って、使用するアイデンティティ ポリシーとアクセス コントロール ポリシーを管理対象デバイスに展開します。
- Firepower Threat Defense VPN モニタリングの説明に従って、VPN ユーザ トラフィックをモニタします。

RADIUS ダイナミック認証の設定

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
エクスポート コンプライアンス	該当なし	Firepower Threat Defense	リーフのみ	Admin

始める前に

- Firepower Threat Defense でこの機能を使用するには、AnyConnect Apex、Apex Plus、または AnyConnect Only ライセンスが必要です。
- RADIUS サーバで参照されている場合、セキュリティ ゾーンやインターフェイス グループには 1 つのインターフェイスのみ設定できます。
- ダイナミック認証が有効になっている RADIUS サーバでダイナミック認証を機能させるためには、Firepower Threat Defense 6.3 以降が必要です。
- RADIUS サーバでのインターフェイスの選択は、Firepower Threat Defense 6.3 以前のリリースではサポートされていません。そのため、インターフェイス オプションは展開時に無視されることをユーザに通知する警告が表示されます。

手順

ステップ 1 ダイナミック認証を使用して、RADIUS サーバ オブジェクトを設定します。RADIUS サーバ グループのオプションを参照してください。

ステップ 2 認可変更（CoA）対応インターフェイスを介して ISE サーバへの適切なルートを設定します。ユーザ制御用 ISE の設定 （8 ページ）を参照してください。

ステップ 3 ダイナミック認証を使用して作成した RADIUS サーバ グループ オブジェクトを使用して、リモート アクセス VPN ポリシーを設定します。m_Platform-Settings-Policy-Management.ditamap#map_391934B1EEA44607ACE8304D51DC10F3を参照してください。

ステップ 4 FlexConfig を介して、DNS サーバの詳細とドメインルックアップ インターフェイスを設定します。FlexConfig オブジェクトの設定を参照してください。

ステップ 5 VNP ネットワーク経由で DNS サーバに到達可能な場合は、リモート アクセス VPN トンネルを介して DNS トラフィックを許可するためのスプリット トンネルをグループ ポリシーに設定します。グループ ポリシー オブジェクトの設定を参照してください。

関連トピック

Firepower Threat Defense ダイナミック認証
インターフェイス オブジェクト：インターフェイスグループとセキュリティ ゾーン
m_FTD_RA_VPNs.ditamap#map_1E3D25E0D45B4C1B970DB24554B17FAE

リモートアクセスVPNアイデンティティソースのトラブルシューティング

- 関連する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ト、ユーザ制御のトラブルシューティング、および Firepower Threat Defense VPN のトラブルシューティング を参照してください。
- リモート アクセス VPN の問題が発生した場合は、Firepower Management Center と管理対象デバイスとの間の接続を確認します。接続に障害が発生している場合、ユーザが既に認識されて Firepower Management Center にダウンロードされている場合を除き、デバイスによって報告されたすべてのリモート アクセス VPN ログインはダウンタイム中に識別されません。

  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（Unknown）]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び識別され、処理されます。
- アクティブ FTP セッションは、イベントの **Unknown** ユーザとして表示されます。これは正常な処理です。アクティブ FTP では、（クライアントではない）サーバが接続を開始し、FTP サーバには関連付けられているユーザ名がないはずだからです。アクティブ FTP の詳細については、RFC 959 を参照してください。

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