



レールムとアイデンティティ ポリシー

レールムは、同じクレデンシャルを共有する 1 つ以上の LDAP または Microsoft Active Directory サーバで構成されます。ユーザおよびユーザ グループ クエリー、ユーザ アクセス コントロール を実行したり、ユーザ エージェント、ISE/ISE-PIC、キャプティブ ポータルを設定したりする場合、レールムを設定する必要があります。1 つ以上のレールムを設定すると、アイデンティティ ポリシーを設定できます。

アイデンティティ ポリシーは、ネットワーク上のトラフィックを権限のあるアイデンティティ ソースおよびレールムと関連付けます。アイデンティティ ポリシーを設定した後、アクセス コントロール ポリシーに関連付け、アクセス コントロール ポリシーをデバイスに展開できます。

レールムの基礎

ライセンス:任意(Any)

レールムは、ASA FirePOWER モジュールとモニタリングの対象サーバ間の接続を確立します。レールムでは、サーバの接続設定と認証フィルタの設定を指定します。レールムでは次のことを実行できます。

- アクティビティをモニタするユーザとユーザ グループとユーザを指定する。
- 正規ユーザに関するユーザ メタデータをサーバに照会する。

レールム内のディレクトリとして複数のサーバを追加できますが、同じ基本レールム情報を共有する必要があります。レールム内のディレクトリは、LDAP サーバのみ、または AD サーバのみである必要があります。レールムを有効にすると、保存された変更は次回 ASA FirePOWER モジュールがサーバに照会するときに適用されます。

ユーザ認識を行うには、サポートされるすべてのサーバタイプのレールムを設定する必要があります。モジュールは、これらの接続を使用して、POP3 ユーザおよび IMAP ユーザに関連付けられているデータをサーバ内で照会します。モジュールは、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、Active Directory、OpenLDAP、または Oracle Directory Server Enterprise Edition サーバ上の LDAP ユーザに関連付けます。たとえば、LDAP ユーザと電子メールアドレスが同じユーザの POP3 ログインをデバイスが検出すると、モジュールは LDAP ユーザのメタデータをそのユーザに関連付けます。

ユーザのアクセス コントロールを実行するために以下を設定できます。

- ユーザ エージェントまたは ISE/ISE-PIC デバイス用に設定された AD サーバのレールム。



(注) SGT ISE 属性条件を設定することを計画しているものの、ユーザ、グループ、レルム、エンドポイント ロケーション、エンドポイント プロファイルの条件の設定は計画していない場合、レルムの設定はオプションです。

- キャプティブ ポータル用に設定された Oracle または OpenLDAP サーバのレルム。

(ユーザ認識またはユーザ制御のために)レルムを設定してユーザをダウンロードする場合、ASA FirePOWER モジュールはサーバに定期的に照会し、前回のクエリ以降にアクティビティが検出された新規ユーザおよび更新されたユーザのメタデータを取得します。

ユーザ アクティビティ データはユーザ アクティビティ データベースに保存され、ユーザのアイデンティティ データはユーザ データベースに保存されます。アクセス コントロールで保存できる使用可能なユーザの最大数はデバイス モデルによって異なります。含めるユーザとグループを選択するときは、ユーザの総数がモデルの上限より少ないことを確認してください。アクセス コントロール パラメータの範囲が広すぎる場合、ASA FirePOWER モジュールはできるだけ多くのユーザに関する情報を取得し、取得できなかったユーザ数をタスク キューで報告します。



(注) LDAP サーバからモジュールによって検出されたユーザを削除しても、ASA FirePOWER モジュールはユーザ データベースからそのユーザを削除しません。そのため、手動で削除する必要があります。ただし、LDAP に対する変更は、ASA FirePOWER モジュールが次に権限のあるユーザのリストを更新したときにアクセス コントロール ルールに反映されます。

レルムがサポートされているサーバ

ライセンス:任意 (Any)

レルムを設定して次のサーバタイプに接続すると、ASA FirePOWER モジュールからの TCP/IP アクセスを提供できます。

表 32-1 レルムがサポートされているサーバ

サーバタイプ (Server Type)	ユーザ認識による データ取得のサ ポート	ユーザ エージェ ントによるデータ 取得のサポート	ISE/ISE-PIC によ るデータ取得のサ ポート	キャプティブ ポータルによる データ取得のサ ポート
Windows Server 2003、 Windows Server 2008、 および Windows Server 2012 上 の Microsoft Active Directory	○	○	○	○ (NTLM キャプ ティブ ポータル を使用する場合、 Windows Server 2003 を除く)

表 32-1 レルムがサポートされているサーバ(続き)

サーバタイプ (Server Type)	ユーザ認識による データ取得のサ ポート	ユーザ エージェ ントによるデータ 取得のサポート	ISE/ISE-PIC によ るデータ取得のサ ポート	キャプティブ ポータルによる データ取得のサ ポート
Windows Server 2003 と Windows Server 2008 上 の Oracle Directory Server Enterprise Edition 7.0	○	[いいえ (No)]	[いいえ (No)]	○
Linux 上の OpenLDAP	○	[いいえ (No)]	[いいえ (No)]	○

サーバ グループの設定に関して次の点に注意してください。

- ユーザ グループまたはグループ内のユーザに対してユーザ制御を実行する場合、サーバでユーザ グループを設定する必要があります。サーバが基本的なオブジェクト階層でユーザを整理している場合、ASA FirePOWER モジュールはユーザ グループ制御を実行できません。最大で 1500 のユーザを含むように LDAP または AD サーバグループのサイズを制限することを推奨します。サイズ超過のグループを含める(または除外する)ようにレルムを設定したり、サイズ超過のユーザ グループをターゲットにしたアクセス コントロール ルールを作成したりすると、パフォーマンス上の問題が生じる可能性があります。
- デフォルトでは、AD サーバはセカンダリ グループから報告するユーザの数を制限します。セカンダリ グループのすべてのユーザが ASA FirePOWER モジュールに報告されるようにこの制限をカスタマイズする必要があります。

サポートされるサーバ フィールド名

ライセンス:任意 (Any)

レルムのサーバは、ASA FirePOWER モジュールがサーバからユーザ メタデータを取得できるように、次の表にリストされているフィールド名を使用する必要があります。サーバ上のフィールド名が正しくない場合、ASA FirePOWER モジュールはそのフィールドの情報を使ってデータベースに入力できなくなります。

表 32-2 ASA FirePOWER フィールドへのサーバフィールドのマッピング

メタデータ	ASA FirePOWER モ ジュール	Active Directory	Oracle Directory Server	OpenLDAP
LDAP ユーザ名	[ユーザ名 (Username)]	samaccountname	cn uid	cn uid
first name	名	givenname	givenname	givenname
last name	姓	sn	sn	sn

表 32-2 ASA FirePOWER フィールドへのサーバフィールドのマッピング(続き)

メタデータ	ASA FirePOWER モジュール	Active Directory	Oracle Directory Server	OpenLDAP
メールアドレス	E メール	メールアドレス userprincipalname (mail に値が設定されていない場合)	メールアドレス	メールアドレス
部署	部署名 (Department)	部署 distinguishedname (department に値が設定されていない場合)	部署	ou
電話番号	電話	telephonenumber	適用対象外	telephonenumber

レルムに関する問題のトラブルシューティング

ライセンス:任意 (Any)

予期しないサーバ接続の動作に気付いたら、レルム設定、デバイス設定、またはサーバ設定の調整を検討してください。

予期しない時間にユーザ タイムアウトが発生する

予期しない間隔でユーザ タイムアウトが実行されていることに気付いたら、ユーザ エージェントまたは ISE/ISE-PIC デバイスの時間が ASA FirePOWER モジュール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。

レルム設定で指定したようにユーザが含まれない、または除外されない

Active Directory サーバのセカンダリ グループのメンバーであるユーザを含めるか除外する、Active Directory サーバのレルムを設定する場合、報告するユーザ数をサーバが制限していることがあります。

デフォルトでは、Active Directory サーバはセカンダリ グループから報告するユーザの数を制限します。セカンダリ グループのすべてのユーザが ASA FirePOWER モジュールに報告されるようにこの制限をカスタマイズする必要があります。

ユーザのダウンロードが遅い

ユーザのダウンロードが遅いことに気付いたら、LDAP および AD サーバ グループに最大 1500 のユーザが含まれることを確認します。サイズ超過のユーザ グループを含めるか除外するようにレルムを設定すると、パフォーマンスの問題が発生する可能性があります。

アイデンティティ ポリシーの基礎

ライセンス:任意 (Any)

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。

- [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [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。
- [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [統合(Integration)] > [アイデンティティ ソース (Identity Sources)] で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、および ISE/ISE-PIC を設定します。
- アイデンティティ ポリシー内で、アクティブ認証のアイデンティティ ソース、キャプティブ ポータルを設定します。

1 つ以上のアイデンティティ ポリシーを設定した後、アクセス コントロール ポリシーの 1 つのアイデンティティ ポリシーを呼び出す必要があります。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し、認証方式がパッシブまたはアクティブであるとき、モジュール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、モジュールはユーザ認証を実行しません。

レルムの作成

ライセンス:Control

レルムの作成方法:

-
- 手順 1 [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [統合(Integration)] の順に選択します。
 - 手順 2 [レルム(Realms)] をクリックします。
 - 手順 3 [新しいレルム(New Realm)] をクリックします。
 - 手順 4 [基本的なレルム情報の設定 \(32-8 ページ\)](#) の説明に従って基本的なレルム情報を設定します。
 - 手順 5 [レルム ディレクトリの設定\(32-8 ページ\)](#) の説明に従ってディレクトリを設定します。
 - 手順 6 [ユーザの自動ダウンロードの設定 \(32-9 ページ\)](#) の説明に従ってユーザとユーザ グループのダウンロード(アクセス コントロールに必要)を設定します。
 - 手順 7 レルム設定を保存します。
 - 手順 8 オプションで、[レルム ユーザ セッション タイムアウトの設定 \(32-9 ページ\)](#) の説明に従ってレルムを編集し、デフォルトのユーザ セッション タイムアウトの設定を変更します。
 - 手順 9 レルム設定を保存します。
-

次の作業

- **レルムの有効化または無効化(32-21 ページ)**の説明に従い、レルムを有効にします。
- オプションで、タスクのステータスをモニタします。[タスクのステータス (Task Status)] ページ([モニタリング (Monitoring)] > [ASA FirePOWER モニタリング (ASA FirePOWER Monitoring)] > [タスクのステータス (Task Status)])を参照してください。

レルム フィールド

ライセンス:任意 (Any)

次のフィールドを使用してレルムを設定します。

レルムの設定フィールド

AD プライマリ ドメイン (AD Primary Domain)

AD レルムのみの場合に、ユーザを認証する必要があるアクティブディレクトリ サーバのドメイン。

AD 参加ユーザ名 (AD Join Username) と AD 参加パスワード (AD Join Password)

Kerberos キャプティブ ポータル アクティブ認証を意図した AD レルムの場合に、クライアントをドメインに参加させるための適切な権限を持つユーザの識別用のユーザ名とパスワード。

Kerberos (または Kerberos をオプションとする場合は 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は、選択する [レルム (Realm)] には、Kerberos キャプティブ ポータル認証を実行できるようにするため、[AD 参加ユーザ名 (AD Join Username)] および [AD 参加パスワード (AD Join Password)] が設定されている必要があります。

説明

(任意)レルムの説明。

[ディレクトリ ユーザ名 (Directory Username)] と [ディレクトリ パスワード (Directory Password)]

取得するユーザ情報に適切な権限を持っているユーザの識別用のユーザ名とパスワード。

ベース DN (Base DN)

ASA FirePOWER モジュールがユーザ データの検索を開始するサーバのディレクトリ ツリー。

通常、ベース DN には、企業ドメインおよび部門を示す基本構造があります。たとえば、Example 社のセキュリティ (Security) 部門のベース DN は、ou=security,dc=example,dc=com となります。

グループ DN (Group DN)

ASA FirePOWER モジュールがグループ属性を持つユーザを検索するサーバのディレクトリ ツリー。

グループ属性 (Group Attribute)

サーバのグループ属性:[メンバー (Member)], [独自のメンバー (Unique Member)], [カスタム (Custom)]。

[名前(Name)]

レalmの一意の名前。

タイプ(Type)

レalm、AD、または LDAP のタイプ。

ユーザセッションのタイムアウト: 認証されたユーザ (User Session Timeout: Authenticated Users)

ユーザセッションがタイムアウトされるまでの最大時間(分単位)。

パッシブ認証されたユーザのセッションがタイムアウトした場合、ユーザは [不明 (Unknown)] と識別され、現在のセッションはアクセス コントロール ルール の設定に応じて許可またはブロックされます。モジュールは、次回ログイン時にユーザを再度識別します。

アクティブ認証された(キャプティブ ポータル)ユーザのセッションがタイムアウトした場合、ユーザは再認証を要求されます。

ユーザセッションのタイムアウト: 認証に失敗したユーザ (User Session Timeout: Failed Authentication Users)

アクティブ認証の試行失敗後にユーザのセッションがタイムアウトとなる時間(分単位)。認証に失敗したユーザのセッションがタイムアウトすると、ユーザは再認証を要求されます。

ユーザセッションのタイムアウト: ゲスト ユーザ (User Session Timeout: Guest Users)

アクティブ認証された(キャプティブ ポータル)ゲスト ユーザのセッションがタイムアウトされるまでの最大時間(分単位)。ユーザのセッションがタイムアウトすると、ユーザは再認証を要求されます。

レalmのディレクトリ フィールド (Realm Directory Fields)

これらの設定は、レalm内の個々のサーバ(ディレクトリ)に適用されます。

暗号化(Encryption)

サーバ接続に使用する暗号化方式。暗号化方式を指定する場合、このフィールドにホスト名を指定する必要があります。

ホスト名/IP アドレス (Hostname/IP Address)

サーバのホスト名または IP アドレス。

[ポート (Port)]

サーバ接続に使用するポート。

SSL 証明書 (SSL Certificate)

サーバへの認証に使用する SSL 証明書。SSL 証明書を使用するには、[暗号化(Encryption)] タイプを設定する必要があります。

認証に証明書を使用する場合、証明書のサーバ名は、サーバの [ホスト名/IP アドレス (Hostname/IP Address)] と一致する必要があります。たとえば、IP アドレスとして 10.10.10.250 を使用し、証明書内で computer1.example.com を使用した場合は、接続が失敗します。

ユーザのダウンロードフィールド

アクセス コントロールのためにダウンロードする (Download for access control)

このチェックボックスをオンにすると、ユーザ データの自動ダウンロードが設定されます。ユーザ認識と、状況によっては、ユーザのアクセス コントロールのためにデータを使用できます。

ダウンロードの頻度を設定するには、[自動ダウンロードの開始時間 (Begin automatic download at)] および [繰り返し設定 (Repeat every)] ドロップダウン メニューを使用します。

基本的なレルム情報の設定

ライセンス:Control

基本的なレルム情報の設定方法:

-
- 手順 1 [新しいレルムの追加 (Add New Realm)] ページで、[名前 (Name)] とオプションで [説明 (Description)] を入力します。
 - 手順 2 ドロップダウン リストから [タイプ (Type)] を選択します。
 - 手順 3 AD レルムを設定する場合は、[AD プライマリ ドメイン (AD Primary Domain)] を入力します。
 - 手順 4 Kerberos キャプティブ ポータル アクティブ 認証を意図した AD レルムを設定する場合は、識別用の [AD 参加ユーザ名 (AD Join Username)] と [AD 参加パスワード (AD Join Password)] には、クライアントをドメインに参加させるための適切な権限を持つユーザの情報を入力します。
 - 手順 5 取得するユーザ情報に適切な権限を持っているユーザの識別用の [ディレクトリ ユーザ名 (Directory Username)] と [ディレクトリ パスワード (Directory Password)] を入力します。
 - 手順 6 ディレクトリの [ベース DN (Base DN)] を入力します。
 - 手順 7 ディレクトリの [グループ DN (Group DN)] を入力します。
 - 手順 8 オプションで、ドロップダウン リストから [グループ属性 (Group Attribute)] を選択します。
 - 手順 9 [OK] をクリックします。
-

次の作業

- [レルム ディレクトリの設定 \(32-8 ページ\)](#) の説明に従ってレルム ディレクトリを設定します。

レルム ディレクトリの設定

ライセンス:Control

レルム ディレクトリの設定方法:

-
- 手順 1 [ディレクトリ (Directory)] タブで、[ディレクトリの追加 (Add Directory)] をクリックします。
 - 手順 2 サーバのホスト名/IP アドレスとポートを入力します。
 - 手順 3 暗号化モードを選択します。

- 手順 4 オプションで、ドロップダウン リストから SSL 証明書を選択します。追加アイコン(+)をクリックすると、オブジェクトを即座に作成することができます。
- 手順 5 接続をテストする場合は、[テスト(Test)] をクリックします。
- 手順 6 [OK] をクリックします。

次の作業

- オプションで、[ユーザの自動ダウンロードの設定 \(32-9 ページ\)](#) の説明に従ってユーザの自動ダウンロードを設定します。

ユーザの自動ダウンロードの設定

ライセンス:Control

含めるグループを指定しなかった場合、ASA FirePOWER モジュールは指定されたパラメータと一致するすべてのグループのユーザ データを取得します。パフォーマンス上の理由から、アクセス コントロールに使用するユーザを表すグループだけを明示的に含めることをお勧めします。

ユーザの自動ダウンロードの設定方法:

- 手順 1 [ユーザのダウンロード(User Download)] タブで、[(ユーザのアクセス コントロールに必要な) ユーザとグループをダウンロードする (Download users and groups (required for user access control))] チェックボックスをオンにします。
- 手順 2 ドロップダウン リストから [自動ダウンロードの開始時間(Begin automatic download at)] の時間を選択します。
- 手順 3 [繰り返し設定(Repeat Every)] ドロップダウン リストからダウンロード間隔を選択します。
- 手順 4 ダウンロードからユーザ グループを含めるか除外するには、[選択可能なグループ(Available Groups)] 列からユーザ グループを選択し、[含めるに追加(Add to Include)] または [除外に追加(Add to Exclude)] をクリックします。
- 手順 5 個々のユーザを含めるか除外するには、[含めるグループ(Groups to Include)] または [除外するグループ(Groups to Exclude)] の下のフィールドにユーザを入力し、[追加(Add)] をクリックします。



(注) ダウンロードからユーザを除外すると、そのユーザを条件として使用するアクセス コントロール ルールを作成できなくなります。複数のユーザはカンマで区切ります。このフィールドでは、アスタリスク(*)をワイルドカード文字として使用できます。

レルム ユーザ セッション タイムアウトの設定

ライセンス:Control



(注) 予期しない間隔でモジュールがユーザ タイムアウトを実行していることに気付いたら、ユーザ エージェントまたは ISE/ISE-PIC デバイスの時間が ASA FirePOWER モジュールの時間と同期されていることを確認します。

レalm ユーザ セッション タイムアウトを設定する方法:

-
- 手順 1 [レalm設定 (Realm Configuration)] タブを選択します。
 - 手順 2 [認証済みユーザ (Authenticated Users)], [認証に失敗したユーザ (Failed Authentication Users)], および [ゲスト ユーザ (Guest Users)] にユーザ セッション タイムアウト値を入力します。
 - 手順 3 [保存 (Save)] をクリックするか、レalmの編集を続けます。
-

アイデンティティ ポリシーの設定

ライセンス:Control

はじめる前に

- [レalmの作成 \(32-5 ページ\)](#) の説明に従って 1 つ以上のレalmを作成し、有効にします。

アイデンティティ ポリシーの設定方法:

Access: Admin/Access Admin/Network Admin

-
- 手順 1 [設定 (Configuration)] > [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [ポリシー (Policies)] > [アイデンティティ ポリシー (Identity Policy)] の順に選択します。
 - 手順 2 [名前 (Name)] を入力し、任意で [説明 (Description)] を入力します。
 - 手順 3 ポリシーにルールを追加する場合は、[アイデンティティ ルールの作成 \(32-14 ページ\)](#) の説明に従って [ルールの追加 (Add Rule)] をクリックします。
 - 手順 4 ルール カテゴリを追加する場合は、[アイデンティティ ルール カテゴリの追加 \(32-22 ページ\)](#) の説明に従って [カテゴリの追加 (Add Category)] をクリックします。
 - 手順 5 キャプティブ ポータルを使用するアクティブ認証を設定する場合は、[キャプティブ ポータル \(アクティブ認証\) の設定 \(32-11 ページ\)](#) の説明に従って [アクティブ認証 (Active Authentication)] をクリックします。
-

次の作業

- 設定変更を展開します。[設定変更の展開 \(4-13 ページ\)](#) 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) フィールド

ライセンス:任意 (Any)

次のフィールドを使用して、キャプティブ ポータルを設定します。

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 ポータル接続に使用するポート番号。このフィールドのポート番号は、`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る必要があります。

最大ログイン試行回数(Maximum login attempts)

ユーザのログイン要求がモジュール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 ユーザに表示する、システム付属またはカスタムの 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[アクティブ認証回答ページ(Active Authentication Response Page)]を選択したら、HTTP 応答ページを認証タイプとするアイデンティティ ルールを 1 つ以上設定する必要があります。

システム付属の HTTP 応答ページには、[ユーザ名 (Username)] と [パスワード (Password)] のフィールドに加え、ユーザがゲストとしてネットワークにアクセスすることを可能にする [ゲストとしてログイン (Login as guest)] ボタンがあります。ログイン方法を 1 つだけ表示する場合は、カスタム HTTP 応答ページを設定します。

キャプティブ ポータル(アクティブ認証)の設定**ライセンス:Control**

キャプティブ ポータル ユーザに表示する HTTP 応答ページは、システム付属またはカスタムのいずれかを選択できます。システム付属の HTTP 応答ページには、[ユーザ名 (Username)] と [パスワード (Password)] のフィールドに加え、ユーザがゲストとしてネットワークにアクセスすることを可能にする [ゲストとしてログイン (Login as guest)] ボタンがあります。ログイン方法を 1 つだけ表示する場合は、カスタム HTTP 応答ページを設定します。

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 アクティブ認証のアイデンティティ ソース \(33-7 ページ\)](#)を参照してください。

はじめる前に

- デバイスが管理している 1 つ以上の ASA FirePOWER デバイスが、ルーテッドモードでバージョン 9.5(2) 以降を実行していることを確認します。
- キャプティブ ポータルに使用するポート宛てのトラフィックを許可するようにアクセス コントロール ルールを設定します。
- HTTPS トラフィックでキャプティブ ポータルを使用してアクティブ認証を実行する場合は、キャプティブ ポータルを使用して認証する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。
- キャプティブ ポータル接続でトラフィックを復号する場合、キャプティブ ポータルに使用するポート宛てのトラフィックを復号する SSL ルールを作成します。
- captive-portal ASA CLI コマンドを使用してアクティブ認証のキャプティブ ポータルを有効にし、『*ASA Firewall Configuration Guide*』(バージョン 9.5(2) 以降)の説明に従ってポートを定義します。
<http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html> [英語]。

キャプティブ ポータルの設定方法:

-
- 手順 1** [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [アイデンティティ ポリシー (Identity Policy)] の順に選択し、アイデンティティ ポリシーを編集します。
- 手順 2** [アクティブ認証(Active Authentication)] をクリックします。

- 手順 3 ドロップダウン リストから、該当する [サーバ証明書 (Server Certificate)] を選択します。オプションで、追加アイコン (+) をクリックしてオブジェクトを即座に作成します。
- 手順 4 [ポート (Port)] を入力し、[最大ログイン試行回数 (Maximum login attempts)] を指定します。
- 手順 5 オプションで、HTTP 応答ページでユーザを認証するには、[アクティブ認証回答ページ (Active Authentication Response Page)] を選択します。
- 手順 6 [保存 (Save)] をクリックします。
- 手順 7 [アイデンティティ ルールの作成 \(32-14 ページ\)](#) の説明に従って [アクション (Action)] として [アクティブ認証 (Active Authentication)] を使用するアイデンティティ ルールを設定します。ステップ 5 で応答ページを選択した場合は、[認証タイプ (Authentication Type)] として HTTP 応答ページを選択する必要もあります。

次の作業

- 設定変更を展開します。[設定変更の展開 \(4-13 ページ\)](#) を参照してください。

アクティブ認証からのアプリケーションの除外

ライセンス:Control

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 (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。

アプリケーションをアクティブ認証から除外する方法:

- 手順 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 (X) 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 (C) 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。

- 手順 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。
- 前の手順で指定した制約を満たすすべてのアプリケーションを追加するには、[フィルタに一致するすべてのアプリケーション (All apps matching the filter)] 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。
- 手順 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。結果は次のもので構成されています。
- 選択したアプリケーション フィルタ
 - 選択した個別の使用可能なアプリケーション、または [フィルタに一致するすべてのアプリケーション (All apps matching the filter)]

次の作業

- [アイデンティティ ルールの作成 \(32-14 ページ\)](#) 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。

アイデンティティ ポリシーとアクセス コントロール ポリシーの関連付け

ライセンス:Control

ASA FirePOWER モジュールに同時に適用できるアイデンティティ ポリシーは 1 つだけです。アイデンティティ ポリシーを個別に適用することはできません。適用されたアイデンティティ ポリシー、または現在適用されているアイデンティティ ポリシーを削除することはできません。

アイデンティティ ポリシーとアクセス コントロール ポリシーを関連付ける方法:

- 手順 1** [設定 (Configuration)] > [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [ポリシー (Policies)] > [アクセス コントロール ポリシー (Access Control Policy)] の順に選択します。
- 手順 2** [詳細設定 (Advanced)] タブを選択します。
- 手順 3** [アイデンティティ ポリシーの設定 (Identity Policy Settings)] の横にある編集アイコン (✎) をクリックします。
- 手順 4** ドロップダウンからアイデンティティ ポリシーを選択します。
- 手順 5** [OK] をクリックします。
- 手順 6** [ASA FirePOWER の変更の保存 (Store ASA FirePOWER Changes)] をクリックして変更を保存します。

アイデンティティ ルールの作成

ライセンス:Control

アイデンティティ ルールの作成方法:

-
- 手順 1 [設定 (Configuration)] > [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [ポリシー (Policies)] > [アイデンティティ ポリシー (Identity Policy)] の順に選択します。
- 手順 2 [ルールの追加 (Add Rule)] をクリックします。
- 手順 3 [基本的なアイデンティティ ルール情報の設定 \(32-16 ページ\)](#) の説明に従ってアイデンティティ ルールの基本的な情報を設定します。
- 手順 4 オプションで、[アイデンティティ ルールへのゾーン条件の追加 \(32-18 ページ\)](#) の説明に従ってゾーン条件を追加します。



(注) 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ゾーン条件を設定する必要があります。

-
- 手順 5 オプションで、[アイデンティティ ルールへのネットワークまたは位置情報条件の追加 \(32-17 ページ\)](#) の説明に従ってネットワークまたは位置情報の条件を追加します。
- 手順 6 オプションで、[アイデンティティ ルールへのポート条件の追加 \(32-17 ページ\)](#) の説明に従ってポート条件を追加します。
- 手順 7 [アイデンティティ ルールでのレルムの関連付けとアクティブ認証設定の設定 \(32-18 ページ\)](#) の説明に従ってルールをレルムに関連付けます。
- 手順 8 [追加 (Add)] をクリックします。
- 手順 9 [ASA FirePOWER の変更の保存 (Store ASA FirePOWER Changes)] をクリックします。
-

次の作業

- 設定変更を展開します。[設定変更の展開 \(4-13 ページ\)](#) 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。

[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)

指定されたレルムでユーザに実行する認証のタイプ。パッシブ認証 (ユーザ エージェントまたは ISE/ISE-PIC)、アクティブ認証 (キャプティブ ポータル)、または認証なしを選択できます。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。

レalm

指定されたアクションを実行するユーザが含まれるレalm。アイデンティティ ルールのレalmとして選択する前に、レalmを完全に設定する必要があります。

Kerberos (または Kerberos をオプションとする場合は 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は、選択する [レalm (Realm)] には、Kerberos キャプティブ ポータル認証を実行できるようにするため、[AD 参加ユーザ名 (AD Join Username)] および [AD 参加パスワード (AD Join Password)] が設定されている必要があります。

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)

このオプションを選択すると、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、アクティブ認証 (キャプティブ ポータル) 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、パッシブ認証で識別できないユーザは [不明 (Unknown)] と識別されます。このフィールドを表示するには、パッシブ認証に対するルール アクションを設定する必要があります。

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、ASDM インターフェイスのすべてのエリアで不明ユーザが特別 ID/ゲストとして識別されます。このフィールドを表示するには、ルール アクションをアクティブ認証に設定するか、[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)] を選択する必要があります。

認証タイプ (Authentication Type)

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alm、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場合は、[NTLM] を選択します。この選択は AD レalmを選択するときのみ使用できます。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。アイデンティティ ルール認証タイプとして [NTLM] を選択した場合、アイデンティティ ルールのレalmとして Windows Server 2003 を使用することはできません。
- 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の場合に AD レalmを選択する場合のみ可能です。ユーザのブラウザで透過的な認証が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。

Kerberos キャプティブ ポータル認証を実行するためには、選択する [レalm (Realm)] 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)] が設定されている必要があります。



(注) 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 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 のいずれか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。この選択は AD レルムを選択するときのみ使用できます。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。

Kerberos キャプティブ ポータル認証を実行するためには、選択する [レルム (Realm)] 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)] が設定されている必要があります。

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 ルールを作成しようとしており、DNS 解決は設定済みである場合、DNS サーバを、キャプティブ ポータル デバイスのホスト名を解決するように設定する必要があります。キャプティブ ポータルのために使用するデバイスのホスト名は、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 FirePOWER モジュールで提供されている、またはカスタムの HTTP 応答ページを使用してユーザを認証する場合は、[HTTP 応答ページ (HTTP Response Page)] を選択します。ユーザは設定された応答ページを使用してネットワークにログインします。

システム付属の HTTP 応答ページには、[ユーザ名 (Username)] と [パスワード (Password)] のフィールドに加え、ユーザがゲストとしてネットワークにアクセスすることを可能にする [ゲストとしてログイン (Login as guest)] ボタンがあります。ログイン方法を 1 つだけ表示する場合は、カスタム HTTP 応答ページを設定します。

ゲストとしてログインするユーザは、Web インターフェイス上ではユーザ名 [ゲスト (Guest)] で表示され、そ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になります。

基本的なアイデンティティ ルール情報の設定

ライセンス:Control

基本的なアイデンティティ ルール情報の設定方法:

-
- 手順 1 アイデンティティ ルール エディタ ページで、[名前 (Name)] を入力します。
 - 手順 2 ルールを有効にするかどうかを指定します。
 - 手順 3 ルール カテゴリにルールを追加するには、[アイデンティティ ルール カテゴリの追加 \(32-22 ページ\)](#)を参照してください。
 - 手順 4 ドロップダウン リストからルールの [アクション (Action)] を選択します。
 - 手順 5 [追加 (Add)] をクリックするか、ルールの編集を続けます。
-

アイデンティティ ルールへのネットワークまたは位置情報条件の追加

ライセンス:Control

アイデンティティ ルールにネットワークまたは位置情報条件を追加する方法:

-
- 手順 1 アイデンティティ ルール エディタ ページで、[ネットワーク (Networks)] タブを選択します。
 - 手順 2 [利用可能なネットワーク (Available Networks)] から、次のように追加するネットワークを見つけます。
 - ネットワーク オブジェクトをオンザフライで追加するには(後で条件に追加できます)、[利用可能なネットワーク (Available Networks)] リストの上にある追加アイコン(+)をクリックします。
 - 追加するネットワーク オブジェクトまたは位置情報オブジェクトを検索するには、適切なタブを選択し、[利用可能なネットワーク (Available Networks)] リストの上にある [名前または値で検索 (Search by name or value)] プロンプトをクリックして、オブジェクトのコンポーネントの 1 つのオブジェクト名または値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。
 - 手順 3 オブジェクトを選択するには、そのオブジェクトをクリックします。すべてのオブジェクトを選択するには、右クリックして [すべて選択 (Select All)] を選択します。
 - 手順 4 [送信元に追加 (Add to Source)] または [宛先に追加 (Add to Destination)] をクリックします。
 - 手順 5 手動で指定する送信元または宛先 IP アドレスまたはアドレス ブロックを追加します。[送信元ネットワーク (Source Networks)] リストまたは [宛先ネットワーク (Destination Networks)] リストの下にある [IP アドレスの入力 (Enter an IP address)] プロンプトをクリックし、1 つの IP アドレスまたはアドレス ブロックを入力して [追加 (Add)] をクリックします。
 - 手順 6 [追加 (Add)] をクリックするか、ルール の編集を続けます。
-

アイデンティティ ルールへのポート条件の追加

ライセンス:Control

アイデンティティ ルールにポート条件を追加する方法:

-
- 手順 1 アイデンティティ ルール エディタ ページで、[ポート (Ports)] タブを選択します。
 - 手順 2 [利用可能なポート (Available Ports)] から追加する TCP ポートを次のように探します。
 - TCP ポート オブジェクトをオンザフライで追加するには(後で条件に追加できます)、[利用可能なポート (Available Ports)] リストの上にある追加アイコン(+)をクリックします。
 - 追加する TCP ベースのポート オブジェクトおよびグループを検索するには、[利用可能なポート (Available Ports)] リストの上にある [名前または値で検索 (Search by name or value)] プロンプトをクリックし、オブジェクトの名前またはオブジェクトのポートの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。たとえば、「443」と入力すると、提供の HTTPS ポート オブジェクトが ASA FirePOWER モジュールに表示されます。
 - 手順 3 TCP ベースのポート オブジェクトを 1 つ選択するには、クリックします。TCP ベースのポート オブジェクトをすべて選択するには、右クリックして [すべて選択 (Select All)] を選択します。非 TCP ベースのポートを含んでいるオブジェクトは、ポート条件に追加できません。

- 手順 4 [送信元に追加(Add to Source)] または [宛先に追加(Add to Destination)] をクリックします。
- 手順 5 送信元または宛先のポートを手動で指定するには、[選択した送信元ポート (Selected Source Ports)] または [選択した宛先ポート (Selected Destination Ports)] リストの下にある [ポート (Port)] にポート番号を入力します。0 ~ 65535 の値を持つ 1 つのポートを指定できます。
- 手順 6 [追加(Add)] をクリックします。



(注) ASA FirePOWER モジュールでは、無効なポート設定はルール条件に追加されません。

- 手順 7 [追加(Add)] をクリックするか、ルールの編集を続けます。

アイデンティティ ルールへのゾーン条件の追加

ライセンス:Control

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。

セキュリティ ゾーンの詳細については、[セキュリティ ゾーンの操作\(2-36 ページ\)](#)を参照してください。

アイデンティティ ルールにゾーン条件を追加する方法:

- 手順 1 アイデンティティ ルール エディタ ページで、[ゾーン (Zones)] タブを選択します。
- 手順 2 [利用可能なゾーン (Available Zones)] から追加するゾーンを見つけます。追加するゾーンを検索するには、[利用可能なゾーン (Available Zones)] リストの上にある [名前を検索 (Search by name)] プロンプトをクリックし、ゾーン名を入力します。入力すると、リストが更新されて一致するゾーンが表示されます。
- 手順 3 クリックすると、ゾーンを選択できます。すべてのゾーンを選択するには、右クリックして [すべて選択 (Select All)] を選択します。
- 手順 4 [送信元に追加(Add to Source)] または [宛先に追加(Add to Destination)] をクリックします。
- 手順 5 [追加(Add)] をクリックするか、ルールの編集を続けます。

アイデンティティ ルールでのレルムの関連付けとアクティブ認証設定の設定

ライセンス:Control

アイデンティティ ルールをレルムに関連付け、オプションで、アクティブ認証の追加設定を設定します。

アイデンティティ ルールをレルムに関連付ける方法:





- 手順 1 アイデンティティ ルール エディタ ページで、[レルムおよび設定 (Realm & Settings)] タブを選択します。

- 手順 2 ドロップダウン リストから [レalm (Realm)] を選択します。
- 手順 3 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)] チェックボックスをオンにします。このチェックボックスは、パッシブ認証ルールを設定するときのみ表示されます。
- 手順 4 ステップ 3 でチェックボックスをオンにした場合、またはこれがアクティブ認証ルールである場合、ステップ 4 に進みます。それ以外の場合は、ステップ 8 に進みます。
- 手順 5 オプションで、[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)] チェックボックスを選択します。
- 手順 6 ドロップダウン リストから [認証タイプ (Authentication Type)] を選択します。
- 手順 7 オプションで、[HTTP ユーザ エージェントの除外 (Exclude HTTP User-Agents)] を使用して、[アクティブ認証からのアプリケーションの除外 \(32-12 ページ\)](#)の説明に従って特定のアプリケーション トラフィックをアクティブ認証から除外します。
- 手順 8 [追加 (Add)] をクリックするか、ルールの編集を続けます。

レalmの管理

ライセンス:Control

レalmの管理方法:

- 手順 1 [設定 (Configuration)] > [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [統合 (Integration)] > [レalm (Realms)] の順に選択します。
- 手順 2 レalmを削除する場合は、削除アイコン()をクリックします。
- 手順 3 レalmを編集する場合は、レalmの横にある編集アイコン()をクリックし、[レalmの作成 \(32-5 ページ\)](#)の説明に従って変更を行います。
- 手順 4 レalmを有効または無効にするには、[レalmの有効化または無効化 \(32-21 ページ\)](#)の説明に従って、有効または無効にするレalmの横の [状態 (State)] スライダをクリックします。
- 手順 5 ユーザとユーザ グループをオンデマンドでダウンロードする場合は、[オンデマンドでのユーザとユーザ グループのダウンロード \(32-20 ページ\)](#)の説明に従って [ダウンロード (Download)] アイコン()をクリックします。
- 手順 6 レalmをコピーする場合は、コピー アイコン()をクリックします。
- 手順 7 レalmを比較する場合は、[レalmの比較 \(32-19 ページ\)](#)を参照してください。

レalmの比較

ライセンス:Control

レalmの比較方法:

- 手順 1 [設定 (Configuration)] > [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [統合 (Integration)] > [レalm (Realms)] の順に選択します。

- 手順 2 [レルムの比較(Compare Realms)] をクリックします。
- 手順 3 [比較対象(Compare Against)] ドロップダウン リストから [レルムの比較(Compare Realm)] を選択します。
- 手順 4 [レルム A(Realm A)] および [レルム B(Realm B)] ドロップダウン リストから比較するレルムを選択します。
- 手順 5 [OK] をクリックします。
- 手順 6 個々の変更を選択する場合は、タイトルバーの上の [前へ(Previous)] または [次へ(Next)] をクリックします。
- 手順 7 オプションで、[比較レポート(Comparison Report)] をクリックして、レルム比較レポートを生成します。
- 手順 8 オプションで、[新しい比較(New Comparison)] をクリックして、新しいレルム比較ビューを生成します。

オンデマンドでのユーザとユーザ グループのダウンロード

ライセンス:Control


レルムのユーザ ダウンロード パラメータまたはグループ ダウンロード パラメータを変更する場合、またはサーバでユーザまたはグループを変更して変更をユーザ制御にすぐに反映させる場合は、サーバからのオンデマンドユーザ ダウンロードの実行を ASA FirePOWER モジュールに強制できます。

ASA FirePOWER モジュールがサーバから取得可能なユーザの最大数はデバイス モデルによって異なります。レルムのダウンロード パラメータの範囲が広すぎる場合、ASA FirePOWER モジュールはできるだけ多くのユーザに関する情報を取得し、取得できなかったユーザ数をタスク キューで報告します。

はじめる前に

- [レルムの有効化または無効化\(32-21 ページ\)](#)の説明に従い、レルムを有効にします。

ユーザとユーザ グループをオンデマンドでダウンロードする方法:

- 手順 1 [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [統合(Integration)] > [レルム(Realms)] の順に選択します。
- 手順 2 ユーザとユーザ グループをダウンロードするレルムの横のダウンロードアイコン() をクリックします。

次の作業

- オプションで、タスクのステータスをモニタします。[タスクのステータス(Task Status)] ページ([モニタリング(Monitoring)] > [ASA FirePOWER モニタリング(ASA FirePOWER Monitoring)] > [タスクのステータス(Task Status)])を参照してください。

レalmの有効化または無効化

ライセンス:Control

レalmが有効になっていなければ、ASA FirePOWER モジュールがサーバに問い合わせることはできません。クエリーを停止するには、レalmを無効にします。

レalmを有効または無効にする方法:

-
- 手順 1 [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [統合(Integration)] > [レalm(Realms)] の順に選択します。
 - 手順 2 有効または無効にするレalmの横にある [状態(State)] スライダーをクリックします。
-



次の作業

- オプションで、タスクのステータスをモニタします。[タスクのステータス(Task Status)] ページ([モニタリング(Monitoring)] > [ASA FirePOWER モニタリング(ASA FirePOWER Monitoring)] > [タスクのステータス(Task Status)]) を参照してください。

アイデンティティ ポリシーの管理

ライセンス:Control



アイデンティティ ポリシーの管理方法:

-
- 手順 1 [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [アイデンティティ ポリシー(Identity Policy)] の順に選択します。
 - 手順 2 ポリシーをコピーする場合は、コピー アイコン() をクリックします。
 - 手順 3 ポリシーのレポートを生成する場合は、レポート アイコン() をクリックします。
-

アイデンティティ ルールの管理

ライセンス:Control

アイデンティティ ルールを管理する方法:

-
- 手順 1 [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [アイデンティティ ポリシー(Identity Policy)] の順に選択します。
 - 手順 2 アイデンティティ ルールを編集する場合は、編集アイコン() をクリックし、[アイデンティティ ルールの作成\(32-14 ページ\)](#)の説明に従って変更を行います。
 - 手順 3 アイデンティティ ルールを削除する場合は、削除アイコン() をクリックします。
 - 手順 4 [ASA FirePOWER の変更の保存(Store ASA FirePOWER Changes)] をクリックします。
-

次の作業

- 設定変更を展開します。[設定変更の展開 \(4-13 ページ\)](#)を参照してください。

アイデンティティ ルール カテゴリの追加

ライセンス:Control

アイデンティティ ルール カテゴリを追加する方法:

-
- 手順 1** アイデンティティ ルール エディタ ページでは、次の選択肢があります。
- 最初の [挿入 (Insert)] ドロップダウン リストから [カテゴリの上 (above Category)] を選択した後、2 番目のドロップダウン リストからカテゴリを選択します。ここで選択したカテゴリの上にルールが配置されます。
 - ドロップダウン リストから [ルールの下 (below rule)] を選択し、既存のルール番号を入力します。このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。
 - ドロップダウン リストから [ルールの上 (above rule)] を選択し、既存のルール番号を入力します。このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。

- 手順 2** [OK] をクリックします。



(注) 削除するカテゴリに含まれるルールは、その上にあるカテゴリに追加されます。

- 手順 3** [追加 (Add)] をクリックするか、ルールの編集を続けます。
-