# レルムとアイデンティティ ポリシー

この章は、次のセクションで構成されています。



## サーバとレルムについて

ライセンス：任意

レルムは、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 グループを指定する。
- 権限のあるユーザに関するユーザ メタデータについてサーバをクエリする。

レ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、同じ基本レルム情報を共有する必要があります。レ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をクエリ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 および IMAP ユーザに関連付けられているデータについてサーバを照会します。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を定期的にクエリして、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 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） モジュールによって検出されたユーザを LDAP サーバから削除しても、ASA FirePOWER モジュールではユーザ データベース内の該当ユーザは削除されないため、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 モジュールが権限のあるユーザのリストを次に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ー

ライセンス：任意

次のタイプのサーバには、ASA FirePOWER モジュールからの TCP/IP アクセスがあれば、レルムを設定して接続できます。 <Table Title:Supported Servers for Realms>

| サーバ タイプ | 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 | 対応 | 対応 | 対応 | 対応（NTLM キャプティブ ポータルを使用する場合、Windows Server 2003 を除く） |
| Windows Server 2003 と Windows Server 2008 上の Oracle Directory Server Enterprise Edition 7.0 | 対応 | 非対応 | 非対応 | 対応 |
| Linux 上の OpenLDAP | 対応 | 非対応 | 非対応 | 対応 |

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。サーバの基本的なオブジェクト階層でユーザが編成されている場合、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。

LDAP または AD サーバ グループのサイズを制限し、含めるユーザ数を最大で 1500 と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。この制限は、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

レルムのサーバでは、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、次の表に記載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用してデータベースに入力できなくなります。

表 *1 : 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 ユーザー名 | Username | samaccountname | cn<br>uid | cn<br>uid |
| 名 | First Name | givenname | givenname | givenname |
| 姓 | Last Name | sn | sn | sn |
| 電子メール アドレス | Email | mail<br>userprincipalname（mail に値が設定されていない場合） | mail | mail |
| department | department | department<br>distinguishedname（department に値が設定されていない場合） | department | ou |
| telephone number | Phone | telephonenumber | 該当なし | 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

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 タイムアウトが行わ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 サーバのレルムを、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または除外するように設定する場合、報告するユーザ数をサーバが制限することがあります。

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。この制限は、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

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。

- [Configuration] > [ASA FirePOWER Configuration] > [Integration] > [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。
- [Configuration] > [ASA FirePOWER Configuration] > [Integration] > [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、モジュールは指定されたレルムとトラフィックとを関連付け、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**：

**ステップ 1** [Configuration] > [ASA FirePOWER Configuration] > [Integration] の順に選択します。 > > >

**ステップ 2** [Realms] をクリックします。

**ステップ 3** [New Realm] をクリックします。

**ステップ 4** の説明に従って、基本的なレルム情報を設定します。 基本的なレルム情報の設定 （8 ページ）

**ステップ 5** の説明に従って、ディレクトリを設定します。 レルム ディレクトリの設定 （9 ページ）

**ステップ 6** 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。 ユーザの自動ダウンロードの設定 （9 ページ）

**ステップ 7** レルム設定を保存します。

**ステップ 8** 必要に応じて、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。 レルム ユーザ セッション タイムアウトの設定 （10 ページ）

**ステップ 9** レルム設定を保存します。

### 次のタスク

### 次の作業

- レルムの有効化または無効化 （22 ページ）の説明に従って、レルムを有効にします。
- 必要に応じて、タスクのステータスをモニタします。[Task Status] ページ（[Monitoring] > > [ASA FirePOWER Monitoring] > > [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

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 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 Active Directory サーバのドメイン。

#### AD Join Username および 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、クライアントをドメインに参加させる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に HTTP ネゴシエート）を、アイデンティティ ルールの [Authentication Type] として選択する場合、選択する [Realm] は、Kerberos キャプティブ ポータル認証を実行できるように、[AD Join Username] と [AD Join Password] を使用して設定する必要があります。

#### Description

（任意）レルムの説明。

#### Directory Username および 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。

#### 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。

#### 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。

#### Group Attribute

サーバのグループ属性：[Member]、[Unique Member]、[Custom]。

#### Name

レルムの一意の名前。

#### Type

レルム、AD、または LDAP のタイプ。

#### User Session Timeout: Authenticated Users

ユーザ セッションがタイムアウトするまでの最大時間（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[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。

#### 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。

#### 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。

## レルムのディレクトリ フィールド

これらの設定は、レルム内の個々のサーバ（ディレクトリ）に適用されます。

**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。

**Hostname / IP Address**

サーバのホスト名または IP アドレス。

**Port**

サーバ接続に使用するポート。

**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、[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、証明書のサーバー名は、サーバーの [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

**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、[Begin automatic download at] および [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**：

**ステップ 1** [Add New Realm] ページで、[Name] および、必要に応じて [Description] を入力します。

**ステップ 2** ドロップダウン リストから [Type] を選択します。

**ステップ 3** AD レルムを設定する場合は、[AD Primary Domain] を入力します。

**ステップ 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、ユーザの識別用の [AD Join Username] と [AD Join Password] を、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で入力します。

**ステップ 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 [Directory Username] と [Directory Password] を入力します。

**ステップ 6** ディレクトリの [Base DN] を入力します。
**ステップ 7** ディレクトリの [Group DN] を入力します。
**ステップ 8** オプションで、ドロップダウン リストから [Group Attribute] を選択します。
**ステップ 9** [OK] をクリックします。

**次のタスク**

- 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 （9 ページ）

# 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**：

**ステップ 1** [Directory] タブで、[Add Directory] をクリックします。
**ステップ 2** サーバのホスト名/IP アドレスとポートを入力します。
**ステップ 3** [暗号化モード（Encryption Mode）] を選択します。
**ステップ 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。
**ステップ 5** 接続をテストする場合は、[Test] をクリックします。
**ステップ 6** [OK] をクリックします。

# 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**：

**ステップ 1** [User Download] タブで、[Download users and groups (required for user access control)] チェックボックスをオンにします。
**ステップ 2** ドロップダウン リストから [Begin automatic download at] の時間を選択します。
**ステップ 3** [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。

**ステップ 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、[Available Groups] 列からユーザ グループを選択し、[Add to Include] または [Add to Exclude] をクリックします。

**ステップ 5** 個々のユーザを含めるか除外するには、[Groups to Include] または [Groups to Exclude] の下のフィールドにユーザを入力し、[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 タイムアウトを行っ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。

**レルム ユーザ セッション タイムアウトを設定する方法**：

**ステップ 1** [Realm Configuration] タブを選択します。

**ステップ 2** [Authenticated Users]、[Failed Authentication Users]、および [Guest Users] にユーザ セッション タイムアウト値を入力します。

**ステップ 3** [Save] をクリックするか、レルムの編集を続けます。

# 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**

- 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。 レルムの作成 （5 ページ）

**アイデンティティ ポリシーの設定方法**：

アクセス：管理者/アクセス管理者/ネットワーク管理者

**ステップ 1** [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Identity Policy] の順に選択します。

**ステップ 2** [Name] を入力し、任意で [Description] を入力します。

**ステップ 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 （14 ページ）の説明に従って、[Add Rule] をクリックします。

**ステップ 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 （23 ページ）の説明に従って、[Add Category] をクリックします。

**ステップ 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 （11 ページ）の説明に従って、[Active Authentication] をクリックします。

# 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

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。

### 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。

### 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。

### 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。

### 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で [Active Authentication Response Page] を選択したら、HTTP 応答ページで 1 つ以上のアイデンティティ ルールを認証タイプ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、[Username] と [Password] フィールドに加え、[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。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。システム提供の HTTP 応答ページには、[Username] と [Password] のフィールドに加え、[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。

キャプティブ ポータルの詳細については、を参照してください。 キャプティブ ポータル アクティブ認証のアイデンティティ ソース

### 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 コンフィギュレーション ガイド（バージョン 9.5(2) 以降）（https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html）の説明に従い、ポートを定義します。

### キャプティブ ポータルの設定方法：

**ステップ 1** [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [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。 > > >

**ステップ 2** [Active Authentication] をクリックします。

**ステップ 3** ドロップダウン リストから、該当する [Server Certificate] を選択します。必要に応じて、追加アイコン（  ）をクリックして、オブジェクトをその場で作成します。

**ステップ 4** [Port] を入力し、[Maximum login attempts] を指定します。

**ステップ 5** オプションで、HTTP 応答ページでユーザを認証するには、[Active Authentication Response Page] を選択します。

**ステップ 6** [**Save**] をクリックします。

**ステップ 7** アイデンティティ ルールの作成 （14 ページ）の説明に従って、[Action] として [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、[Authentication Type] として HTTP 応答ページを選択する必要もあります。

### 次のタスク

- 設定変更を展開します。を参照してください。 設定変更の導入

# 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**：

**ステップ 1** アイデンティティ ルール エディタ ページの [Realm & Settings] タブで、[Application Filters] リストにある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、[Check All] または [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、[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** [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、[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、[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 [All apps matching the filter]

**次のタスク**

- 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 ルールの作成 （14 ページ）

# 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 モジュールには、現在適用されている 1 つのアイデンティティ 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**：

**ステップ 1** [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。
**ステップ 2** [Advanced] タブを選択します。
**ステップ 3** [Identity Policy Settings] の横にある編集アイコン（）をクリックします。
**ステップ 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。
**ステップ 5** [OK] をクリックします。
**ステップ 6** [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**：

**ステップ 1** [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Identity Policy] の順に選択します。 > > >
**ステップ 2** [Add Rule] をクリックします。
**ステップ 3** 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。 基本的なアイデンティティ ルール情報の設定 （17 ページ）
**ステップ 4** 必要に応じて、の説明に従って、ゾーン条件を追加します。 アイデンティティ ルールへのゾーン条件の追加 （19 ページ）

（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。

**ステップ 5** 必要に応じて、の説明に従って、ネットワークまたは地理位置情報の条件を追加します。 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 （18 ページ）

**ステップ 6** 必要に応じて、の説明に従って、ポート条件を追加します。 アイデンティティ ルールへのポート条件の追加 （18 ページ）

**ステップ 7** の説明に従って、ルールをレルムに関連付けます。 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 （20 ページ）

**ステップ 8** [Add] をクリックします。

**ステップ 9** [Store ASA FirePOWER Changes] をクリックします。

### 次のタスク

- 設定変更を展開します。を参照してください。 設定変更の導入

# アイデンティティ ルール フィールド

次のフィールドを使用して、アイデンティティ ルールを設定します。

### Enabled

このオプションを選択すると、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。

### 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。

### Realm

指定された**アクション**の実行対象にな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。

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 [Authentication Type] として選択する場合、選択する [Realm] は、Kerberos キャプティブ ポータル認証を実行できるように、[AD Join Username] と [AD Join Password] を使用して設定する必要があります。

#### 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 [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。

#### 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、[Use active authentication if passive authentication cannot identify user] を選択する必要があります。

#### 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 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 レルムを選択するときにのみ使用できます。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 ルールのレルムとして 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。

選択する [Realm] は、Kerberos キャプティブ ポータル認証を実行するために、[AD Join Username] および [AD Join Password] を使用して設定する必要があります。

（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 を選択できるようにするには、[HTTP Negotiate] 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。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。

選択する [Realm] は、Kerberos キャプティブ ポータル認証を実行するために、[AD Join Username] および [AD Join Password] を使用して設定する必要があります。

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、キャプティブ ポータル デバイスのホスト名を解決する 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 モジュール提供のページ、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 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。

システム提供の HTTP 応答ページには、[Username] と [Password] のフィールドに加え、[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。

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**：

**ステップ 1** アイデンティティ ルール エディタ ページで、[Name] を入力します。

**ステップ 2** ルールを有効にするかどうか [Enabled] を指定します。

**ステップ 3** ルール カテゴリにルールを追加するには、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 （23 ページ）

**ステップ 4** ドロップダウン リストからルールの [Action] を選択します。

**ステップ 5** [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地理位置情報条件を追加する方法**：

**ステップ 1** アイデンティティ ルール エディタ ページで、[Networks] タブを選択します。

**ステップ 2** [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（後で条件に追加可能）をその場で追加するには、[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地理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、[Available Networks] リストの上にある [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。入力を開始するとリストが更新され、一致するオブジェクトが表示されます。

**ステップ 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 [Select All] を選択します。

**ステップ 4** [Add to Source] または [Add to Destination] をクリックします。

**ステップ 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。

**ステップ 6** [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**：

**ステップ 1** アイデンティティ ルール エディタ ページで、[Ports] タブを選択します。

**ステップ 2** [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（後で条件に追加可能）をその場で追加するには、[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、[Available Ports] リストの上にある [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。入力を開始するとリストが更新され、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、ASA FirePOWER モジュールに提供されている HTTP ポート オブジェクトが表示されます。

**ステップ 3** TCP ベースのポート オブジェクトを 1 つ選択するには、それをクリックします。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 [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。

**ステップ 4** [Add to Source] または [Add to Destination] をクリックします。

**ステップ 5** 送信元または宛先のポートを手動で指定するには、[Selected Source Ports] または [Selected Destination Ports] リストの下にある [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。

**ステップ 6** [Add] をクリックします。

（注） ASA FirePOWER モジュールでは、無効な設定となるルール条件にはポートが追加されません。

**ステップ 7** [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、を参照してください。 セキュリティ ゾーンの操作

**アイデンティティ ルールにゾーン条件を追加する方法**：

**ステップ 1** アイデンティティ ルール エディタ ページで、[Zones] タブを選択します。

**ステップ 2** [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、[Available Zones] リストの上にある [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。

**ステップ 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 [Select All] を選択します。

**ステップ 4** [Add to Source] または [Add to Destination] をクリックします。

**ステップ 5** [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**：

**ステップ 1** アイデンティティ ルール エディタ ページで、[Realm & Settings] タブを選択します。

**ステップ 2** ドロップダウン リストから [Realm] を選択します。

**ステップ 3** オプションで、[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にのみ表示されます。

**ステップ 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。

**ステップ 5** オプションで、[Identify as Special Identities/Guest if authentication cannot identify user] チェックボックスを選択します。

**ステップ 6** ドロップダウン リストから [Authentication Type] を選択します。

**ステップ 7** 必要に応じて、[Exclude HTTP User-Agents] を使用し、アクティブ認証からのアプリケーションの除外 （13 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。

**ステップ 8** [Add] をクリックするか、ルールの編集を続けます。

# レルムの管理

ライセンス：Control

**レルムの管理方法**：

**ステップ 1** [Configuration] > [ASA FirePOWER Configuration] > [Integration] > [Realms] の順に選択します。 > > >

**ステップ 2** レルムを削除する場合は、削除アイコン（）をクリックします。

**ステップ 3** レルムを編集する場合は、レルムの横にある編集アイコン（）をクリックし、レルムの作成 （5 ページ）の説明に従って変更を行います。

**ステップ 4** レルムを有効または無効にするには、レルムの有効化または無効化 （22 ページ）の説明に従って、有効または無効にするレルムの横の [State] スライダをクリックします。

**ステップ 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 （21 ページ）の説明に従ってダウンロード アイコン（）をクリックします。

**ステップ 6** レルムをコピーする場合は、コピー アイコン（）をクリックします。

**ステップ 7** レルムを比較する場合は、レルムの比較 （21 ページ）を参照してください。

# レルムの比較

ライセンス：Control

**レルムの比較方法**：

**ステップ 1** [Configuration] > [ASA FirePOWER Configuration] > [Integration] > [Realms] の順に選択します。
**ステップ 2** [Compare Realms] をクリックします。
**ステップ 3** [Compare Against] ドロップダウン リストから [Compare Realm] を選択します。
**ステップ 4** [Realm A] および [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。
**ステップ 5** [OK] をクリックします。
**ステップ 6** 個々の変更を選択する場合は、タイトル バーの上の [Previous] または [Next] をクリックします。
**ステップ 7** 必要に応じて、[Comparison Report] をクリックして、レルム比較レポートを生成します。
**ステップ 8** 必要に応じて、[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 （22 ページ）の説明に従って、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**：

**ステップ 1** [Configuration] > [ASA FirePOWER Configuration] > [Integration] > [Realms] の順に選択します。 > > >
**ステップ 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。

**次のタスク**

- 必要に応じて、タスクのステータスをモニタします。[Task Status] ページ（[Monitoring] > > [ASA FirePOWER Monitoring] > > [Task Status]）を参照してください。

# レルムの有効化または無効化

ライセンス：Control

ASA FirePOWER モジュールがサーバにクエリできるのは、有効になっているレルムだけです。問い合わせを停止するには、レルムを無効にします。

**レルムを有効または無効にする方法**：

**ステップ 1** [Configuration] > [ASA FirePOWER Configuration] > [Integration] > [Realms] の順に選択します。 > > >

**ステップ 2** 有効または無効にするレルムの横にある [State] スライダをクリックします。

**次のタスク**

- 必要に応じて、タスクのステータスをモニタします。[Task Status] ページ（[Monitoring] > [ASA FirePOWER Monitoring] > [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**：

**ステップ 1** [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Identity Policy] の順に選択します。

**ステップ 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。

**ステップ 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**：

**ステップ 1** [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Identity Policy] の順に選択します。

**ステップ 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 （14 ページ）の説明に従って変更を行います。

**ステップ 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。

**ステップ 4** [Store ASA FirePOWER Changes] をクリックします。

### 次のタスク

- 設定変更を展開します。設定変更の導入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：**

**ステップ 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 [Insert] ドロップダウン リストから [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 [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 [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。

**ステップ 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。

**ステップ 3** [Add] をクリックするか、ルールの編集を続けます。