キャプティブ ポータルによるユーザの制御

- キャプティブ ポータルのアイデンティティ ソース （1 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 （2 ページ）
- ユーザ制御のためのキャプティブ ポータルの設定方法 （4 ページ）
- キャプティブ ポータルのアイデンティティ ソースのトラブルシューティング （15 ページ）
- キャプティブ ポータルの履歴 （16 ページ）

キャプティブ ポータルのアイデンティティ ソース

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、ユーザがネットワークに対し、管理対象デバイスを使用して認証を行うアクティブ認証方式です。

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 （4 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

（注） リモート アクセス VPN ユーザがセキュア ゲートウェイとして機能している管理対象デバイスを介してアクティブに認証されている場合、アイデンティティ ポリシーで設定されている場合でも、キャプティブ ポータルのアクティブ認証は実行されません。

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。

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。
- 最大ログイン試行回数のカウントとして数えられるログイン試行の失敗から次の失敗までには最大 5 分という制限があります。5 分という制限の設定は変更できません

  （最大ログイン試行回数は **[分析（Analysis）]** > **[接続（Connections）]** > **[イベント（Events）]** で接続イベントに表示されます）。

  ログイン失敗の間に 5 分以上の間隔がある場合は、ユーザは引き続き認証のキャプティブ ポータルにリダイレクトされ、失敗したログイン ユーザまたはゲスト ユーザには指定されず、Firepower Management Center に報告されることはありません。
- ユーザが確実にログアウトする唯一の方法は、ブラウザをいったん閉じ、再度開くことです。それを実行しなくても、ユーザがキャプティブ ポータルからログアウトし、同じブラウザを使用して認証を受けずにネットワークにアクセスできる場合があります。
- 親ドメインのレルムを作成し、管理対象デバイスがその親ドメインの子へのログインを検出した場合、管理対象デバイスはそのユーザのその後のログアウトを検出しません。
- （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、https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-and-configuration-guides-list.html の『*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。
- 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。

- 管理対象デバイスの通過が許可されている HTTP 以外のトラフィックまたは HTTPS トラフィックの量を制限するには、アイデンティティ ポリシーの [ポート（Ports）] タブ ページで一般的な HTTP ポートと HTTPS ポートを入力する必要があります。

  管理対象デバイスは、着信要求に HTTP プロトコルまたは HTTPS プロトコルが使用されていないと判断した場合、以前に非表示にしたユーザを [保留中（Pending）] から [不明（Unknown）] に変更します。管理対象デバイスがユーザを [保留中（Pending）] から別の状態に変更するとすぐに、そのトラフィックに対してアクセス コントロール ポリシー、QoS ポリシー、および SSL ポリシーを適用できます。他のポリシーで HTTP 以外のトラフィックまたは HTTPS トラフィックが許可されていない場合は、キャプティブ ポータルのポートにアイデンティティ ポリシーを設定することによって、望ましくないトラフィックが管理対象デバイスを通過できないようにします。

ユーザ制御のためのキャプティブ ポータルの設定方法

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。

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（6 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（2 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。

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（6 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 （8 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 （9 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 （10 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 （11 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 （6 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 （13 ページ）
PKI 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 （15 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 （4 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。

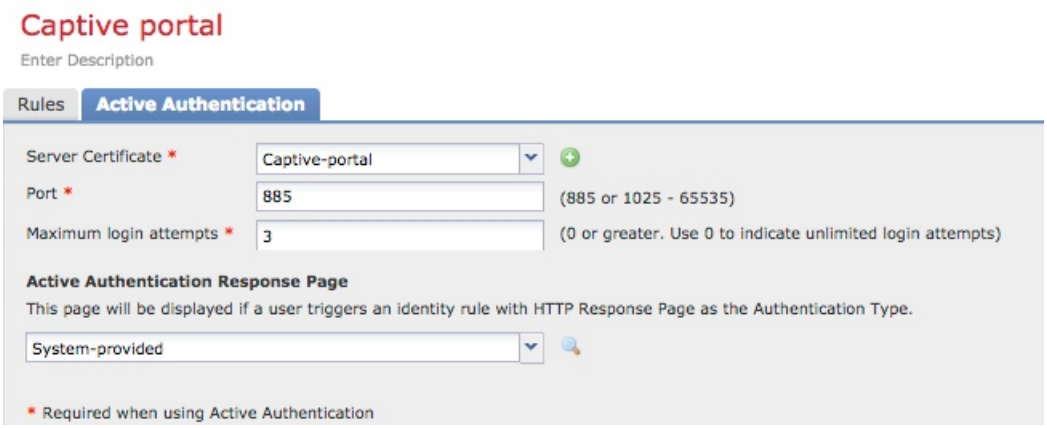
ステップ 4 [アクティブ認証（Active Authentication）] タブをクリックします。

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。

（注） キャプティブ ポータルは、デジタル署名アルゴリズム（DSA）証明書または楕円曲線デジタル署名アルゴリズム（ECDSA）証明書の使用をサポートしていません。

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 （12 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、HTTP および HTTPS 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/VPN アイデンティティを確立できない場合にアクティブ認証を使用（Use active authentication if passive or VPN identity cannot be established）] 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 （12 ページ）を参照してください。

ステップ 16 リストから [認証プロトコル（Authentication Protocol）] 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 （13 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 （8 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 （6 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 （4 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。

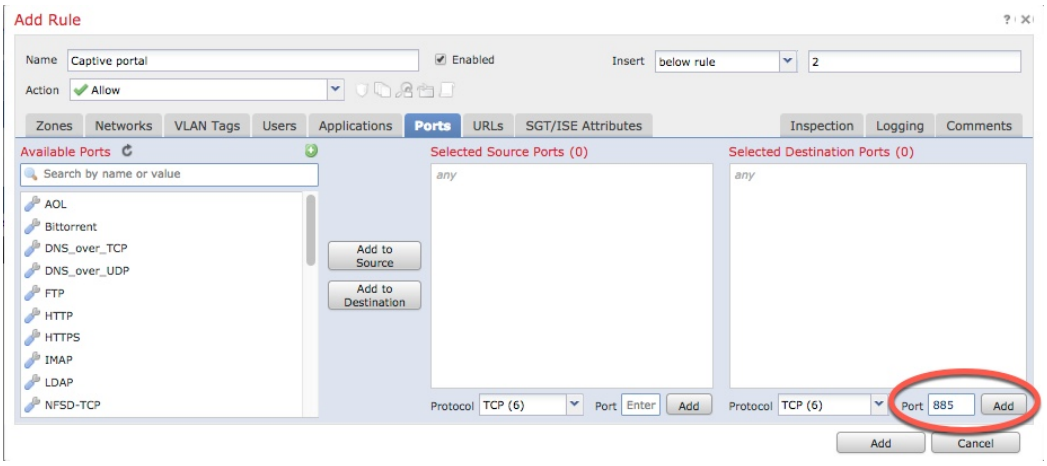
ステップ 3 [アクション（Action）] 一覧から、[許可（Allow）] を選択します。

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 （9 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 （4 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 （10 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 （4 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。

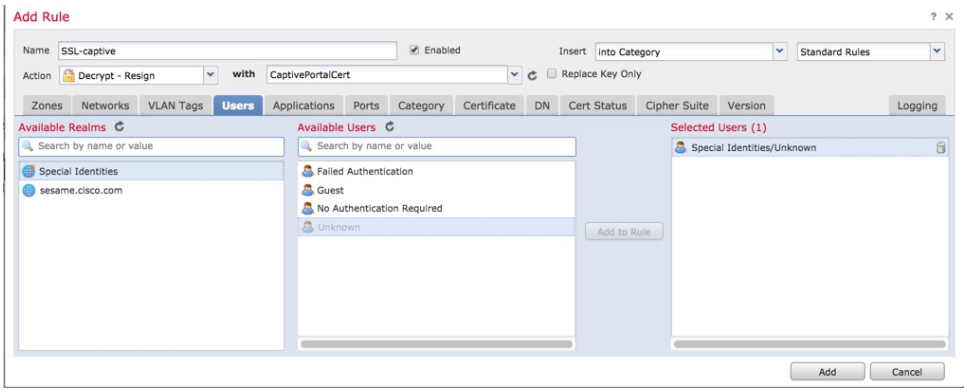
ステップ 10 [ユーザ（Users）] タブをクリックします。

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）TLS/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 （11 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 （4 ページ）を参照してください。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御（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 （8 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。

（注） キャプティブ ポータルは、デジタル署名アルゴリズム（DSA）証明書または楕円曲線デジタル署名アルゴリズム（ECDSA）証明書の使用をサポートしていません。

[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）

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（**Access**）
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。

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。

- ユーザが確実にログアウトする唯一の方法は、ブラウザをいったん閉じ、再度開くことです。それを実行しなくても、ユーザがキャプティブ ポータルからログアウトし、同じブラウザを使用して認証を受けずにネットワークにアクセスできる場合があります。
- 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。

キャプティブ ポータルの履歴

機能	バージョン（Version）	詳細
ゲスト ログイン。	6.1.0	ユーザは、キャプティブ ポータルを使用してゲストとしてログインできます。
キャプティブ ポータル。	6.0	導入された機能。キャプティブ ポータルを使用して、ブラウザ ウィンドウにプロンプトが表示されたときにクレデンシャルを入力するよう、ユーザに要求することができます。このマッピングでは、ユーザまたはユーザのグループに基づいたポリシーを使用することもできます。