



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 \(14 ページ\)](#)
- [キャプティブ ポータルの履歴 \(15 ページ\)](#)

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。失敗した試行によって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、[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、指定されたレール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り過ぎないようにします。

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数	サポートされるドメイン数	アクセス
任意	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。

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を設定](#)
- [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 \(14 ページ\)](#)

[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。

-
- 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。

Captive portal
Enter Description

Rules **Active Authentication**

Server Certificate * Captive-portal

Port * 885 (885 or 1025 - 65535)

Maximum login attempts * 3 (0 or greater. Use 0 to indicate unlimited login attempts)

Active Authentication Response Page
This page will be displayed if a user triggers an identity rule with HTTP Response Page as the Authentication Type.

System-provided

* Required when using Active Authentication

- 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。

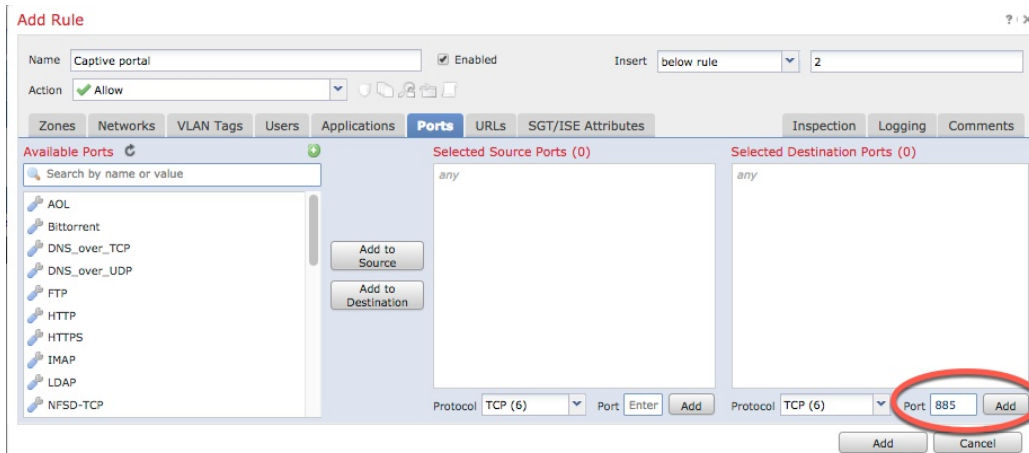
キャプティブポータルの設定パート2：TCPポートアクセスコントロールルールの作成

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。

- 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（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。

-
- 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、ルールのプリエンブ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

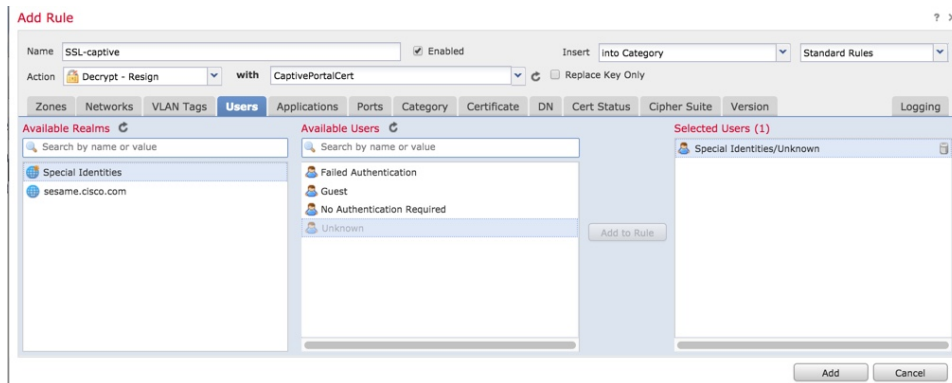
この手順では、トラフィックがキャプティブポータルに到達する前に、トラフィックを復号して再署名するSSLアクセスポリシーを作成する方法について説明します。キャプティブポータルは、トラフィックが復号された後にのみトラフィックを認証できます。

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。

- 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。

- 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。

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。

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数	サポートされるドメイン数	アクセス
任意	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。

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、[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。

- 表示される個別のアプリケーションを絞り込むには、[名前を検索 (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。
- 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	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。

