



アイデンティティ ソース：キャプティブポータル

- [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ライセンス要件 \(2 ページ\)](#)
- [キャプティブポータルの要件と前提条件 \(2 ページ\)](#)
- [キャプティブポータルのガイドラインと制限事項 \(3 ページ\)](#)
- [ユーザー制御のためのキャプティブポータルの構成方法 \(6 ページ\)](#)
- [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 \(21 ページ\)](#)
- [キャプティブポータルの履歴 \(23 ページ\)](#)

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、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。キャプティブポータルは、ユーザー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。（RA-VPNは別のタイプのアクティブ認証です）。認証レلم（Microsoft AD など）に照会してユーザーを認証するパッシブ認証とは異なり、アクティブ認証では、ユーザーに対して、管理対象デバイスによってログインページが表示されます。

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に Microsoft Azure AD (SAML) レلمを使用するには、「[Microsoft Azure AD \(SAML\) realm for active authentication \(captive portal\) の作成](#)」を参照してください。



(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ーがデータベース内のユーザー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ーアクティビティタイプは [認証失敗ユーザー (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ー認識とユーザー制御に使用できません。

関連トピック

[ユーザー制御のためのキャプティブポータルの構成方法 \(6 ページ\)](#)

ホスト名のリダイレクトについて

(Snort 3 のみ。) アクティブ認証アイデンティティルールは、設定されたインターフェイスを使用してキャプティブポータルポートにリダイレクトします。通常、リダイレクトは IP アドレスに対して行われるため、信頼できない証明書エラーが発生する場合があります。この動作は中間者攻撃に似ているため、ユーザーは信頼できない証明書を受け入れることに消極的である可能性があります。

この問題を回避するために、管理対象デバイスの完全修飾ドメイン名 (FQDN) を使用するようにキャプティブポータルを設定できます。適切に設定された証明書を使用すると、ユーザーは信頼できない証明書エラーを受け取ることがなくなり、認証がよりシームレスになり、安全性が向上します。

関連トピック

[ホスト名ネットワークルール条件へのリダイレクト](#)

キャプティブポータルのライセンス要件

Threat Defense License

任意

キャプティブポータルの要件と前提条件

Supported domains

Any

User roles

- Admin
- Access Admin
- Network Admin

キャプティブポータルのガイドラインと制限事項

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ーはFirewall Threat Defenseを使用して認証を行ってからネットワークにアクセスします。



- (注) リモートアクセスVPNユーザー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通じ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。

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、アクセスコントロールポリシーはネットワーク内のリソースへのアクセスを定義します。たとえば、US-West/FinanceグループのユーザーをEngineeringサーバーへのアクセスから除外したり、ユーザーがネットワーク上の安全でないアプリケーションにアクセスするのを禁止したりできます。

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イデンティティポリシーの [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。

アクティブな認証ルールに [アクティブ認証 (Active Authentication)] ルールアクションが含まれるか、[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ます。それぞれのケースで、システムはTLS/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** TLS/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 a decryption policy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、割り当てられた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がアイデンティティルールに一致するユーザーを認証する場合、ダウンロードされていない Microsoft Active Directory または LDAP グループ内のユーザーは不明として識別されます。ユーザーが不明として識別されるのを回避するには、キャプティブポータルで認証するすべてのグループのユーザーをダウンロードするようにレルムまたはレルムシーケンスを設定します。不明なユーザーは、関連付けられたアクセスコントロールポリシーに従って処理されます。アクセスコントロールポリシーが不明なユーザーをブロックするように構成されている場合、これらのユーザーはブロックされます。

システムによってレルムまたはレルムシーケンス内のすべてのユーザーが確実にダウンロードされるようにするには、グループがレルムの設定の [使用可能グループ (Available Groups)] リストに含まれていることを確認します。

ユーザーとグループの同期の詳細については、[ユーザーとグループを同期する](#)を参照してください。

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アイデンティティ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ルール条件をアクセスコントロールポリシーで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と関連づけられた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アイデンティティルールが含まれており、ルーテッドインターフェイスが設定されている1つ以上のデバイスを管理する Secure Firewall Management Center にポリシーを展開すると、ポリシーの展開は成功し、ルーテッドインターフェイスはアクティブ認証を実行します。

必要な証明書と認証局

ユーザーの制御および認識のためにキャプティブポータルを使用する前に、以下のすべてが必要です。

- Microsoft AD で認証する場合は、サーバーのルート証明書をエクスポートし、信頼できる CA 証明書として Secure Firewall Management Center にインポートします。
- アイデンティティポリシーが展開されている管理対象デバイスで認証するための、内部証明書オブジェクト。
- 必要な復号ルールの内部認証局。

内部証明書と内部認証局は、復号ポリシーの作成時に作成できます。

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。

- キャプティブポータルは HTTP/3 QUIC 接続をサポートしていません。
- 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に数えられるログイン試行の失敗から次の失敗までには制限があり、最大5分です。5分の制限の設定は変更できません

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

ログイン失敗の間に5分以上の間隔がある場合は、ユーザーは認証のために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ーまたはゲストユーザーには指定されず、Secure Firewall Management Center に報告されることはありません。

- キャプティブポータルは、TLS v1.0 接続をネゴシエートしません。
TLS v1.1、v1.2、および TLS 1.3 接続のみがサポートされています。
- ユーザーをキャプティブポータルから安全にログアウトし、ユーザーが再度ログインできないようにするために、管理者はセッションを閉じることができます：**Analysis > Users heading > Active Sessions**。ユーザーがブラウザを閉じた場合も、ブラウザは自動的に再認証されません。
- 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ーのその後のログアウトを検出しません。
- アクセス制御ルールは、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、a decryption policy を使用して、認証対象のユーザー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ーの 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ー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ーを [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ーを [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はアクセス制御、QoS、および decryption policies 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。

Kerberos の前提条件

Kerberos 認証を使用している場合、管理対象デバイスのホスト名は 15 文字未満にする必要があります (Windows で設定されている NetBIOS の制限)。そのようにしないと、キャプティブポータル認証が失敗します。管理対象デバイスのホスト名は、デバイスのセットアップ時に

設定します。詳細については、Microsoft のマニュアルサイト「[Naming conventions in Active Directory for computers, domains, sites, and OUs](#)」で、次のような記事を参照してください。

DNS はホスト名に対して 64KB 以下の応答を返す必要があります。それ以外の場合、AD 接続テストは失敗します。この制限は両方向に適用され、[RFC 6891 セクション 6.2.5](#) で説明されています。

ユーザー制御のためのキャプティブポータルの構成方法

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、LDAP レルムか、Microsoft AD レルムまたはレルムシーケンス、Microsoft Azure AD (SAML) レルム、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、a decryption policy をセットアップし、アイデンティティポリシーと decryption policies を同じアクセスコントロールポリシーに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。



- (注) Microsoft Azure AD (SAML) レルムをキャプティブポータルとして使用するには、「[Microsoft Azure AD \(SAML\) realm for active authentication \(captive portal\) を作成する方法](#)」を参照してください。

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 Secure Firewall Management Center によって管理されていることを確認します。
- キャプティブポータルで暗号化認証を使用するには、Secure Firewall 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使用できるようにするか、管理対象デバイスを認証するための 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](#) 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、LDAP レルムか、Microsoft AD レルムと必要に応じてレルムシーケンスを作成し、有効化します。

- [LDAP レルムまたは Active Directory \(AD\) レルムおよびレルムディレクトリを作成する](#)
- [ユーザーとグループを同期する](#)

システムによってレルムまたはレルムシーケンス内のすべてのユーザーが確実にダウンロードされるようにするには、グループがレルムの設定の [使用可能グループ (Available Groups)] リストに含まれていることを確認します。

詳細については、「[ユーザーとグループを同期する](#)」を参照してください。

ステップ2 必要な証明書と認証局を取得します。
以下のすべてが必要です。

- Microsoft AD で認証する場合は、サーバーのルート証明書をエクスポートし、信頼できる CA 証明書として Secure Firewall Management Center にインポートします。
- アイデンティティポリシーが展開されている管理対象デバイスで認証するための、内部証明書オブジェクト。
- 必要な復号ルール of 内部認証局。

内部証明書と内部認証局は、復号ポリシーの作成時に作成できます。

ステップ3 関連付けられた信頼できる認証局を使用してネットワークオブジェクトを作成します。
[ネットワークオブジェクトの作成 \(8 ページ\)](#) を参照してください。

ステップ4 アクティブ認証ルールを含む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、[アクティブ認証ルールを含むアイデンティティポリシーを作成します。\(10 ページ\)](#) 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、[TCP ポートアクセスコントロールルールの作成 \(13 ページ\)](#) を参照してください。

ステップ6 別のアクセスコントロールルールを追加して、選択したレルムまたはレルムシーケンスのユーザー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。

詳細については、[ユーザーのアクセスコントロールルールの作成 \(14 ページ\)](#) を参照してください。

ステップ7 キャプティブポータルユーザーが 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)] なユーザー用の [復号-再署名 (Decrypt - Resign)] ルールを用いて a decryption policy 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自体を [不明 (Unknown)] ユーザーと認識します。

[アウトバウンドルールを使用した復号ポリシーの作成 \(15 ページ\)](#)

ステップ 8 アイデンティティと decryption policies 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 3）。

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ーを認証します。

詳細については、[アクセス コントロール ポリシーと decryption policies の関連付け](#)（17 ページ）を参照してください。

次のタスク

を参照してください[ネットワークオブジェクトの作成](#)（8 ページ）。

関連トピック

[キャプティブポータルからアプリケーションを除外する](#)（20 ページ）

[PKI](#)

[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](#)（21 ページ）

[Snort 再起動のシナリオ](#)

ネットワークオブジェクトの作成

このタスクでは、アイデンティティソースとしてのキャプティブポータルの設定を開始する方法について説明します。

始める前に

（Snort 3 のみ。）DNS サーバーを使用して完全修飾ホスト名（FQDN）を作成し、Firewall Threat Defense の内部証明書を Firewall Management Center にアップロードします。これまでに行っていない場合は、[このようリソース](#)を参照できます。Firewall Management Center で管理されるデバイスの 1 つにあるルーテッドインターフェイスの IP アドレスを指定します。

ネットワークオブジェクトの詳細については、[ホスト名ネットワークルール条件へのリダイレクト](#)を参照してください。

手順

-
- ステップ 1 まだ Firewall 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 **Objects > Object Management** をクリックします。
 - ステップ 3 [PKI] を展開します。
 - ステップ 4 [内部証明書（Internal Cert）] をクリックします。
 - ステップ 5 [内部証明書の追加（Add Internal Cert）] をクリックします。
 - ステップ 6 [名前（Name）] フィールドに、内部証明書を識別する名前を入力します（たとえば、MyCaptivePortal）。

- ステップ 7** [証明書データ (Certificate Data)]フィールドで、証明書を貼り付けるか、[参照 (Browse)]ボタンを使用して検索します。
- 証明書の共通名は、キャプティブポータルユーザーの認証に使用する FDQN と正確に一致する必要があります。
- ステップ 8** [キー (Key)]フィールドで、証明書の秘密キーを貼り付けるか、[参照 (Browse)]ボタンを使用して検索します。
- ステップ 9** 証明書が暗号化されている場合は、[暗号化 (Encrypted)]チェックボックスをオンにして、隣のフィールドにパスワードを入力します。
- ステップ 10** [保存 (Save)]をクリックします。
- ステップ 11** [ネットワーク (Network)]をクリックします。
- ステップ 12** [ネットワークの追加 (Add Network)]>[オブジェクトの追加 (Add Object)]をクリックします。
- ステップ 13** [名前 (Name)]フィールドに、オブジェクトを識別する名前を入力します（たとえば、**MyCaptivePortalNetwork**）。
- ステップ 14** [FDQN] をクリックし、フィールドにキャプティブポータルの FDQN の名前を入力します。
- ステップ 15** [ルックアップ (Lookup)]のオプションをクリックします。
- 次の図は例を示しています。

アクティブ認証ルールを含むアイデンティティポリシーを作成します。

New Network Object ?

Name

Description

Network
 Host Range Network FQDN

Note:
You can use FQDN network objects in access, prefilter and translated destination in NAT rules only.

Lookup:

Allow Overrides

Cancel **Save**

ステップ 16 [保存 (Save)] をクリックします。

次のタスク

アクティブ認証ルールを含むアイデンティティポリシーを作成します。 (10 ページ)

アクティブ認証ルールを含むアイデンティティポリシーを作成します。

始める前に

複数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 を使用するとともに、キャプティブポータルと TLS/SSL 復号の両方に Firewall Management Center サーバー証明書を使用して、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、[ユーザー制御のためのキャプティブポータルの構成方法（6ページ）](#)を参照してください。

手順

-
- ステップ1** Firewall 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** [**Policies > Access Control heading > Identity**] をクリックして、アイデンティティポリシーを作成するか編集します。
- 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** リストから適切なルートサーバー証明書を選択するか、**Add (+)** をクリックして、証明書を追加します。
- 詳細については、「[Active Directory \(AD\) または LDAP に安全に接続する](#)」を参照してください。
- (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** [ホスト名へのリダイレクト (Redirect to Host Name)] フィールドで、前に作成したネットワークオブジェクトをクリックするか、**Add (+)** をクリックします。
- ステップ7** [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8** ユーザーが前回とは異なる管理対象デバイスを使用してネットワークにアクセスするたびに再認証を要求するには、[ファイアウォール全体でアクティブ認証を共有 (Share active authentication across firewalls)] をオフにして Firewall Management Center を有効にします。
このオプションの詳細については、[キャプティブポータルフィールド（18ページ）](#)を参照してください。
- ステップ9** (オプション) [キャプティブポータルフィールド（18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。

アクティブ認証ルールを含むアイデンティティポリシーを作成します。

Rules	Active Authentication	Identity Source
<p>i Values on this page are only required when an active authentication Identity rule is created with AD/LDAP realm.</p>		
Server Certificate *	MyCaptivePortalNetwork	+
Redirect to Host Name ?	auth.example.com	+ ▲ Supported only in Snort 3.0 or later
Port *	885	(885 or 1025 - 65535)
Maximum login attempts *	3	(0 or greater. Use 0 to indicate unlimited login attempts)
Share active authentication sessions across firewalls	<input checked="" type="checkbox"/>	▲ Supported only in 7.4.1 and later
<p>Active Authentication Response Page</p> <p>This page will be displayed if a user triggers an identity rule with HTTP Response Page as the Authentication Type.</p> <p>System-provided</p>		

- ステップ 10** (以前のバージョンからバージョン7.4.1にアップグレードしており、レルムシーケンスでユーザーを認証する場合のみ)。 **Edit** (✎) をクリックし、[カスタム認証フォームの更新 \(13 ページ\)](#) を参照します。
- ステップ 11** [保存 (Save)] をクリックします。
- ステップ 12** [ルール (Rules)] をクリックします。
- ステップ 13** [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、**Edit** (✎) をクリックして既存のルールを編集します。
- ステップ 14** ルールの [名前 (Name)] を入力します。
- ステップ 15** [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。
- ステップ 16** [レルムおよび設定 (Realm & Settings)] をクリックします。
- ステップ 17** [レルム (Realms)] 一覧から、ユーザー認証に使用するレルムまたはレルムシーケンスを選択します。
- ステップ 18** (オプション) [認証でユーザー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 \(18 ページ\)](#) を参照してください。
- ステップ 19** リストから [認証プロトコル (Authentication Protocol)] を 1 つ選択します。
- NTLM**、**Kerberos**、または**HTTP ネゴシエート**認証プロトコルを選択した場合、レルムシーケンスを使用してユーザーを認証することは「できません」。代わりに、**HTTP 基本**または**HTTP 応答ページ**を選択してください。
- ステップ 20** (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アプリケーションを除外する \(20 ページ\)](#) を参照してください。
- ステップ 21** [アイデンティティルールの条件](#)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 22 [追加 (Add)] をクリックします。

ステップ 23 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

[TCP ポート アクセス コントロール ルールの作成 \(13 ページ\)](#) に進みます。

カスタム認証フォームの更新

以前のリリースからバージョン 7.4.1 (またはそれ以降) にアップグレードしたら、次の行をカスタム認証フォームに追加して、ユーザーがキャプティブポータルで認証するときにドメインのリストを表示できるようにする必要があります (このタスクは、HTTP 応答ページ認証タイプを使用する場合は常に必要です。ユーザーが別の認証タイプを使用してレルムで認証する場合は、このタスクはオプションです)。

アイデンティティルールの [アクティブ認証 (Active Authentication)] タブページで、**Edit** (🔗) をクリックし、フォームの、ユーザーにログインを要求する部分に、次の情報を入力します。

```
<select name="realm" id="realm"></select>
```

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、[アクティブ認証ルールを含むアイデンティティポリシーを作成します。\(10 ページ\)](#) 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、[ユーザー制御のためのキャプティブポータルの構成方法 \(6 ページ\)](#) を参照してください。

手順

ステップ 1 Firewall 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 [PKI](#)の説明に従って、キャプティブポータルの証明書を作成します (まだ作成していない場合)。

ステップ 3 [[Policies > Access Control heading > Access Control](#)] をクリックして、アクセスコントロールポリシーを作成するか、編集します。

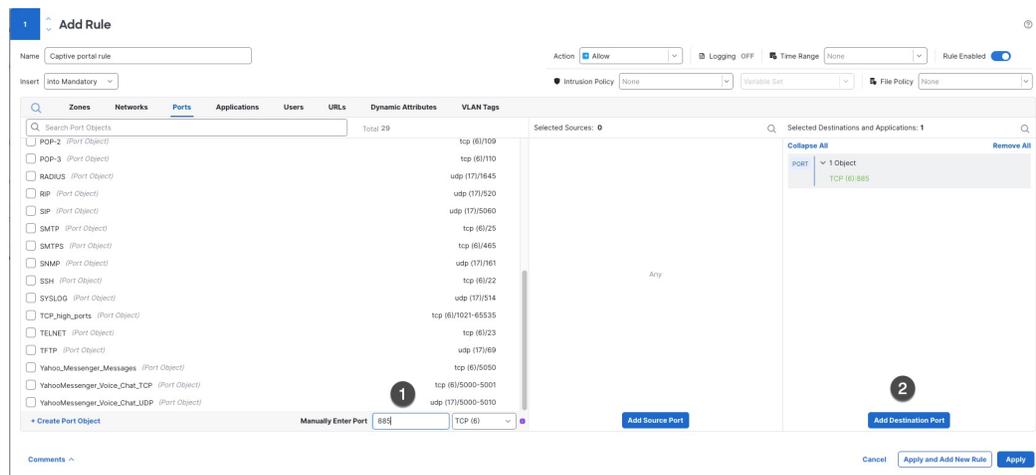
ステップ 4 [ルール追加 (Add Rule)] をクリックします。

ステップ 5 ルールの [名前 (Name)] を入力します。

ステップ 6 [アクション (Action)] 一覧から、[許可 (Allow)] を選択します。

ユーザーのアクセスコントロールルールの作成

- ステップ7** [ポート (Ports)] をクリックします。
- ステップ8** [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9** [ポート (Port)] フィールドに **885** と入力します。
- ステップ10** [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11** ページ下部の [追加 (Add)] をクリックします。

次のタスク

[ユーザーのアクセスコントロールルールの作成 \(14 ページ\)](#) に進みます。

ユーザーの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、[ユーザー制御のためのキャプティブポータルの構成方法 \(6 ページ\)](#) 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 [ユーザー (Users)] 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、**Refresh** (🔄) をクリックします。
- ステップ 7 [使用可能なユーザー (Available Users)] 一覧で、ルールに追加するユーザーを選択し、[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) **アイデンティティ ルールの条件**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

[アウトバウンド ルールを使用した復号ポリシーの作成 \(15 ページ\)](#)

アウトバウンド ルールを使用した復号ポリシーの作成

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 a decryption policy 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

アウトバウンドサーバー (つまり、キャプティブポータルユーザーの認証のためにトラフィックを復号する管理対象デバイス) の内部認証局 (CA) が必要です。この証明書は、管理対象デバイスでキャプティブポータルを認証するために使用する内部証明書とは異なる必要があります。

手順

- ステップ 1 まだ Firewall 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 **Policies > Access Control heading > Decryption** をクリックします。
- 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 [名前 (Name)] に一意のポリシー名を入力し、オプションで [説明 (Description)] にポリシーの説明を入力します。

ステップ5 [アウトバウンド接続 (Outbound Connections)] タブをクリックします。

ステップ6 ルールの証明書をアップロードまたは選択します。

CA とネットワーク/ポートの各組み合わせに対して1つのルールが作成されます。

ステップ7 (任意) ネットワークとポートを選択します。

詳細については、次を参照してください。

- [復号ルール条件](#)
- [ネットワークルールの条件](#)
- [ポートルールの条件](#)

ステップ8 [保存 (Save)] をクリックします。

ステップ9 作成した復号ポリシーの横にある **Edit** (🔗) をクリックします。

ステップ10 キャプティブポータルの復号ルールの横にある **Edit** (🔗) をクリックします。

ステップ11 [ユーザー (Users)] をクリックします。

ステップ12 [使用可能なレルム (Available Realms)] 一覧の上にある **Refresh** (🔄) をクリックします。

ステップ13 [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14 [使用可能なユーザー (Available Users)] 一覧で、[不明 (Unknown)] をクリックします。

ステップ15 [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 16 (オプション) [復号ルール条件](#)の説明に従って、他のオプションを設定します。

ステップ 17 [追加 (Add)] をクリックします。

次のタスク

[アクセスコントロールポリシーと decryption policies の関連付け \(17 ページ\)](#)

アクセスコントロールポリシーと decryption policies の関連付け

この手順では、アイデンティティポリシーと TLS/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、ユーザー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、[ユーザー制御のためのキャプティブポータルの構成方法 \(6 ページ\)](#) を参照してください。

手順

ステップ 1 [**Policies > Access Control heading > Access Control**] をクリックして、[TCP ポートアクセスコントロールルールの作成 \(13 ページ\)](#) で言及されているとおり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 **View** (👁) 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 (Identity)] という文字をクリックします。
- 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 decryption policy 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** [デバイスにアクセス コントロール ポリシーを割り当てる](#)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。
- 『Cisco Secure Firewall Management Center Administration Guide』の「Using Workflows」の説明に従ってユーザーアクティビティをモニターします。

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 [Active Authentication] タブページ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](#)」および「[キャプティブポータルからアプリケーションを除外する \(20 ページ\)](#)」も参照してください。

サーバー証明書 (Server Certificate)

キャプティブポータルデーモンが示す内部証明書。



- (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。キャプティブポータルに使用する TCP ポートを使用してアクセス制御ルールを設定し、アイデンティティポリシーをそのアクセス コントロール ポリシーに関連付ける必要があります。詳細については、[TCP ポート アクセス コントロール ルールの作成 \(13 ページ\)](#) を参照してください。

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。

ファイアウォール全体でアクティブ認証セッションを共有 (Share active authentication sessions across firewalls)

以前に接続していたデバイスとは異なる管理対象デバイスに認証セッションが送信されたときに、ユーザーの認証が必要かどうかを決定します。ユーザーがロケーションまたはサ

イトを変更するたびに認証する必要がある組織の場合は、このオプションを無効にする必要があります。

- (デフォルト。以前の動作を継続します)。アクティブな認証アイデンティティルールに関連付けられた管理対象デバイスでの認証をユーザーに許可するには、このチェックボックスをオンにします。
- アクティブな認証ルールが展開されている別の管理対象デバイスでユーザーがすでに認証されている場合でも、別の管理対象デバイスでの認証をユーザーに要求する場合は、このボックスをオフにします。ロケーションまたはサイトごとに認証が必要な組織で、管理対象デバイスがサイトごとに展開されている場合は、このオプションを使用します。

管理対象デバイスは、クラスタ化されているか、または同じデバイスであるかのように機能する高可用性ペアのデバイスです。特に次のような場合です。

- 同じクラスタまたは高可用性ペア内の管理対象デバイス：ユーザーセッションを保存して、ペア全体の一貫性を維持します。フェールオーバー時は、セカンダリに現在のユーザーセッションデータが保持されます。
- 異なるクラスタまたは高可用性ペアの管理対象デバイス：ユーザーセッションデータはこれらのデバイスと共有されないため、保存されません。

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ー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)] を選択した後、[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、[ユーザー名 (Username)] および [パスワード (Password)] フィールドとレルムのリスト (レルムシーケンスでの認証を選択した場合) に加え、[ゲストとしてログイン (Login as guest)] ボタンがあり、ユーザー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。

応答ページでログインしたときにユーザーに表示される内容の例を「[アクティブ認証ルールによるサンプルアイデンティティポリシーの作成](#)」に示します。

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。 **View** (👁) 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、 **Edit** (✎) 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アプリケーションを除外する

アプリケーション（HTTP User-Agent 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。



(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 まだ Firewall 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 **Policies > Access Control heading > Identity** をクリックします。

ステップ 3 キャプティブポータルルールを含むアイデンティティポリシーを編集します。

ステップ 4 [レルムと設定 (Realm & Settings)] タブページで、[HTTPユーザーエージェントの除外 (HTTP User Agent Exclusions)] を展開します。

- 最初の列で、アプリケーションをフィルタリングする各項目の横にあるチェックボックスをオンにしてから、1 つ以上のアプリケーションを選択し、[Add to Rule] をクリックします。

チェックボックスはまとめて AND 結合されます。

- 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、**Clear** (⊗) 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、**Reload** (⌂) 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 5 [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、**Clear** (⊗) 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、**Reload** (🔄) をクリックします。

ステップ 6 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、[レルムとユーザーのダウンロードをトラブルシューティングする](#)および[ユーザー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管理対象デバイスの時刻は、Firewall 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。

詳細については、[ホスト名のリダイレクトについて \(2 ページ\)](#) を参照してください。

- Kerberos 認証を使用している場合、管理対象デバイスのホスト名は 15 文字未満にする必要があります (Windows で設定されている NetBIOS の制限)。そのようにしないと、キャプティブポータル認証が失敗します。管理対象デバイスのホスト名は、デバイスのセットアップ時に設定します。詳細については、Microsoft のマニュアルサイト「[Naming conventions in Active Directory for computers, domains, sites, and OUs](#)」で、次のような記事を参照してください。
- DNS はホスト名に対して 64KB 以下の応答を返す必要があります。それ以外の場合、AD 接続テストは失敗します。この制限は両方向に適用され、[RFC 6891 セクション 6.2.5](#) で説明されています。

- キャプティブポータルが正しく設定されていても、IPアドレスまたは完全修飾ドメイン名（FQDN）へのリダイレクトが失敗する場合は、エンドポイントセキュリティソフトウェアを無効にします。このタイプのソフトウェアは、リダイレクトを妨げる可能性があります。
- **Kerberos**（または Kerberos をオプションとする場合は **HTTP Negotiate**）をアイデンティティルールの [Authentication Type] として選択する場合は、選択する [Realm] には、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するため、[AD Join Username] および [AD Join Password] が設定されている必要があります。
- アイデンティティルールの [Authentication Type] として [HTTP Basic] を選択した場合、ネットワーク上のユーザー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。
- Firewall 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、ユーザーが以前に認識され Firewall 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ーは、Firewall Management Center で [不明 (Unknown)] のユーザーとして記録されます。ダウンタイム後、不明のユーザー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。
- Kerberos 認証が成功するには、管理対象デバイスのホスト名が 15 文字未満である必要があります。
- ユーザーをキャプティブポータルから安全にログアウトし、ユーザーが再度ログインできないようにするために、管理者はセッションを閉じることができます：**Analysis > Users heading > Active Sessions**。ユーザーがブラウザを閉じた場合も、ブラウザは自動的に再認証されません。
- **Active FTP sessions are displayed as the Unknown user in events.** 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）サーバーが接続を開始し、FTP サーバーには関連付けられているユーザー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がアイデンティティルールに一致するユーザーを認証する場合、ダウンロードされていない Microsoft Active Directory または LDAP グループ内のユーザーは不明として識別されます。ユーザーが不明として識別されるのを回避するには、キャプティブポータルで認証するすべてのグループのユーザーをダウンロードするようにレルムまたはレルムシーケンスを設定します。不明なユーザーは、関連付けられたアクセスコントロールポリシーに従って処理されます。アクセスコントロールポリシーが不明なユーザーをブロックするように構成されている場合、これらのユーザーはブロックされます。

システムによってレルムまたはレルムシーケンス内のすべてのユーザーが確実にダウンロードされるようにするには、グループがレルムの設定の [使用可能グループ (Available Groups)] リストに含まれていることを確認します。

詳細については、「[ユーザーとグループを同期する](#)」を参照してください。

キャプティブポータルの履歴

機能	Minimum Firewall Management Center Firewall Management Center	Minimum Firewall Threat Defense	詳細
レルムまたはレルムシーケンスを使用したアクティブ認証。	7.4.1	7.4.1	<p>LDAP レルム、Microsoft Active Directory レルム、またはレルムシーケンスに対してアクティブ認証を設定できます。さらに、レルムまたはレルムシーケンスを使用してアクティブ認証にフォールバックするパッシブ認証ルールを設定できます。必要に応じて、アクセス制御ルールで同じ ID ポリシーを共有する管理対象デバイス間でセッションを共有できます。</p> <p>さらに、以前にアクセスしたデバイスとは別の管理対象デバイスを使用してシステムにアクセスするときに、ユーザーに再認証を要求するオプションがあります。</p> <p>Microsoft Azure Active Directory は、キャプティブポータルでは使用できません。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> • [ポリシー (Policies)] > [アイデンティティ (Identity)] > (ポリシーの編集) > [アクティブ認証 (Active Authentication)] > [ファイアウォール全体でアクティブ認証セッションを共有 (Share active authentication sessions across firewalls)] • [IDポリシー (Identity policy)] > (編集) > [ルールの追加 (Add Rule)] > [パッシブ認証 (Passive Authentication)] > [レルムと設定 (Realms & Settings)] > [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)] • [IDポリシー (Identity policy)] > (編集) > [ルールの追加 (Add Rule)] > [アクティブ認証 (Active Authentication)] > [レルムと設定 (Realms & Settings)] > [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)]

機能	Minimum Firewall Management Center Firewall Management Center	Minimum Firewall Threat Defense	詳細
ファイアウォール全体でアクティブ認証セッションを共有します。	7.4.1	7.4.1	<p>以前に接続していたデバイスとは異なる管理対象デバイスに認証セッションが送信されたときに、ユーザーの認証が必要かどうかを決定します。ユーザーがロケーションまたはサイトを変更するたびに認証する必要がある組織の場合は、このオプションを無効にする必要があります。</p> <ul style="list-style-type: none"> • (デフォルト) 有効にすると、ユーザーはアクティブな認証アイデンティティルールに関連付けられた管理対象デバイスで認証できます。 • アクティブな認証ルールが展開されている別の管理対象デバイスでユーザーがすでに認証されている場合でも、別の管理対象デバイスでの認証をユーザーに要求する場合は無効にします。 <p>新規/変更された画面：[ポリシー (Policies)] > [アイデンティティ (Identity)] > (ポリシーの編集) > [アクティブ認証 (Active Authentication)] > [ファイアウォール全体でアクティブ認証セッションを共有 (Share active authentication sessions across firewalls)]</p>
ホスト名のリダイレクト。	7.1.0	7.1.0 (Snort 3)	キャプティブポータルをアクティブな認証要求に使用できるインターフェイスの完全修飾ホスト名 (FQDN) を含むネットワークオブジェクトを使用できます。
ゲストログイン。	6.1.0	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。	6.0.0	6.0.0	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ー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。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。