



キャプティブポータルによるユーザーの制御

- 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約事項 (3 ページ)
- ユーザー制御のためのキャプティブ ポータルの設定方法 (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）。認証ルーム（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。

■ ホスト名のリダイレクトについて

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す。

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設定方法 \(6 ページ\)](#)

ホスト名のリダイレクトについて

(Snort3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にリダイレクト](#)

キャプティブポータルのライセンス要件

Threat Defense ライセンス

いずれか (Any)

従来のライセンス

Control

キャプティブポータルの要件と前提条件

サポートされるドメイン

任意

ユーザーの役割

- ・管理者
- ・アクセス管理者
- ・ネットワーク管理者

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。

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 復号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の同期](#)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。

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 [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。
- キャプティブポータルでレルムシーケンスを使用することはできません。
- 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：[分析 (Analysis)] > [ユーザー (Users)] 見出し > [アクティブセッション (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、復号ポリシーを使用して、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、および復号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。

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設定方法

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、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、復号ポリシーをセットアップし、アイデンティティポリシーと復号ポリシー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。

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 レルムを作成し、有効化します。

- LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成
- ユーザーとグループの同期

レルムシーケンスは、キャプティブポータルではサポートされていません。

システムによってレルム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の同期](#)」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。
- 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。

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。

[キャプティブポータルの設定パート1：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イデンティティポリシーを作成します。

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 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2：イデンティティポリシーおよびアクティブ認証ルールの作成（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、[キャプティブポータルの設定パート3：TCPポートアクセスコントロールルールの作成（12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、[キャプティブポータルの設定パート4：ユーザー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）]ルールを用いて復号ポリシーを設定します。

■ キャプティブポータルの設定パート1：ネットワークオブジェクトの作成

HTTPS トライ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。

[キャプティブポータルの例：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復号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、[キャプティブポータルの設定パート6：アクセスコントロールポリシーへのアイデンティティと復号ポリシーの関連付け（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[キャプティブポータルの設定パート1：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のアプリケーションの除外（19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](#)

キャプティブポータルの設定パート1：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 Management Center にアップロードします。これまでに行ったことがない場合は、[このようなリソースを参照できます](#)。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にリダイレクト](#)を参照してください。

手順

ステップ1 まだ 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 [オブジェクト (Objects)] > [オブジェクト管理 (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。

■ キャプティブポータルの設定パート2：アイデンティティポリシーおよびアクティブ認証ルールの作成

New Network Object

Name: MyCaptivePortalNetwork

Description:

Network:
 Host
 Range
 Network
 FQDN
 mycaptiveportal.example.com

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

Lookup:
 Resolve within IPv4 and IPv6

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

[キャプティブポータルの設定パート2：アイデンティティポリシーおよびアクティブ認証ルールの作成 \(10 ページ\)](#)

キャプティブポータルの設定パート2：アイデンティティポリシーおよびアクティブ認証ルールの作成

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設定方法（6ページ）](#)を参照してください。

手順

ステップ1 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 リストから適切なルートサーバー証明書を選択するか、[追加 (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 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、[追加 (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 (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。

次の図は例を示しています。

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9 [保存 (Save)] をクリックします。

ステップ10 [ルール (Rules)] をクリックします。

■ キャプティブポータルの設定パート3：TCPポートアクセスコントロールルールの作成

ステップ11 [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 (Edit)] (筆記用具アイコン) をクリックして既存のルールを編集します。

ステップ12 ルールの [名前 (Name)] を入力します。

ステップ13 [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14 [realmおよび設定 (Realm & Settings)] をクリックします。

ステップ15 [realm (Realms)] 一覧から、ユーザー認証に使用するrealmを選択します。
realmシーケンスはサポートされていません。

ステップ16 (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17 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18 (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 \(19ページ\)](#) を参照してください。

ステップ19 [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20 [追加 (Add)] をクリックします。

ステップ21 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3：TCPポートアクセスコントロールルールの作成 \(12ページ\)](#) に進みます。

キャプティブポータルの設定パート3：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2：アイデンティティポリシーおよびアクティブ認証ルールの作成 \(10ページ\)](#) 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設定方法 \(6ページ\)](#) を参照してください。

手順

ステップ1 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 [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [アクセスコントロール (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または編集します。

ステップ4 [ルールの追加 (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。

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。

The screenshot shows the 'Add Rule' dialog box. The 'Ports' tab is selected. In the 'Available Ports' list, '885' is selected and highlighted with a red oval. The 'Selected Destination Ports' list shows 'any'. At the bottom, the 'Protocol' dropdown is set to 'TCP (6)', the 'Port' field contains '885', and the 'Add' button is highlighted with a red oval.

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

[キャプティブポータルの設定パート4：ユーザー 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。

キャプティブポータルの設定パート4：ユーザー 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 ポータルの設定方法（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、[更新 (Refresh)] (C) 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例：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）](#)

キャプティブポータルの例：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復号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

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 [ポリシー (Policies)] > [アクセス制御 (Access Control)] 見出し > [復号 (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)] に一意のポリシーネームを入力し、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。

■ キャプティブポータルの例：アウトバウンドルールを使用した復号ポリシーの作成

Create Decryption Policy

A decryption policy is not required to only perform application or URL discovery; instead, you can use TLS 1.3 Server Identity Discovery on the access control policy.

Name*
Captive Portal decrypt

Description

Outbound Connections (User Protection) Inbound Connections (Server Protection)

How Outbound Protection Works
Outbound protection matches traffic based on the referenced internal CA certificate's signature algorithm type, in addition to any configured rule conditions.

Internal CA
A rule will be auto-created for the selected certificate authority.

Download
CaptivePortalCA Associated: 2 Networks, 1 Port
See how to configure

Cancel Save

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 [編集 (Edit)] (edit icon) 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 [編集 (Edit)] (edit icon) をクリックします。

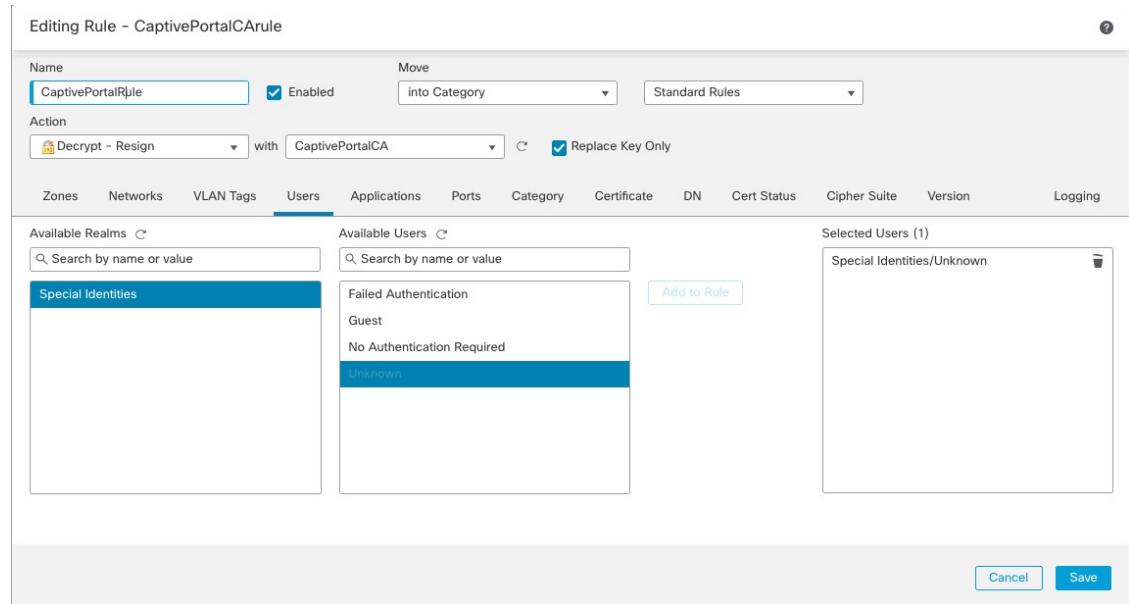
ステップ11 [ユーザー (Users)] をクリックします。

ステップ12 [使用可能なrealm (Available Realms)]一覧の上にある[更新 (Refresh)] (C) をクリックします。

ステップ13 [使用可能なrealm (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。



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

[キャプティブポータルの設定パート6：アクセスコントロールポリシーへのアイデンティティと復号ポリシーの関連付け \(17ページ\)](#)

キャプティブポータルの設定パート6：アクセスコントロールポリシーへのアイデンティティと復号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設定方法（6 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3：TCPポートアクセスコントロールルールの作成（12 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 (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復号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。
- [Cisco Secure Firewall Management Center アドミニストレーションガイド](#) 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のアプリケーションの除外（19 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、[キャプティブポータルの設定パート3：TCPポートアクセスコントロールルールの作成 \(12ページ\)](#)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。

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 (HTTP 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。

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 (View)] (oculars) 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 (Edit)] (pencil) 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

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。

■ キャプティブポータルからのアプリケーションの除外



(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 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)] > [アクセス制御 (Access Control)] 見出し > [アイデンティティ (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 [realm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、[クリア (Clear)] (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 (C) 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 (Clear)] (X) 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 (C) 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のトラブルシート](#)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。

■ 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

- **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に、[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オ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：[分析 (Analysis)] > [ユーザー (Users)] 見出し > [アクティブセッション (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の同期](#)」を参照してください。

キャプティブポータルの履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
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、ユーザー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。

■ キャプティブポータルの履歴

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。