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

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）。認証レルム（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。

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

（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

任意（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 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 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、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。

- ユーザーが確実にログアウトする唯一の方法は、ユーザーが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、ユーザーがキャプティブ 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 レルムまたはレルムシーケンス、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。

（注） Microsoft Azure Active Directory は、キャプティブポータルではサポートされていません。

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 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、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 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

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入手します。
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 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）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、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。

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。

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 （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

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、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。

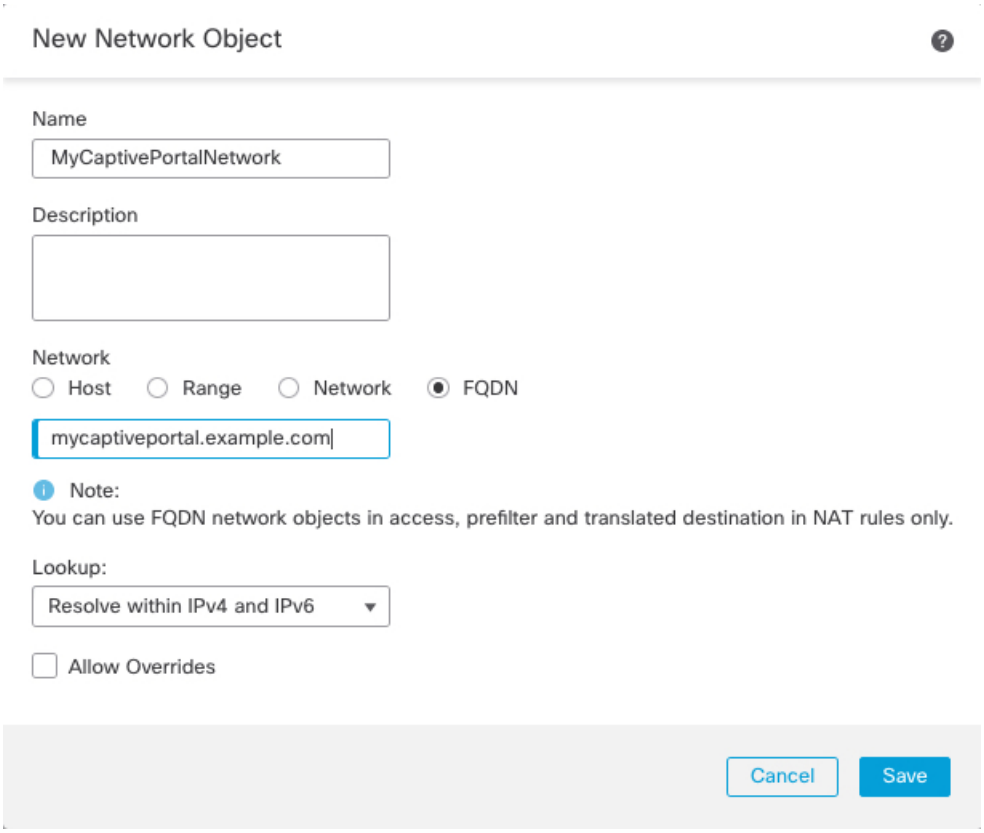
ステップ 12 **[ネットワークの追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックします。

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。



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 [サーバー証明書（Server Certificate）] を選択するか、**Add** ( ) をクリックして証明書を追加します。

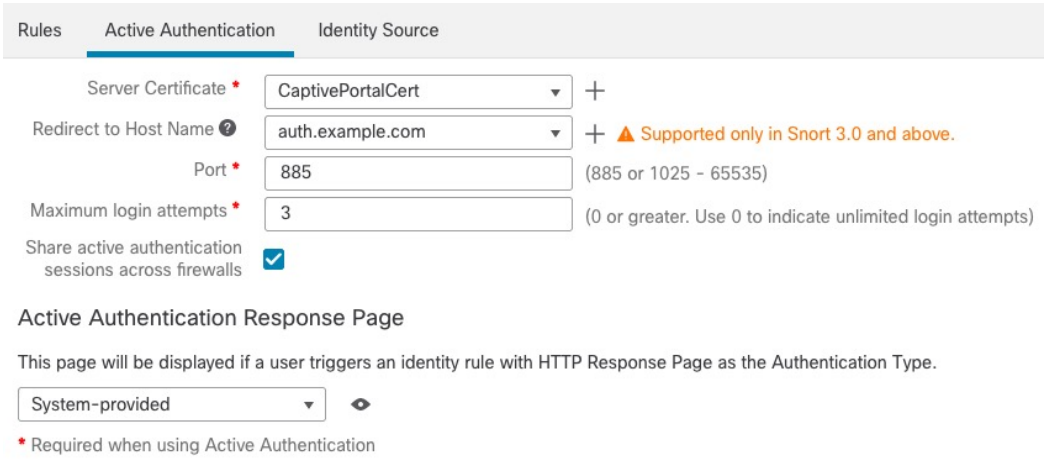
（注） キャプティブ ポータルは、デジタル署名アルゴリズム（DSA）証明書または楕円曲線デジタル署名アルゴリズム（ECDSA）証明書の使用をサポートしていません。

ステップ 6 [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 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。



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）。**[編集（Edit）]**（✎）をクリックし、カスタム認証フォームの更新 （12 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、**[編集（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 ポータルからのアプリケーションの除外 （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

「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。

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、**[編集（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>
```

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。

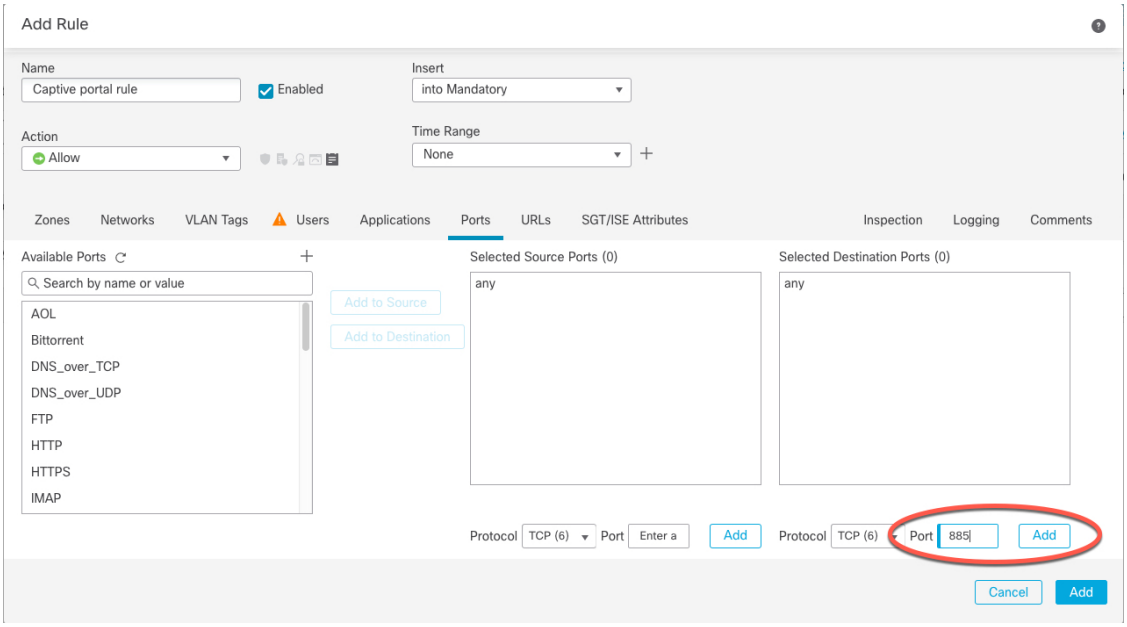
ステップ 6 [アクション（Action）] 一覧から、[許可（Allow）] を選択します。

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。



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）]**（  ） 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

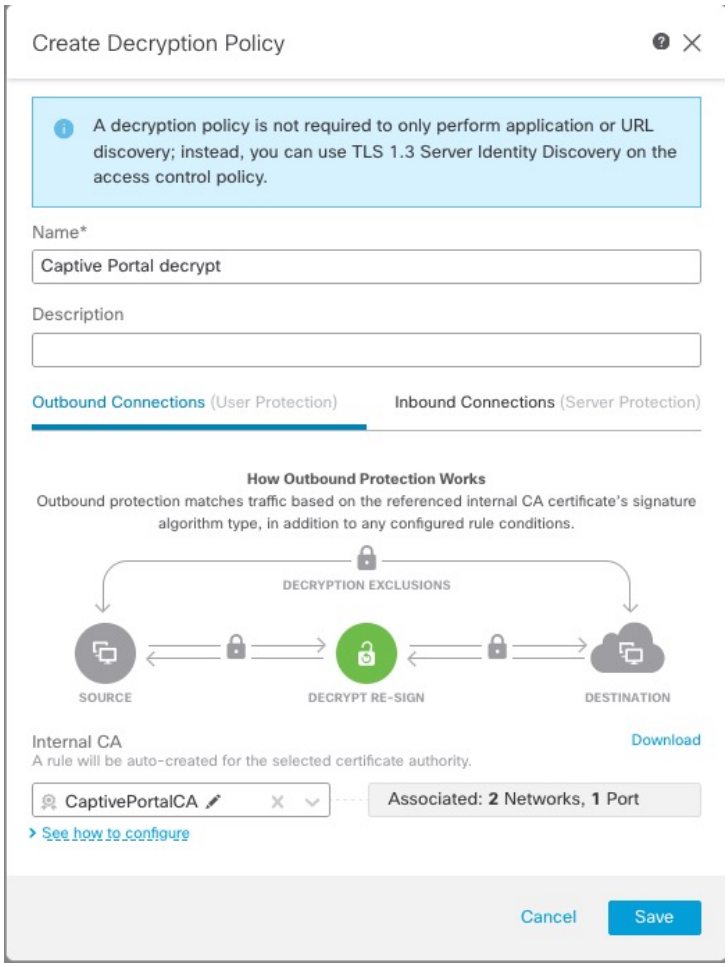
ステップ 1 まだ Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセスコントロール（Access Control）] > [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）]**（✎）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）]**（✎）をクリックします。

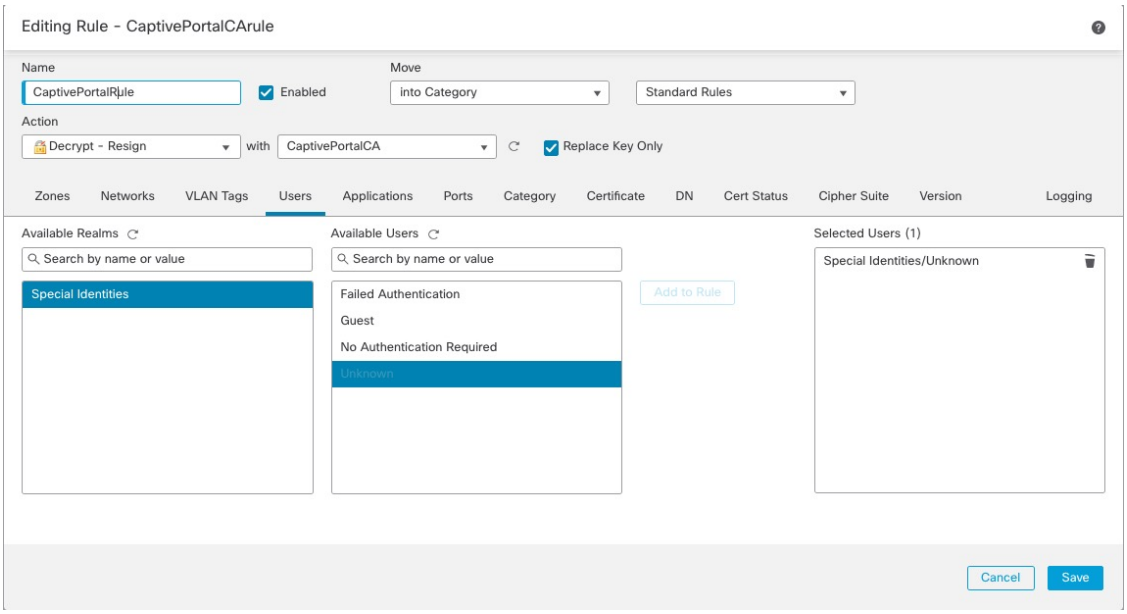
ステップ 11 [ユーザー（Users）] をクリックします。

ステップ 12 [使用可能なレルム（Available Realms）] 一覧の上にある **[更新（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（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

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）]（👁） 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（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 （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、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。

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。[表示（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、**[編集（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。

（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）]** > **[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 [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、[クリア（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 [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（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のトラブルシューティング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、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。

- 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 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、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、ユーザー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。
- 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 Management Center/Cloud-delivered Management Center	最小 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 2023 年 MM 月 DD 日	7.4.1	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。 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。 Microsoft Azure Active Directory は、キャプティブポータルでは使用できません。 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）]** • **[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	最小 Management Center/Management Center	最小 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	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) 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。 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）]**
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。

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。