リモートアクセス VPN によるユーザーの制御

次のトピックでは、リモート アクセス VPN によりユーザー認識とユーザー制御を実行する方法について説明します。

リモート アクセス VPN アイデンティティ ソース

Secure Client はエンドポイントデバイスでサポートされている唯一のクライアントで、Threat Defense デバイスへのリモート VPN 接続が可能です。

新しいリモート アクセス VPN ポリシーの作成の説明に従って安全な VPN ゲートウェイを設定する場合、ユーザーが Active Directory リポジトリ内にいる場合は、それらのユーザーのアイデンティティ ポリシーを設定して、アクセス コントロール ポリシーにアイデンティティ ポリシーを関連付けることができます。

（注） ユーザーアイデンティティと RADIUS をアイデンティティソースとしてリモートアクセス VPN を使用する場合は、レルムを設定する必要があります（[オブジェクト（Objects）]>[オブジェクト管理（Object Management）]>[AAAサーバー（AAA Server）]>[RADIUSサーバーグループ（RADIUS Server Group）]）。

リモート ユーザーから提供されるログイン情報は、LDAP または AD レルムまたは RADIUS サーバー グループによって検証されます。これらのエンティティは、Secure Firewall Threat Defense セキュア ゲートウェイと統合されます。

（注） ユーザーが認証ソースとして Active Directory を使用してリモートアクセス VPN で認証を受ける場合、ユーザーは自分のユーザー名を使用してログインする必要があります。`domain\username` または `username@domain` 形式は失敗します。（Active Directory はこのユーザー名をログオン名、または場合によっては `sAMAccountName` と呼んでいます）。詳細については、MSDN でユーザーの名前付け属性を参照してください。

認証に RADIUS を使用する場合、ユーザーは前述のどの形式でもログインできます。

VPN 接続経由で認証されると、リモート ユーザーには *VPN ID* が適用されます。この VPN ID は、そのリモート ユーザーに属しているネットワーク トラフィックを認識し、フィルタリングするために Secure Firewall Threat Defense のセキュア ゲートウェイ上のアイデンティティ ポリシーで使用されます。

アイデンティティ ポリシーはアクセス コントロール ポリシーと関連付けられ、これにより、誰がネットワーク リソースにアクセスできるかが決まります。リモート ユーザーがブロックされるか、またはネットワーク リソースにアクセスできるかはこのようにして決まります。

関連トピック

VPN の概要
リモート アクセス VPN の概要
VPN の基本
リモート アクセス VPN の機能
リモート アクセス VPN のガイドラインと制限事項
新しいリモート アクセス VPN ポリシーの作成

ユーザー制御用 RA VPN の設定

始める前に

- 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の説明に従って、レルムを作成します。
- 認証、認可、および監査（AAA）を使用するには、RADIUS サーバーグループの追加の説明に従って RADIUS サーバー グループを設定します。

手順

ステップ 1 Management Center にログインします。

ステップ 2 **[デバイス（Devices）]** > **[VPN]** > **[リモートアクセス（Remote Access）]** の順にクリックします。

ステップ 3 新しいリモート アクセス VPN ポリシーの作成を参照してください。

次のタスク

- アイデンティティ ポリシーの作成の説明に従って、制御するユーザーおよび他のオプションを、アイデンティティ ポリシーを使って指定します。
- アクセス制御への他のポリシーの関連付けの説明に従って、アイデンティティ ルールをアクセス コントロール ポリシーに関連付けます。このポリシーは、トラフィックをフィルタし、オプションで検査します。
- 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。
- VPN セッションとユーザー情報の説明に従って、VPN ユーザートラフィックをモニターします。

リモート アクセス VPN 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。
- リモート アクセス VPN の問題が発生した場合は、Management Center と管理対象デバイスとの間の接続を確認します。接続に障害が発生している場合、ユーザが既に認識されて Management Center にダウンロードされている場合を除き、デバイスによって報告されたすべてのリモート アクセス VPN ログインはダウンタイム中に識別されません。

  識別されていないユーザは、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（Unknown）]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び識別され、処理されます。
- 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。
- 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。

VPN 統計の設定が正しくない

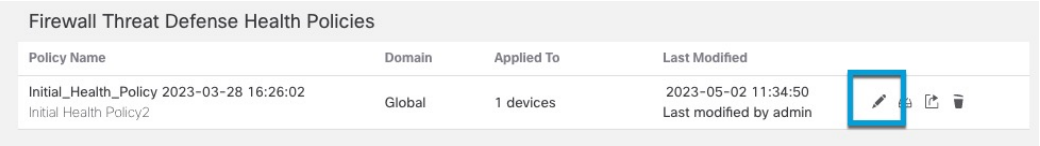
このタスクでは、正常性ポリシーで [VPN統計（VPN Statistics）] 設定を有効または無効にした後に実行する必要がある手順について説明します。このタスクを実行しない場合は、管理対象デバイスの正常性ポリシーの設定が正しくないことを意味します。

手順

ステップ 1 まだ Secure 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 **システム**（⚙）> **[正常性（Health）]** > **[ポリシー（Policy）]** をクリックします。

ステップ 3 [Firewall Threat Defense正常性ポリシー（Firewall Threat Defense Health Policies）] で、編集するポリシーの横にある **[編集（Edit）]**（✎） をクリックします。



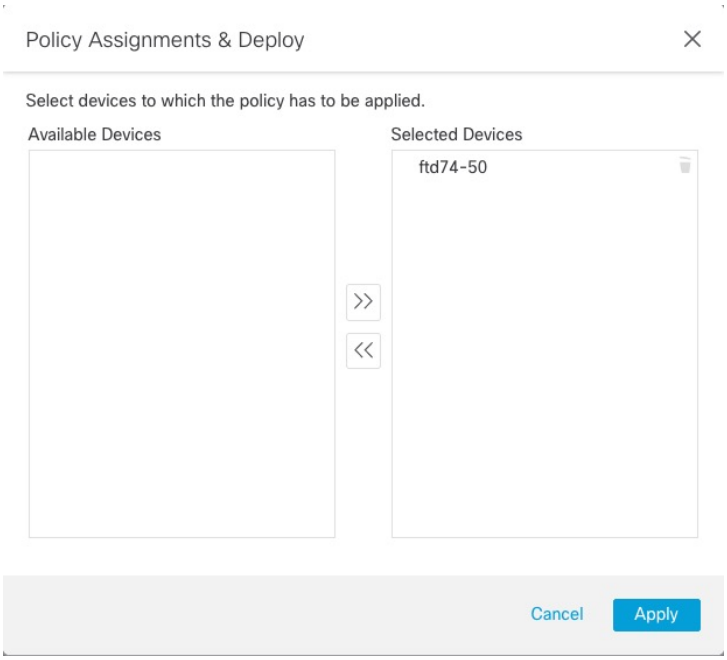
ステップ 4 [正常性モジュール（Health Modules）] タブページで、下にスクロールして [VPN統計（VPN Statistics）] を見つけます。

ステップ 5 VPN 統計の設定が正しいことを確認するか、必要に応じて変更します。

ステップ 6 設定を変更した場合は、[保存（Save）] をクリックし、[キャンセル（Cancel）] をクリックして正常性ポリシーに戻ります。

ステップ 7 [Firewall Threat Defense正常性ポリシー（Firewall Threat Defense Health Policies）]で、 [正常性ポリシーの展開（Deploy health policy）]（🚀） をクリックしてポリシーを適用します。

ステップ 8 [ポリシーの割り当てと展開（Policy Assignments & Deploy）] ダイアログボックスで、正常性ポリシーを展開するデバイスを [選択したデバイス（Selected Devices）] フィールドに移動します。



ステップ 9 [適用（Apply）] をクリックします。
正常性ポリシーが展開されると、メッセージが表示されます。

ステップ 10 正常性ポリシーの展開が完了したら、**[ポリシー（Policies）]**>**[アクセス制御（Access Control）]** をクリックしてアクセス コントロール ポリシーを編集します。

ステップ 11 編集するポリシーの横にある編集 **[編集（Edit）]**（ ） をクリックします。

ステップ 12 名前の変更など、ポリシーにマイナー変更を加えます。

ステップ 13 アクセス コントロール ポリシーを保存します。

ステップ 14 設定変更を展開します設定変更の展開を参照してください。。

RA VPN の履歴

機能	最小 Management Center	最小 Threat Defense	詳細
リモート アクセス VPN	6.2.1	いずれか	導入された機能。RA VPN により、インターネットに接続されたラップトップまたはデスクトップ コンピュータや、Android または Apple iOS モバイル デバイスを使用して、個々のユーザがリモート ロケーションからプライベート ビジネス ネットワークに接続することができます。リモートユーザーは、共有メディアやインターネットを介してデータを転送するために不可欠な暗号化技術を使用して、セキュアに機密性を保持してデータを転送します。

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。