VPN 3000 コンセントレータでの Cisco VPN クライアント ユーザおよびグループ アトリビュートの処理

内容

概要

このドキュメントでは、VPNコンセントレータでCisco VPN Clientが認証される方法と、Cisco VPN 3000コンセントレータがユーザ属性とグループ属性を使用する方法について説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco VPN 3000コンセントレータに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、「シスコ テクニカル ティップスの表記法」を参照してください。

VPN ClientがVPN 3000コンセントレータに接続する

VPN ClientがVPN 3000コンセントレータに接続すると、最大4つの認証を実行できます。

1. グループが認証されます。（これは「トンネルグループ」とも呼ばれます）。
2. ユーザが認証されます。
3. （オプション）ユーザが別のグループの一部である場合、このグループは次に認証されます。ユーザが別のグループまたはトンネルグループに属していない場合、ユーザはデフォルトでベースグループに設定され、この手順は実行されません。
4. ステップ1の「トンネルグループ」が再度認証されます。(これは、「グループロック」機能を使用する場合に行います。この機能は、バージョン2.1以降で使用できます)。

これは、内部データベースを介して認証されたVPN Clientのイベントログに表示されるイベントの例です（「testuser」はグループ「Engineering」の一部です）。

```
1 12/09/1999 11:03:46.470 SEV=6 AUTH/4 RPT=6491 80.50.0.4
Authentication successful: handle = 642, server = Internal, user = Tunnel_Group
2 12/09/1999 11:03:52.100 SEV=6 AUTH/4 RPT=6492 80.50.0.4
Authentication successful: handle = 643, server = Internal, user = testuser
3 12/09/1999 11:03:52.200 SEV=6 AUTH/4 RPT=6493 80.50.0.4
Authentication successful: handle = 643, server = Internal, user = Engineering
4 12/09/1999 11:03:52.310 SEV=6 AUTH/4 RPT=6494 80.50.0.4
Authentication successful: handle = 643, server = Internal, user = Tunnel_Group
```

注：これらのイベントを表示するには、[Configuration] > [**System**] > [**Events**] > [**Classes**]で重大度1 ~ 6の認証イベントクラスを設定する必要があります。

グループロック機能：グループ – Tunnel_Groupでグループロック機能が有効になっている場合、ユーザは接続するためにTunnel_Groupの一部である必要があります。前の例では、すべての同じイベントが表示されていますが、「testuser」はGroup - Tunnel_Groupの一部ではなくGroup - Engineeringの一部であるため、接続できません。次のイベントも表示されます。

```
5 12/09/1999 11:35:08.760 SEV=4 IKE/60 RPT=1 80.50.0.4
User [ testuser ]
User (testuser) not member of group (Tunnel_Group), authentication failed.
```

グループロック機能と設定例についての詳細は、『RADIUSサーバを使用したVPN 3000コンセントレータグループへのユーザのロック』を参照してください。

RADIUSを介した外部でのグループおよびユーザの認証

VPN 3000コンセントレータは、RADIUSサーバを介してユーザとグループを外部で認証するように設定することもできます。この場合も、VPNコンセントレータでグループ名を設定する必要がありますが、グループタイプは「外部」として設定されます。

- RADIUSサーバがベンダー固有属性(VSA)をサポートしている場合、外部グループはCisco/Altiga属性を返すことができます。
- RADIUSによって返されないCisco/Altiga属性は、デフォルトでベースグループの値に設定されます。
- RADIUSサーバがVSAをサポートしていない場合、すべての属性はデフォルトでベースグループ属性に設定されます。

注：RADIUSサーバーは、グループ名をユーザー名と異なるものではありません。RADIUSサーバ

上のグループは、標準ユーザと同様に設定されます。

次の手順では、ユーザとグループの両方が外部で認証されている場合に、IPSecクライアントがVPN 3000コンセントレータに接続するとどうなるかについて説明します。内部ケースと同様に、最大4つの認証を実行できます。

1. グループはRADIUS経由で認証されます。RADIUSサーバは、グループに対して多数の属性を返すことも、まったく返すこともできません。少なくとも、RADIUSサーバは、ユーザの認証方法をVPNコンセントレータに指示するために、Cisco/Altiga属性「IPSec Authentication = RADIUS」を返す必要があります。そうでない場合は、ベースグループのIPSec認証方式を「RADIUS」に設定する必要があります。
2. ユーザはRADIUS経由で認証されます。RADIUSサーバは、ユーザに対して多数の属性を返すことも、まったく返すこともできません。RADIUSサーバが属性CLASS(標準RADIUS属性#25)を返す場合、VPN 3000コンセントレータはその属性をグループ名として使用し、ステップ3に移動します。そうでない場合は、ステップ4に進みます。
3. ユーザのグループは、次にRADIUS経由で認証されます。RADIUSサーバは、グループに対して多数の属性を返すことも、まったく返すこともできません。
4. ステップ1の「トンネルグループ」は、RADIUS経由で再度認証されます。認証サブシステムは、ステップ1の認証の属性（ある場合）を保存していないため、トンネルグループを再度認証する必要があります。これは、「グループロック」機能が使用されている場合に実行されます。

VPN 3000 Concentrator がユーザおよびグループ属性を利用する方法

VPN 3000コンセントレータがユーザとグループを認証した後、受信した属性を整理する必要があります。VPNコンセントレータは、この優先順位の属性を使用します。認証が内部または外部のどちらで行われたかは問題ではありません。

1. **ユーザ属性**：他のすべての属性よりも優先されます。
2. **グループ属性**：ユーザ属性に含まれていない属性は、グループ属性によって入力されます。同じものはすべて、ユーザ属性によって上書きされます。
3. **トンネルグループ属性**：ユーザ属性またはグループ属性に存在しない属性は、トンネルグループ属性によって入力されます。同じものはすべて、ユーザ属性によって上書きされます。
4. **Base Group attributes**:User、Group、またはTunnel Group属性に含まれていない属性は、Base Group属性によって入力されます。

関連情報

- Cisco VPN 3000 シリーズ コンセントレータに関するサポート ページ
- Cisco VPN Client に関するサポート ページ
- IPSec に関するサポート ページ
- RADIUS に関するサポート ページ
- Requests for Comments (RFCs)
- テクニカルサポート - Cisco Systems