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

目次

概要

Cisco VPN Clients が VPN コンセントレータでどのように認証される、そしてどのように Cisco VPN 3000 コンセントレータがユーザおよびグループ属性を利用するかこの資料に記述されています。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

この文書に記載されている情報は Cisco VPN 3000 コンセントレータに基づいています。

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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分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 クライアントは VPN 3000 コンセントレータに接続します

VPN クライアントが VPN 3000 コンセントレータに接続するとき、4 まで認証は起こることができます。

1. グループは認証されます。（これは頻繁に「トンネル グループ呼出されます。」）
2. ユーザは認証されます。
3. ユーザが別のグループの一部である場合（オプションの）、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かトンネル グループに属さない場合、基礎群およびこのステップへのユーザーの既定は発生しません。
4. ステップ 1 からの「トンネル グループ」は再度認証されます。（これは" Group Lock " 機能が使用されればされます。 この機能はバージョン 2.1 または それ 以降で利用できます。）

これは VPN クライアントについては内部データベースによって認証されるイベントログで参照するイベントの例です（「testuser」はグループ「エンジニアリング」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参照するために、**Configuration > System > Events > Classes** の重大度 1-6 で AUTHイベント クラスを設定して下さい。

グループ ロック 機能-グループ ロック 機能がグループで- Tunnel_Group、有効に なれば ユーザ 接続するべき Tunnel_Group の一部はある必要があります。 前例では、全く同じイベントを参照しますが、グループの一部-グループのエンジニアリングおよびない一部- Tunnel_Group であるので「testuser」は接続しません。 またこのイベントを参照します:

```
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.
```

グループについてのその他の情報に関しては機能をロックすれば設定 例は、RADIUS サーバを使用する VPN 3000 コンセントレータ グループへのユーザのロックを示します。

外部に 認証するグループおよびユーザ RADIUS によって

VPN 3000 コンセントレータはまた RADIUSサーバを通してユーザおよびグループを外部に認証するために設定することができます。 これはまだグループの名前が VPN コンセントレータで設定されるように要求しますがグループ タイプは「外部で設定されます」。

- 外部 の グループは RADIUSサーバがベンダ別の属性（VSAs）をサポートする場合 Cisco/Altiga 属性を戻すことができます。
- 基礎群の値に RADIUS デフォルトで戻らない Cisco/Altiga 属性。
- RADIUSサーバが VSAs をサポートしない場合、すべての属性は基本グループ属性にデフォルトで設定されます。

注: RADIUSサーバはユーザネームとグループ名を別様に扱いません。 RADIUSサーバのグループは標準ユーザと同様に設定されます。

ユーザおよびグループが両方外部に認証される場合 IPSecクライアントが VPN 3000 コンセントレータに接続すると起こる何がこれらのステップ輪郭。 類似した 内部 ケースは、4 まで認証起こることができます。

1. グループは RADIUS によって認証されます。 RADIUSサーバはグループまたは皆無のための多くの属性を戻すことができます。 少くとも、RADIUSサーバはユーザを認証する方法を VPN コンセントレータに言う Cisco/Altiga アトリビュート「IPSec 認証 = RADIUS」を戻す必要があります。 そうでなかったら、基礎群の IPSec 認証認証方法は「RADIUS に設定 される必要があります」。
2. ユーザは RADIUS によって認証されます。 RADIUSサーバはユーザまたは皆無のための多くの属性を戻すことができます。 RADIUSサーバがステップ 4.に属性クラス (標準 RADIUS属性 #25) を、ステップ 3 にグループ名および移動として、さもないと帰因する VPN 3000 コンセントレータ使用それ行けば戻せば。
3. ユーザ· グループは RADIUS によって次に認証されます。 RADIUSサーバはグループまたは皆無のための多くの属性を戻すことができます。
4. ステップ 1 からの「トンネル グループ」は RADIUS によって再度認証されます。 認証 サブシステムはステップ 1.で認証からの属性を (もしあれば) 保存しなかったのでトンネル グループを再度認証する必要があります。 これは" Group Lock " 機能が使用されればされます。

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およびグループを認証した後、受け取った属性を編成する必要があります。 VPN コンセントレータはこの選択の順序で属性を利用します。 認証が内部または外部で実行された場合重要ではありません:

1. **ユーザ属性**—これらは他に優先します。
2. **グループ属性**—ユーザ属性から抜けているどの属性でもグループ属性によって記入されます。 同じであるユーザ属性によって無効になります。
3. **トンネル グループ属性**—ユーザから抜けているどの属性でもかグループ属性はトンネル グループ属性によって記入されます。 同じであるユーザ属性によって無効になります。
4. **基本グループ属性**—ユーザ、グループ、またはトンネル グループ属性から抜けているどの属性でも基本グループ属性によって記入されます。

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 (RFC)
- テクニカルサポート - Cisco Systems