Traitement d'attribut de groupe et d'utilisateur de client VPN Cisco sur le concentrateur VPN 3000

Contenu

Introduction

Ce document décrit comment les clients VPN Cisco sont authentifiés sur le concentrateur VPN et comment le concentrateur VPN Cisco 3000 utilise les attributs Utilisateur et Groupe.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations de ce document sont basées sur le concentrateur Cisco VPN 3000.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Le client VPN se connecte à un concentrateur VPN 3000

Lorsqu'un client VPN se connecte à un concentrateur VPN 3000, jusqu'à quatre authentifications

peuvent être effectuées.

1. Le groupe est authentifié. (Il s'agit souvent du groupe de tunnels.)
2. L'utilisateur est authentifié.
3. (Facultatif) Si l'utilisateur fait partie d'un autre groupe, ce groupe est ensuite authentifié. Si l'utilisateur n'appartient à aucun autre groupe ou groupe de tunnels, l'utilisateur utilise par défaut le groupe de base et cette étape ne se produit PAS.
4. Le groupe de tunnels de l'étape 1 est de nouveau authentifié. (Ceci est fait au cas où la fonction de verrouillage de groupe est utilisée. Cette fonctionnalité est disponible dans la version 2.1 ou ultérieure.)

Voici un exemple des événements que vous voyez dans le journal des événements d'un client VPN authentifié via la base de données interne (« testuser » fait partie du groupe « Engineering »).

```
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
```

Remarque : Pour voir ces événements, vous devez configurer la classe d'événements d'authentification avec la gravité 1-6 dans **Configuration > System > Events > Classes**.

Fonction de verrouillage de groupe - Si la fonction de verrouillage de groupe est activée sur Groupe - Groupe_Tunnel, l'utilisateur doit faire partie de Groupe_Tunnel pour se connecter. Dans l'exemple précédent, vous voyez tous les mêmes événements, mais « testuser » ne se connecte pas parce qu'ils font partie du groupe - Ingénierie et non du groupe - Tunnel_Group. Cet événement s'affiche également :

```
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.
```

Pour plus d'informations sur la fonctionnalité de verrouillage de groupe et un exemple de configuration, référez-vous à Verrouiller les utilisateurs dans un groupe de concentrateurs VPN 3000 à l'aide d'un serveur RADIUS.

Authentification externe des groupes et des utilisateurs via RADIUS

Le concentrateur VPN 3000 peut également être configuré pour authentifier les utilisateurs et les groupes en externe via un serveur RADIUS. Cela nécessite toujours que les noms des groupes soient configurés sur le concentrateur VPN, mais le type de groupe est configuré comme « Externe ».

- Les groupes externes peuvent renvoyer des attributs Cisco/Altiga si le serveur RADIUS prend en charge les attributs spécifiques au fournisseur (VSA).
- Tous les attributs Cisco/Altiga NON retournés par RADIUS par défaut aux valeurs du groupe de base.

- Si le serveur RADIUS ne prend PAS en charge les VSA, tous les attributs par défaut sont ceux du groupe de base.

Remarque : un serveur RADIUS traite les noms de groupe de la même manière que les noms d'utilisateurs. Un groupe sur un serveur RADIUS est configuré comme un utilisateur standard.

Ces étapes décrivent ce qui se passe lorsqu'un client IPSec se connecte au concentrateur VPN 3000 si les utilisateurs et les groupes sont tous deux authentifiés en externe. Comme dans le cas interne, jusqu'à quatre authentifications peuvent être effectuées.

1. Le groupe est authentifié via RADIUS. Le serveur RADIUS peut renvoyer de nombreux attributs pour le groupe ou aucun. Au minimum, le serveur RADIUS doit retourner l'attribut Cisco/Altiga « Authentification IPSec = RADIUS » pour indiquer au concentrateur VPN comment authentifier l'utilisateur. Si ce n'est pas le cas, la méthode d'authentification IPSec du groupe de base doit être définie sur RADIUS.
2. L'utilisateur est authentifié via RADIUS. Le serveur RADIUS peut renvoyer de nombreux attributs pour l'utilisateur ou aucun. Si le serveur RADIUS renvoie l'attribut CLASS (attribut RADIUS standard n° 25), le concentrateur VPN 3000 utilise cet attribut comme nom de groupe et passe à l'étape 3, ou passe à l'étape 4.
3. Le groupe de l'utilisateur est ensuite authentifié via RADIUS. Le serveur RADIUS peut renvoyer de nombreux attributs pour le groupe ou aucun.
4. Le groupe de tunnels de l'étape 1 est de nouveau authentifié via RADIUS. Le sous-système d'authentification doit authentifier à nouveau le groupe de tunnels car il n'a pas stocké les attributs (le cas échéant) de l'authentification à l'étape 1. Cela se fait au cas où la fonction de verrouillage de groupe est utilisée.

Utilisation des attributs utilisateur et de groupe par le concentrateur VPN 3000

Une fois que le concentrateur VPN 3000 a authentifié l'utilisateur et le ou les groupes, il doit organiser les attributs qu'il a reçus. Le concentrateur VPN utilise les attributs dans cet ordre de préférence. Peu importe que l'authentification ait été effectuée en interne ou en externe :

1. **Attributs utilisateur** : ceux-ci ont préséance sur tous les autres.
2. **Attributs de groupe** : tous les attributs manquants des attributs Utilisateur sont remplis par les attributs Groupe. Tous ceux qui sont identiques sont remplacés par les attributs Utilisateur.
3. **Attributs de groupe de tunnels** - Tous les attributs manquants des attributs Utilisateur ou Groupe sont remplis par les attributs Groupe de tunnels. Tous ceux qui sont identiques sont remplacés par les attributs Utilisateur.
4. **Attributs de groupe de base** : tous les attributs manquants des attributs Utilisateur, Groupe ou Groupe de tunnels sont remplis par les attributs de groupe de base.

Informations connexes

- Page d'assistance des concentrateurs VPN Cisco 3000
- Cisco VPN Client Support Page
- Page d'assistance IPsec
- Page d'assistance RADIUS

- Demandes de commentaires (RFC)
- Support technique - Cisco Systems