Verrouillage des utilisateurs dans un groupe de concentrateurs VPN 3000 à l'aide d'un serveur RADIUS

Contenu

Introduction

Le concentrateur de Cisco VPN 3000 a la capacité de verrouiller des utilisateurs sur un groupe de concentrateur qui ignore le groupe que l'utilisateur a configuré dans le Cisco VPN 3000 Client. De cette façon, des restrictions d'accès peuvent être appliquées à de divers groupes configurés sur le concentrateur VPN avec l'assurance que les utilisateurs sont verrouillés dans ce groupe avec le serveur de RAYON.

Détails de ce document comment installer cette caractéristique sur le Cisco Secure ACS pour Windows et Cisco Secure pour UNIX (CSUnix).

La configuration sur le concentrateur VPN est semblable à une configuration standard. La capacité de verrouiller des utilisateurs sur un groupe défini sur le concentrateur VPN est activée en définissant un attribut de retour dans le profil d'utilisateur RADIUS. Cet attribut contient le nom de groupe de concentrateur VPN sur lequel l'administrateur que veut on verrouille l'utilisateur. Cet attribut est l'attribut de classe (attribut RADIUS numéro 25 IETF), et doit être retourné au concentrateur VPN dans ce format :

```
OU=groupname;
```

là où le *groupname* est le nom du groupe sur le concentrateur VPN ce l'utilisateur verrouille sur. *L'OU* doit être en majuscules, et il doit y a un point-virgule à l'extrémité.

Dans cet exemple, le logiciel de client VPN est distribué à tous les utilisateurs avec un profil de connexion existante utilisant un *nom de groupe de* « chacun » et de mot de passe « quelque

chose ». Chaque utilisateur a un nom d'utilisateur/mot de passe discret (dans cet exemple, le nom d'utilisateur/mot de passe est TEST/TEST). Quand le nom d'utilisateur est envoyé au serveur de RAYON, le serveur de RAYON envoie en bas des informations sur le *vrai groupe* que l'utilisateur doit être dedans. Dans l'exemple, c'est « filtergroup. »

Ce faisant, vous pouvez complètement contrôler l'affectation de groupe sur le serveur de RAYON transparent aux utilisateurs. Si le serveur de RAYON n'affecte pas un groupe à l'utilisateur, l'utilisateur reste dans le « chacun » groupe. Puisque le « chacun » groupe a les filtres très restrictifs, l'utilisateur ne peut passer aucun trafic. Si le serveur de RAYON affecte un groupe à l'utilisateur, l'utilisateur hérite des attributs, y compris le filtre moins-restrictif, particulier au groupe. Dans cet exemple, vous appliquez un filtre au groupe « filtergroup » sur le concentrateur VPN pour permettre tout le trafic.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

Remarque: Ceci a été également avec succès testé avec le concentrateur 4.1.7 ACS 3.3, VPN, et le client vpn 4.0.5.

- Version 4.0(1)Rel de gamme de concentrateurs de Cisco VPN 3000
- Version 4.0(1)Rel de Client VPN Cisco
- Cisco Secure ACS pour des versions 2.4 à 3.2 de Windows
- Cisco Secure pour des versions 2.3, 2.5, et 2.6 d'UNIX

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

Configurez le concentrateur de Cisco VPN 3000

Remarque: Cette configuration suppose que le concentrateur VPN est déjà installé avec des adresses IP, passerelle par défaut, des pools d'adresses, et ainsi de suite. L'utilisateur doit pouvoir authentifier localement avant la continuation. Si cela ne fonctionne pas, alors ces modifications ne fonctionneront pas.

1. Sous la **configuration** > le **système** > les **serveurs** > l'**authentification**, ajoutez l'adresse IP du

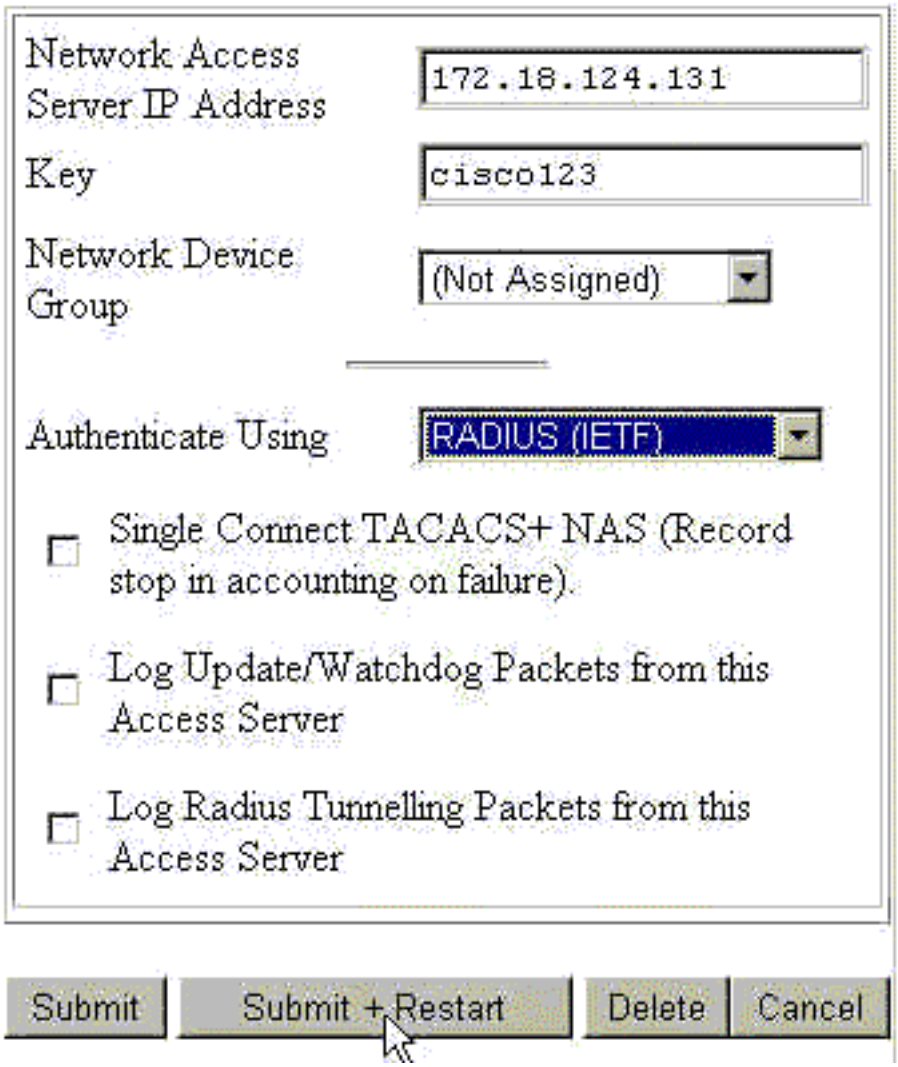
serveur de RAYON.
2. Une fois que vous avez ajouté le serveur, utilisez la touche "TEST" pour vérifier que vous pouvez authentifier l'utilisateur avec succès.Si ceci ne fonctionne pas, le verrouillage de groupe ne fonctionne pas.
3. Définissez un filtre que les baisses accèdent à tout dans le réseau interne.Ceci est appliqué pour grouper « chacun » de sorte que même si les utilisateurs peuvent authentifier dans ce groupe et rester dans lui, ils ne peuvent toujours pas accéder à n'importe quoi.
4. Selon la **configuration** > la **Gestion des stratégies** > la **gestion de trafic** > les **règles**, ajoutez une règle appelée **Drop All** et laissez tout aux par défaut.
5. Sous le **Configuration > Policy Management > Traffic Management > Filters**, créez un filtre appelé **Drop All**, laissez tout aux par défaut, et ajoutez la baisse toute la règle à elle.
6. Sous le **Configuration > User Management > Groups** ajoutez un groupe appelé **chacun**.C'est le groupe que tous les utilisateurs ont préconfiguré dans le client vpn. Ils authentifient dans ce groupe au commencement, et sont alors verrouillés dans un groupe différent après authentification de l'utilisateur. Définissez le groupe normalement. Veillez-vous pour ajouter la baisse tout le filtre (que vous avez juste créé) sous le général tableau afin d'utiliser l'authentification de RAYON pour des utilisateurs dans ce groupe, placez le type du groupe (sous l'onglet d'identité) pour être **interne** et l'authentification (sous l'onglet d'IPSec) au **RAYON**. Assurez-vous que la caractéristique de verrouillage de groupe n'est pas vérifiée ce groupe.**Remarque:** Même si vous ne définissez pas une baisse tout le filtre, assurez-vous qu'il y a au moins un filtre défini ici.
7. Définissez le groupe de destination final de l'utilisateur (l'exemple est « filtergroup »), appliquant un filtre.**Remarque:** Vous devez définir un filtre ici. Si vous ne voulez pas ne bloquer aucun trafic pour ces utilisateurs, en créez « permettent tout le » filtre et appliquent « dans » et « » ordonne à lui. Vous devez définir un filtre d'un certain aimable afin de passer le trafic. Afin d'utiliser l'authentification de RAYON pour des utilisateurs dans ce groupe, placez le type du groupe (sous l'onglet d'identité) pour être **interne** et l'authentification (sous l'onglet d'IPSec) au **RAYON**. Assurez-vous que la caractéristique de verrouillage de groupe n'est pas vérifiée ce groupe.

Configurez le serveur de RAYON

Cisco Secure ACS pour Windows

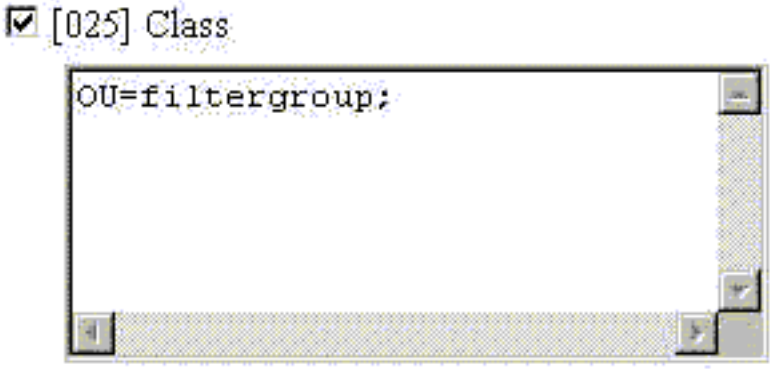
Ces étapes ont installé votre Cisco Secure ACS pour que le serveur de RAYON de Windows verrouille un utilisateur sur un groupe configuré particulier sur le concentrateur VPN. Maintenez dans l'esprit que les groupes définis sur le serveur de RAYON n'ont rien à faire avec des groupes définis sur le concentrateur VPN. Vous pouvez utiliser des groupes sur le serveur de RAYON pour faciliter la gestion de vos utilisateurs. Les noms ne doivent pas apparier ce qui est configuré sur le concentrateur VPN.

1. Ajoutez le concentrateur VPN comme serveur d'accès à distance (NAS) sur le serveur de RAYON sous la section de configuration réseau.Ajoutez l'adresse IP du concentrateur VPN dans la case d'adresse IP de NAS.Ajoutez la même clé que vous avez définie plus tôt sur le concentrateur VPN dans la case principale.De l'authentifier utilisant le menu déroulant, **RAYON** choisi **(IETF)**.Cliquez sur Submit **+**



reprise.

2. Sous la configuration d'interface, le **RAYON** choisi **(IETF)** et s'assurent que l'attribut **25 (classe)** est vérifié.Ceci te permet pour le changer dans le groupe/configuration utilisateur.
3. Ajoutez l'utilisateur.Dans cet exemple, l'utilisateur s'appelle le « TEST. » Cet utilisateur peut être dans n'importe quel Cisco Secure ACS pour le groupe de Windows. Autre que le dépassement en bas de l'attribut 25 pour dire au concentrateur VPN quel groupe utiliser pour l'utilisateur, là n'est aucune corrélation entre le Cisco Secure ACS pour des groupes de Windows et des groupes de concentrateur VPN. Cet utilisateur est placé dans "Group_1."
4. Sous le Group Setup, éditez les configurations sur le groupe (dans notre exemple, c'est "Group_1").
5. Cliquez sur le bouton vert de **RAYON IETF** pour vous porter aux attributs appropriés.
6. Faites descendre l'écran et modifiez l'attribut 25.
7. Ajoutez l'attribut comme affiché ici. Substituez le nom de groupe que vous voulez verrouiller les utilisateurs sur pour le filtergroup.Assurez-vous que l'OU est en majuscules et c'il y a un point-virgule après le nom de



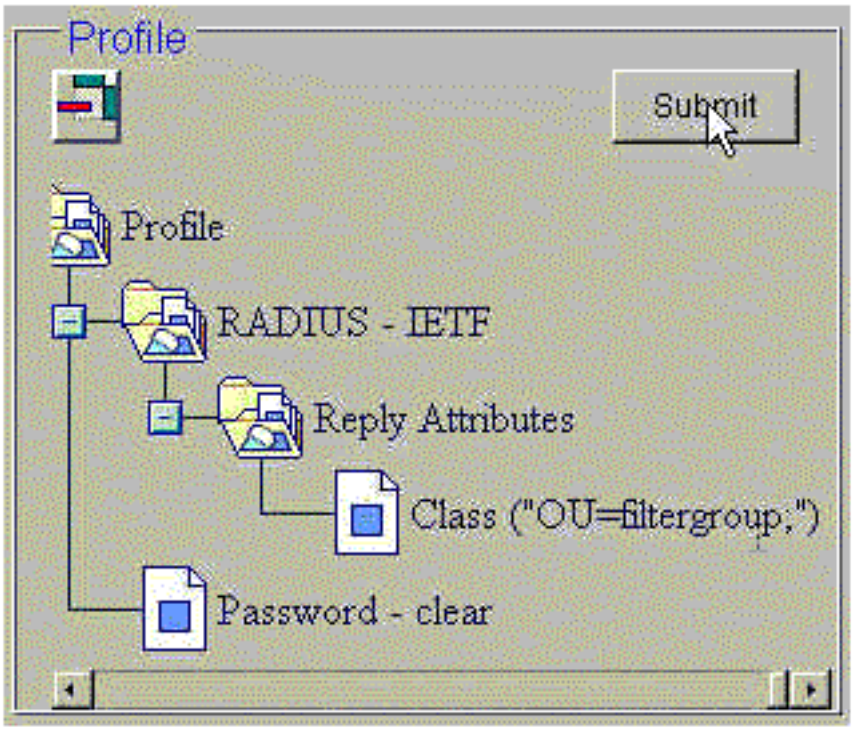
groupe.

8. Cliquez sur Submit **+ reprise**.

Cisco Secure pour l'UNIX

Ces étapes ont installé votre serveur de RAYON de Cisco Secure UNIX pour verrouiller un utilisateur sur un groupe configuré particulier sur le concentrateur VPN. Maintenez dans l'esprit que les groupes définis sur le serveur de RAYON n'ont rien à faire avec des groupes définis sur le concentrateur VPN. Vous pouvez utiliser des groupes sur le serveur de RAYON pour faciliter la gestion de vos utilisateurs. Les noms ne doivent pas apparier ce qui est configuré sur le concentrateur VPN.

1. Ajoutez le concentrateur VPN dedans en tant que NAS sur le serveur de RAYON sous la section avancée.Choisissez un dictionnaire qui permet l'attribut 25 à envoyer comme réponse-attribut. Par exemple, IETF ou Ascend.
2. Ajoutez l'utilisateur.Dans cet exemple, l'utilisateur est « TEST. » Cet utilisateur peut être dans n'importe quel groupe de Cisco Secure UNIX ou aucun groupe. Autre que le dépassement en bas de l'attribut 25 pour dire au concentrateur VPN quel groupe utiliser pour l'utilisateur, là n'est aucune corrélation entre les groupes de Cisco Secure UNIX et les groupes de concentrateur VPN.
3. Sous le profil d'utilisateur/groupe, définissez un attribut de retour du RAYON (IETF).
4. Ajoutez l'attribut de classe, attribuez le numéro **25**, et faites sa valeur **OU=filtergroup ;**. Substituez le groupe défini sur le concentrateur VPN au filtergroup.**Remarque:** Dans Cisco Secure UNIX, définissez l'attribut entouré par des guillemets. Ils sont éliminés outre de quand l'attribut est envoyé au concentrateur VPN. Le profil d'utilisateur/groupe devrait sembler semblable à



ceci.

5. Cliquez sur Submit pour sauvegarder chaque entrée.Les entrées de finition de Cisco Secure UNIX ressemblent à cette sortie :`# ./ViewProfile -p 9900 -u NAS.172.18.124.132`

```
User Profile Information
user = NAS.172.18.124.132{
profile_id = 68
profile_cycle = 1
NASNAME="172.18.124.132"
SharedSecret="cisco"
RadiusVendor="IETF"
Dictionary="DICTIONARY.IETF"

}

# ./ViewProfile -p 9900 -u TEST
User Profile Information
user = TEST{
profile_id = 70
set server current-failed-logins = 0
profile_cycle = 3
password = clear "********"
radius=IETF {
check_items= {
2="TEST"
}
reply_attributes= {
25="OU=filtergroup"
 !--- The semi-colon does NOT appear !--- after the group name, even though it has to be
included !--- when it defines the attribute via the GUI. } } } # ./ViewProfile -p 9900 -u
filtergroup User Profile Information user = filtergroup{ profile_id = 80 profile_cycle = 1
radius=IETF { check_items= { 2="filtergroup" } } } # ./ViewProfile -p 9900 -u Everyone User
Profile Information user = Everyone{ profile_id = 67 profile_cycle = 1 radius=IETF {
check_items= { 2="Anything" } } }
```

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Attribut d'utilisateur et de groupe de Cisco VPN 3000 Client traitant sur le concentrateur VPN 3000
- Page de support technologique de RAYON (Remote Authentication Dial-In User Service)
- Pages de support de Concentrateurs de la gamme Cisco VPN 3000
- Pages de support de Cisco VPN 3000 Client
- Pages de support produit de protocole de sécurité IP (IPSec)
- Demandes de commentaires (RFC)
- Cisco Secure ACS pour la page de support produit de Windows
- Notes de terrain en Produits de Sécurité
- Cisco Secure ACS pour la page de support produit Unix
- Support technique - Cisco Systems