Sperren von Benutzern in eine VPN 300-Concentrator-Gruppe mithilfe eines RADIUS-Servers

Inhalt

Einführung

Der Cisco VPN 3000 Concentrator kann Benutzer in eine Concentrator-Gruppe sperren, die die Gruppe überschreibt, die der Benutzer im Cisco VPN 3000-Client konfiguriert hat. Auf diese Weise können Zugriffsbeschränkungen auf verschiedene Gruppen angewendet werden, die im VPN Concentrator konfiguriert sind, mit der Garantie, dass die Benutzer mit dem RADIUS-Server in diese Gruppe eingebunden sind.

Dieses Dokument beschreibt die Einrichtung dieser Funktion auf Cisco Secure ACS für Windows und Cisco Secure für UNIX (CSUnix).

Die Konfiguration auf dem VPN Concentrator ähnelt einer Standardkonfiguration. Die Möglichkeit, Benutzer in einer im VPN Concentrator definierten Gruppe zu sperren, wird durch die Definition eines Rückgabeattributs im RADIUS-Benutzerprofil aktiviert. Dieses Attribut enthält den Gruppennamen des VPN-Konzentrators, in den der Administrator den Benutzer sperren möchte. Dieses Attribut ist das Class-Attribut (IETF RADIUS-Attributnummer 25) und muss in folgendem Format an den VPN-Konzentrator zurückgegeben werden:

```
OU=groupname;
```

wobei *groupname* der Name der Gruppe im VPN-Concentrator ist, der der Benutzer sperrt. *OU* muss in Großbuchstaben sein, und am Ende muss ein Semikolon vorhanden sein.

In diesem Beispiel wird die VPN-Client-Software an alle Benutzer mit einem bestehenden

Verbindungsprofil verteilt. Dabei wird ein *Gruppenname* "Everyone" und das Passwort "Anything" verwendet. Jeder Benutzer hat einen eigenen Benutzernamen/ein eigenes Kennwort (in diesem Beispiel ist der Benutzername/das Kennwort TEST/TEST). Wenn der Benutzername an den RADIUS-Server gesendet wird, sendet der RADIUS-Server Informationen über die *tatsächliche Gruppe*, in der sich der Benutzer befinden soll. Im Beispiel ist es "filtergroup".

Dadurch können Sie die Gruppenzuweisung auf dem RADIUS-Server vollständig und für die Benutzer transparent steuern. Wenn der RADIUS-Server dem Benutzer keine Gruppe zuweist, bleibt der Benutzer in der Gruppe "Jeder". Da die Gruppe "Jeder" sehr restriktive Filter hat, kann der Benutzer keinen Datenverkehr weiterleiten. Weist der RADIUS-Server dem Benutzer eine Gruppe zu, erbt der Benutzer die Attribute, einschließlich des weniger restriktiven Filters, insbesondere für die Gruppe. In diesem Beispiel wenden Sie einen Filter auf die Gruppe "Filtergruppe" des VPN-Konzentrators an, um den gesamten Datenverkehr zuzulassen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

Hinweis: Dies wurde auch mit ACS 3.3, VPN Concentrator 4.1.7 und VPN Client 4.0.5 erfolgreich getestet.

- Cisco VPN Concentrator der Serie 300, Version 4.0(1)Rel
- Cisco VPN Client Version 4.0(1)Rel
- Cisco Secure ACS für Windows 2.4 bis 3.2
- Cisco Secure für UNIX 2.3, 2.5 und 2.6

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions.

Konfigurieren des Cisco VPN 3000 Concentrator

Hinweis: Bei dieser Konfiguration wird davon ausgegangen, dass der VPN Concentrator bereits über IP-Adressen, Standard-Gateway, Adresspools usw. eingerichtet ist. Der Benutzer muss sich vor dem Fortfahren lokal authentifizieren können. Wenn das nicht funktioniert, werden diese Änderungen nicht funktionieren.

1. Fügen Sie unter **Configuration > System > Servers > Authentication** (Konfiguration **> System > Server > Authentifizierung**) die IP-Adresse des RADIUS-Servers hinzu.
2. Nachdem Sie den Server hinzugefügt haben, können Sie mithilfe der **Test-**Schaltfläche überprüfen, ob Sie den Benutzer erfolgreich authentifizieren können.Wenn dies nicht funktioniert, funktioniert die Gruppensperre nicht.
3. Definieren Sie einen Filter, der den Zugriff auf alles im internen Netzwerk blockiert.Dies wird auf die Gruppe "Jeder" angewendet, sodass selbst wenn sich die Benutzer bei dieser Gruppe authentifizieren und in dieser bleiben können, sie immer noch nicht auf irgendetwas zugreifen können.
4. Fügen Sie unter **Konfiguration > Richtlinienmanagement > Datenverkehrsverwaltung > Regeln** eine Regel namens **Alle löschen hinzu, und belassen Sie alle Standardeinstellungen.**
5. Erstellen Sie unter **Konfiguration > Richtlinienmanagement > Datenverkehrsverwaltung > Filter** einen Filter namens **Alle löschen, übernehmen Sie alle Standardeinstellungen, und fügen Sie der Regel Alle löschen hinzu.**
6. Fügen Sie unter **Konfiguration > Benutzerverwaltung > Gruppen** die Gruppe **Jeder hinzu**.Dies ist die Gruppe, die alle Benutzer im VPN-Client vorkonfiguriert haben. Sie authentifizieren sich zunächst bei dieser Gruppe und sind dann nach der Benutzerauthentifizierung in eine andere Gruppe gesperrt. Definieren Sie die Gruppe normal. Stellen Sie sicher, dass Sie den Filter Alle löschen (den Sie gerade erstellt haben) auf der Registerkarte Allgemein hinzufügen. Um die RADIUS-Authentifizierung für Benutzer in dieser Gruppe zu verwenden, legen Sie für den Gruppentyp (unter der Registerkarte Identität) **Interne** und für die Authentifizierung (unter der Registerkarte IPSec) **RADIUS** fest. Stellen Sie sicher, dass die Gruppensperrfunktion nicht für diese Gruppe aktiviert ist.**Hinweis:** Auch wenn Sie keinen Filter für "Alle löschen" definieren, stellen Sie sicher, dass mindestens ein Filter definiert ist.
7. Definieren Sie die ultimative Zielgruppe des Benutzers (das Beispiel ist "Filtergruppe"), und wenden Sie einen Filter an.**Hinweis:** Sie müssen hier einen Filter definieren. Wenn Sie keinen Datenverkehr für diese Benutzer blockieren möchten, erstellen Sie einen Filter "Alle zulassen", und wenden Sie die Regeln "Alle Ein" und "Beliebig" an. Sie müssen einen Filter definieren, um Datenverkehr zu übergeben. Um die RADIUS-Authentifizierung für Benutzer in dieser Gruppe zu verwenden, legen Sie für den Gruppentyp (unter der Registerkarte Identität) **Interne** und für die Authentifizierung (unter der Registerkarte IPSec) **RADIUS** fest. Stellen Sie sicher, dass die Gruppensperrfunktion nicht für diese Gruppe aktiviert ist.

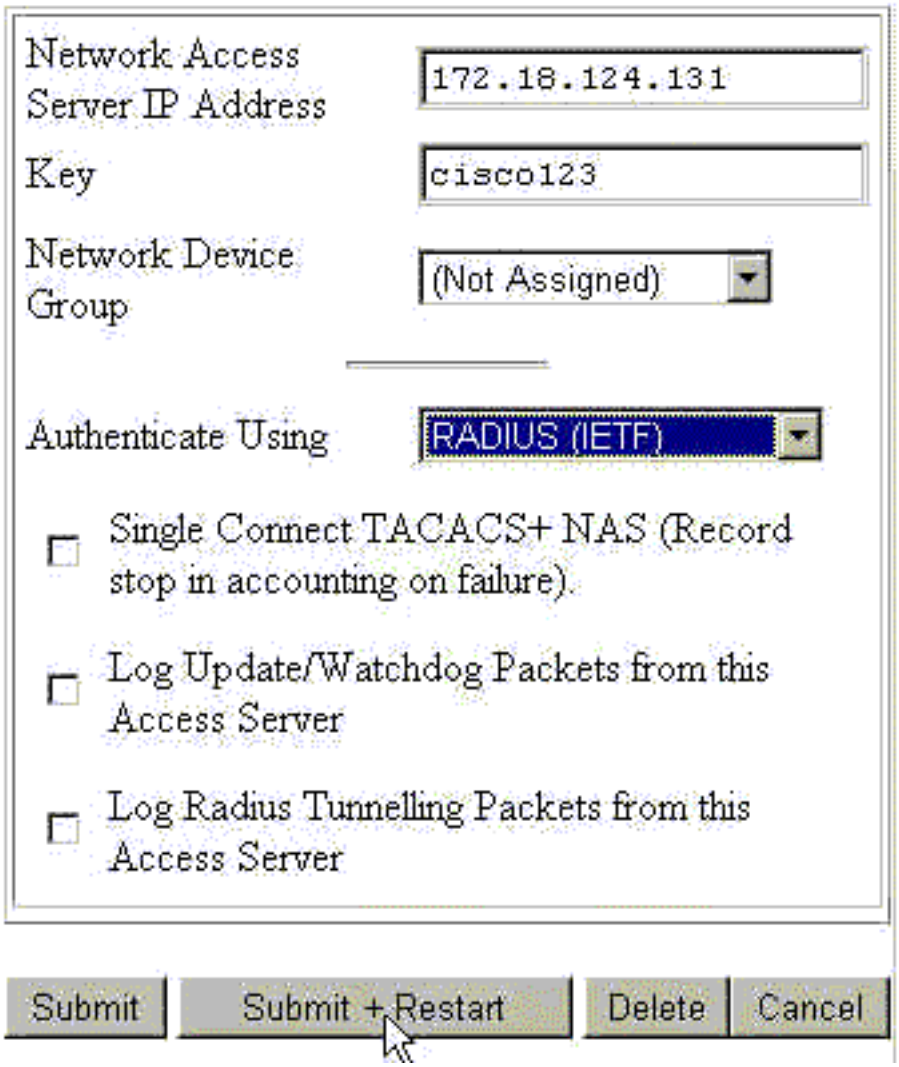
Konfigurieren des RADIUS-Servers

Cisco Secure ACS für Windows

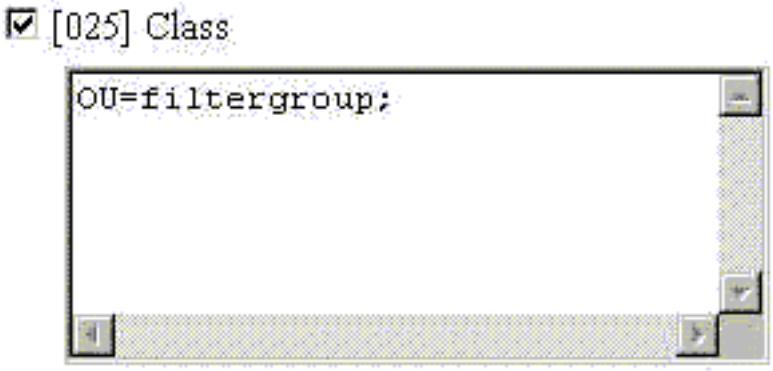
Mit diesen Schritten wird Ihr Cisco Secure ACS für Windows RADIUS-Server eingerichtet, um einen Benutzer in einer bestimmten Gruppe zu sperren, die auf dem VPN Concentrator konfiguriert ist. Beachten Sie, dass auf dem RADIUS-Server definierte Gruppen nichts mit im VPN-Konzentrator definierten Gruppen zu tun haben. Sie können Gruppen auf dem RADIUS-Server verwenden, um die Administration Ihrer Benutzer zu vereinfachen. Die Namen müssen nicht mit den im VPN Concentrator konfigurierten Namen übereinstimmen.

1. Fügen Sie den VPN Concentrator als Network Access Server (NAS) auf dem RADIUS-Server unter dem Abschnitt Network Configuration (Netzwerkkonfiguration) hinzu.Fügen Sie die IP-Adresse des VPN Concentrator im Feld "NAS IP Address" (NAS-IP-Adresse) hinzu.Fügen Sie im Feld Schlüssel den gleichen Schlüssel hinzu, den Sie zuvor im VPN-

Konzentrator definiert haben.Wählen Sie im Dropdown-Menü Authenticate Using (Authentifizierung über Verwendung) die Option **RADIUS (IETF)** aus.Klicken Sie auf **Senden + Neu starten**.



2. Wählen Sie unter Schnittstellenkonfiguration **RADIUS (IETF)** aus, und stellen Sie sicher, dass das Attribut **25 (Class)** aktiviert ist.Auf diese Weise können Sie sie in der Gruppen-/Benutzerkonfiguration ändern.
3. Fügen Sie den Benutzer hinzu.In diesem Beispiel wird der Benutzer als "TEST" bezeichnet. Dieser Benutzer kann sich in einer beliebigen Cisco Secure ACS für Windows-Gruppe befinden. Abgesehen von der Weitergabe des Attributs 25, um dem VPN Concentrator mitzuteilen, welche Gruppe der Benutzer verwenden soll, besteht keine Korrelation zwischen Cisco Secure ACS für Windows-Gruppen und VPN Concentrator-Gruppen. Dieser Benutzer wird in "Gruppe_1" abgelegt.
4. Bearbeiten Sie unter "Gruppeneinrichtung" die Einstellungen für die Gruppe (in unserem Beispiel lautet dies "Gruppe_1").
5. Klicken Sie auf die grüne **IETF RADIUS-**Schaltfläche, um die entsprechenden Attribute anzuzeigen.
6. Blättern Sie nach unten, und ändern Sie das Attribut 25.
7. Fügen Sie das Attribut wie hier gezeigt hinzu. Ersetzen Sie den Gruppennamen, in dem Sie die Benutzer für die Filtergruppe sperren möchten.Stellen Sie sicher, dass OU in Großbuchstaben angegeben ist und dass ein Semikolon nach dem Gruppennamen



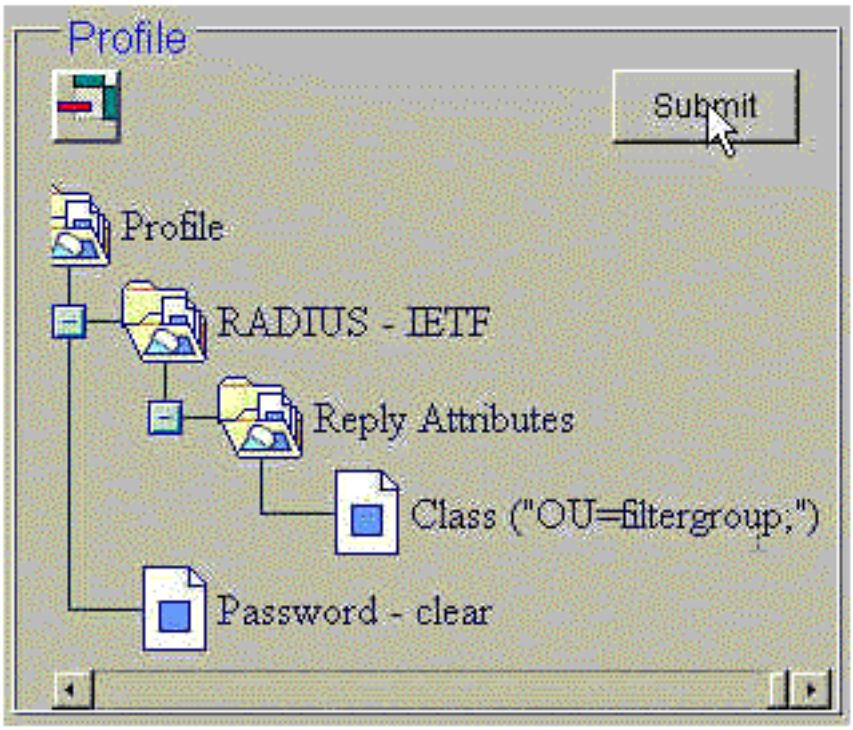
vorhanden ist.

8. Klicken Sie auf **Senden + Neu starten**.

Cisco Secure für UNIX

Mit diesen Schritten wird Ihr Cisco Secure UNIX RADIUS-Server eingerichtet, um einen Benutzer in einer bestimmten Gruppe zu sperren, die im VPN Concentrator konfiguriert wurde. Beachten Sie, dass auf dem RADIUS-Server definierte Gruppen nichts mit im VPN-Konzentrator definierten Gruppen zu tun haben. Sie können Gruppen auf dem RADIUS-Server verwenden, um die Administration Ihrer Benutzer zu vereinfachen. Die Namen müssen nicht mit den im VPN Concentrator konfigurierten Namen übereinstimmen.

1. Fügen Sie den VPN Concentrator als NAS auf dem RADIUS-Server unter dem Abschnitt "Erweitert" hinzu.Wählen Sie ein Wörterbuch aus, das das Senden des Attributs 25 als Antwortattribut zulässt. Zum Beispiel IETF oder Ascend.
2. Fügen Sie den Benutzer hinzu.In diesem Beispiel lautet der Benutzer "TEST". Dieser Benutzer kann einer beliebigen Cisco Secure UNIX-Gruppe oder keiner Gruppe angehören. Abgesehen von der Weitergabe des Attributs 25, um dem VPN Concentrator mitzuteilen, welche Gruppe der Benutzer verwenden soll, besteht keine Korrelation zwischen Cisco Secure UNIX-Gruppen und VPN Concentrator-Gruppen.
3. Definieren Sie unter dem Benutzer-/Gruppenprofil ein RADIUS (IETF)-Rückgabeattribut.
4. Fügen Sie das Class-Attribut, die Attributnummer **25 hinzu**, und geben Sie den Wert **OU=filtergruppe;**. Ersetzen Sie die im VPN-Konzentrator definierte Gruppe durch die Filtergruppe.**Hinweis:** Definieren Sie in Cisco Secure UNIX das Attribut, das von Anführungszeichen umgeben ist. Sie werden entfernt, wenn das Attribut an den VPN-Konzentrator gesendet wird. Das Benutzer-/Gruppenprofil sollte ähnlich



aussehen.

5. Klicken Sie auf **Senden**, um jeden Eintrag zu speichern.Die fertigen Cisco Secure UNIX-Einträge erscheinen ähnlich der folgenden Ausgabe:

```
# ./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" } } }
```

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Cisco VPN 3000 Client Benutzer- und Gruppenattribut-Verarbeitung im VPN 3000-Concentrator
- Technologieunterstützung für RADIUS (Remote Authentication Dial-In User Service)
- Cisco VPN Concentrators der Serie 3000 - Support-Seiten
- Cisco VPN 3000 Client - Support-Seiten
- Support-Seiten für IP Security Protocol (IPSec)
- Anforderungen für Kommentare (RFCs)
- Support-Seite für Cisco Secure ACS für Windows-Produkte
- Problemhinweise zu Security-Produkten
- Support-Seite für Cisco Secure ACS für UNIX-Produkte
- Technischer Support - Cisco Systems