Blocco degli utenti in un gruppo di concentratori VPN 3000 tramite un server RADIUS

Sommario

Introduzione

Cisco VPN 3000 Concentrator può bloccare gli utenti in un gruppo Concentrator che ignora il gruppo configurato dall'utente nel client Cisco VPN 3000. In questo modo, le restrizioni di accesso possono essere applicate a vari gruppi configurati sul concentratore VPN con la garanzia che gli utenti siano bloccati in quel gruppo con il server RADIUS.

In questo documento viene descritto come configurare questa funzione su Cisco Secure ACS per Windows e Cisco Secure per UNIX (CSUnix).

La configurazione di VPN Concentrator è simile a una configurazione standard. La possibilità di bloccare gli utenti in un gruppo definito in VPN Concentrator è abilitata definendo un attributo restituito nel profilo utente RADIUS. Questo attributo contiene il nome del gruppo VPN Concentrator a cui l'amministratore desidera bloccare l'utente. Questo attributo è l'attributo Class (IETF RADIUS numero attributo 25) e deve essere restituito al concentratore VPN nel seguente formato:

```
OU=groupname;
```

dove *groupname* è il nome del gruppo nel concentratore VPN a cui l'utente si blocca. *L'unità organizzativa* deve essere in maiuscolo e alla fine deve essere presente un punto e virgola.

In questo esempio, il software VPN Client viene distribuito a tutti gli utenti con un profilo di connessione esistente utilizzando un *nome* di *gruppo* "Everyone" e una password "Anything". Ogni utente dispone di un nome utente/password discreto (in questo esempio, il nome utente/password è TEST/TEST). Quando il nome dell'utente viene inviato al server RADIUS, il

server RADIUS invia informazioni sul *gruppo reale* in cui l'utente deve trovarsi. Nell'esempio, questo valore è "filtergroup".

In questo modo è possibile controllare completamente l'assegnazione dei gruppi sul server RADIUS in modo trasparente per gli utenti. Se il server RADIUS non assegna un gruppo all'utente, quest'ultimo rimane nel gruppo Everyone. Poiché il gruppo "Everyone" dispone di filtri molto restrittivi, l'utente non può passare alcun traffico. Se il server RADIUS non assegna un gruppo all'utente, questi eredita gli attributi, incluso il filtro meno restrittivo, specifici del gruppo. Nell'esempio, viene applicato un filtro al gruppo "filtergroup" su VPN Concentrator per consentire tutto il traffico.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

Nota: anche questo software è stato testato con ACS 3.3, VPN Concentrator 4.1.7 e VPN Client 4.0.5.

- Cisco VPN serie 3000 Concentrator versione 4.0(1)Rel
- Cisco VPN Client versione 4.0(1)Rel
- Cisco Secure ACS per Windows versioni da 2.4 a 3.2
- Cisco Secure per UNIX versioni 2.3, 2.5 e 2.6

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Configurazione di Cisco VPN 3000 Concentrator

Nota: in questa configurazione si presume che il concentratore VPN sia già configurato con indirizzi IP, gateway predefinito, pool di indirizzi e così via. L'utente deve essere in grado di eseguire l'autenticazione localmente prima di continuare. Se non funziona, le modifiche non funzioneranno.

1. In **Configurazione > Sistema > Server > Autenticazione**, aggiungere l'indirizzo IP del server RADIUS.
2. Dopo aver aggiunto il server, utilizzare il pulsante **Test** per verificare che sia possibile

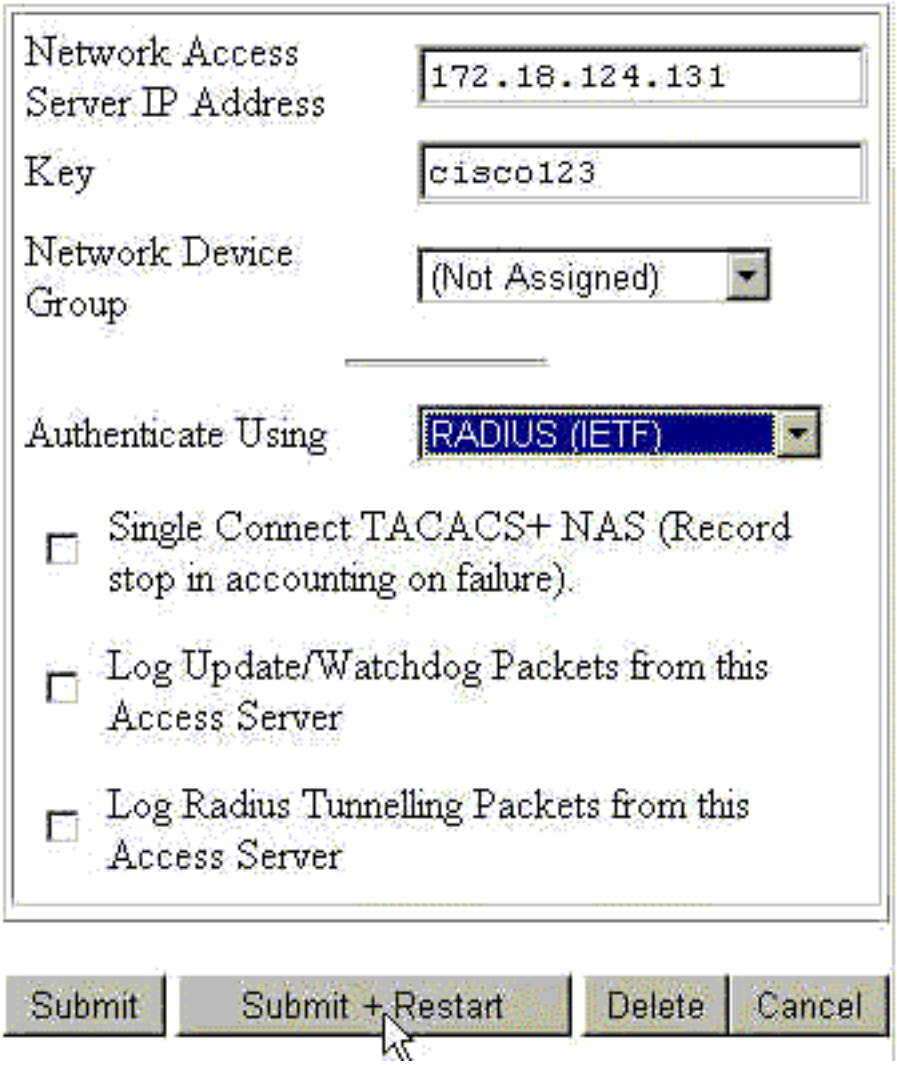
autenticare correttamente l'utente.Se l'operazione non riesce, il blocco del gruppo non funziona.
3. Definire un filtro che elimina l'accesso a tutti gli elementi della rete interna.Questo viene applicato al gruppo "Everyone" in modo che, anche se gli utenti possono autenticarsi in questo gruppo e rimanere in esso, non sono comunque in grado di accedere a nulla.
4. In Configurazione > **Gestione criteri** > **Gestione traffico** > **Regole**, aggiungere una regola denominata **Elimina tutto** e lasciare tutti i valori predefiniti.
5. In Configurazione > **Gestione criteri** > **Gestione traffico** > **Filtri**, creare un filtro denominato **Elimina tutto**, mantenere i valori predefiniti e aggiungere la regola Elimina tutto.
6. In **Configurazione** > **Gestione utente** > **Gruppi** aggiungere un gruppo denominato **Everyone**.Questo è il gruppo che tutti gli utenti hanno preconfigurato nel client VPN. Inizialmente vengono autenticati in questo gruppo e quindi bloccati in un gruppo diverso dopo l'autenticazione dell'utente. Definite il gruppo normalmente. Assicurarsi di aggiungere il filtro Elimina tutto (appena creato) nella scheda Generale. Per utilizzare l'autenticazione RADIUS per gli utenti di questo gruppo, impostare il Tipo del gruppo (nella scheda Identità) su **Interno** e Autenticazione (nella scheda IPSec) su **RADIUS**. Assicurarsi che la funzione Blocco gruppo non sia selezionata per questo gruppo.**Nota:** anche se non si definisce un filtro Elimina tutto, verificare che sia definito almeno un filtro.
7. Definire il gruppo di destinazione finale dell'utente (l'esempio è "filtergroup"), applicando un filtro.**Nota:** è necessario definire un filtro. Se non si desidera bloccare il traffico per questi utenti, creare un filtro "Consenti tutto" e applicarvi le regole "Qualsiasi entrata" e "Qualsiasi uscita". È necessario definire un filtro per poter passare il traffico. Per utilizzare l'autenticazione RADIUS per gli utenti di questo gruppo, impostare il Tipo del gruppo (nella scheda Identità) su **Interno** e Autenticazione (nella scheda IPSec) su **RADIUS**. Assicurarsi che la funzione Blocco gruppo non sia selezionata per questo gruppo.

Configurazione del server RADIUS

Cisco Secure ACS per Windows

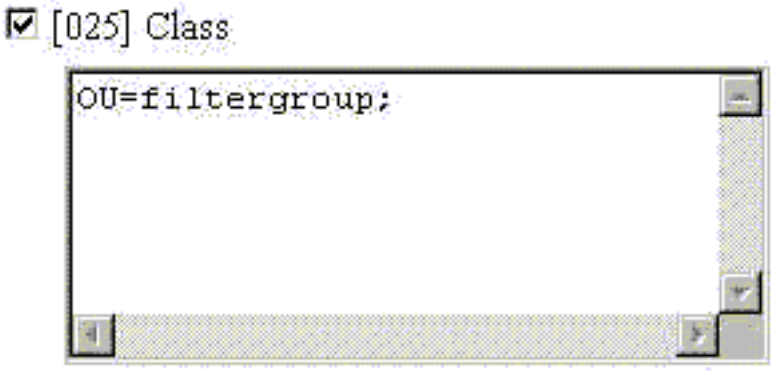
In questa procedura viene descritto come configurare il server Cisco Secure ACS per Windows RADIUS in modo da bloccare un utente in un particolare gruppo configurato nel concentratore VPN. I gruppi definiti nel server RADIUS non hanno nulla a che fare con i gruppi definiti nel concentratore VPN. È possibile utilizzare i gruppi nel server RADIUS per semplificare l'amministrazione degli utenti. I nomi non devono corrispondere a quelli configurati nel concentratore VPN.

1. Aggiungere il concentratore VPN come server di accesso alla rete (NAS) sul server RADIUS nella sezione Configurazione di rete.Aggiungere l'indirizzo IP del concentratore VPN nella casella Indirizzo IP NAS.Aggiungere la stessa chiave definita in precedenza nel concentratore VPN nella casella Chiave.Dal menu a discesa Autentica con, selezionare **RADIUS (IETF)**.Fare clic su **Invia +**



Riavvia.

2. In Configurazione interfaccia selezionare **RADIUS (IETF)** e assicurarsi che l'attributo **25 (Classe)** sia selezionato.In questo modo, è possibile modificarla nella configurazione gruppo/utente.
3. Aggiungere l'utente.In questo esempio, l'utente è denominato "TEST". Questo utente può essere incluso in qualsiasi gruppo Cisco Secure ACS for Windows. A parte il passaggio dell'attributo 25 per indicare a VPN Concentrator quale gruppo utilizzare per l'utente, non esiste correlazione tra Cisco Secure ACS per gruppi Windows e gruppi VPN Concentrator. L'utente è posizionato in "Group_1".
4. In Configurazione gruppo modificare le impostazioni del gruppo (nell'esempio riportato è "Gruppo_1").
5. Fare clic sul pulsante verde **IETF RADIUS** per visualizzare gli attributi appropriati.
6. Scorrere verso il basso e modificare l'attributo 25.
7. Aggiungere l'attributo come illustrato di seguito. Sostituire il nome del gruppo in cui si desidera bloccare gli utenti per il filtergroup.Assicurarsi che il nome dell'unità organizzativa sia in lettere maiuscole e che dopo il nome del gruppo sia presente un punto e



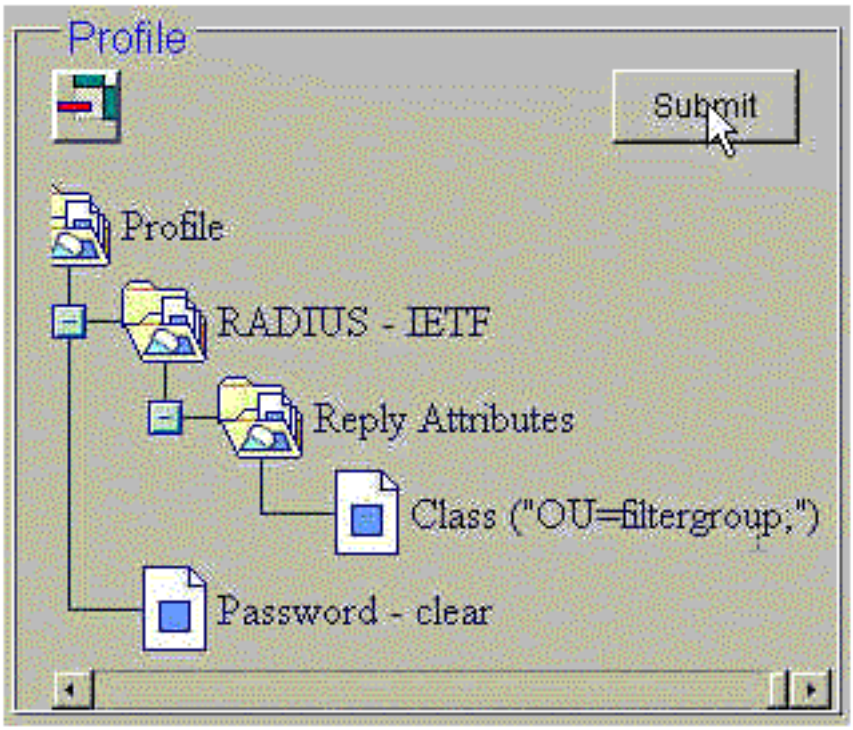
virgola.

8. Fare clic su **Invia + Riavvia**.

Cisco Secure per UNIX

Questa procedura consente di configurare il server RADIUS Cisco Secure UNIX per bloccare un utente in un particolare gruppo configurato sul concentratore VPN. I gruppi definiti nel server RADIUS non hanno nulla a che fare con i gruppi definiti nel concentratore VPN. È possibile utilizzare i gruppi nel server RADIUS per semplificare l'amministrazione degli utenti. I nomi non devono corrispondere a quelli configurati nel concentratore VPN.

1. Aggiungere VPN Concentrator come NAS sul server RADIUS nella sezione Advanced.Scegliere un dizionario che consenta l'invio dell'attributo 25 come attributo di risposta. Ad esempio, IETF o Ascend.
2. Aggiungere l'utente.In questo esempio, l'utente è "TEST". L'utente può appartenere a qualsiasi gruppo Cisco Secure UNIX o a nessun gruppo. A parte il passaggio dell'attributo 25 per indicare a VPN Concentrator quale gruppo utilizzare per l'utente, non esiste correlazione tra i gruppi Cisco Secure UNIX e i gruppi VPN Concentrator.
3. Nel profilo utente/gruppo definire un attributo restituito RADIUS (IETF).
4. Aggiungere l'attributo Class, numero attributo **25**, e rendere il relativo valore **OU=filtergroup;**. Sostituire il gruppo definito in VPN Concentrator con filtergroup.**Nota:** in Cisco Secure UNIX definire l'attributo racchiuso tra virgolette. Vengono eliminati quando l'attributo viene inviato al concentratore VPN. Il profilo utente/gruppo dovrebbe essere simile a



questo.

5. Fare clic su **Submit** (Invia) per salvare ciascuna voce.Le voci Cisco Secure UNIX completate sono simili all'output seguente:

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

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Cisco VPN 3000 Client User and Group Attribute Processing su VPN 3000 Concentrator
- Pagina di supporto per la tecnologia RADIUS (Remote Authentication Dial-In User Service)
- Pagine di supporto per Cisco VPN serie 3000 concentrator
- Pagine di supporto client Cisco VPN 3000
- Pagine di supporto dei prodotti IP Security Protocol (IPSec)
- RFC (Requests for Comments)
- Pagina di supporto dei prodotti Cisco Secure ACS per Windows
- Avvisi sui prodotti per la sicurezza
- Pagina di supporto dei prodotti Cisco Secure ACS per UNIX
- Supporto tecnico – Cisco Systems