Elaborazione degli attributi di utenti e gruppi di Cisco VPN Client sul concentratore VPN 3000

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Convenzioni
VPN Client si connette a un concentratore VPN 3000
Autenticazione esterna di gruppi e utenti tramite RADIUS
Utilizzo degli attributi di utenti e gruppi da parte di VPN 3000 Concentrator
Informazioni correlate

Introduzione

Questo documento descrive come i client VPN Cisco vengono autenticati su VPN Concentrator e come Cisco VPN 3000 Concentrator utilizza gli attributi User e Group.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco VPN 3000 Concentrator.

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.

VPN Client si connette a un concentratore VPN 3000

Quando un client VPN si connette a un concentratore VPN 3000, possono essere eseguite fino a quattro autenticazioni.

1. Il gruppo viene autenticato. (Questo gruppo viene spesso denominato "Gruppo di tunnel").
2. L'utente viene autenticato.
3. (Facoltativo) Se l'utente fa parte di un altro gruppo, il gruppo viene autenticato successivamente. Se l'utente non appartiene a un altro gruppo o al gruppo di tunnel, per impostazione predefinita viene utilizzato il gruppo base e questo passaggio NON viene eseguito.
4. Il "Gruppo di tunnel" del passo 1 viene autenticato di nuovo. (Questa operazione viene eseguita se viene utilizzata la funzione "Group Lock". Questa funzionalità è disponibile nella versione 2.1 o successiva.)

Questo è un esempio degli eventi visualizzati nel registro eventi per un client VPN autenticato tramite il database interno (testuser fa parte del gruppo "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
```

Nota: per visualizzare questi eventi, è necessario configurare la classe di evento Auth con la severità 1-6 in **Configurazione > Sistema > Eventi > Classi**.

Funzione Group Lock: se la funzione Group Lock è abilitata in Group - Tunnel_Group, l'utente deve far parte di Tunnel_Group per connettersi. Nell'esempio precedente vengono visualizzati tutti gli stessi eventi, ma "testuser" non si connette perché fanno parte di Group - Engineering e non di Group - Tunnel_Group. Verrà inoltre visualizzato questo evento:

```
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.
```

Per ulteriori informazioni sulla funzione Group Lock e per una configurazione di esempio, fare riferimento a Blocco di utenti in un gruppo di concentratori VPN 3000 tramite un server RADIUS.

Autenticazione esterna di gruppi e utenti tramite RADIUS

VPN 3000 Concentrator può anche essere configurato per autenticare utenti e gruppi esternamente tramite un server RADIUS. È comunque necessario configurare i nomi dei gruppi nel concentratore VPN, ma il tipo di gruppo è configurato come "Esterno".

- I gruppi esterni possono restituire gli attributi Cisco/Altiga se il server RADIUS supporta attributi specifici del fornitore (VSA).
- Tutti gli attributi Cisco/Altiga NON restituiti da RADIUS assumono i valori del gruppo base.
- Se il server RADIUS NON supporta le VSA, per impostazione predefinita verranno utilizzati gli attributi del gruppo base.

Nota: un server RADIUS tratta i nomi dei gruppi in modo analogo ai nomi degli utenti. Un gruppo su un server RADIUS è configurato come un utente standard.

In questa procedura viene descritto cosa succede quando un client IPSec si connette a VPN 3000 Concentrator se sia gli utenti che i gruppi vengono autenticati esternamente. Analogamente al caso interno, è possibile eseguire fino a quattro autenticazioni.

1. Il gruppo viene autenticato tramite RADIUS. Il server RADIUS può restituire molti attributi per il gruppo o nessuno. Il server RADIUS deve restituire almeno l'attributo Cisco/Altiga "IPSec Authentication = RADIUS" per indicare al concentratore VPN come autenticare l'utente. In caso contrario, il metodo di autenticazione IPSec del gruppo di base deve essere impostato su "RADIUS".
2. L'utente viene autenticato tramite RADIUS. Il server RADIUS può restituire molti attributi per l'utente o nessuno. Se il server RADIUS restituisce l'attributo CLASS (attributo RADIUS standard n. 25), il concentratore VPN 3000 utilizza tale attributo come nome del gruppo e passa al passaggio 3, altrimenti passa al passaggio 4.
3. Il gruppo dell'utente viene autenticato successivamente tramite RADIUS. Il server RADIUS può restituire molti attributi per il gruppo o nessuno.
4. Il "Gruppo di tunnel" della fase 1 viene autenticato nuovamente tramite RADIUS. Il sottosistema di autenticazione deve autenticare nuovamente il gruppo di tunnel perché non ha memorizzato gli attributi (se presenti) dell'autenticazione nel passo 1. Questa operazione viene eseguita nel caso in cui venga utilizzata la funzione "Blocco gruppo".

Utilizzo degli attributi di utenti e gruppi da parte di VPN 3000 Concentrator

Dopo aver autenticato l'utente e i gruppi, VPN 3000 Concentrator deve organizzare gli attributi ricevuti. VPN Concentrator utilizza gli attributi in questo ordine di preferenza. Non importa se l'autenticazione è stata eseguita internamente o esternamente:

1. **Attributi utente**: questi hanno la precedenza su tutti gli altri.
2. **Attributi gruppo** - Gli eventuali attributi mancanti negli attributi Utente vengono inseriti dagli attributi Gruppo. Gli attributi uguali vengono sostituiti dagli attributi User.
3. **Attributi del gruppo di tunnel**: tutti gli attributi mancanti dagli attributi Utente o Gruppo vengono inseriti dagli attributi Gruppo di tunnel. Gli attributi uguali vengono sostituiti dagli attributi User.
4. **Attributi del gruppo base**: tutti gli attributi mancanti dagli attributi Utente, Gruppo o Gruppo tunnel vengono inseriti dagli attributi Gruppo base.

Informazioni correlate

- Cisco VPN serie 3000 Concentrator Support Page
- Pagina di supporto per Cisco VPN Client
- Pagina di supporto per IPSec
- Pagina di supporto RADIUS
- RFC (Requests for Comments)
- Supporto tecnico – Cisco Systems