Procesamiento de atributo de grupo y usuario de Cisco VPN Client en el concentrador VPN 3000

Contenido

Introducción

Este documento describe cómo se autentican los Cisco VPN Clients en el VPN Concentrator y cómo el Cisco VPN 3000 Concentrator utiliza los atributos Usuario y Grupo.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en el Cisco VPN 3000 Concentrator.

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.

Convenciones

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

VPN Client se conecta a un concentrador VPN 3000

Cuando un cliente VPN se conecta a un concentrador VPN 3000, pueden realizarse hasta cuatro

autenticaciones.

1. El grupo está autenticado. (Esto se denomina a menudo "Grupo de Túnel").
2. El usuario está autenticado.
3. (Opcional) Si el Usuario forma parte de otro Grupo, este Grupo se autenticará a continuación. Si el usuario no pertenece a otro grupo o al grupo de túnel, el usuario tomará de forma predeterminada el grupo base y este paso NO se producirá.
4. El "Grupo de Túnel" del Paso 1 se autentica nuevamente. (Esto se hace en caso de que se utilice la función "Bloqueo de grupo". Esta función está disponible en la versión 2.1 o posterior.)

Este es un ejemplo de los eventos que se ven en el Registro de eventos para un cliente VPN autenticado a través de la base de datos interna ("testuser" forma parte del grupo "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: Para ver estos eventos, debe configurar la clase de evento de autenticación con gravedad 1-6 en **Configuración > Sistema > Eventos > Clases.**

Función de bloqueo de grupo: si la función de bloqueo de grupo está activada en Grupo - Grupo_de_túnel, el usuario debe formar parte de Grupo_de_túnel para conectarse. En el ejemplo anterior, verá todos los mismos eventos, pero "testuser" no se conecta porque forman parte del grupo - Ingeniería y no del grupo - Grupo_de_túnel. También puede ver este 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.
```

Para obtener información adicional sobre la función Bloqueo de grupo y una configuración de ejemplo, refiérase a Bloqueo de Usuarios en un Grupo de Concentradores VPN 3000 Usando un Servidor RADIUS.

Autenticar grupos y usuarios externamente a través de RADIUS

El concentrador VPN 3000 también se puede configurar para autenticar usuarios y grupos externamente a través de un servidor RADIUS. Esto aún requiere que los nombres de los grupos se configuren en el concentrador VPN, pero el tipo de grupo se configura como "Externo".

- Los grupos externos pueden devolver atributos de Cisco/Altiga si el servidor RADIUS admite atributos específicos del proveedor (VSA).
- Cualquier atributo de Cisco/Altiga NO devuelto por RADIUS de forma predeterminada a los valores del grupo base.
- Si el servidor RADIUS NO admite VSA, TODOS los atributos son predeterminados en los atributos del grupo base.

Nota: Un servidor RADIUS trata los nombres de grupo de forma no diferente a los nombres de usuario. Un grupo en un servidor RADIUS se configura igual que un usuario estándar.

Estos pasos describen lo que sucede cuando un cliente IPSec se conecta al concentrador VPN 3000 si tanto los usuarios como los grupos se autentican externamente. Al igual que en el caso interno, se pueden realizar hasta cuatro autenticaciones.

1. El grupo se autentica a través de RADIUS. El servidor RADIUS puede devolver muchos atributos para el grupo o ninguno en absoluto. Como mínimo, el servidor RADIUS necesita devolver el atributo de Cisco/Altiga "Autenticación IPSec = RADIUS" para decirle al concentrador VPN cómo autenticar al usuario. Si no es así, el método de autenticación IPSec del grupo base debe establecerse en "RADIUS".
2. El usuario se autentica a través de RADIUS. El servidor RADIUS puede devolver muchos atributos para el usuario o ninguno en absoluto. Si el servidor RADIUS devuelve el atributo CLASS (atributo RADIUS estándar #25), el concentrador VPN 3000 utiliza ese atributo como nombre de grupo y pasa al paso 3, o bien va al paso 4.
3. El grupo del usuario se autentica a continuación a través de RADIUS. El servidor RADIUS puede devolver muchos atributos para el grupo o ninguno en absoluto.
4. El "Grupo de Túnel" del Paso 1 se autentica nuevamente a través de RADIUS. El subsistema de autenticación debe autenticar al Grupo de Túnel de nuevo porque no ha almacenado los atributos (si los hubiera) de la autenticación en el Paso 1. Esto se hace en caso de que se utilice la función "Bloqueo de grupo".

Cómo el concentrador VPN 3000 utiliza atributos de usuario y de grupo

Después de que el VPN 3000 Concentrator haya autenticado al Usuario y a los Grupos, debe organizar los atributos que ha recibido. El concentrador VPN utiliza los atributos en este orden de preferencia. No importa si la autenticación se realizó interna o externamente:

1. **Atributos de usuario**: éstos tienen prioridad sobre todos los demás.
2. **Atributos de grupo**: los atributos de grupo rellenan todos los atributos que faltan en los atributos de usuario. Los atributos de usuario invalidan cualquier elemento que sea el mismo.
3. **Atributos del Grupo de Túnel**: los atributos del Grupo de Túnel rellenan todos los atributos que faltan en los atributos Usuario o Grupo. Los atributos de usuario invalidan cualquier elemento que sea el mismo.
4. **Atributos de grupo base**: los atributos de grupo base rellenan todos los atributos que faltan en los atributos Usuario, Grupo o Grupo de túnel.

Información Relacionada

- Página de soporte del concentrador de la serie Cisco VPN 3000
- Página de soporte para cliente Cisco VPN
- Página de soporte de IPSec
- Página de soporte de RADIUS
- Solicitudes de Comentarios (RFC)
- Soporte Técnico - Cisco Systems