Bloqueo de usuarios a un grupo concentrador VPN 3000 usando un servidor RADIUS.

Contenido

Introducción

El Cisco VPN 3000 Concentrator tiene la capacidad de bloquear a los usuarios en un grupo del concentrador que reemplace al grupo que el usuario ha configurado en el Cliente Cisco VPN 3000. De esta manera, las restricciones de acceso se pueden aplicar a los diversos grupos configurados en el concentrador VPN con la garantía que los usuarios son bloqueados en ese grupo con el servidor de RADIUS.

Detalles de este documento cómo configurar esta característica en el Cisco Secure ACS for Windows y Cisco seguro para UNIX (CSUnix).

La configuración en el concentrador VPN es similar a una configuración estándar. La capacidad de bloquear a los usuarios en un grupo definido en el concentrador VPN es habilitada definiendo un atributo de vuelta en el perfil del usuario de RADIUS. Este atributo contiene el nombre del grupo del concentrador VPN en el cual el administrador quisiera que el usuario fuera bloqueado. Este atributo es el atributo de clase (atributo IETF RADIUS número 25), y tiene que ser vuelto al concentrador VPN en este formato:

```
OU=groupname;
```

donde está el nombre el *nombre de grupo del* grupo en el concentrador VPN ese el usuario bloquea en. *El OU* tiene que estar con mayúsculas, y debe haber un punto y coma en el extremo.

En este ejemplo, el software cliente VPN se distribuye a todos los usuarios con un perfil de la conexión existente usando un *nombre del grupo* “todo el mundo” y de la contraseña “cualquier cosa”. Cada usuario tiene un nombre de usuario discreto/una contraseña (en este ejemplo, el

nombre de usuario/la contraseña es TEST/TEST). Cuando el nombre de usuario se envía al servidor de RADIUS, el servidor de RADIUS envía abajo de la información sobre el *grupo real* que el usuario debe estar adentro. En el ejemplo, es “filtergroup.”

De esta manera, usted puede controlar totalmente la asignación del grupo en el servidor de RADIUS transparente a los usuarios. Si el servidor de RADIUS no asigna a un grupo al usuario, el usuario sigue siendo en “todo el mundo” grupo. Puesto que “todo el mundo” grupo tiene mismo filtros restrictivos, el usuario no puede pasar ningún tráfico. Si el servidor de RADIUS asigna a un grupo al usuario, el usuario hereda los atributos, incluyendo el filtro menos-restrictivo, determinado al grupo. En este ejemplo, usted aplica un filtro al grupo “filtergroup” en el concentrador VPN para permitir todo el tráfico.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

Nota: Esto también fue probada con éxito con ACS 3.3, el concentrador VPN 4.1.7, y el cliente VPN 4.0.5.

- Versión 4.0(1)Rel del Cisco VPN 3000 Concentrator Series
- Cliente VPN de Cisco versión 4.0(1)Rel
- Versiones 2.4 a 3.2 del Cisco Secure ACS for Windows
- Cisco seguro para las versiones de UNIX 2.3, 2.5, y 2.6

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Configure el Cisco VPN 3000 Concentrator

Nota: Esta configuración asume que el concentrador VPN está configurado ya con los IP Addresses, default gateway, las agrupaciones de direcciones, y así sucesivamente. El usuario debe poder autenticar localmente antes de continuar. Si eso no trabaja, después estos cambios no trabajarán.

1. Bajo el **Configuration (Configuración) > Sytem (Sistema) > Servers (Servidores) > Authentication (Autenticación)**, agregue la dirección IP del servidor de RADIUS.

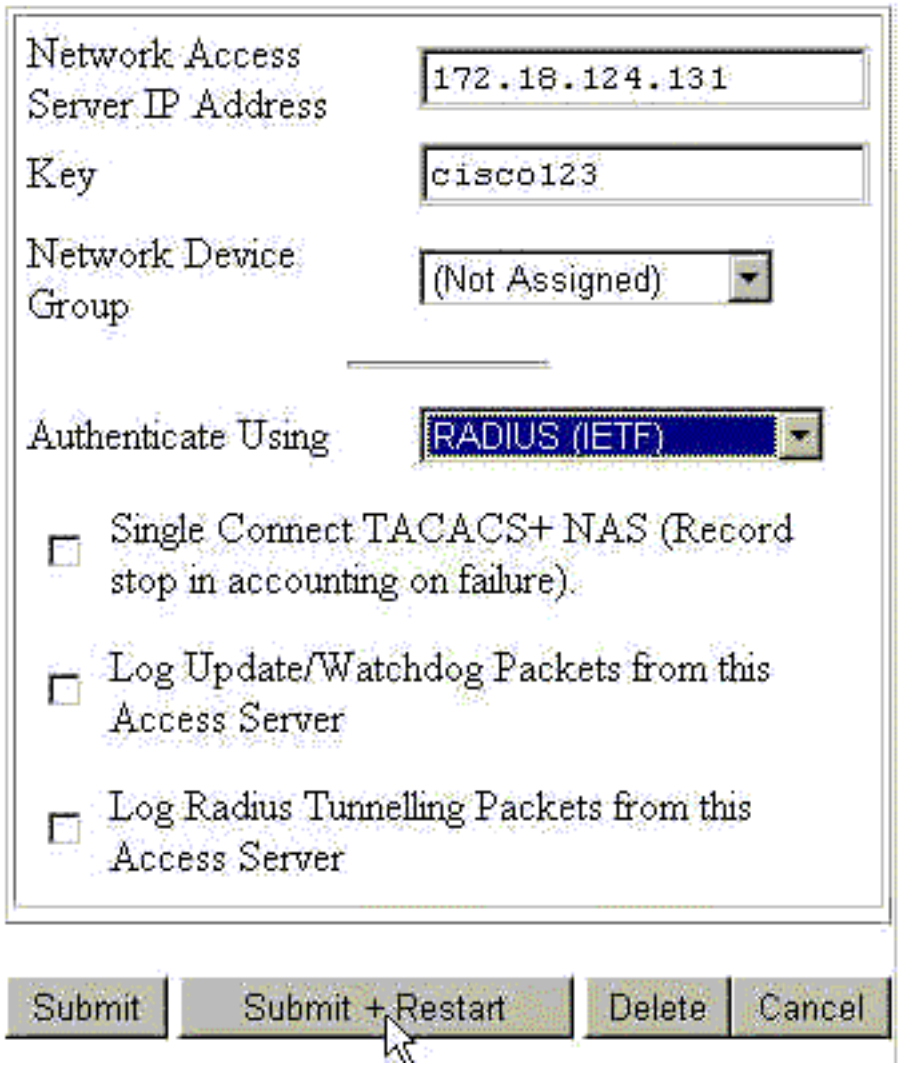
2. Una vez que usted ha agregado el servidor, utilice el **botón Test Button** para verificar que usted puede autenticar al usuario con éxito.Si esto no trabaja, el bloqueo del grupo no funciona.
3. Defina un filtro que los descensos accedan todo en la red interna.Aplicar esto para agrupar “todo el mundo” para incluso si los usuarios pueden autenticar en este grupo y permanecer en él, ellos todavía no puede acceder cualquier cosa.
4. Bajo el **Configuration (Configuración) > Policy Management (Administración de políticas) > Traffic Management (Administración de tráfico) > Rules (Reglas)**, agregue una regla llamada **Drop All** y deje todo en los valores por defecto.
5. Bajo el **Configuration (Configuración) > Policy Management (Administración de políticas) > Traffic Management (Administración de tráfico) > Filters (Filtros)**, cree un filtro llamado **Drop All**, deje todo en los valores por defecto, y agregue el descenso toda la regla a ella.
6. Bajo el **Configuration (Configuración)>User Management (Administración del usuario) >Groups (Grupos)** agregue a un grupo llamado **todo el mundo**.Éste es el grupo que todos los usuarios han preconfigurado en el cliente VPN. Autentican en este grupo inicialmente, y después son bloqueados en un diverso grupo después de la autenticación de usuario. Defina al grupo normalmente. Aseegurese le agregar el descenso todo el filtro (ese usted acaba de crear) bajo el general cuadro para utilizar la autenticación de RADIUS para los usuarios en este grupo, fije el tipo del grupo (bajo lengueta de la identidad) para ser **interno** y la autenticación (bajo lengueta del IPSec) al **RADIUS**. Aseegurese al grupo que la característica del bloqueo no se marca para saber si hay este grupo.**Nota:** Incluso si usted no define un descenso todo el filtro, aseegurese allí es por lo menos un filtro definido aquí.
7. Defina el grupo del destino final del usuario (el ejemplo es “filtergroup”), aplicando un filtro.**Nota:** Usted debe definir un filtro aquí. Si usted no quiere bloquear ningún tráfico para estos usuarios, cree “permiten todo el” filtro y aplican el “ningunos en” y “” excluye a él. Usted debe definir un filtro de algún bueno para pasar el tráfico. Para utilizar la autenticación de RADIUS para los usuarios en este grupo, fije el tipo del grupo (bajo lengueta de la identidad) para ser **interno** y la autenticación (bajo lengueta del IPSec) al **RADIUS**. Aseegurese al grupo que la característica del bloqueo no se marca para saber si hay este grupo.

Configure al servidor de RADIUS

Cisco Secure ACS for Windows

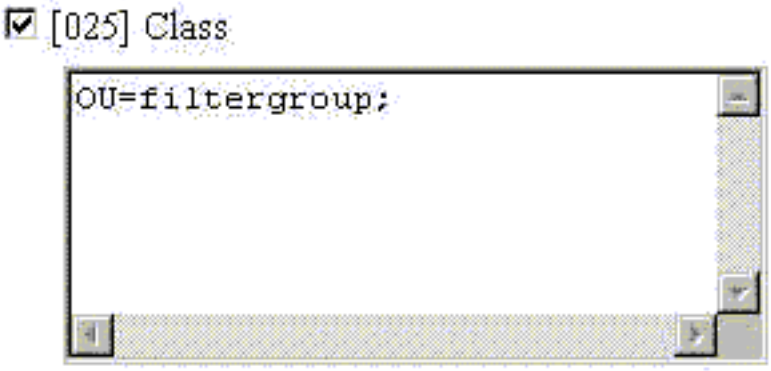
Estos pasos configuran a su servidor de RADIUS del Cisco Secure ACS for Windows para bloquear a un usuario en un grupo determinado configurado en el concentrador VPN. Tenga presente que los grupos definieron en el servidor de RADIUS no tienen nada hacer con los grupos definidos en el concentrador VPN. Usted puede utilizar a los grupos en el servidor de RADIUS para hacer la administración de sus usuarios más fácil. Los nombres no tienen que hacer juego qué se configura en el concentrador VPN.

1. Agregue el concentrador VPN como servidor de acceso a la red (NAS) en el servidor de RADIUS bajo sección de configuración de red.Agregue la dirección IP del concentrador VPN en la casilla de IP Addresses NAS.Agregue la misma clave que usted definió anterior en el concentrador VPN en la casilla para la clave.De la autenticidad usando el menú desplegable, seleccione **RADIUS (IETF)**.Tecleo **Submit +**



Restart.

2. Bajo configuración de la interfaz, se marca el **RADIUS** selecto **(IETF)** y se aseegura el atributo **25 (clase)**.Esto permite que usted lo cambie en el grupo/configuración de usuario.
3. Agregue al usuario.En este ejemplo, llaman el usuario “PRUEBA.” Este usuario puede estar en cualquier grupo del Cisco Secure ACS for Windows. Con excepción del paso abajo del atributo 25 para decir al concentrador VPN qué grupo no es ninguna correlación utilizar para el usuario, allí entre los grupos del Cisco Secure ACS for Windows y los grupos del concentrador VPN. Colocan a este usuario en el "Group_1."
4. Bajo configuración de grupo, edite las configuraciones en el grupo (en nuestro ejemplo, éste es el "Group_1").
5. Haga clic el botón verde del **IETF RADIUS** para llevarle a los atributos apropiados.
6. Navegue hacia abajo y modifique el atributo 25.
7. Agregue el atributo como se muestra aquí. Substituya el nombre del grupo que usted quiere para bloquear a los usuarios en para el filtergroup.Aseegurese el OU está con mayúsculas y eso allí es un punto y coma después del nombre del



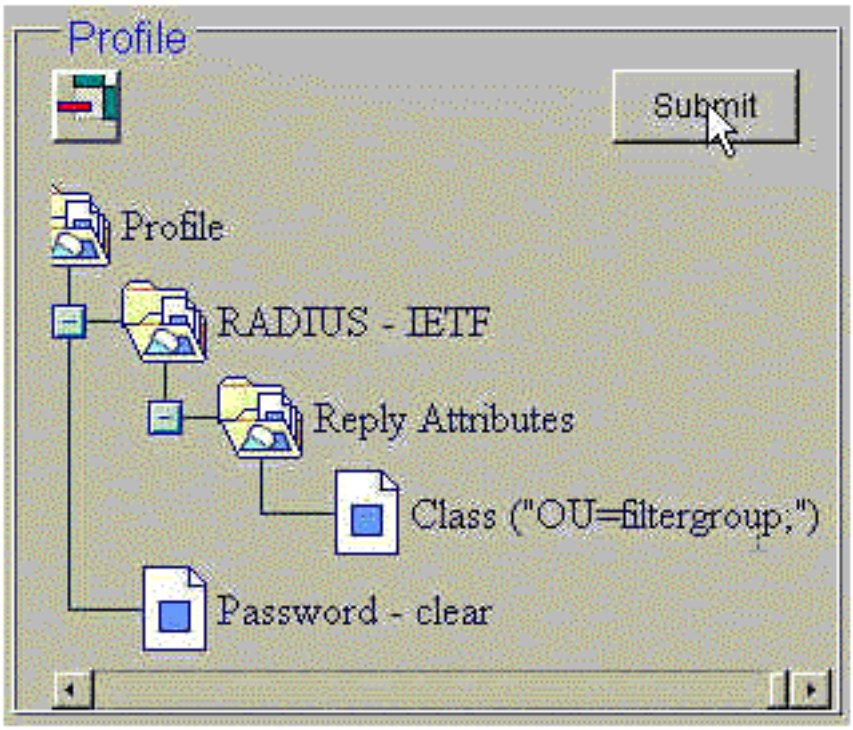
grupo.

8. Tecleo **Submit + Restart**.

Cisco seguro para UNIX

Estos pasos configuran su Cisco aseguran el servidor del UNIX RADIUS para bloquear a un usuario en un grupo determinado configurado en el concentrador VPN. Tenga presente que los grupos definieron en el servidor de RADIUS no tienen nada hacer con los grupos definidos en el concentrador VPN. Usted puede utilizar a los grupos en el servidor de RADIUS para hacer la administración de sus usuarios más fácil. Los nombres no tienen que hacer juego qué se configura en el concentrador VPN.

1. Agregue el concentrador VPN adentro como NAS en el servidor de RADIUS bajo sección avanzada.Elija un diccionario que permita que el atributo 25 sea enviado como contestación-atributo. Por ejemplo, el IETF o asciende.
2. Agregue al usuario.En este ejemplo, el usuario es “PRUEBA.” Este usuario puede estar en cualquier grupo seguro de Cisco UNIX o ningún grupo. Con excepción del paso abajo del atributo 25 para decir al concentrador VPN qué grupo no es ninguna correlación utilizar para el usuario, allí entre los grupos seguros de Cisco UNIX y los grupos del concentrador VPN.
3. Bajo el usuario/perfil del grupo, defina un atributo de la vuelta RADIUS (IETF).
4. Agregue el atributo de clase, el número de atributo **25**, y haga su valor **OU=filtergroup;**. Substituya al grupo definido en el concentrador VPN para el filtergroup.**Nota:** En Cisco UNIX seguro, defina el atributo rodeado por las comillas. Se eliminan de cuando el atributo se envía al concentrador VPN. El usuario/el perfil del grupo debe parecer similares a



esto.

5. El tecleo **somete** para salvar cada entrada.Las entradas Unix seguras acabadas de Cisco aparecen similares a esta salida:

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

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Usuario y Procesamiento de atributos del grupo de Cliente Cisco VPN 3000 en el concentrador VPN 3000
- Página de soporte de la tecnología del RADIUS (Servicio de usuario de acceso telefónico de autenticación remota)
- Páginas de soporte del Concentradores Cisco VPN de la serie 3000
- Páginas de soporte de VPN 3000 Client de Cisco
- Páginas de soprte del producto del IP Security Protocol (IPSec)
- Solicitudes de Comentarios (RFC)
- Página de soprte del producto del Cisco Secure ACS for Windows
- Field Notice de los productos de seguridad
- Cisco Secure ACS para la Página de soporte del producto UNIX
- Soporte Técnico - Cisco Systems