Configure el Concentradores Cisco VPN de la serie 3000 para soportar la característica de vencimiento de contraseña de NT con el servidor de RADIUS

Contenido

Introducción

Este documento incluye las instrucciones paso a paso en cómo configurar el Concentradores Cisco VPN de la serie 3000 para soportar la característica de vencimiento de contraseña de NT usando el servidor de RADIUS.

Refiera a VPN 3000 RADIUS con la función de vencimiento usando el Servidor de autenticación de Internet de Microsoft para aprender un scenerio más casi igual con el Internet Authentication Server (IAS).

prerrequisitos

Requisitos

- Si servidor su servidor de RADIUS y autenticación de dominio de NT están en dos máquinas distintas, aseegurese que usted ha establecido la conectividad del IP entre las dos máquinas.

- Aseegurese que usted ha establecido la conectividad del IP del concentrador al servidor de RADIUS. Si el servidor de RADIUS está hacia la interfaz pública, no olvide abrir el puerto RADIUS en el Filtro público.
- Asegure ese usted puede conectarse al concentrador del usando la base de datos de usuarios interna del cliente VPN. El si esto no está configurado, refiere por favor a configurar el IPSec - Cliente VPN del Cisco 3000 al concentrador VPN 3000.

Nota: La característica de vencimiento de contraseña no se puede utilizar con la red VPN o los clientes VPN SSL.

Componentes Utilizados

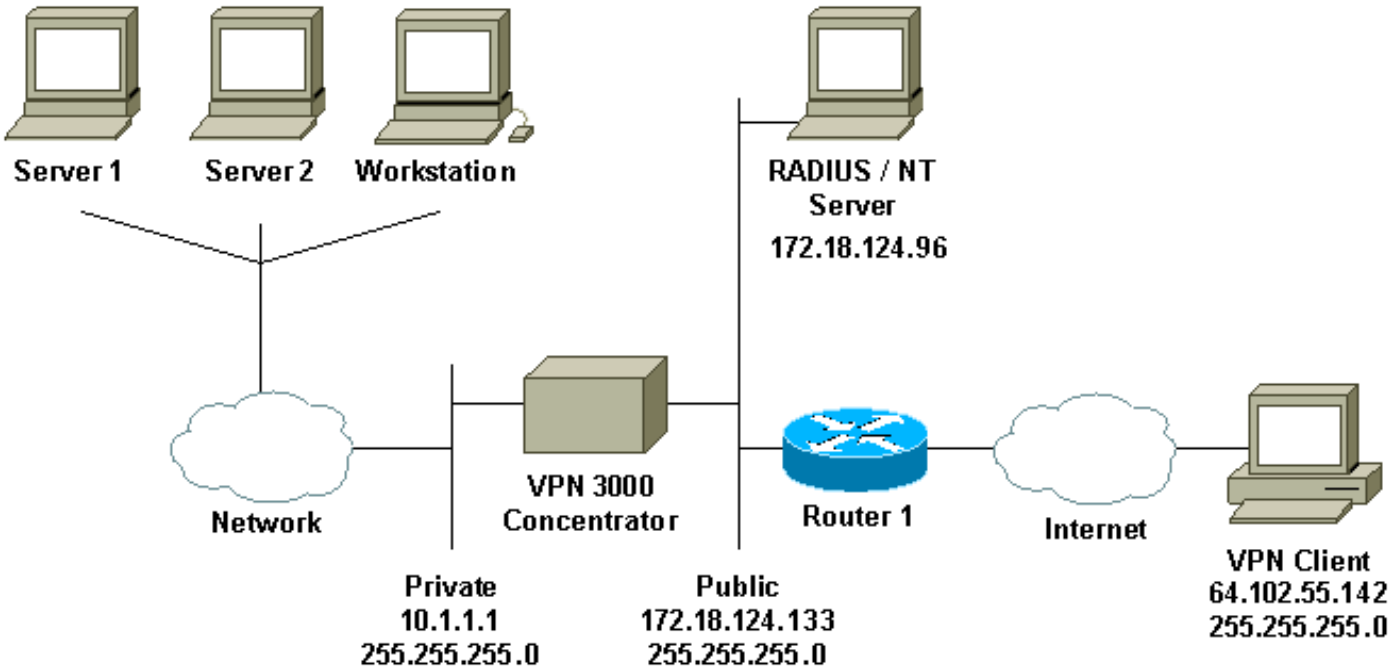
Esta configuración fue desarrollada y probada utilizando las versiones de software y hardware indicadas a continuación.

- Versión de software concentradora VPN 3000 4.7
- Versión 3.5 del cliente de VPN
- Cisco seguro para el servidor Active Directory del Microsoft Windows 2000 de la versión 3.0 de NT (CSNT) para la autenticación de usuario

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.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Notas de diagrama

1. El servidor de RADIUS en esta configuración está en la interfaz pública. Si éste es el caso con su configuración específica, cree por favor dos reglas en su Filtro público para permitir que el tráfico de RADIUS ingrese y que deje el concentrador.

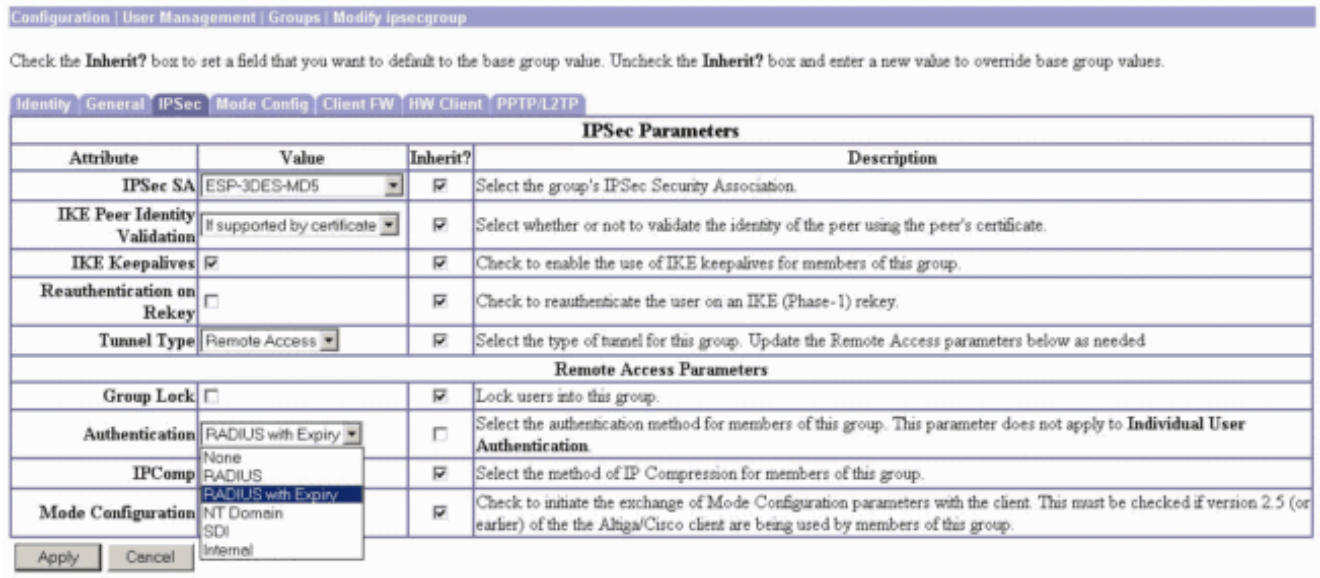
2. Este configuración muestra el software CSNT y servicios de autenticación de dominio de NT que se ejecutan en la misma máquina. Estos elementos se pueden funcionar con en dos máquinas distintas si se requiere por parte de su configuración.

Configuración del concentrador VPN 3000

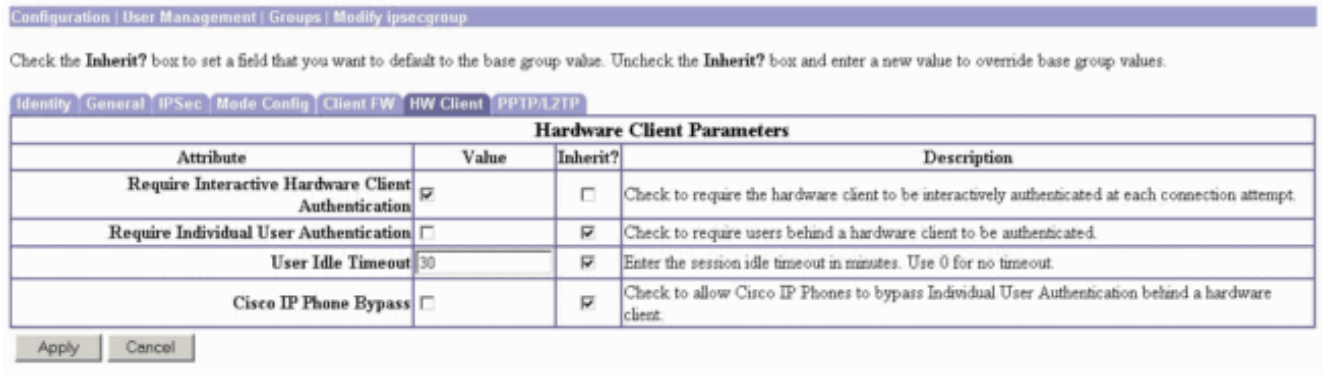
Configuración del grupo

1. Para configurar al grupo para validar los parámetros del vencimiento de contraseña de NT del servidor de RADIUS, ir al **Configuration (Configuración)>User Management (Administración del usuario) >Groups (Grupos)**, seleccionar su grupo de la lista, y el tecleo **modifica al grupo**. El ejemplo debajo de las demostraciones cómo modificar a un grupo nombró el "ipsecgroup."

2. Va a la lengueta del **IPSec**, se aseegura que el **RADIUS con el vencimiento** está seleccionado para el atributo de la **autenticación**.

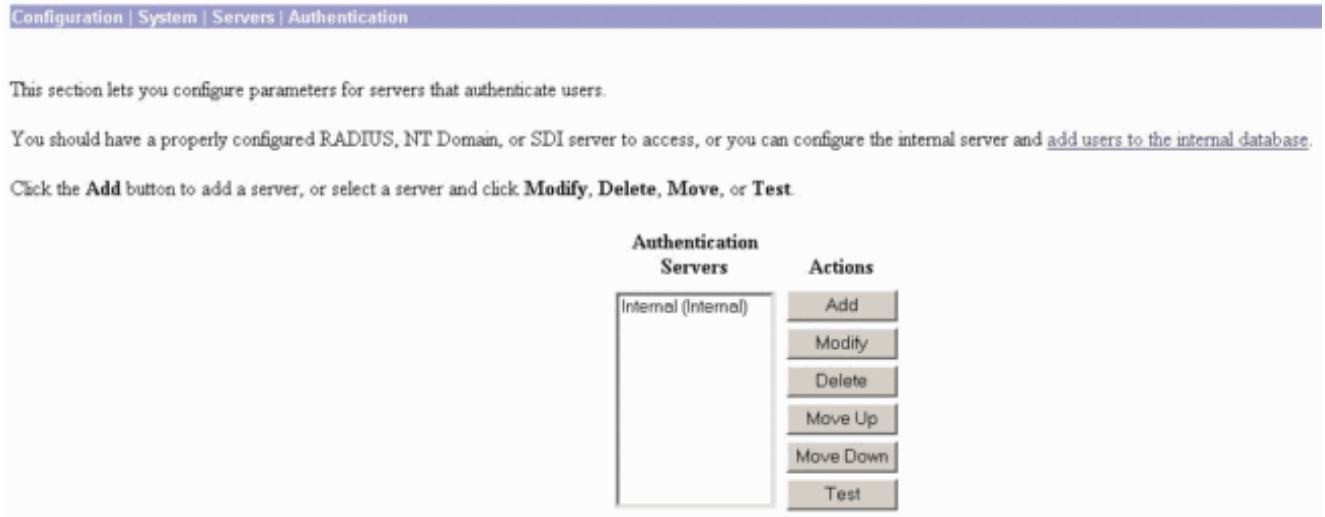


3. Si usted quisiera que esta característica fuera habilitada en el VPN 3002 Hardware Clients, vaya a la lengueta del **cliente HW**, se aseegura que el **Require Interactive Hardware Client Authentication** está habilitado, después hacer clic **se aplica**.

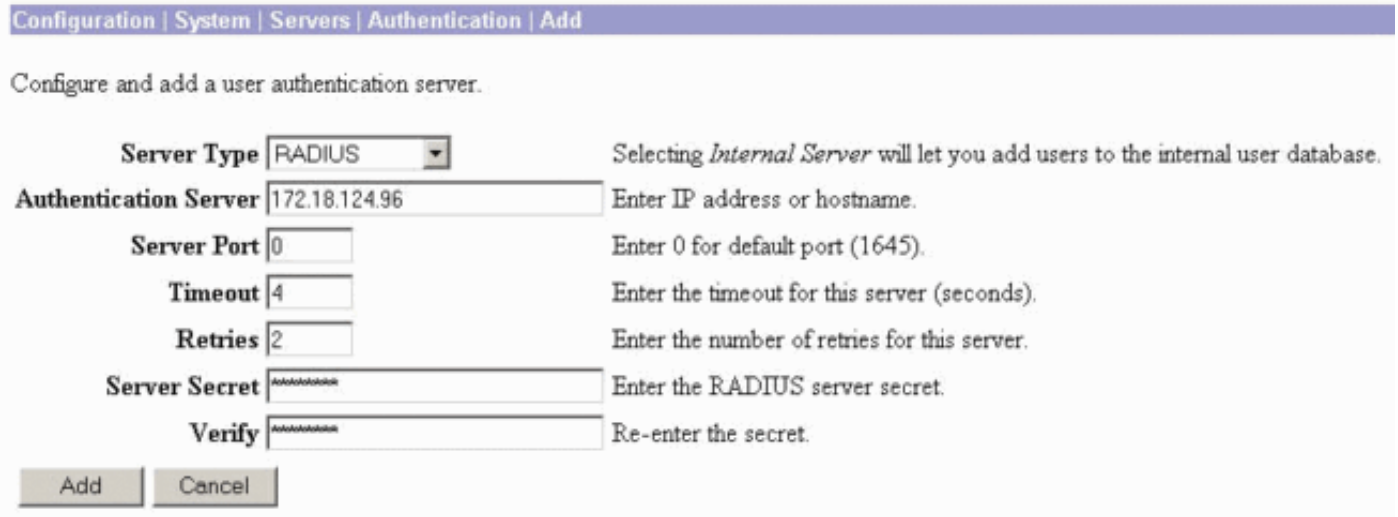


Configuración RADIUS

1. Para configurar las configuraciones del servidor de RADIUS en el concentrador, vaya al **Configuration (Configuración) > Sytem (Sistema) > Servers (Servidores) > Authentication (Autenticación) >**
   Add.



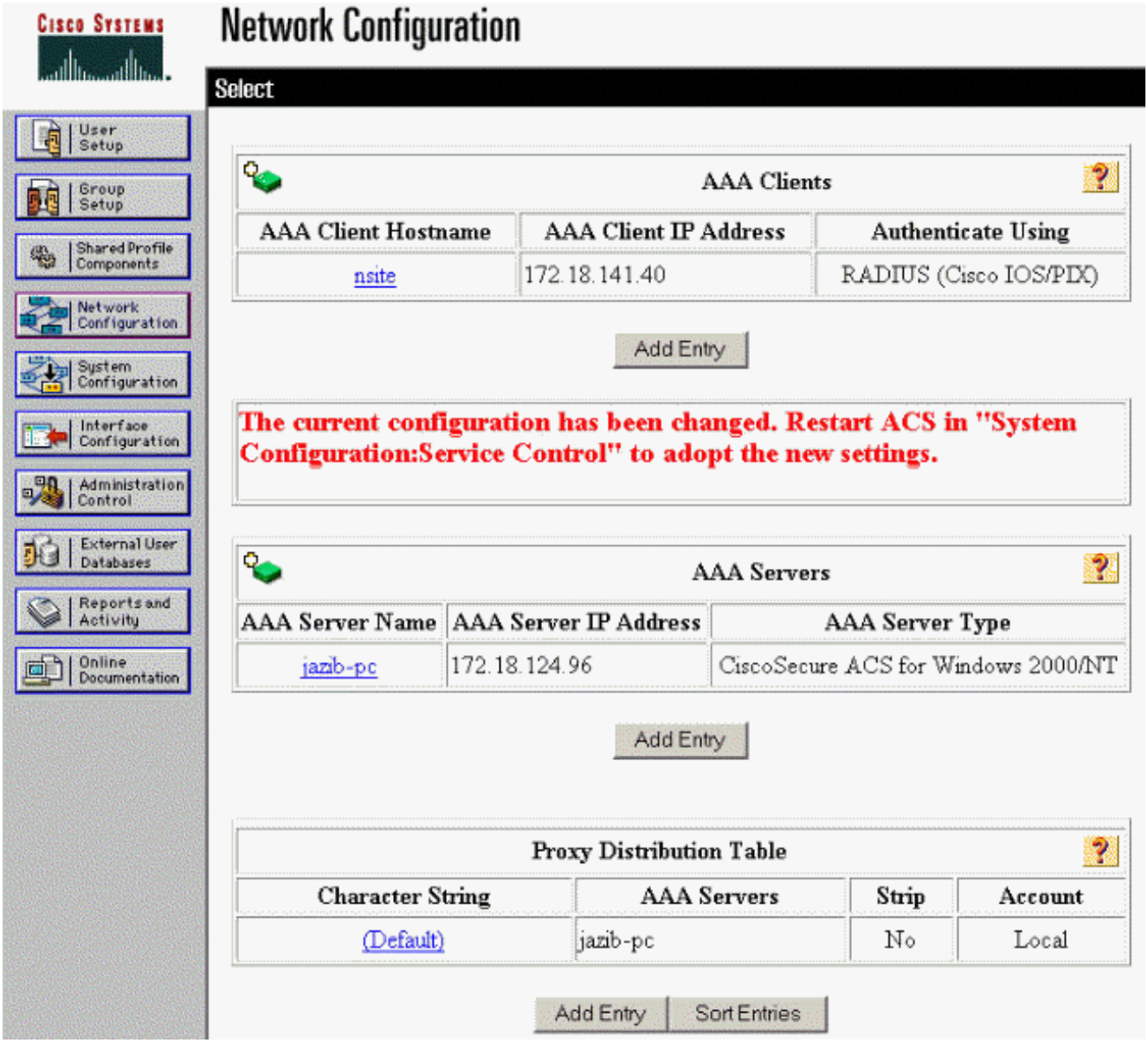
2. En la pantalla Add, teclee adentro los valores que corresponden al servidor de RADIUS y al haga click en AddEl ejemplo abajo utiliza los valores siguientes.`Server Type:` **`RADIUS`**
   `Authentication Server:` **`172.18.124.96`** `Server Port =` **`0`** `(for default of 1645) Timeout =` **`4`**
   `Reties =` **`2`** `Server Secret =` **`cisco123`** `Verify:` **`cisco123`**



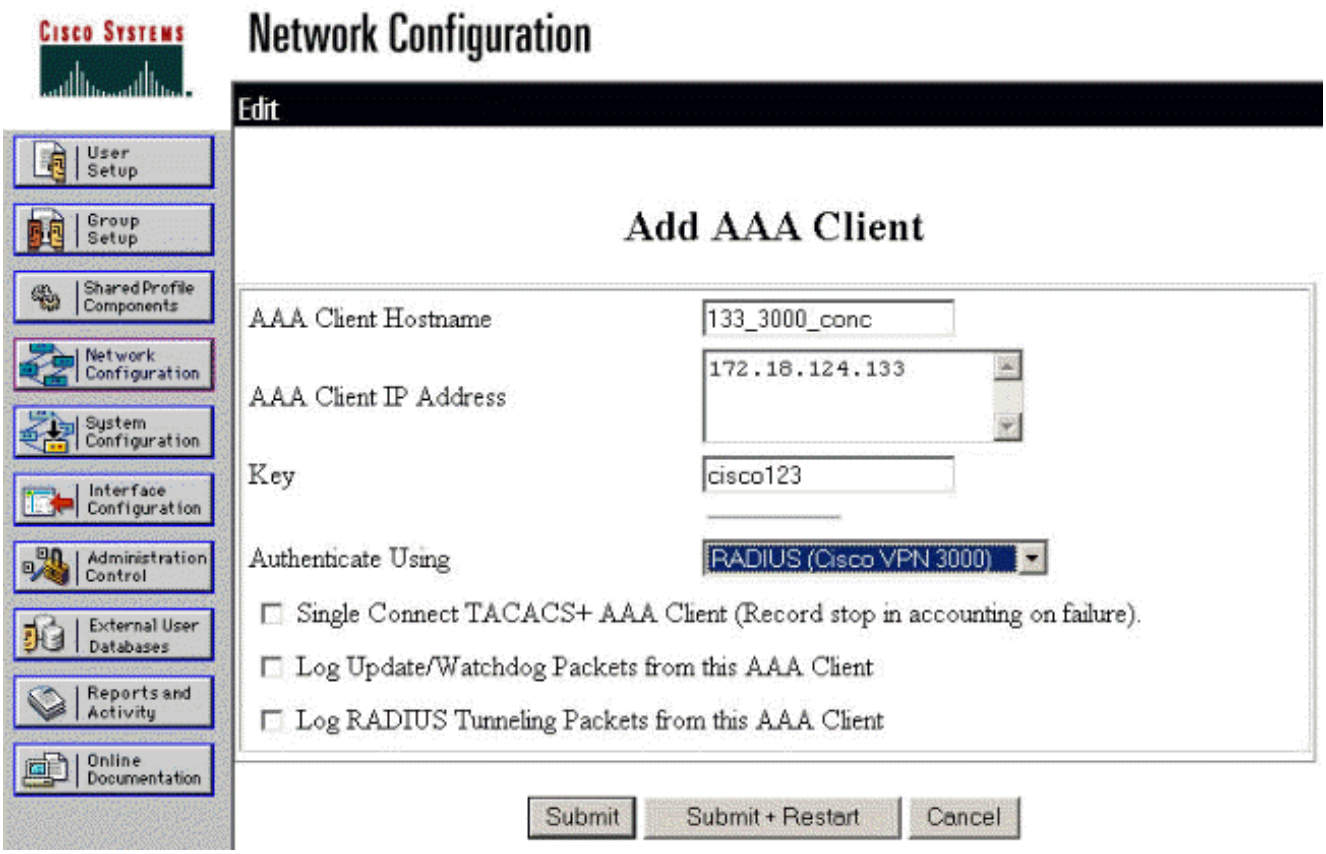
Configuración del servidor de Cisco Secure NT RADIUS

Configuración de una entrada para el concentrador VPN 3000

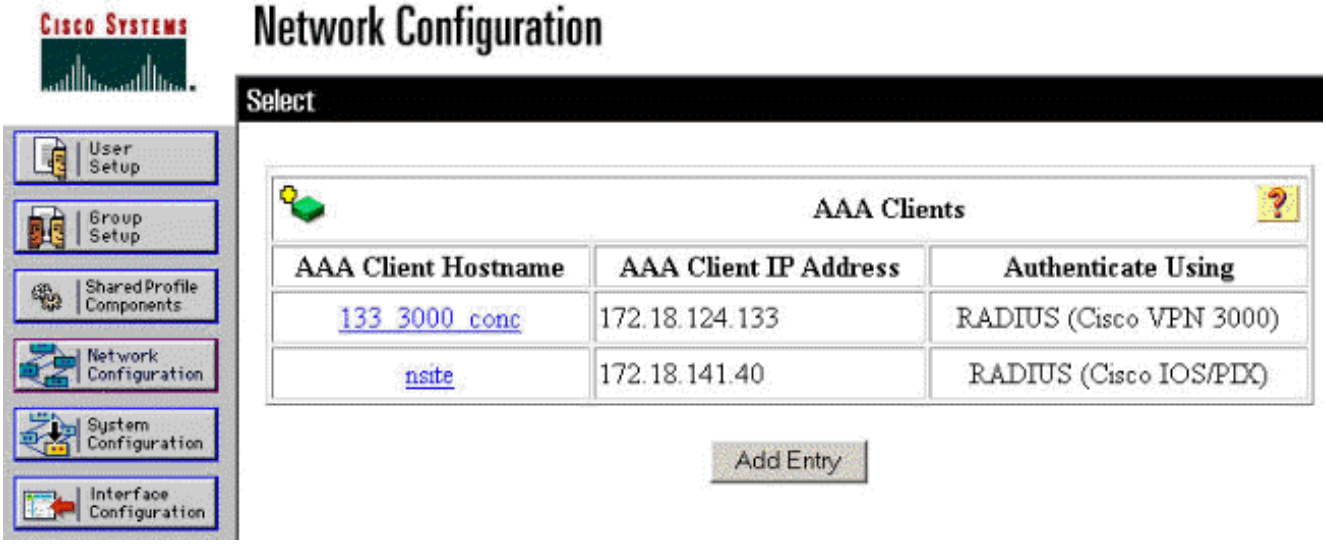
1. Registro en el CSNT y **configuración de red del** tecleo en el panel izquierdo. Bajo los “clientes AAA,” el tecleo **agrega la entrada**.



2. En “agregue la pantalla al cliente AAA”, teclee adentro los valores apropiados para agregar el concentrador como el cliente RADIUS, después haga clic **Submit + Restart**.El ejemplo abajo utiliza los valores siguientes.`AAA Client Hostname = 133_3000_conc AAA Client IP Address = 172.18.124.133 Key = cisco123 Authenticate using = RADIUS (Cisco VPN 3000)`

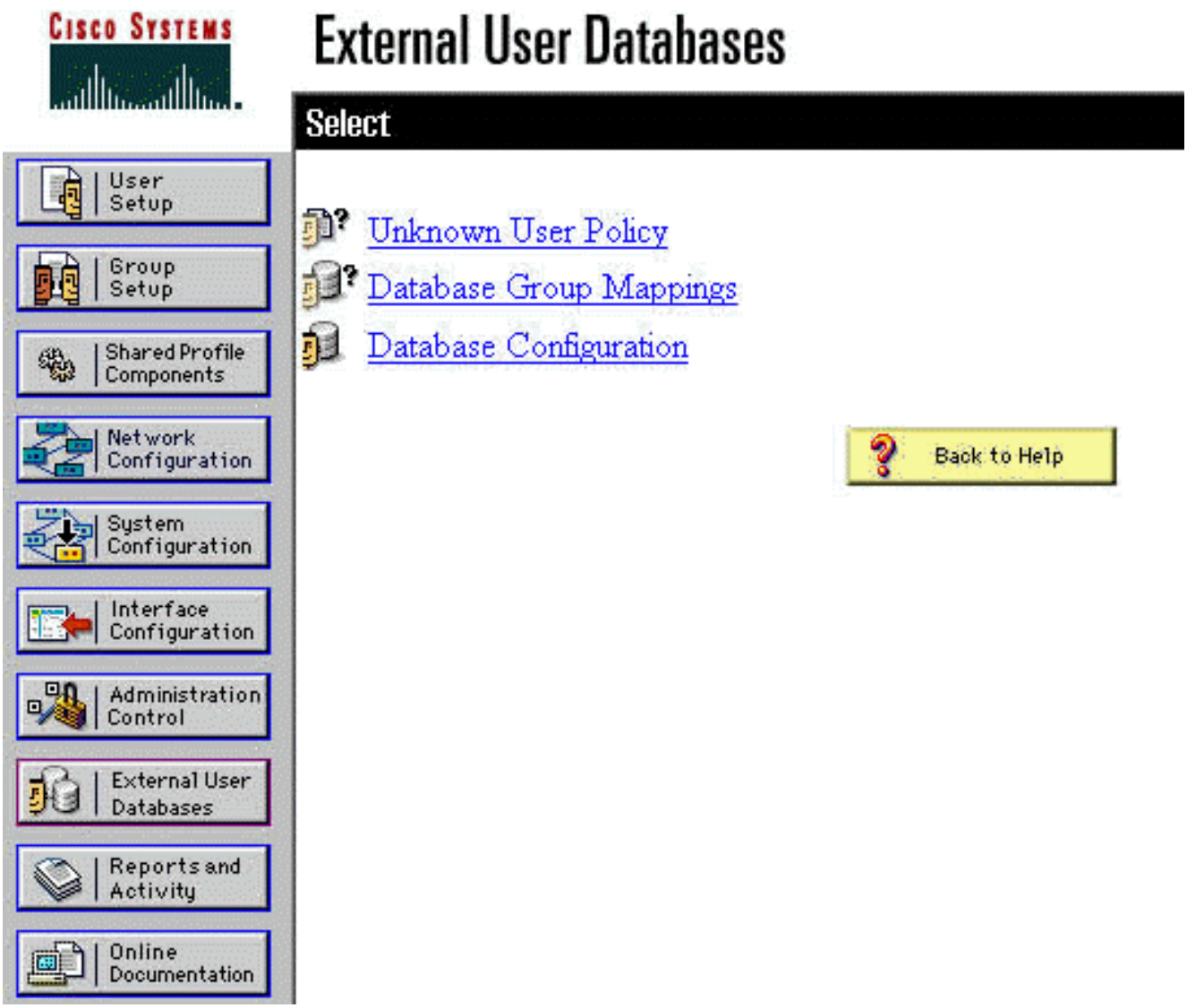


Una entrada para su concentrador 3000 aparecerá bajo sección de los "**clientes AAA**".

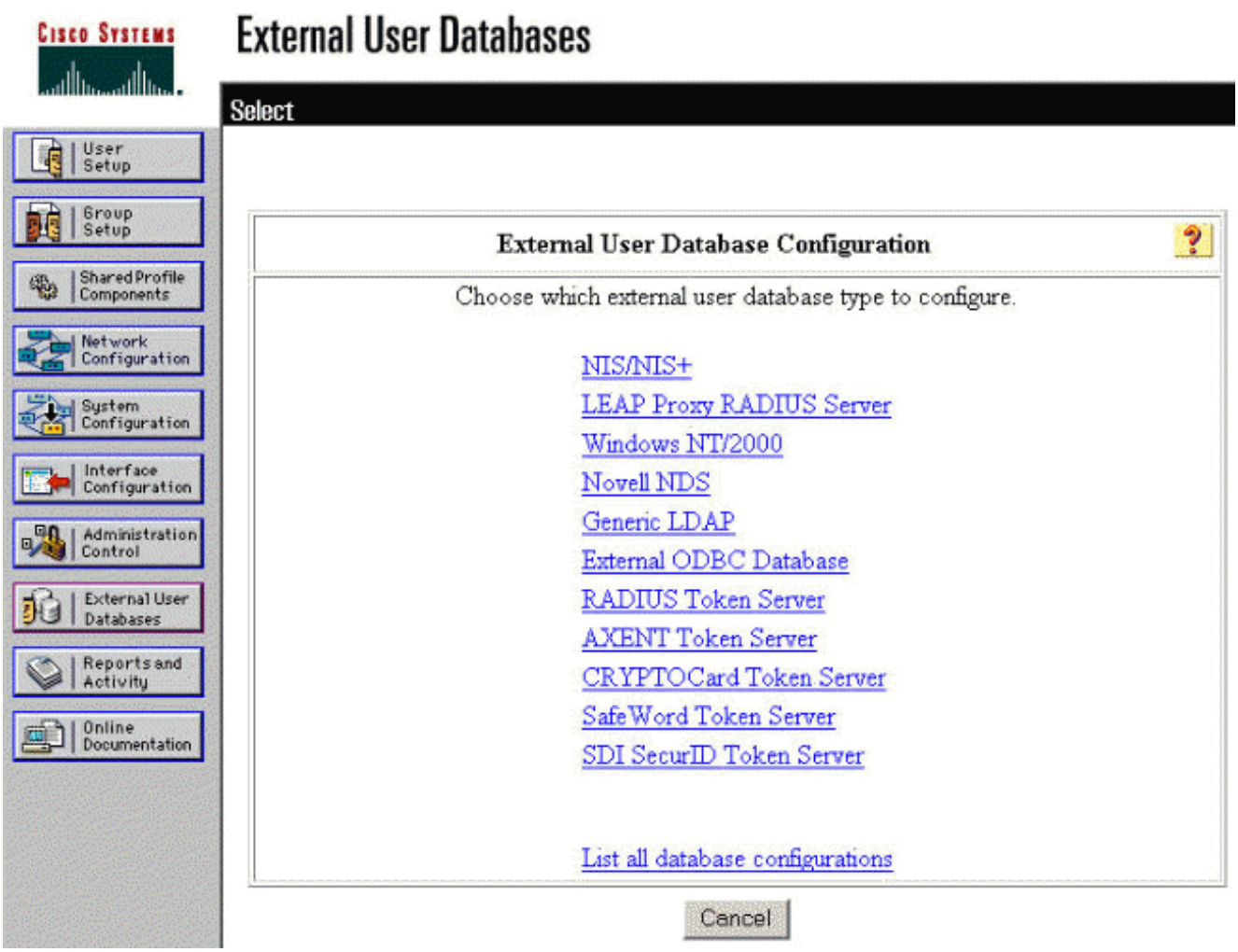


Configuración de la política de usuario desconocido para la autenticación de dominio NT

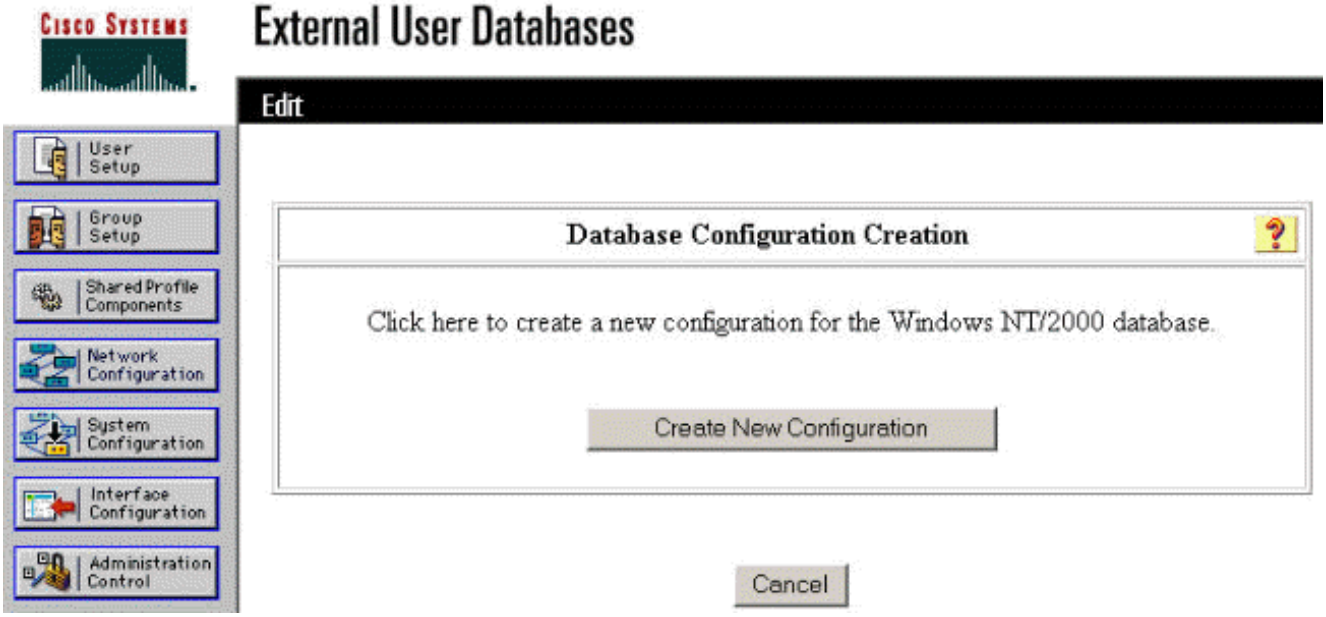
1. Para configurar la autenticación de usuario en el servidor de RADIUS como parte de la Política de usuario desconocido, **Base de datos de usuarios externa del** tecleo en el panel izquierdo, entonces para hacer clic el link para la **configuración de la base de datos**.



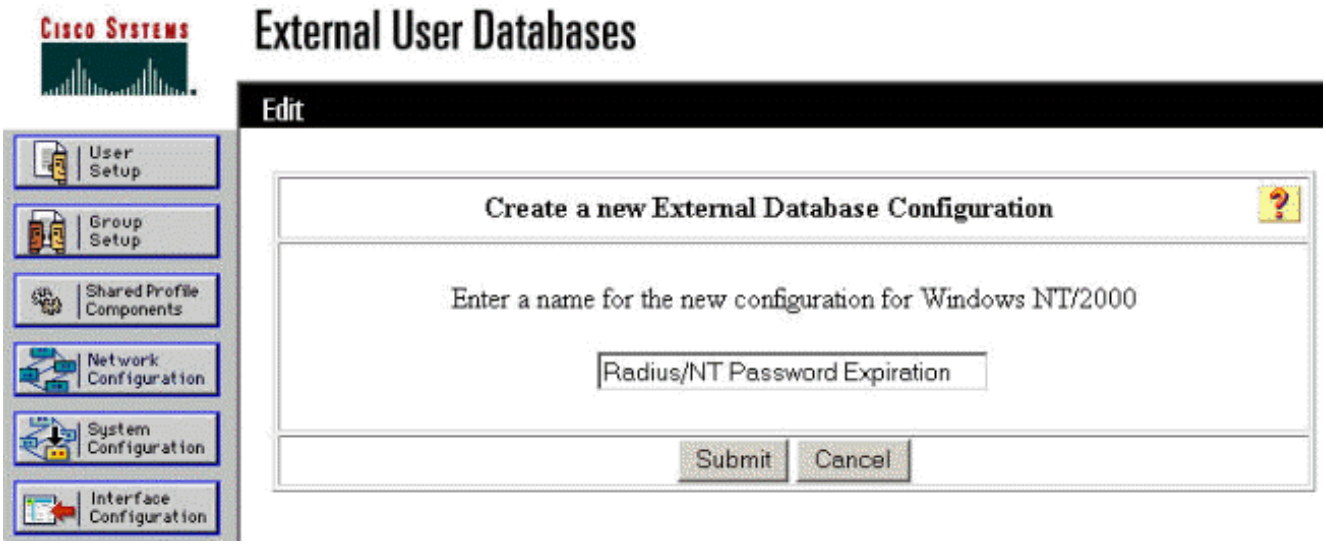
2. Bajo “Configuración de base de datos de usuarios externa,” tecleo **Windows Nt/2000**.



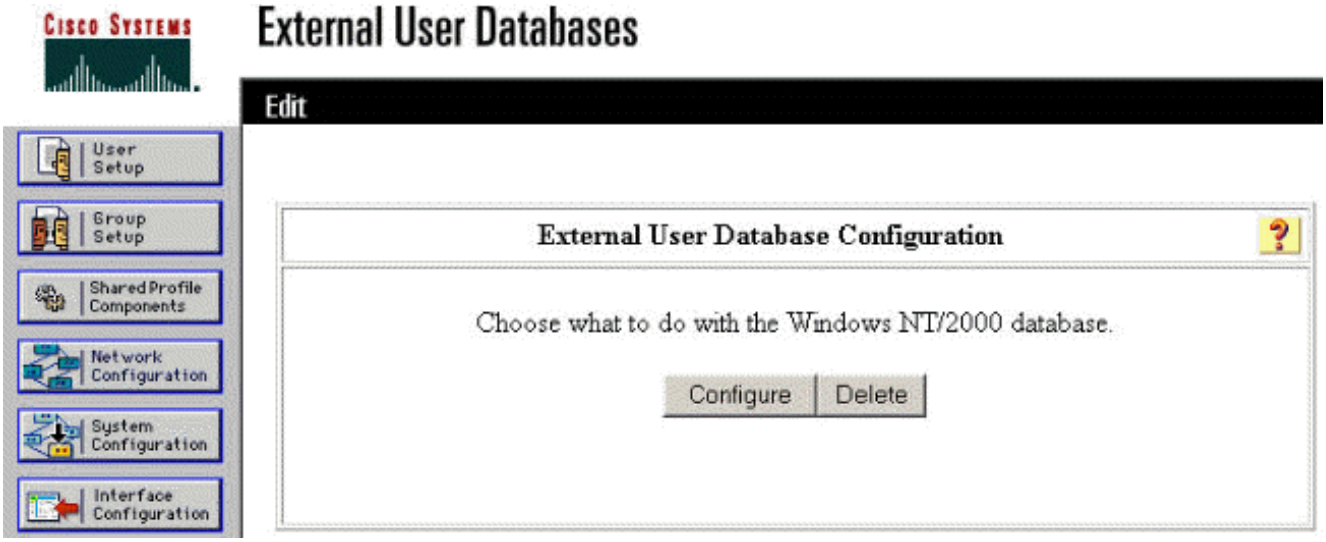
3. En “la pantalla de la creación de la configuración de la base de datos”, el tecleo **crea la nueva configuración**.



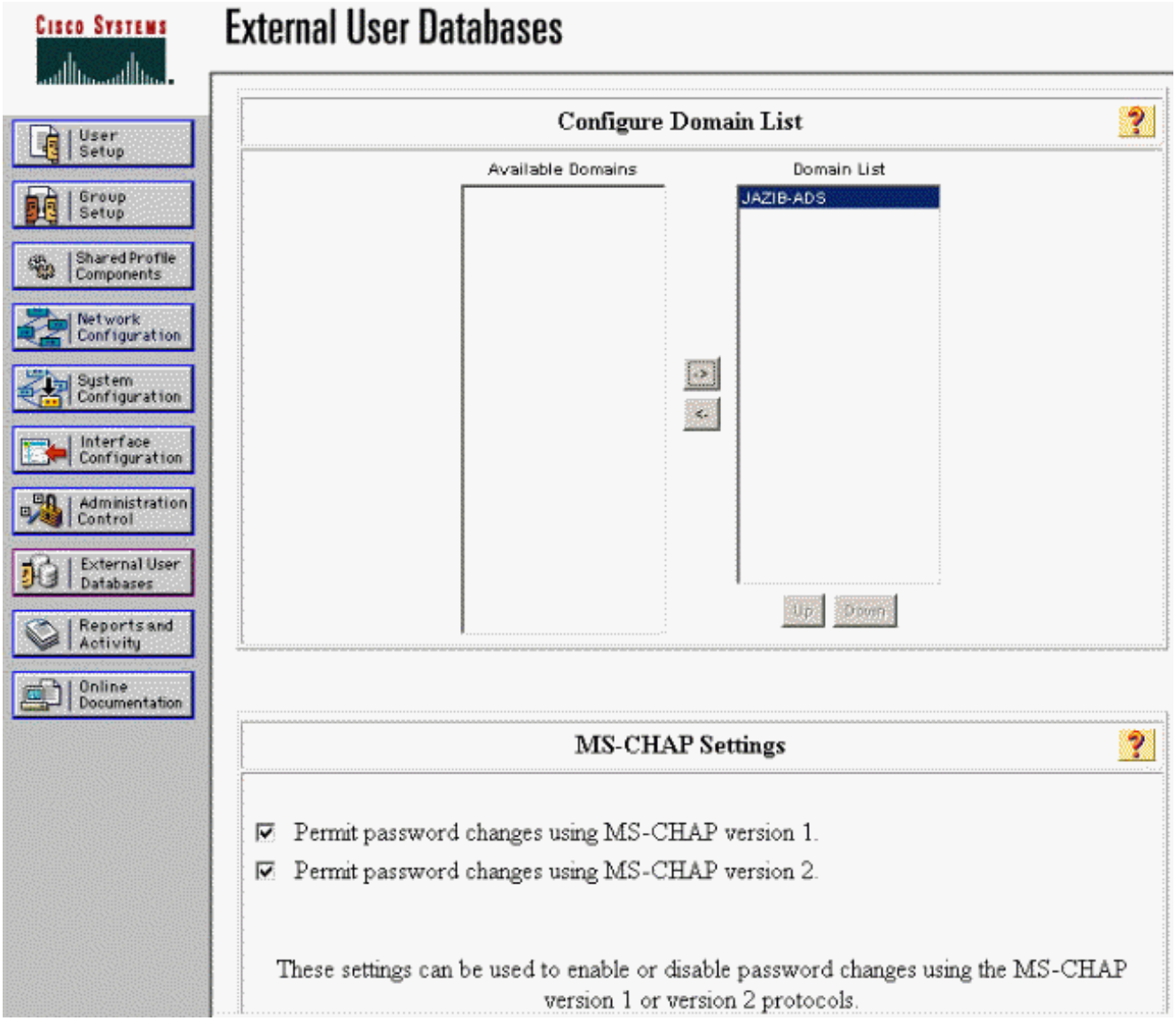
4. Cuando se le pregunte, teclee un nombre para la autenticación NT/2000 y el tecleo **somete**. El ejemplo abajo muestra el nombre “vencimiento de contraseña Radius/NT.”



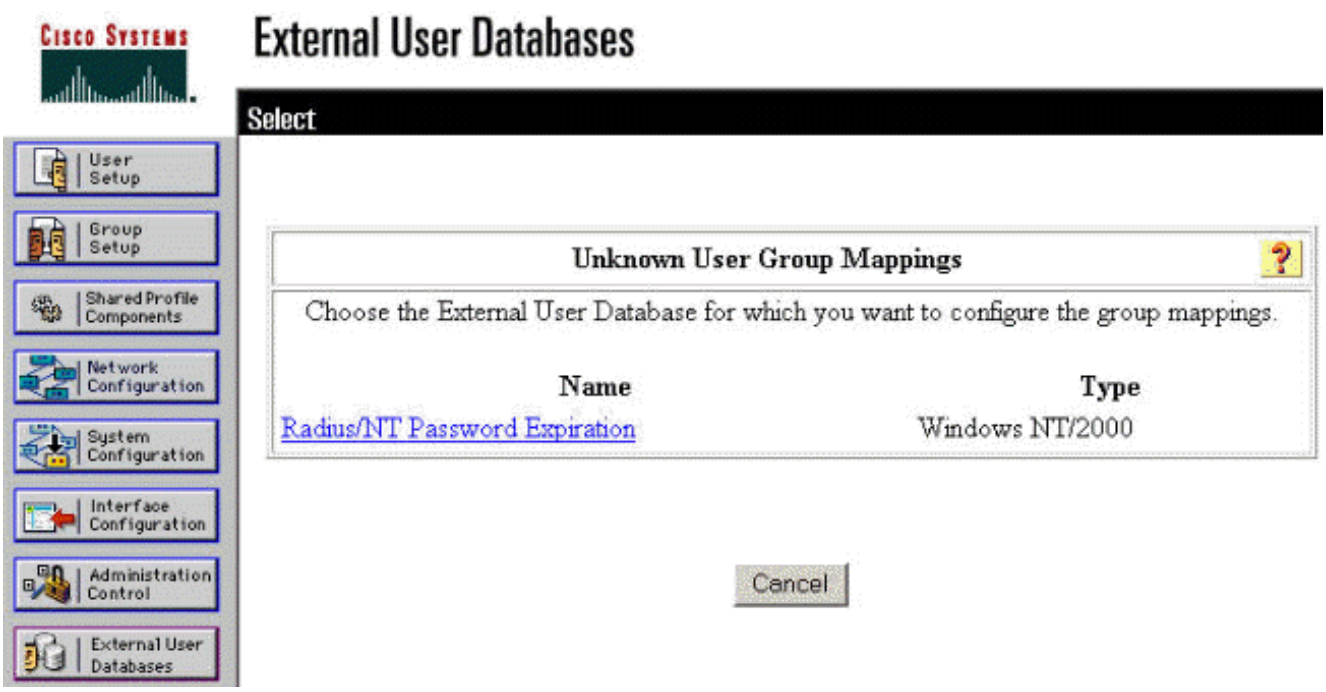
5. Hacen clic la **configuración** para configurar el Domain Name para la autenticación de usuario.



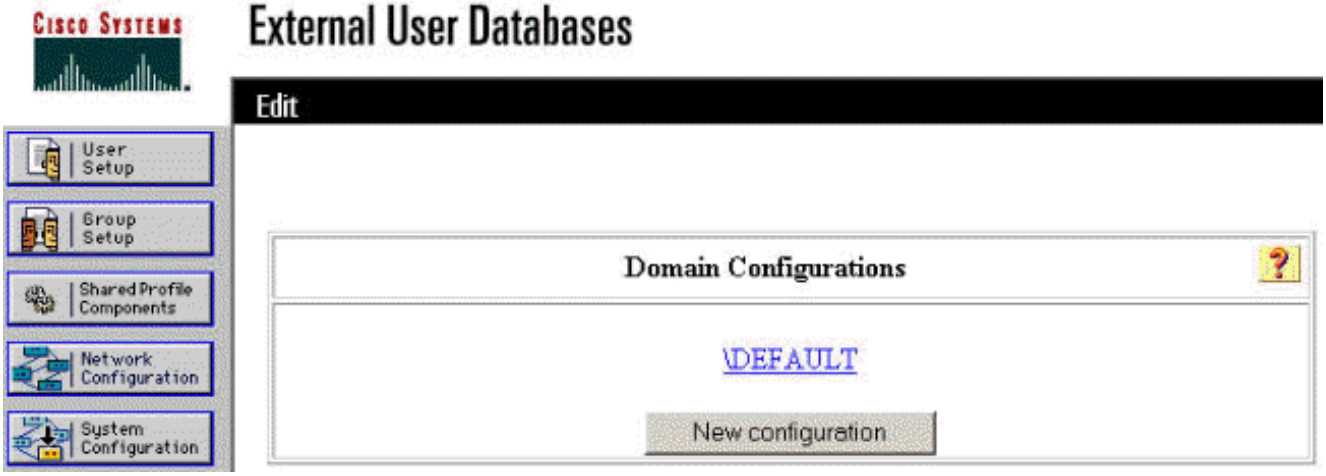
6. Seleccionan su dominio de NT de los “dominios disponibles,” entonces hacen clic el botón de la flecha correcta para agregarlo al “lista de dominio.” Bajo “configuraciones MS-CHAP,” asegúrese de que las opciones para los **cambios de la contraseña del permiso usando la versión MS-CHAP 1** y la **versión 2** estén seleccionadas. El tecleo **somete** cuando le hacen.



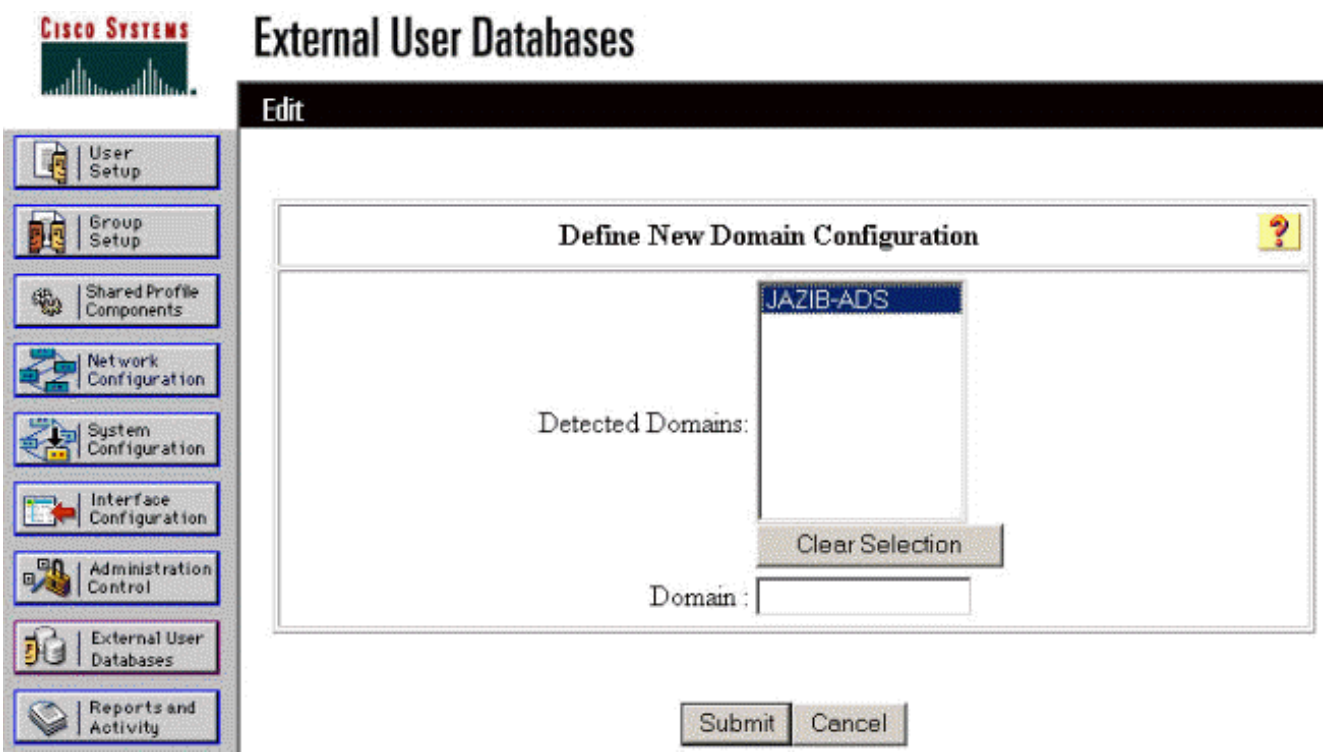
7. Haga clic la **Base de datos de usuarios externa** en el panel izquierdo, después haga clic el link para los **Mapeo de grupo de base de datos** (como se ve en este ejemplo). Usted debe ver una entrada para su base de datos externa previamente configurada. El ejemplo abajo muestra una entrada para el “vencimiento de contraseña Radius/NT,” la base de datos que acabamos de
configurar.



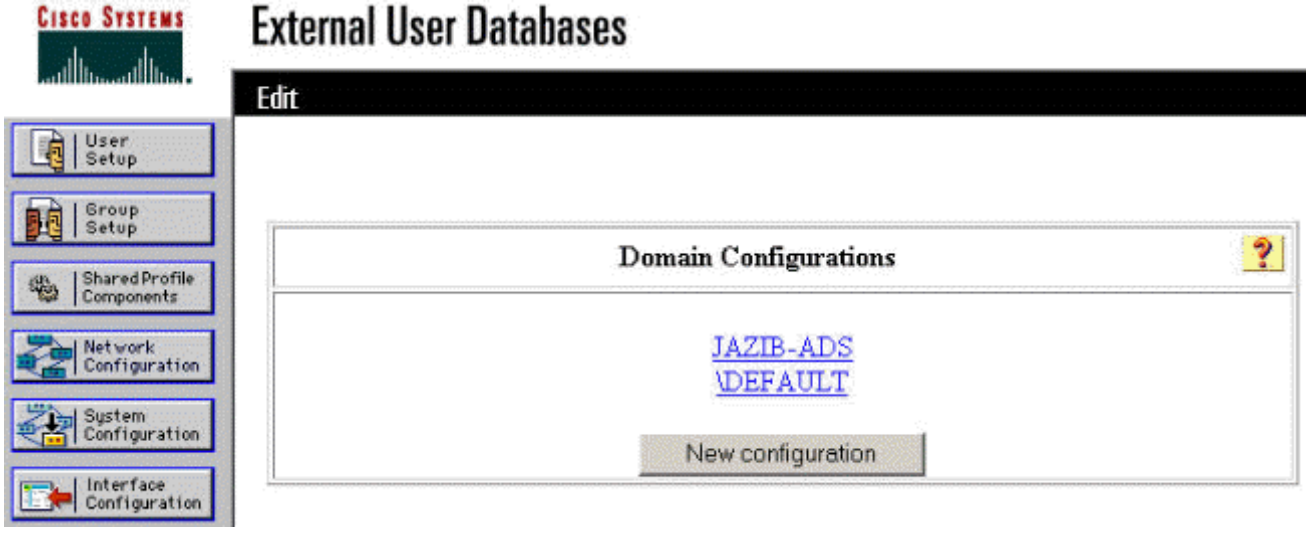
8. En las “configuraciones del dominio” defienda, haga clic la **nueva configuración** para agregar las configuraciones del
dominio.



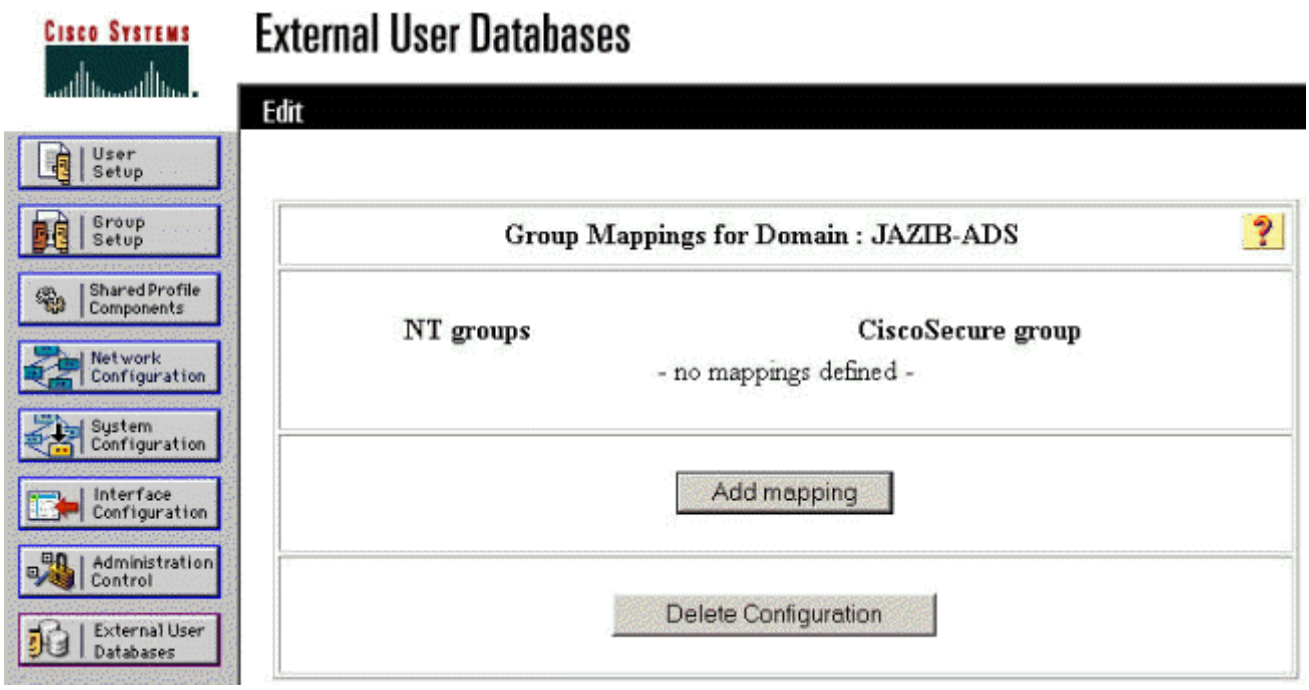
9. Seleccione su dominio de la lista de “detectó los dominios” y el tecleo **para someter**. El ejemplo abajo muestra un dominio nombrado “JAZIB-
ADS.”



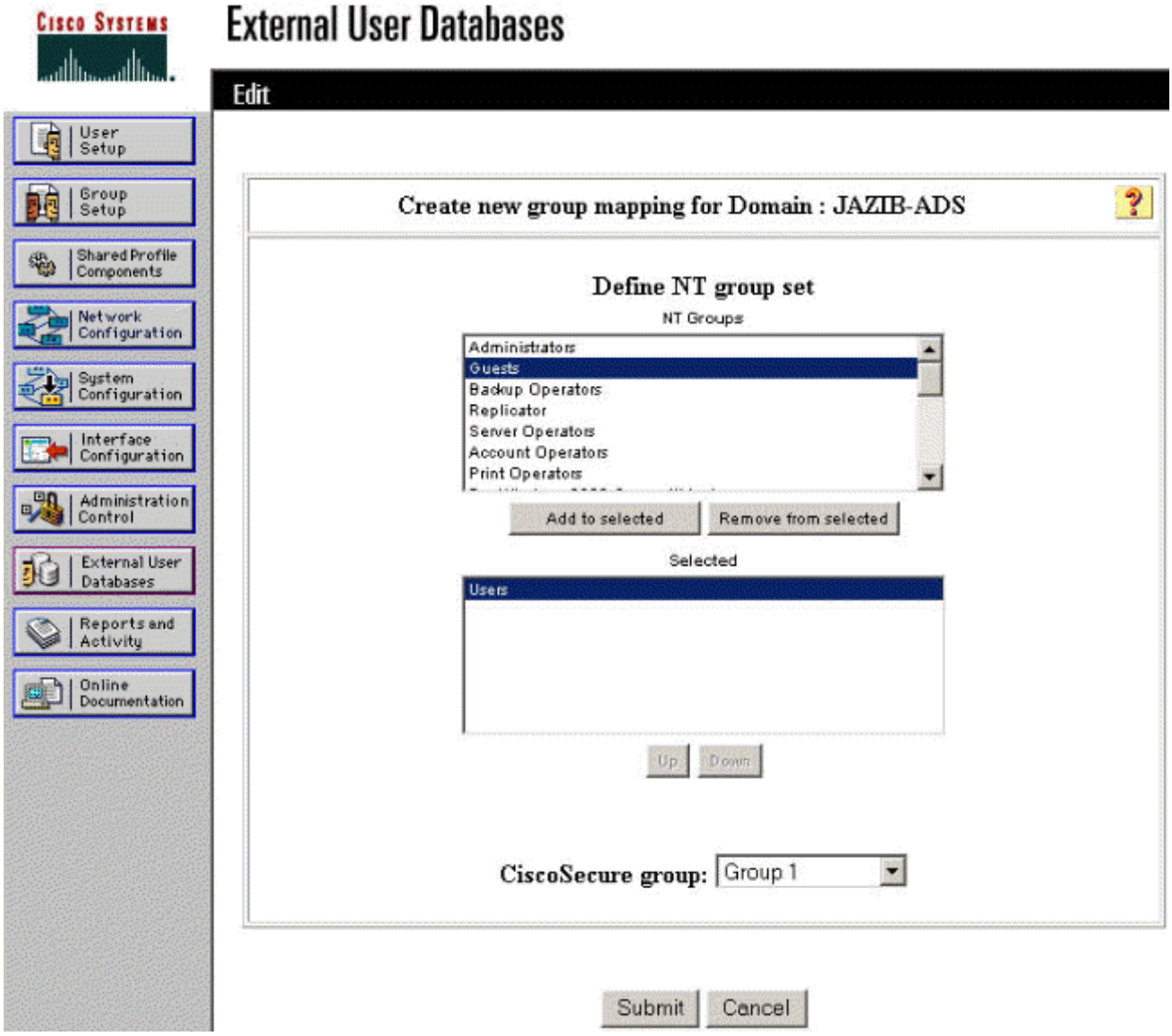
10. Hacen clic en su Domain Name para configurar los mappings del grupo. Este ejemplo muestra el dominio “JAZIB-ADS.”



11. El tecleo **agrega la asignación** para definir las asignaciones del grupo.

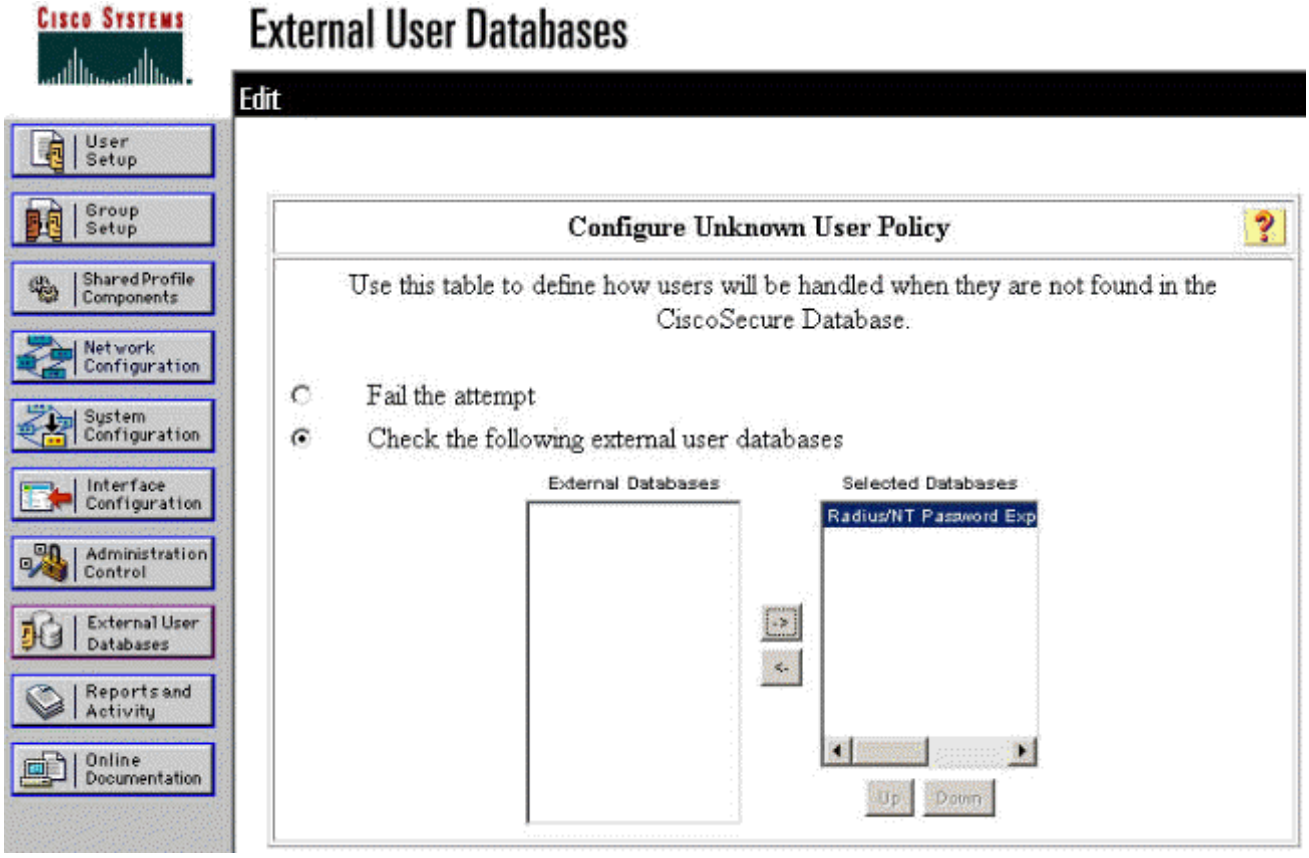


12. En “cree la pantalla de la nueva asignación del grupo”, asocie al grupo en el dominio de NT a un grupo en el servidor del CSNT RADIUS, después haga clic **somete**. Las correspondencias abajo del ejemplo “usuarios” del grupo de NT grupo 1." al grupo RADIUS “



13. **La Base de datos de usuarios externa del** tecleo en el panel izquierdo, entonces hace clic

el link para la **Política de usuario desconocido** (como se ve en este ejemplo). Aseegurese que la opción para el **control las Bases de datos de usuarios externas siguientes** está seleccionada. Haga clic el botón de la flecha correcta para mover la base de datos externa previamente configurada desde la lista de “bases de datos externas” a la lista de “bases de datos
seleccionadas.”

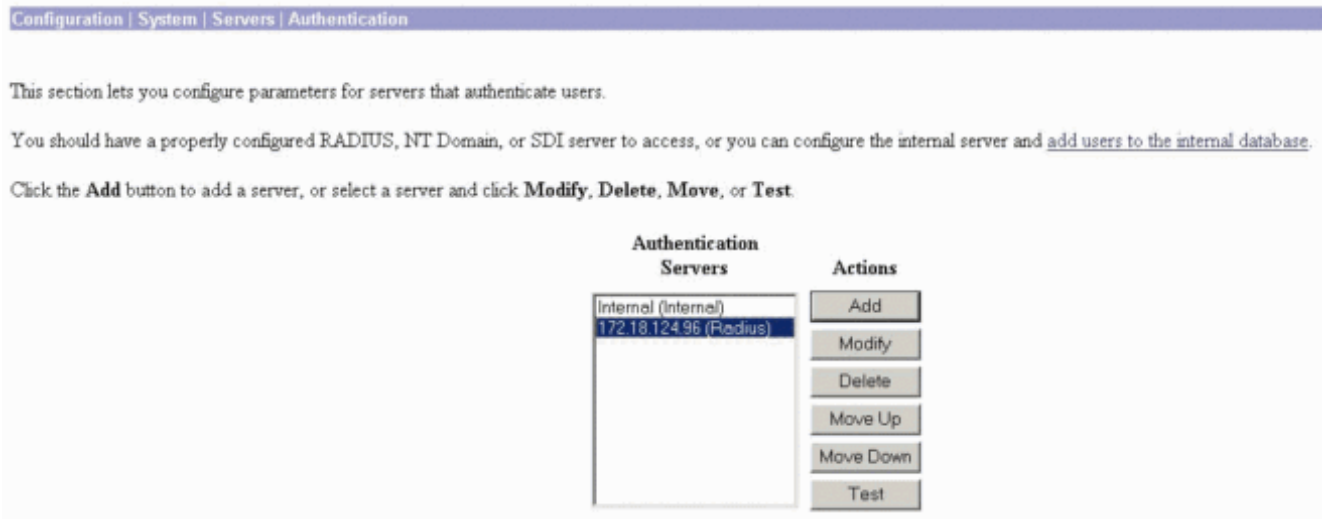


Prueba de la característica de vencimiento de contraseña de NT/RADIUS

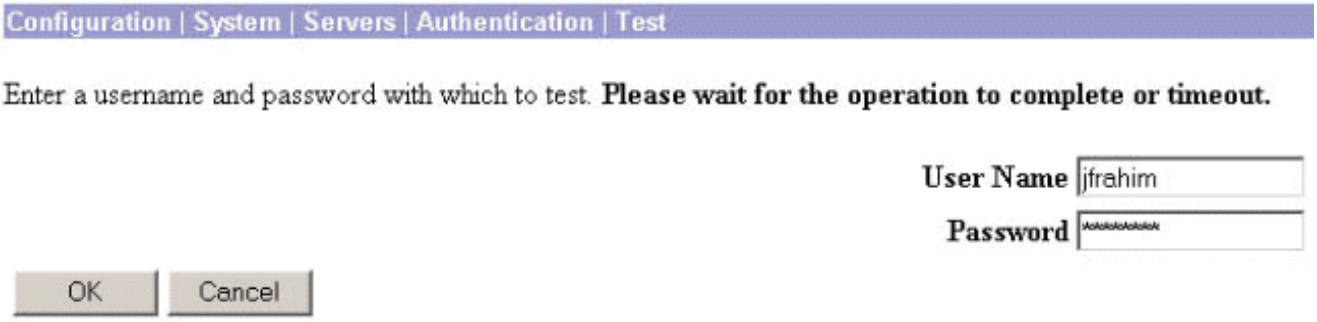
El concentrador ofrece una función para probar la autenticación de RADIUS. Para probar esta característica correctamente, aseegurese que usted sigue los siguientes pasos cuidadosamente.

Prueba de autenticación de RADIUS.

1. Vaya al **Configuration (Configuración) > Sytem (Sistema) > Servers (Servidores) > Authentication (Autenticación)**. Seleccione a su servidor de RADIUS y haga clic la **prueba**.



2. Cuando se le pregunte, teclee su nombre de usuario de dominio de NT y contraseña, y después haga clic la **AUTORIZACIÓN**. El ejemplo debajo del Nombre de usuario “jfrahim” de las demostraciones configuró en el servidor del dominio de NT con el "cisco123" como la contraseña.



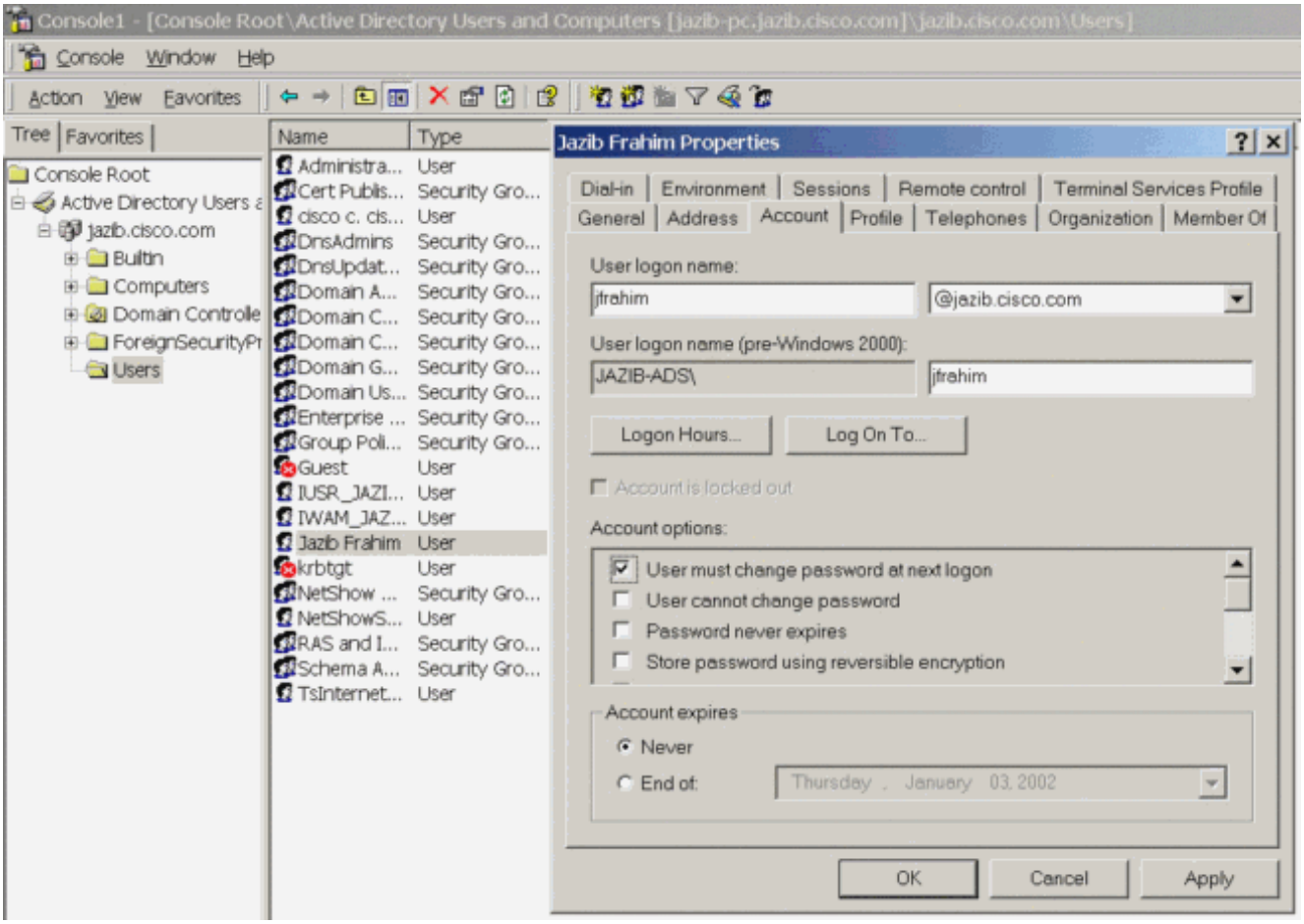
3. Si su autenticación se configura correctamente, usted debe conseguir un mensaje que expone la “autenticación

acertado.” Si usted recibe cualquier mensaje con excepción del que está mostrado arriba, hay cierta configuración o Problema de conexión. Relance por favor la configuración y los pasos de prueba delineados en este documento para asegurarse de que todas las configuraciones fueron hechas correctamente. También verifique la conectividad IP entre sus dispositivos.

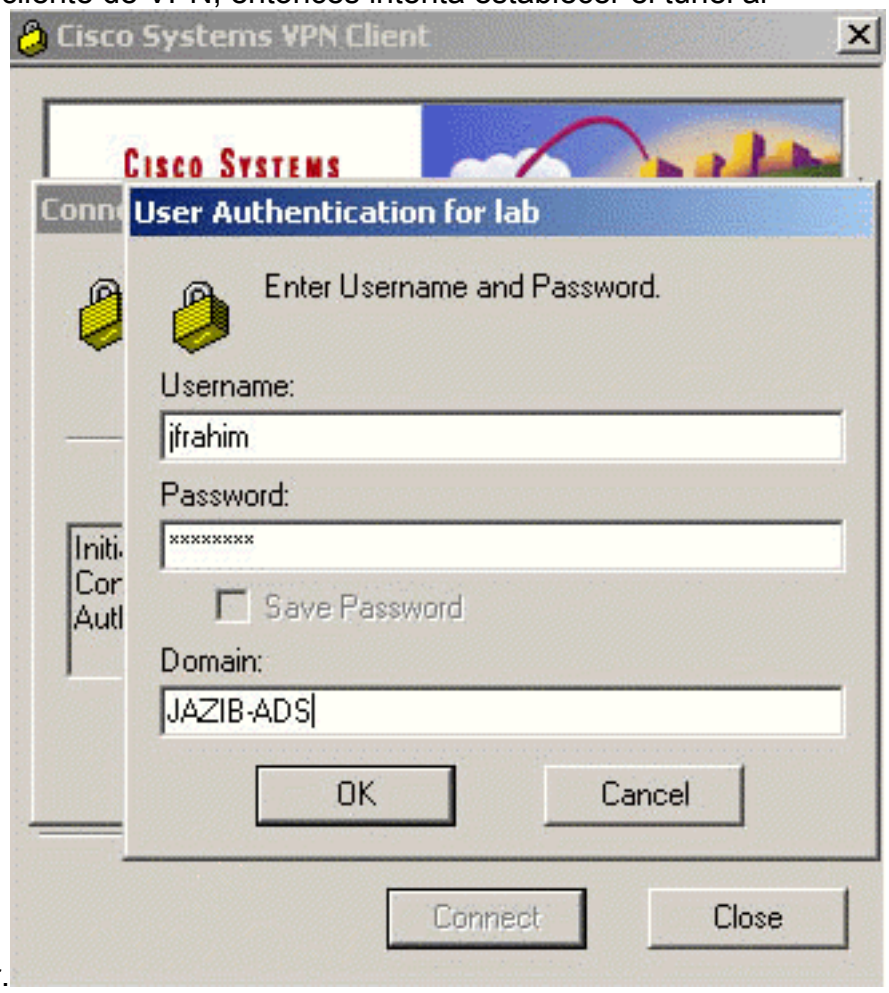
Autenticación de dominio NT real mediante el proxy de RADIUS para probar la característica de vencimiento de contraseña

1. Si definen al usuario ya en el servidor del dominio, modifique las propiedades de modo que se indique al usuario que cambie la contraseña en el inicio siguiente. Vaya a la lengueta de la “cuenta” del cuadro de diálogo de las propiedades de usuario, seleccionan la opción para

usuario **debe cambiar la contraseña en el inicio siguiente**, después hace clic la **AUTORIZACIÓN**.



2. El Ejecute el cliente de VPN, entonces intenta establecer el túnel al concentrador.



3. Durante la autenticación de usuario, a le debe indican que cambie la contraseña.

Información Relacionada

- Concentrador Cisco VPN serie 3000
- IPSec
- Cisco Secure Access Control Server para Windows
- RADIUS
- Solicitudes de Comentarios (RFC)