Cisco Secure ACS: Restricciones del acceso a la red con los clientes AAA para los usuarios y los grupos de usuarios

Contenido

Introducción

Este documento describe cómo configurar las Restricciones del acceso a la red (NAR) en la versión 4.x de Cisco Secure Access Control Server (ACS) con los clientes AAA (incluidos los routers, PIX, ASA, controladores inalámbricos) para los usuarios y grupos de usuarios.

prerrequisitos

Requisitos

Este documento se crea con la suposición que configuran y trabajan el Cisco Secure ACS y a los clientes AAA correctamente.

Componentes Utilizados

La información en este documento se basa en el 3.0 del Cisco Secure ACS y posterior.

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

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Restricciones de acceso a la red

Esta sección describe los NAR, y proporciona las Instrucciones detalladas de configurar y de manejar los NAR compartidos.

Esta sección contiene estos temas:

- Sobre las restricciones del acceso a la red
- Agregue un NAR compartido
- Edite un NAR compartido
- Borre un NAR compartido

Sobre las restricciones del acceso a la red

Un NAR es una definición, que usted hace en el ACS, de las condiciones adicionales que usted debe cumplir antes de que un usuario pueda acceder la red. El ACS aplica estas condiciones usando la información de los atributos que sus clientes AAA envían. Aunque usted pueda configurar los NAR de varias maneras, todos se basan en la información de atributo que corresponde con que un cliente AAA envía. Por lo tanto, usted debe entender el formato y el contenido de los atributos que sus clientes AAA envían si usted quiere emplear los NAR eficaces.

Cuando usted configura un NAR, usted puede elegir si el filtro actúa positivamente o negativamente. Es decir, en el NAR usted especifica si al acceso a la red del permit or deny, sobre la base de la información enviada de los clientes AAA cuando está comparado a la información salvada en el NAR. Sin embargo, si un NAR no encuentra la información suficiente para actuar, omite el acceso negado. Esta tabla muestra estas condiciones:

	Basado en IP	No IP basado	Información insuficiente
Permiso	Acceso concedido	Acceso negado	Acceso negado
Niegue	Acceso negado	Acceso concedido	Acceso negado

El ACS apoya dos tipos de filtros NAR:

- **Filtros basados en IP** — Acceso basado en IP del límite de los filtros NAR basado en los IP Addresses del cliente del usuario final y del cliente AAA. Vea la sección alrededor de basada en IP de los filtros NAR para más información.
- **filtros NON-IP-basados** — acceso NON-IP-basado del límite de los filtros NAR basado en la comparación de cadenas simple de un valor enviado del cliente AAA. El valor puede ser el número del Calling Line Identification (CLI), el número del Dialed Number Identification Service (DNIS), la dirección MAC, u otro valor que origina del cliente. Para este tipo de NAR a actuar, el valor en la descripción NAR debe hacer juego exactamente qué se está enviando

del cliente, que incluye se utiliza cualquier formato. Por ejemplo, el (217) 555-4534 del número de teléfono no hace juego 217-555-4534. Vea la sección alrededor NON-IP-basada de los filtros NAR para más información.

Usted puede definir un NAR para, y aplica lo, a un usuario o a un grupo de usuarios específico. Vea las restricciones del acceso a la red del conjunto para un usuario o fije las restricciones del acceso a la red para las secciones de un grupo de usuarios para más información. Sin embargo, en la sección de los componentes del perfil compartidos del ACS usted puede crear y nombrar un NAR compartido sin directamente la citación de cualquier usuario o grupo de usuarios. Usted da a NAR compartido un nombre que se pueda referir a otras partes de la interfaz Web ACS. Entonces, cuando usted configura los usuarios o a los grupos de usuarios, usted no puede seleccionar ninguno, uno, o las restricciones compartidas múltiplo ser aplicado. Cuando usted especifica la aplicación de los NAR compartidos múltiplo a un usuario o a un grupo de usuarios, usted elige uno de dos criterios del acceso:

- Todos los filtros seleccionados deben permitir.
- Cualquier un filtro seleccionado debe permitir.

Usted debe entender el orden de preferencia que se relaciona con los diversos tipos de NAR. Ésta es la orden de la filtración NAR:

1. NAR compartido en el nivel del usuario
2. NAR compartido en el nivel de grupo
3. NAR NON-compartido en el nivel del usuario
4. NAR NON-compartido en el nivel de grupo

Usted debe también entender que la **negación del acceso en cualquier nivel toma la precedencia sobre las configuraciones en otro nivel que no niegan el acceso**. Ésta es la una excepción en el ACS a la regla que las configuraciones del nivel de usuario reemplazan las configuraciones del grupo-nivel. Por ejemplo, un usuario determinado no pudo tener ninguna restricción NAR en el nivel del usuario que se aplica. Sin embargo, si ese usuario pertenece a un grupo que sea restringido por un NAR compartido o NON-compartido, niegan el usuario el acceso.

Los NAR compartidos se mantienen la base de datos interna ACS. Usted puede utilizar las características de reserva ACS y del restore para sostener, y las restablece. Usted puede también replicar los NAR compartidos, junto con otras configuraciones, a los ACS secundarios.

Sobre los filtros basados en IP NAR

Para los filtros basados en IP NAR, el ACS utiliza los atributos como se muestra, que depende del protocolo AAA del pedido de autenticación:

- **Si usted está utilizando el TACACS+** — El campo del `rem_addr del` cuerpo del paquete del comienzo TACACS+ se utiliza.**Note**: Cuando un pedido de autenticación es remitido por el proxy a un ACS, cualquier NAR para las peticiones TACACS+ se aplica a la dirección IP del servidor de AAA de la expedición, no a la dirección IP del cliente AAA el originar.
- **Si usted está utilizando RADIUS IETF** — `La llamar-estación-identificación` (atributo 31) debe ser utilizada.**Note**: Los filtros basados en IP NAR funcionan solamente si el ACS recibe atributos Llamar-Estación-identificación del radio los 31) (. La Llamar-Estación-identificación (31) debe contener un IP Address válido. Si no hace, caerá a las reglas DNIS.

Los clientes AAA que no proporcionan la suficiente información de la dirección IP (por ejemplo, algunos tipos de Firewall) no soportan las funciones completas NAR.

Otros atributos para las restricciones **basadas en IP**, por el protocolo, incluyen los campos NAR como se muestra:

- **Si usted está utilizando el TACACS+** — Los campos NAR en el ACS utilizan estos valores:**Cliente AAA** — El Nas-ip-address se toma de la dirección de origen en el socket entre el ACS y el cliente TACACS+.**Puerto** — El campo de puerto se toma del cuerpo del paquete del comienzo TACACS+.

Sobre los filtros NON-IP-basados NAR

Un filtro NON-IP-basado NAR (es decir, un filtro DNIS/CLI-based NAR) es una lista de llamada o de punta permitida o negada de las ubicaciones del acceso que usted puede utilizar para restringir a un cliente AAA cuando usted no tiene una conexión basada en IP establecida. La característica NON-IP-basada NAR utiliza generalmente el número CLI y el número DNIS.

Sin embargo, cuando usted ingresa un IP Address en lugar del CLI, usted puede utilizar el filtro NON-IP-basado; incluso cuando el cliente AAA no utiliza una versión de software de Cisco IOS® que soporte el CLI o el DNIS. En otra excepción a ingresar un CLI, usted puede ingresar un MAC address al acceso del permit or deny. Por ejemplo, cuando usted está utilizando a un cliente AAA del Cisco Aironet. Asimismo, usted podría ingresar el MAC address del Cisco Aironet AP en lugar del DNIS. El formato de lo que usted especifica en el cuadro CLI — CLI, dirección IP, o dirección MAC — debe hacer juego el formato de lo que usted recibe de su cliente AAA. Usted puede determinar este formato de su archivo de registro del RADIO.

Los atributos para las restricciones DNIS/CLI-based, por el protocolo, incluyen los campos NAR como se muestra:

- **Si usted está utilizando el TACACS+** — Los campos NAR enumerados emplean estos valores:**Cliente AAA** — `El Nas-ip-address` se toma de la dirección de origen en el socket entre el ACS y el cliente TACACS+.**Puerto** — El campo de `puerto` en el cuerpo del paquete del comienzo TACACS+ se utiliza.**CLI** — El campo del REM-`addr` en el cuerpo del paquete del comienzo TACACS+ se utiliza.**DNIS** — El campo del REM-`addr` tomado del cuerpo del paquete del comienzo TACACS+ se utiliza. En los casos en los cuales los datos del REM-addr comienzan con la raya vertical (/), el campo DNIS contiene los datos del REM-addr sin la raya vertical (/).**Note**: Cuando un pedido de autenticación es remitido por el proxy a un ACS, cualquier NAR para las peticiones TACACS+ se aplica a la dirección IP del servidor de AAA de la expedición, no a la dirección IP del cliente AAA el originar.
- **Si usted está utilizando el RADIUS** — Los campos NAR enumerados utilizan estos valores:**Cliente AAA** — `El Nas-ip-address` (se utiliza el atributo 4) o, si no existe el Nas-ip-address, el NAS-`identificador` (atributo de RADIUS 32).**Puerto** — `El NAS-puerto` (se utiliza el atributo 5) o, si no existe el NAS-puerto, el `nas-port-id` (atributo 87).**CLI** — Se utiliza El llamar-estación-`ID` (atributo 31).**DNIS** — Se utiliza El llamar-estación-`ID` (atributo 30).

Cuando usted especifica un NAR, usted puede utilizar un asterisco (*) como comodín para cualquier valor, o como parte de cualquier valor para establecer un rango. Todos los valores o condiciones en una descripción NAR se deben cumplir para que el NAR restrinja el acceso. Esto significa que los valores contienen un boleano Y.

Agregue un NAR compartido

Usted puede crear un NAR compartido que contenga muchas restricciones de acceso. Aunque la

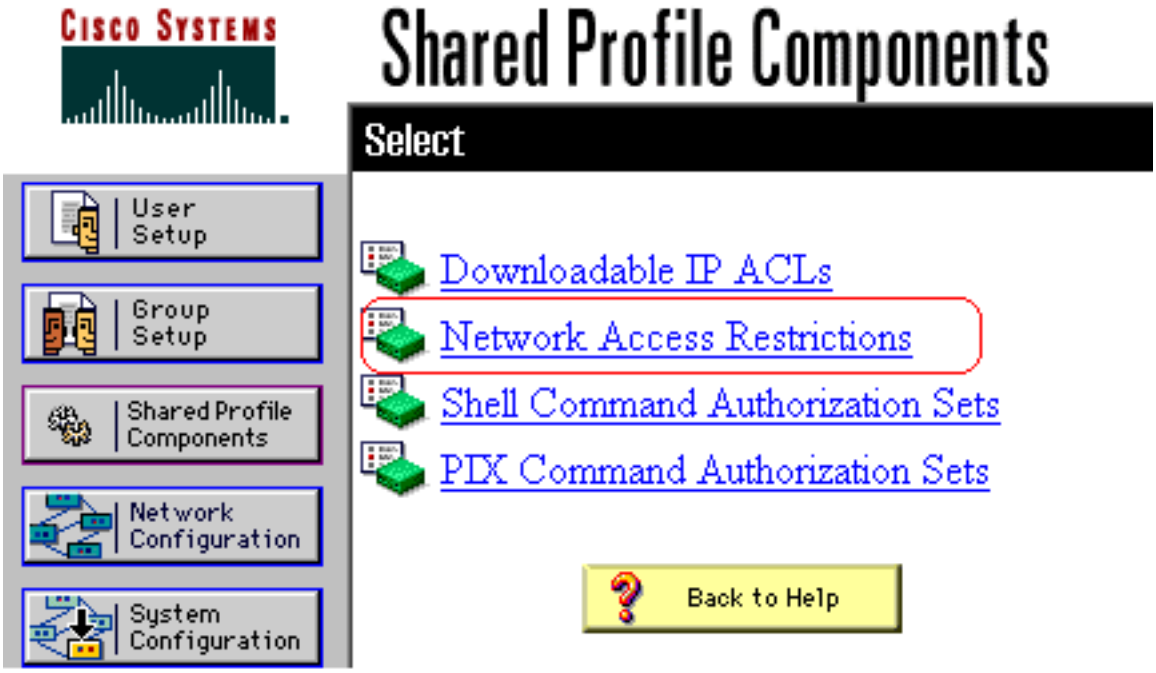
interfaz Web ACS no aplique los límites al número de restricciones de acceso en un NAR compartido o a la longitud de cada restricción de acceso, usted debe adherirse a estos límites:

- La combinación de campos para cada elemnto de línea no puede exceder 1024 caracteres.
- El NAR compartido no puede tener más de 16 KB de los caracteres. Los elementos de la cantidad de líneas soportados dependen de la longitud de cada elemnto de línea. Por ejemplo, si usted crea un CLI/DNIS-based NAR donde están 10 caracteres los nombres del cliente AAA, los números del puerto son 5 caracteres, las entradas CLI son 15 caracteres, y las entradas DNIS son 20 caracteres, usted pueden agregar 450 elemntos de línea antes de que usted alcance el límite 16 KB.

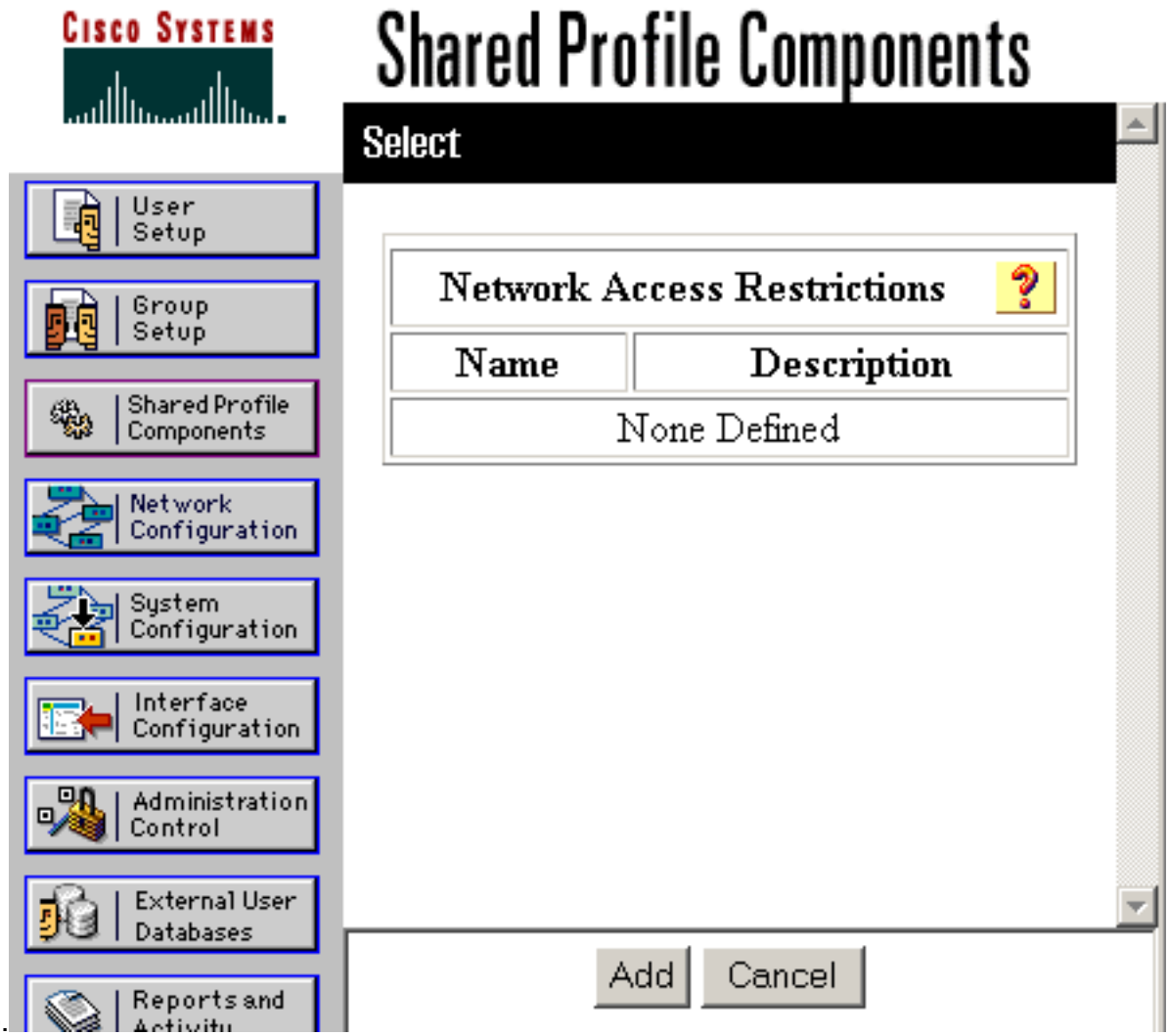
Note: Antes de que usted defina un NAR, asegúrese que usted haya establecido los elementos que usted se prepone utilizar en ese NAR. Por lo tanto, usted debe haber especificado todo el NAFs y NDGs, y haber definido a todos los clientes AAA relevantes, antes de que usted les haga a la parte de la definición NAR. Vea alrededor la sección de las restricciones del acceso a la red para más información.

Complete estos pasos para agregar un NAR compartido:

1. En la barra de navegación, haga clic a los **componentes del perfil compartidos**.La ventana de los componentes del perfil compartidos aparece.

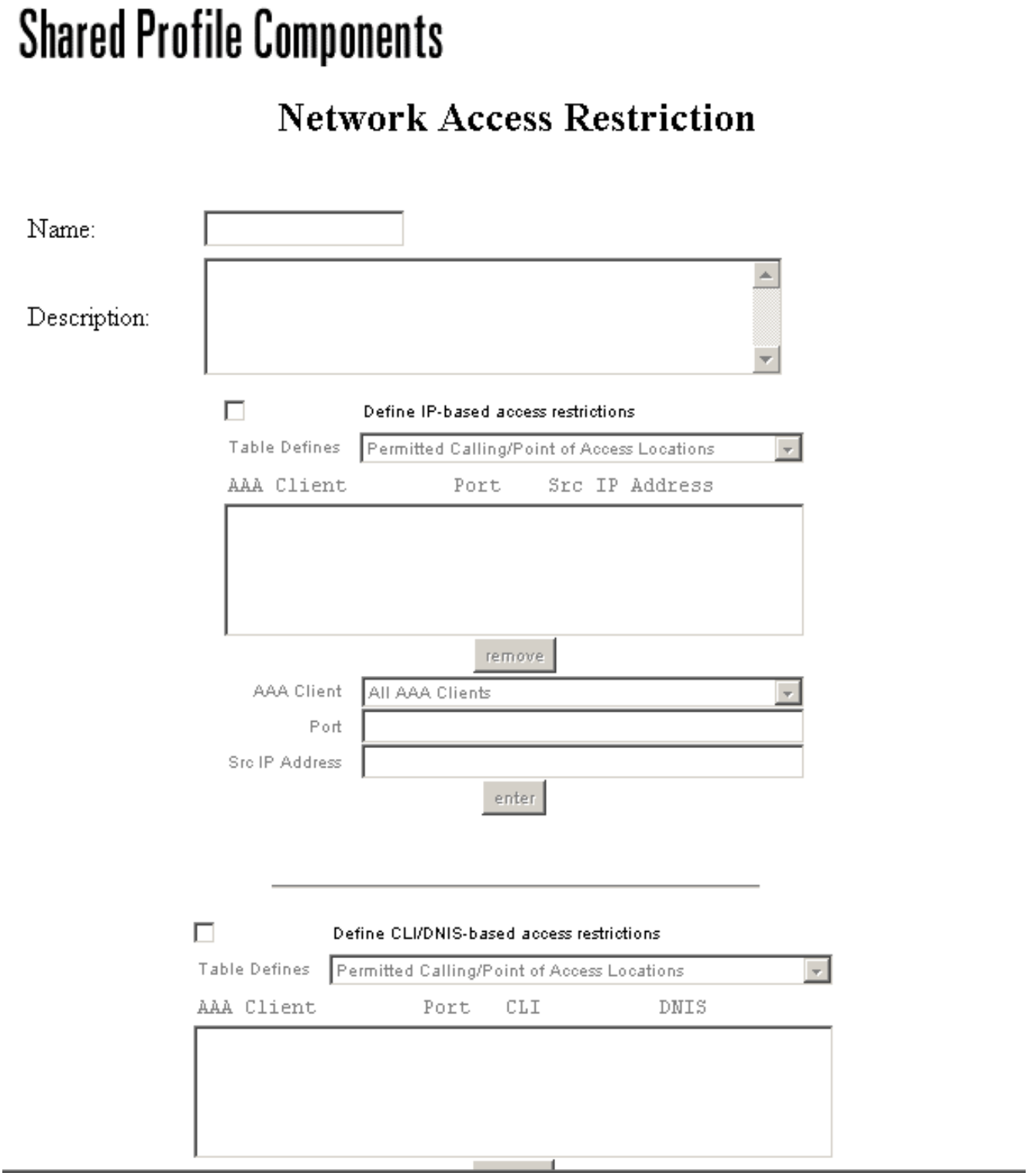


2. **Restricciones del acceso a la red del**



tecleo.

3. Haga clic en Add (Agregar).La ventana de la restricción del acceso a la red aparece.



4. En el cuadro de nombre, ingrese un nombre para el nuevo NAR compartido.**Note**: El nombre puede contener hasta 31 caracteres. El llevar y los espacios finales no se permiten. Los nombres no pueden contener estos caracteres: corchete izquierdo ([), right bracket (]), coma (,), o raya vertical (/).
5. En el rectángulo de la descripción, ingrese una descripción del nuevo NAR compartido. La descripción puede ser hasta 30,000 caracteres.
6. Si usted quiere al permit or deny el acceso basado en el IP Addressing:Marque la casilla de verificación **basada en IP de las descripciones del acceso de la definición**.Para especificar si usted está enumerando los direccionamientos se permiten o se niegan que, de la tabla define la lista, seleccionan el valor aplicable.Seleccione o ingrese la información aplicable en cada uno de estos rectángulos:**Cliente AAA** — Seleccione **todos los clientes AAA**, o el nombre del NDG, o del cliente AAA NAF, o individual, a quien se permite o se niega el

acceso.**Puerto** — Ingrese el número del puerto al cual usted quiere al permit or deny el acceso. Usted puede utilizar el asterisco (*) como comodín al acceso del permit or deny a todos los puertos en el cliente AAA seleccionado.**IP Address del src** — Ingrese el IP Address para filtrar en al realizar las restricciones de acceso. Usted puede utilizar el asterisco (*) como comodín para especificar todos los IP Addresses.**Note**: El número total de caracteres en la lista del cliente AAA, y el puerto y las casillas de IP Addresses del src, no deben exceder de 1024. Aunque el ACS valide más de 1024 caracteres cuando usted agrega un NAR, usted no puede editar el NAR y el ACS no puede aplicarlo exactamente a los usuarios.El tecleo **ingresa**.El cliente AAA, el puerto, y la información de dirección aparecen como elemnto de línea en la tabla.Relance los pasos c y d para ingresar los elemntos de línea basados en IP adicionales.

7. Si usted quiere al permit or deny el acceso basado en la llamada de la ubicación o de los valores con excepción de los IP Addresses:Marque la casilla de verificación **basada CLI/DNIS de las restricciones de acceso de la definición**.Para especificar si usted está enumerando las ubicaciones se permiten que o negado de la tabla define la lista, seleccione el valor aplicable.Para especificar a los clientes a quienes este NAR se aplica, seleccione uno de estos valores de la lista del cliente AAA:El nombre del NDGEl nombre del cliente AAA determinadoTodos los clientes AAA**Consejo:** Solamente NDGs que usted ha configurado ya es mencionado.Para especificar la información en la cual este NAR debe filtrar, ingrese los valores en estos rectángulos, como aplicable:**Consejo:** Usted puede ingresar un asterisco (*) como comodín para especificar **todos** como valor.**Puerto** — Ingrese el número del puerto en el cual filtrar.**CLI** — Ingrese el número CLI en el cual filtrar. Usted puede también utilizar este cuadro para restringir el acceso basado en los valores con excepción de los CLI, tales como una dirección IP o una dirección MAC. Vea alrededor la sección de las restricciones del acceso a la red para más información.**DNIS** — Ingrese el número que es marcado adentro en a cuál para filtrar.**Note**: El número total de caracteres en la lista del cliente AAA y los cuadros del puerto, CLI, y DNIS no debe exceder de 1024. Aunque el ACS valide más de 1024 caracteres cuando usted agrega un NAR, usted no puede editar el NAR y el ACS no puede aplicarlo exactamente a los usuarios.El tecleo **ingresa**.La información que especifica el elemnto de línea NAR aparece en la tabla.Relance los pasos c a e para ingresar los elemntos de línea NON-IP-basados adicionales NAR.El tecleo **somete** para salvar la definición compartida NAR.El ACS guarda el NAR compartido y lo enumera en la tabla de las **restricciones del acceso a la red**.

Edite un NAR compartido

Complete estos pasos para editar un NAR compartido:

1. En la barra de navegación, haga clic a los **componentes del perfil compartidos**.La ventana de los componentes del perfil compartidos aparece.
2. **Restricciones del acceso a la red del** tecleo.La tabla de las restricciones del acceso a la red aparece.
3. En la columna del nombre, haga clic el NAR compartido que usted quiere editar.La ventana de la restricción del acceso a la red aparece y visualiza la información para el NAR seleccionado.
4. Edite el nombre o la descripción del NAR, como aplicable. La descripción puede ser hasta 30,000 caracteres.
5. Para editar un elemnto de línea en la tabla basada en IP de las restricciones de

acceso:Haga doble clic el elemnto de línea que usted quiere editar.La información para el elemnto de línea se quita de la tabla y se escribe a los cuadros bajo la tabla.Edite la información, cuanto sea necesario.**Note**: El número total de caracteres en la lista del cliente AAA y el puerto y las casillas de IP Addresses del src no debe exceder de 1024. Aunque el ACS pueda validar más de 1024 caracteres cuando usted agrega un NAR, usted no puede editar tal NAR y ACS no puede aplicarlo exactamente a los usuarios.El tecleo **ingresa**.La información editada para este elemnto de línea se escribe a la tabla basada en IP de las restricciones de acceso.

6. Para quitar un elemnto de línea de la tabla basada en IP de las restricciones de acceso:Seleccione el elemnto de línea.Bajo la tabla, el tecleo **quita**.El elemnto de línea se quita de la tabla basada en IP de las restricciones de acceso.
7. Para editar un elemnto de línea en la tabla de las restricciones de acceso CLI/DNIS:Haga doble clic el elemnto de línea que usted quiere editar.La información para el elemnto de línea se quita de la tabla y se escribe a los cuadros bajo la tabla.Edite la información, cuanto sea necesario.**Note**: El número total de caracteres en la lista del cliente AAA y los cuadros del puerto, CLI, y DNIS no debe exceder de 1024. Aunque el ACS pueda validar más de 1024 caracteres cuando usted agrega un NAR, usted no puede editar tal NAR y ACS no puede aplicarlo exactamente a los usuarios.El tecleo **ingresa**La información editada para este elemnto de línea se escribe a la tabla de las restricciones de acceso CLI/DNIS.
8. Para quitar un elemnto de línea de la tabla de las restricciones de acceso CLI/DNIS:Seleccione el elemnto de línea.Bajo la tabla, el tecleo **quita**.El elemnto de línea se quita de la tabla de las restricciones de acceso CLI/DNIS.
9. El tecleo **somete** para salvar los cambios que usted ha realizado.El ACS entra el filtro de nuevo con la nueva información, que toma el efecto inmediatamente.

Borre un NAR compartido

Note: Asegúrese de que usted quite la asociación de un NAR compartido a cualquier usuario o agrúpelo antes de que usted borre ese NAR.

Complete estos pasos para borrar un NAR compartido:

1. En la barra de navegación, haga clic a los **componentes del perfil compartidos**.La ventana de los componentes del perfil compartidos aparece.
2. **Restricciones del acceso a la red del** tecleo.
3. Haga clic el nombre del NAR compartido que usted quiere borrar.La ventana de la restricción del acceso a la red aparece y visualiza la información para el NAR seleccionado.
4. En la parte inferior de la ventana, **cancelación del** tecleo.Un cuadro de diálogo le advierte que usted esté a punto de borrar un NAR compartido.
5. Haga Click en OK para confirmar que usted quiere borrar el NAR compartido.Se borra El NAR compartido seleccionado.

Fije las restricciones del acceso a la red para un usuario

Usted utiliza la tabla de las restricciones del acceso a la red en el área avanzada de las configuraciones de la configuración de usuario para fijar los NAR de tres maneras:

- Aplique los NAR compartidos existentes por nombre.

- Defina las restricciones de acceso basadas en IP al acceso del usuario del permit or deny a un cliente AAA especificado o a los puertos especificados en un cliente AAA cuando se ha establecido una conexión IP.
- Defina las restricciones de acceso CLI/DNIS-based al acceso del usuario del permit or deny basado en el CLI/DNIS se utiliza que.**Note**: Usted puede también utilizar el área de las restricciones de acceso CLI/DNIS-based para especificar otros valores. Vea la sección de las restricciones del acceso a la red para más información.

Típicamente, usted define los NAR (compartidos) dentro de la sección compartida de los componentes de modo que usted pueda aplicar estas restricciones a más de un grupo o usuario. Vea el agregar una sección compartida NAR para más información. Usted debe haber seleccionado la casilla de verificación de las **restricciones del acceso a la red del nivel de usuario** en la página opciones avanzada de la sección de configuración de la interfaz para que este conjunto de opciones aparezca en la interfaz Web.

Sin embargo, usted puede también utilizar el ACS para definir y para aplicar un NAR para un único usuario dentro de la sección de configuración de usuario. Usted debe haber habilitado las **restricciones del acceso a la red del nivel de usuario** que fijan en la página opciones avanzada de la sección de configuración de la interfaz para que las opciones de filtro basadas en IP del único usuario y las opciones de filtro del único usuario CLI/DNIS-based aparezcan en la interfaz Web.

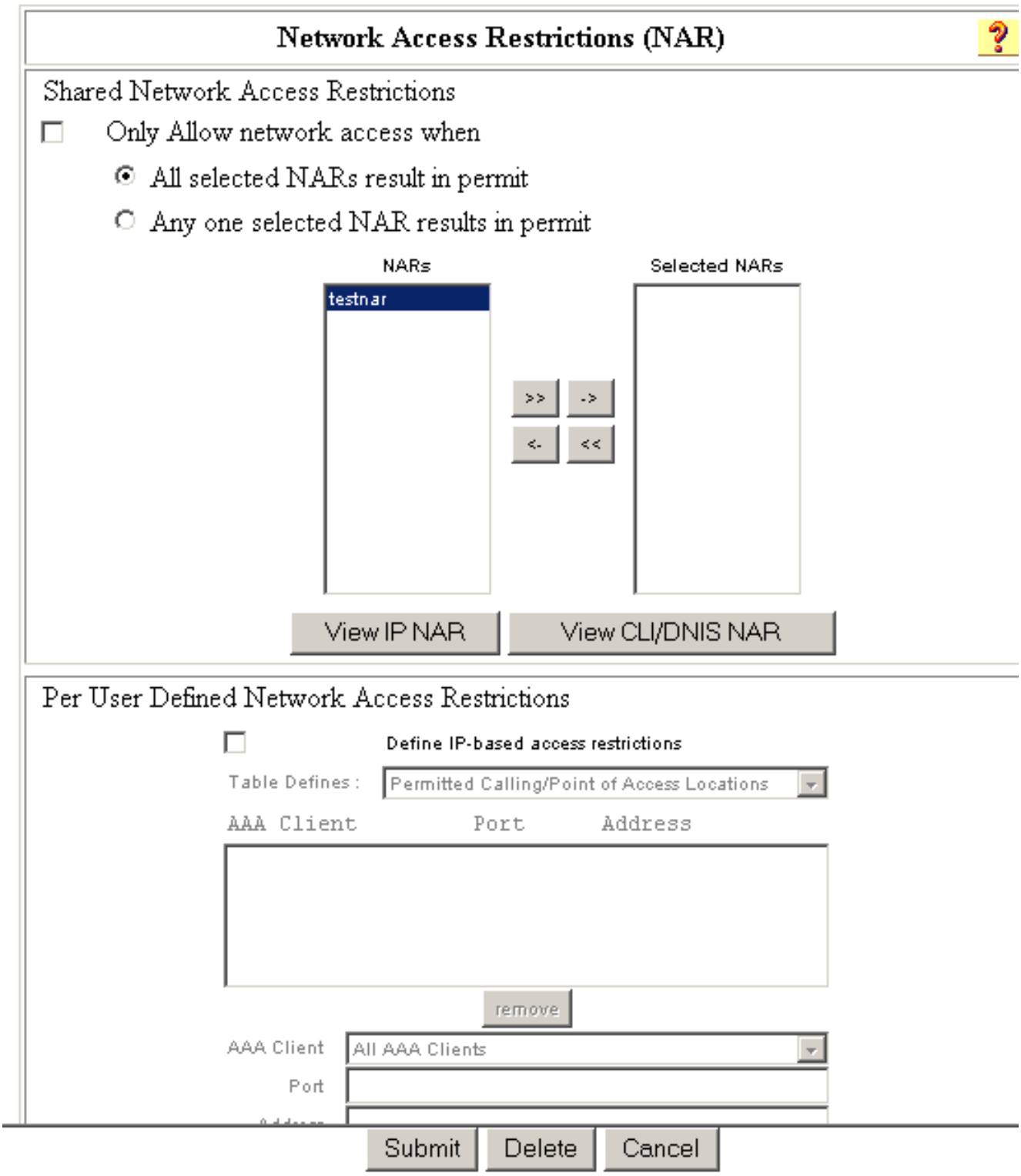
Note: Cuando un pedido de autenticación es remitido por el proxy a un ACS, cualquier NAR para las peticiones del Terminal Access Controller Access Control System (TACACS+) se aplica a la dirección IP del servidor de AAA de la expedición, no a la dirección IP del cliente AAA el originar.

Cuando usted crea las restricciones de acceso sobre por usuario una base, el ACS no aplica los límites al número de restricciones de acceso y no aplica un límite a la longitud de cada restricción de acceso. Sin embargo, hay límites estrictos:

- La combinación de campos para cada elemnto de línea no puede exceder 1024 caracteres de largo.
- El NAR compartido no puede tener más de 16 KB de los caracteres. Los elementos de la cantidad de líneas soportados dependen de la longitud de cada elemnto de línea. Por ejemplo, si usted crea un CLI/DNIS-based NAR donde están 10 caracteres los nombres del cliente AAA, los números del puerto son 5 caracteres, las entradas CLI son 15 caracteres, y las entradas DNIS son 20 caracteres, usted pueden agregar 450 elemntos de línea antes de que usted alcance el límite 16 KB.

Complete estos pasos para fijar los NAR para un usuario:

1. Realice los pasos 1 a 3 de agregar una cuenta de usuario básica.La configuración de usuario edita la ventana se abre. El nombre de usuario que usted agrega o edita aparece en la cima de la
ventana.



2. Para aplicar un NAR compartido previamente configurado a este usuario:**Note**: Para aplicar un NAR compartido, usted debe haber configuradolo bajo restricciones del acceso a la red en la sección de los componentes del perfil compartidos. Vea el agregar una sección compartida NAR para más información.Marque el **único permiten el acceso a la red cuando** casilla de verificación.Para especificar si un o todo el NAR compartidos deben solicitar el usuario para ser acceso permitido, seleccione uno, como aplicable:Todos los NAR

seleccionados dan lugar al permiso.Cualquier resultados seleccionados un NAR en el permiso.Seleccione un nombre compartido NAR en la lista NAR, y después haga clic --> (botón de la flecha correcta) trasladarse el nombre a los NAR seleccionados enumere.**Consejo:** Para ver los detalles del servidor de los NAR compartidos que usted ha seleccionado para aplicarse, usted puede hacer clic **IP NAR de la visión** o **ver CLID/DNIS NAR**, como aplicable.

3. Para definir y aplicar un NAR, para este usuario determinado, que permite o niega este acceso del usuario basado en la dirección IP, o dirección IP y puerto:**Note**: Usted debe definir la mayoría de los NAR dentro de la sección compartida de los componentes de modo que usted pueda aplicarlos a más de un grupo o usuario. Vea el agregar una sección compartida NAR para más información.En la tabla de las restricciones del acceso a la red, debajo por las restricciones definidas por el usario del acceso a la red, marque la casilla de verificación **basada en IP de las restricciones de acceso de la definición**.Para especificar si el anuncio subsiguiente especifica los IP Addresses permitidos o negados, de la tabla define la lista, eligen uno:**Permitted Calling/Point of Access LocationsDenied Calling/Point of Access Locations**Seleccione o ingrese la información en estos rectángulos:**Cliente AAA** — Seleccione **todos los clientes AAA**, o el nombre de un grupo de dispositivos de red (NDG), o el nombre del cliente AAA individual, a quien al acceso del permit or deny.**Puerto** — Ingrese el número del puerto al cual al acceso del permit or deny. Usted puede utilizar el asterisco (*) como comodín al acceso del permit or deny a todos los puertos en el cliente AAA seleccionado.**Direccionamiento** — Ingrese el IP Address o los direccionamientos para utilizar al realizar las restricciones de acceso. Usted puede utilizar el asterisco (*) como comodín.**Note**: El número total de caracteres en la lista del cliente AAA, y el puerto y las casillas de IP Addresses del src no deben exceder de 1024. Aunque el ACS valide más de 1024 caracteres cuando usted agrega un NAR, usted no puede editar el NAR y el ACS no puede aplicarlo exactamente a los usuarios.El tecleo **ingresa**.El cliente AAA, el puerto, y la información de dirección especificados aparece en la tabla sobre la lista del cliente AAA.
4. Para permit or deny este acceso del usuario basado en la llamada de la ubicación o de los valores con excepción de una dirección IP establecida:Marque la casilla de verificación **basada CLI/DNIS de las restricciones de acceso de la definición**.Para especificar si el anuncio subsiguiente especifica los valores permitidos o negados, de la tabla define la lista, eligen uno:**Permitted Calling/Point of Access LocationsDenied Calling/Point of Access Locations**Complete los cuadros como se muestra:**Note**: Usted debe hacer una entrada en cada cuadro. Usted puede utilizar el asterisco (*) como comodín para el todo o una parte de un valor. El formato que usted utiliza debe hacer juego el formato de la cadena que usted recibe de su cliente AAA. Usted puede determinar este formato de su archivo de registro del RADIO.**Cliente AAA** — Seleccione **todos los clientes AAA**, o el nombre del NDG, o el nombre del cliente AAA individual, a quien al acceso del permit or deny.**PUERTO** — Ingrese el número del puerto al cual al acceso del permit or deny. Usted puede utilizar el asterisco (*) como comodín al acceso del permit or deny a todos los puertos.**CLI** — Ingrese el número CLI al cual al acceso del permit or deny. Usted puede utilizar el asterisco (*) como comodín al acceso del permit or deny basó en la parte del número.**Consejo:** Utilice la entrada CLI si usted quiere restringir el acceso basado en otros valores tales como un MAC Address del cliente del Cisco Aironet. Vea alrededor la sección de las restricciones del acceso a la red para más información.**DNIS** — Ingrese el número DNIS al cual al acceso del permit or deny. Utilice esta entrada para restringir el acceso basado en el número en el cual el usuario marcará. Usted puede utilizar el asterisco (*) como comodín al acceso del permit or deny basó en la parte del número.**Consejo:** Utilice la selección DNIS si usted quiere restringir el

acceso basado en otros valores tales como una dirección MAC del Cisco Aironet AP. Vea alrededor la sección de las restricciones del acceso a la red para más información.**Note**: El número total de caracteres en la lista del cliente AAA y los cuadros del **puerto**, **CLI** y **DNIS** no debe exceder de 1024. Aunque el ACS valide más de 1024 caracteres cuando usted agrega un NAR, usted no puede editar el NAR y el ACS no puede aplicarlo exactamente a los usuarios.El tecleo **ingresa**.La información que especifica al cliente AAA, el puerto, el CLI, y el DNIS aparece en la tabla sobre la lista del cliente AAA.
5. Si le acaban que configura las opciones de la cuenta de usuario, el tecleo **somete** para registrar las opciones.

Fije las restricciones del acceso a la red para un grupo de usuarios

Usted utiliza la tabla de las restricciones del acceso a la red en la configuración de grupo para aplicar los NAR de tres maneras distintas:

- Aplique los NAR compartidos existentes por nombre.
- Defina las restricciones de acceso basadas en IP del grupo al acceso del permit or deny a un cliente AAA especificado o a los puertos especificados en un cliente AAA cuando se ha establecido una conexión IP.
- Defina el grupo NAR CLI/DNIS-based al acceso del permit or deny a, o ambos, el número CLI o el número DNIS usado.**Note**: Usted puede también utilizar el área de las restricciones de acceso CLI/DNIS-based para especificar otros valores. Vea alrededor la sección de las restricciones del acceso a la red para más información.

Típicamente, usted define los NAR (compartidos) dentro de la sección compartida de los componentes de modo que estas restricciones puedan aplicarse a más de un grupo o usuario. Vea el agregar una sección compartida NAR para más información. Usted debe marcar la casilla de verificación de la **restricción de acceso de la red compartida del Grupo-nivel** en la **página opciones avanzada de la** sección de configuración de la interfaz para que estas opciones aparezcan en la interfaz Web ACS.

Sin embargo, usted puede también utilizar el ACS para definir y para aplicar un NAR para un solo grupo dentro de la **sección de configuración de grupo**. Usted debe marcar la configuración de la **restricción del acceso a la red del Grupo-nivel** conforme a la página opciones avanzada de la sección de configuración de la interfaz para que las opciones de filtro basadas en IP del solo grupo y las solas opciones de filtro del grupo CLI/DNIS-based aparezcan en la interfaz Web ACS.

Note: Cuando un pedido de autenticación es remitido por el proxy a un servidor ACS, cualquier NAR para los pedidos de RADIUS se aplica a la dirección IP del servidor de AAA de la expedición, no a la dirección IP del cliente AAA el originar.

Complete estos pasos para fijar los NAR para un grupo de usuarios:

1. En la barra de navegación, haga clic la **configuración de grupo**.La ventana selecta de la configuración de grupo se abre.
2. De la lista del grupo, seleccione a un grupo, y después haga clic **editan las configuraciones**.El nombre del grupo aparece en la cima de la ventana de las configuraciones de
grupo.