NetScreen conceptos y ejemplos

Manual de referencia de ScreenOS

Volumen 8: Autenticación de usuarios

ScreenOS 5.1.0

Ref. 093-1373-000-SP

Revisión B

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with NetScreen's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR NETSCREEN REPRESENTATIVE FOR A COPY.

Contenido

Prefacio

El Volumen 8, “Autenticación de usuarios” describe los métodos de ScreenOS para autenticar diferentes tipos de usuarios. Contiene una introducción a la autenticación de usuarios, presenta las dos ubicaciones en las que se puede almacenar la base de datos de perfiles de usuarios (la base de datos interna y un servidor de autenticación externo), y luego proporciona numerosos ejemplos para configurar la autenticación, usuarios y grupos de usuarios IKE, XAuth y L2TP. También se tratan algunos otros aspectos de la autenticación de usuarios, como cambiar los mensajes de bienvenida de inicio de sesión, crear usuarios de múltiple tipos (por ejemplo, un usuario IKE/XAuth) y utilizar expresiones de grupos en directivas que aplican la autenticación.

CONVENCIONES

Este documento contiene distintos tipos de convenciones, que se explican en las siguientes secciones:

Convenciones de la interfaz de línea de comandos (CLI)

Las siguientes convenciones se utilizan para representar la sintaxis de los comandos de la interfaz de línea de comandos (CLI):

- Los comandos entre corchetes [ ] son opcionales.
- Los elementos entre llaves { } son obligatorios.
- Si existen dos o más opciones alternativas, aparecerán separadas entre sí por barras verticales (|). Por ejemplo:

  ```
  set interface { ethernet1 | ethernet2 | ethernet3 } manage
  ```

  significa "establecer las opciones de administración de la interfaz ethernet1, ethernet2 o ethernet3".
- Las variables aparecen en *cursiva*. Por ejemplo:

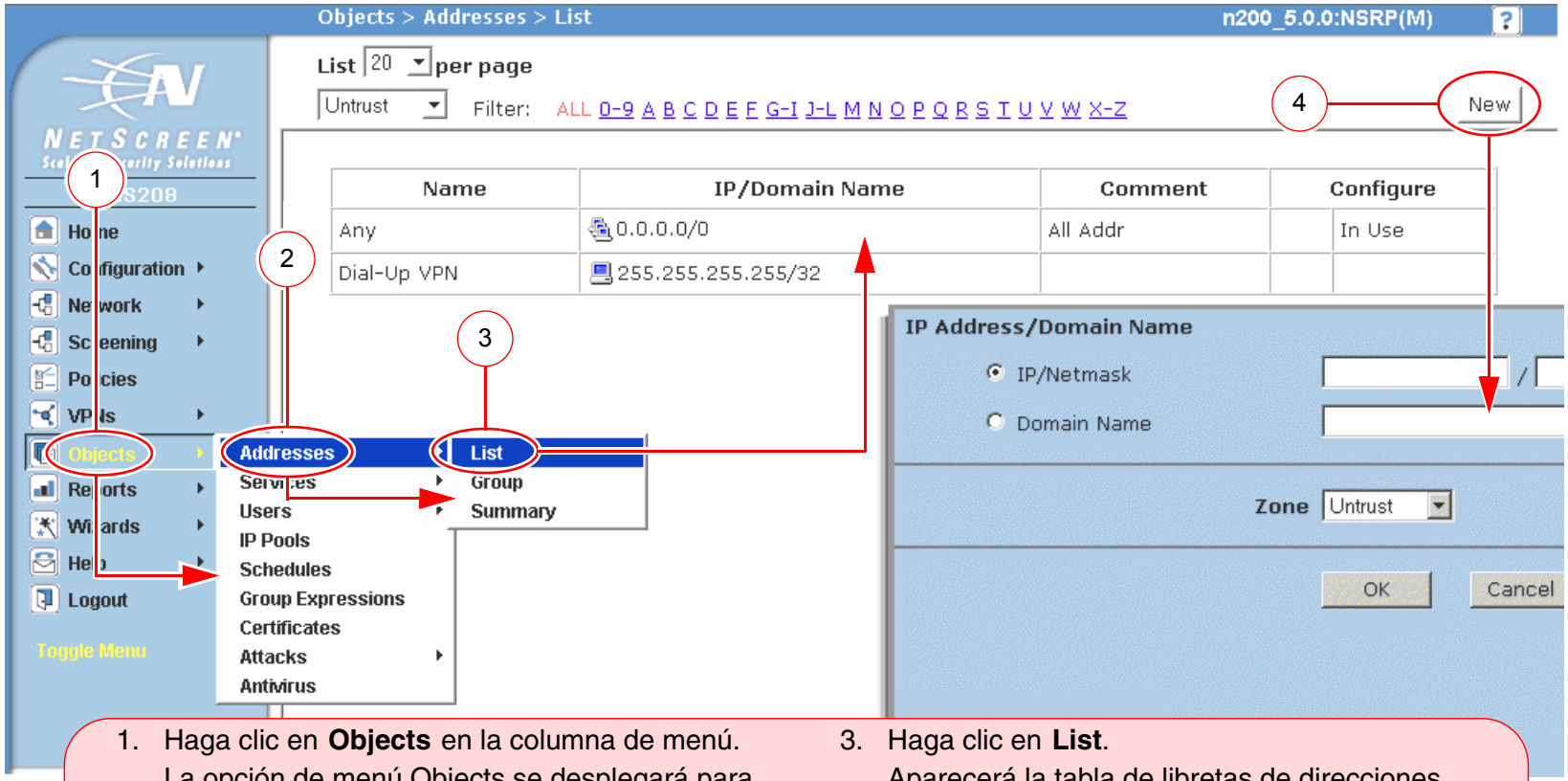
  ```
  set admin user name password
  ```

Los comandos CLI insertados en el contexto de una frase aparecen en **negrita** (salvo en el caso de las variables, que siempre aparecen en *cursiva*). Por ejemplo: "Utilice el comando **get system** para visualizar el número de serie de un dispositivo NetScreen".

Nota: *Para escribir palabras clave, basta con introducir los primeros caracteres que permitan al sistema reconocer de forma inequívoca la palabra que se está introduciendo. Por ejemplo, es suficiente escribir* ***set adm u joe j12fmt54*** *para que el sistema reconozca el comando* ***set admin user joe j12fmt54****. Aunque este método se puede utilizar para introducir comandos, en la presente documentación todos ellos se representan con sus palabras completas.*

Convenciones de la interfaz gráfica (WebUI)

En este manual se utiliza la comilla angular (>) para indicar las rutas de navegación de la WebUI por las que se pasa al hacer clic en opciones de menú y vínculos. Por ejemplo, la ruta para abrir el cuadro de diálogo de configuración de direcciones se representa como sigue: **Objects > Addresses > List > New**. A continuación se muestra la secuencia de navegación.



1. Haga clic en **Objects** en la columna de menú.
   La opción de menú Objects se desplegará para mostrar las opciones subordinadas que contiene.
2. (Menú Applet) Sitúe el mouse sobre **Addresses**.
   (Menú DHTML) Haga clic en **Addresses**.
   La opción de menú Addresses se desplegará para mostrar las opciones subordinadas que contiene.
3. Haga clic en **List**.
   Aparecerá la tabla de libretas de direcciones.
4. Haga clic en el vínculo **New**.
   Aparecerá el cuadro de diálogo de configuración de nuevas direcciones.

Para llevar a cabo una tarea en la WebUI, en primer lugar debe acceder al cuadro de diálogo apropiado, donde podrá definir objetos y establecer parámetros de ajuste. El conjunto de instrucciones de cada tarea se divide en dos partes: la ruta de navegación y los datos de configuración. Por ejemplo, el siguiente conjunto de instrucciones incluye la ruta al cuadro de diálogo de configuración de direcciones y los ajustes de configuración que se deben realizar:

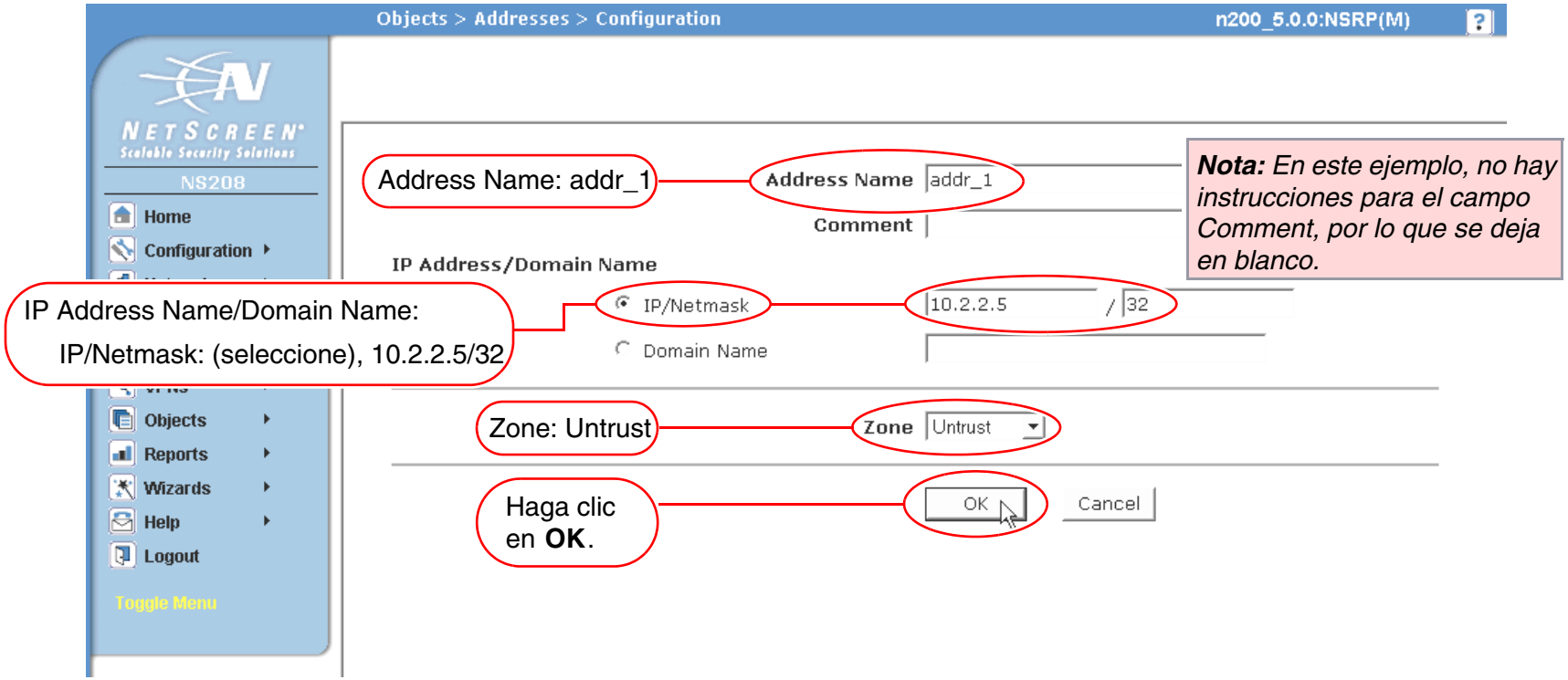
Objects > Addresses > List > New: Introduzca los siguientes datos y haga clic en **OK**:

Address Name: addr_1

IP Address/Domain Name:

IP/Netmask: (seleccione), 10.2.2.5/32

Zone: Untrust

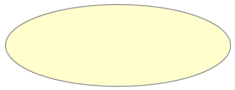


Convenciones para las ilustraciones

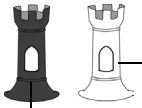
Los siguientes gráficos conforman el conjunto básico de imágenes utilizado en las ilustraciones de este manual:

Dispositivo NetScreen genérico

Dominio de enrutamiento virtual



Zona de seguridad



Interfaces de zonas de seguridad

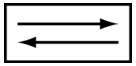
Blanca = interfaz de zona protegida (ejemplo: zona Trust)

Negra = interfaz de zona externa (ejemplo: zona sin confianza o zona Untrust)

Interfaz de túnel

Túnel VPN

Icono de enrutador (router)

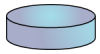


Icono de conmutador (switch)

Red de área local (LAN) con una única subred

(ejemplo: 10.1.1.0/24)

Internet



Rango de direcciones IP dinámicas (DIP)

Equipo de escritorio

Equipo portátil

Dispositivo de red genérico

(ejemplos: servidor NAT, concentrador de acceso)

Servidor

Convenciones de nomenclatura y conjuntos de caracteres

ScreenOS emplea las siguientes convenciones relativas a los nombres de objetos (como direcciones, usuarios administradores, servidores de autenticación, puertas de enlace IKE, sistemas virtuales, túneles de VPN y zonas) definidas en las configuraciones de ScreenOS.

- Si la secuencia de caracteres que conforma un nombre contiene al menos un espacio, la cadena completa deberá entrecomillarse mediante comillas dobles (“); por ejemplo, **set address trust “local LAN” 10.1.1.0/24**.
- NetScreen eliminará cualquier espacio al comienzo o al final de una cadena entrecomillada; por ejemplo, **“ local LAN ”** se transformará en **“local LAN”**.
- NetScreen tratará varios espacios consecutivos como uno solo.
- En las cadenas de nombres se distingue entre mayúsculas y minúsculas; por el contrario, en muchas palabras clave de la interfaz de línea de comandos pueden utilizarse indistintamente. Por ejemplo, **“local LAN”** es distinto de **“local lan”**.

ScreenOS admite los siguientes conjuntos de caracteres:

- Conjuntos de caracteres de un byte (SBCS) y conjuntos de caracteres de múltiples bytes (MBCS). Algunos ejemplos de SBCS son los juegos de caracteres ASCII, europeo y hebreo. Entre los conjuntos MBCS, también conocidos como conjuntos de caracteres de doble byte (DBCS), se encuentran el chino, el coreano y el japonés.

  Nota: *Una conexión de consola sólo admite conjuntos SBCS. La WebUI admite tanto SBCS como MBCS, según el conjunto de caracteres que admita el explorador web.*

- Caracteres ASCII desde el 32 (0x20 en hexadecimal) al 255 (0xff); a excepción de las comillas dobles (“), que tienen un significado especial como delimitadores de cadenas de nombres que contengan espacios.

DOCUMENTACIÓN DE NETSCREEN DE JUNIPER NETWORKS

Para obtener documentación técnica sobre cualquier producto NetScreen de Juniper Networks, visite www.juniper.net/techpubs/.

Para obtener soporte técnico, abra un expediente de soporte utilizando el vínculo “Case Manager” en la página web http://www.juniper.net/support/ o llame al teléfono 1-888-314-JTAC (si llama desde los EE.UU.) o al +1-408-745-9500 (si llama desde fuera de los EE.UU.).

Si encuentra algún error o omisión en esta documentación, póngase en contacto con nosotros a través de la siguiente dirección de correo electrónico:

techpubs-comments@juniper.net

1

Autenticación

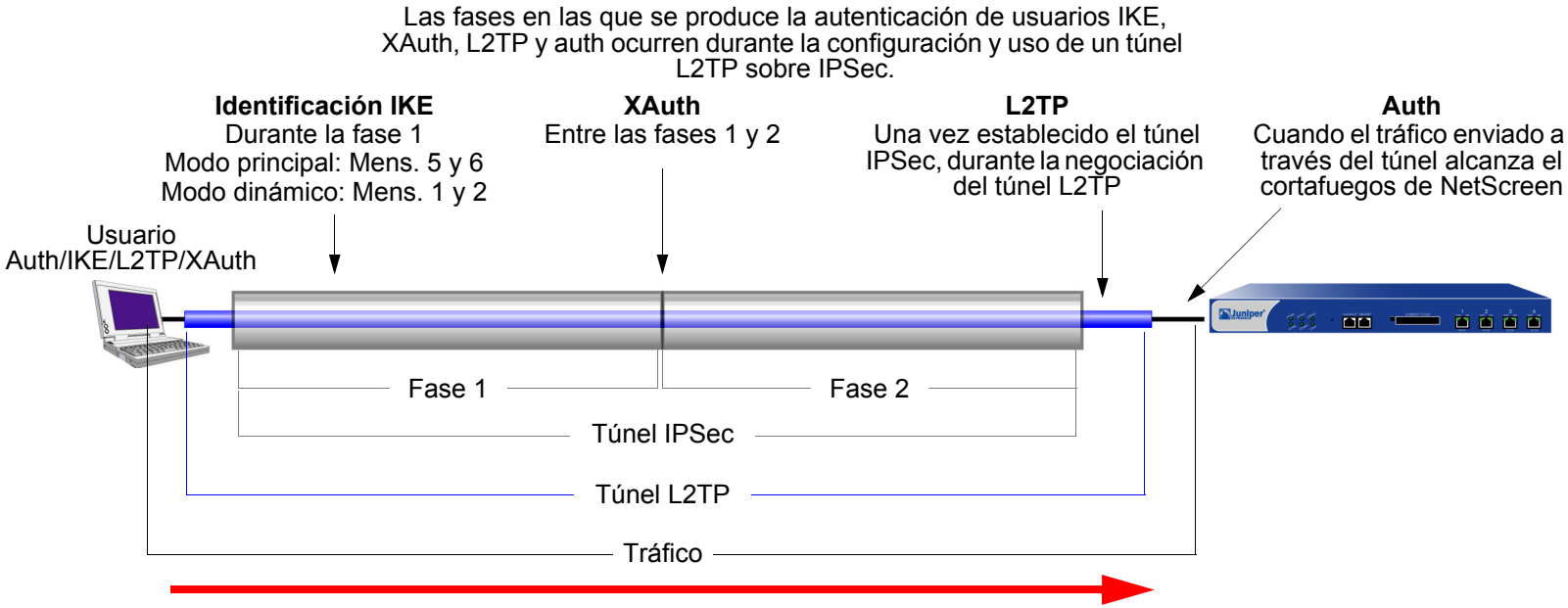
Después de una introducción general a los diferentes tipos de autenticación disponibles para los diferentes tipos de usuarios de la red, este capítulo dedica una breve sección a la autenticación del usuario administrador (admin). A continuación, proporciona información sobre la combinación de diferentes tipos de usuarios, la utilización de expresiones de grupos y cómo personalizar los mensajes de bienvenida que aparecen al iniciar una sesión HTTP, FTP, L2TP, Telnet y XAuth. Este material se presenta en las siguientes secciones:

TIPOS DE AUTENTICACIONES DE USUARIOS

En los siguientes capítulos se describen los diferentes tipos de usuarios y grupos de usuarios que se pueden crear y cómo utilizarlos al configurar directivas, puertas de enlace IKE y túneles L2TP:

- “Usuarios de autenticación” en la página 43
- “Usuarios y grupos de usuarios IKE” en la página 78
- “Usuarios y grupos de usuarios XAuth” en la página 83
- “Usuarios y grupos de usuarios L2TP” en la página 107

El dispositivo NetScreen autentica los diferentes tipos de usuarios en diversas etapas durante el proceso de conexión. Para hacerse una idea de cuándo entran en acción las técnicas de autenticación IKE, XAuth, L2TP y auth durante la creación de un túnel VPN “L2TP-over-IPSec” (L2TP sobre IPSec), consulte la ilustración siguiente:



Nota: Dado que tanto XAuth como L2TP proporcionan autenticación de usuarios y asignaciones de direcciones, rara vez se utilizan juntos. Se muestran juntos aquí solamente para ilustrar cuándo se produce cada tipo de autenticación durante la creación de un túnel VPN.

USUARIOS CON PERMISOS DE ADMINISTRADOR

Los usuarios con permisos de administrador son los administradores de un dispositivo NetScreen. Hay cinco clases de usuarios con permisos de administrador:

- Administrador raíz (“root admin”)
- Administrador de lectura/escritura de nivel raíz (“root-level read/write admin”)
- Administrador de sólo lectura de nivel raíz (“root-level read-only admin”)
- Administrador Vsys (“Vsys admin”)
- Administrador Vsys de sólo lectura (“Vsys read-only admin”)

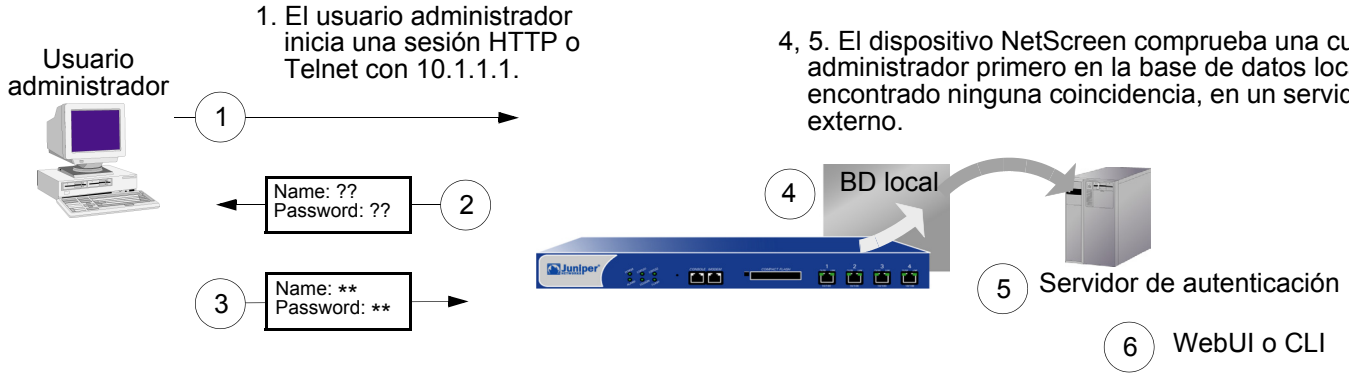
> ***Nota:*** *Para obtener información sobre los privilegios de cada tipo de usuario administrador y ver ejemplos de creación, modificación y eliminación de usuarios administradores, consulte “Administración” en la página* ***3****-1.*

Aunque el perfil del usuario raíz de un dispositivo NetScreen debe almacenarse en la base de datos local, puede almacenar usuarios vsys y usuarios administradores de nivel raíz con privilegios de lectura/escritura y privilegios de sólo lectura en la base de datos local o en un servidor de autenticación externo.

Si almacena cuentas de usuarios administradores en un servidor de autenticación RADIUS externo y carga el archivo de diccionario de NetScreen en el servidor de autenticación (consulte “Archivo de diccionario de NetScreen” en la página 26), puede optar por consultar los privilegios de administrador definidos en el servidor. Opcionalmente, puede especificar un nivel de privilegios que se aplicará globalmente a todos los usuarios con permisos de administrador almacenados en ese servidor de autenticación. Puede especificar privilegios de lectura/escritura o de sólo lectura. Si almacena usuarios con permisos de administrador en un servidor de autenticación SecurID o LDAP externo, o en un servidor RADIUS sin el archivo de diccionario de NetScreen, no podrá definir sus atributos de privilegios en el servidor de autenticación. Por lo tanto, debe asignarles un nivel de privilegios en el dispositivo NetScreen.

Si se establecen en el dispositivo NetScreen:	y el servidor RADIUS tiene cargado el archivo de diccionario de NetScreen:	y un servidor SecurID, LDAP o RADIUS sin el archivo de diccionario de NetScreen:
Obtener privilegios del servidor RADIUS	Asignar los privilegios apropiados	Falla el inicio de sesión del admin de nivel raíz o vsys
Asignar privilegios de lectura/escritura al admin externo	Asignar privilegios de lectura/escritura de nivel raíz o vsys	Asignar privilegios de lectura/escritura de nivel raíz Falla el inicio de sesión del admin vsys
Asignar privilegios de sólo lectura al admin externo	Asignar privilegios de sólo lectura de nivel raíz o vsys	Asignar privilegios de sólo lectura de nivel raíz Falla el inicio de sesión del admin vsys

El proceso de autenticación del administrador ocurre según se muestra en la ilustración siguiente:



USUARIOS DE MÚLTIPLES TIPOS

Puede combinar usuarios de autenticación, IKE, L2TP o XAuth para crear las siguientes combinaciones y almacenarlas en la base de datos local:

- Usuario Auth/IKE
- Usuario Auth/L2TP
- Usuario Auth/IKE/L2TP
- Usuario IKE/L2TP
- Usuario Auth/XAuth
- Usuario Auth/IKE/XAuth
- Usuario IKE/XAuth
- Usuario L2TP/XAuth
- Usuario IKE/L2TP/XAuth
- Usuario Auth/IKE/L2TP/XAuth

Aunque puede crear todas las combinaciones indicadas al definir cuentas de usuarios de múltiples tipos en la base de datos local, tenga en cuenta los puntos siguientes antes de crearlos:

- Combinar un usuario del tipo IKE con cualquier otro tipo de usuario limita el potencial de ampliación. Las cuentas de usuario IKE deben almacenarse en la base de datos local. Si crea cuentas de usuario auth/IKE, IKE/L2TP o IKE/XAuth y el número de usuarios crece más allá de la capacidad de la base de datos local, no podrá reubicar estas cuentas en un servidor de autenticación externo. Si mantiene las cuentas de usuario IKE separadas de otros tipos de cuentas, tiene la posibilidad de mover las cuentas de usuario que no sean IKE a un servidor de autenticación externo en caso de necesidad.
- L2TP y XAuth proporcionan los mismos servicios: autenticación de usuarios remotos y asignación de las direcciones IP propia, de los servidores DNS y de los servidores WINS. No se recomienda utilizar L2TP y XAuth juntos para un túnel L2TP-over-IPSec. Ambos protocolos no sólo cumplen los mismos objetivos; además, las asignaciones de direcciones L2TP sobreescriben las asignaciones de direcciones XAuth una vez finalizadas las negociaciones IKE de la Fase 2 e iniciadas las negociaciones de L2TP.
- Si crea una cuenta de usuario de múltiples tipos en la base de datos local combinando auth/L2TP o auth/XAuth, se deberá utilizar el mismo nombre de usuario y contraseña para ambos inicios de sesión.

  Aunque resulta más cómodo crear una sola cuenta de usuario de múltiples tipos, separar los tipos de usuario en dos cuentas independientes permite aumentar la seguridad. Por ejemplo, puede almacenar una cuenta de usuario de autenticación en un servidor de autenticación externo y una cuenta de usuario XAuth en la base de datos local. Puede entonces asignar diferentes nombres de usuario de inicio de sesión y contraseñas a cada cuenta, y hacer referencia al usuario XAuth en la configuración de la puerta de enlace IKE y al usuario de autenticación en la configuración de la directiva. El usuario VPN de acceso telefónico deberá autenticarse dos veces, posiblemente con dos nombres de usuario y contraseñas totalmente diferentes.

EXPRESIONES DE GRUPOS

Una expresión de grupo es una instrucción que se puede utilizar en directivas para condicionar los requisitos de autenticación. Las expresiones de grupos permiten combinar usuarios, grupos de usuarios u otras expresiones de grupos como alternativas para la autenticación (“a” O “b”), o como requisitos para la autenticación (“a” Y “b”). También puede utilizar expresiones de grupos para excluir a un usuario, grupo de usuarios u otra expresión de grupo (NO “c”).

Nota: *Aunque las expresiones de grupos se definen en el dispositivo NetScreen (y se almacenan en la base de datos local), los usuarios y grupos de usuarios a los que se hace referencia en las expresiones de grupos deben almacenarse en un servidor RADIUS externo. Un servidor RADIUS permite a los usuarios pertenecer a más de un grupo. La base de datos local no lo permite.*

Las expresiones de grupos utilizan los tres operadores OR, AND y NOT. Los objetos en la expresión a los que se refieren OR, AND y NOT pueden ser un usuario de autenticación, un grupo de usuarios de autenticación o una expresión de grupos previamente definida.

Usuarios

OR: Si el aspecto de autenticación de una directiva especifica que el usuario sea “a” O “b”, el dispositivo NetScreen autentica al usuario si es cualquiera de ellos.

AND: El uso de AND en una expresión de grupos requiere que al menos uno de los dos objetos de la expresión sea un grupo de usuarios o una expresión de grupos. (No es lógico exigir a un usuario que sea a la vez el usuario “a” Y el usuario “b”). Si el aspecto de autenticación de una directiva requiere que el usuario sea “a” Y miembro del grupo “b”, el dispositivo NetScreen solamente autentica al usuario si se cumplen ambas condiciones.

NOT: Si el aspecto de autenticación de una directiva especifica que el usuario sea cualquier persona salvo el usuario “c” (NOT “c”), entonces el dispositivo NetScreen lo autentica siempre que no sea dicho usuario.

Grupos de usuarios

OR: Si el aspecto de autenticación de una directiva especifica que el usuario debe pertenecer al grupo “a” O al grupo “b”, entonces el dispositivo NetScreen lo autentica si pertenece a cualquiera de esos grupos.

AND: Si el aspecto de autenticación de una directiva requiere que el usuario pertenezca al grupo “a” Y al grupo “b”, el dispositivo NetScreen solamente lo autentica si pertenece a ambos grupos.

NOT: Si el aspecto de autenticación de una directiva especifica que el usuario debe pertenecer a cualquier grupo con excepción del grupo “c” (NOT “c”), el dispositivo NetScreen autentica a usuario si no pertenece a ese grupo.

Expresiones de grupos

OR: Si el aspecto de autenticación de una directiva especifica que el usuario debe coincidir con la descripción de la expresión de grupo “a” O con la expresión de grupo “b”, el dispositivo NetScreen autentica al usuario si se le puede aplicar cualquiera de esas expresiones.

AND: Si el aspecto de autenticación de una directiva especifica que el usuario debe coincidir con la descripción de la expresión de grupo “a” Y con la expresión de grupo “b”, el dispositivo NetScreen solamente autentica al usuario si se le pueden aplicar ambas expresiones de grupo.

NOT: Si el aspecto de autenticación de una directiva especifica que el usuario no debe coincidir con la descripción de la expresión de grupo “c” (NOT “c”), entonces el dispositivo NetScreen solamente autentica al usuario si éste no coincide con esa expresión de grupo.

Ejemplo: Expresiones de grupos (AND)

En este ejemplo se crea la expresión de grupo “s+m”, que significa “sales AND marketing”. Previamente habrá creado los grupos de usuarios de autenticación “sales” y “marketing” en un servidor de autenticación RADIUS externo llamado “radius1” y los habrá alimentado con los usuarios. (Para ver un ejemplo de configuración de un servidor de autenticación RADIUS externo, consulte el “Ejemplo: Servidor de autenticación RADIUS” en la página 34). A continuación, utilizará esa expresión de grupo en una directiva intrazonal[1] cuyo componente de autenticación requiere que el usuario sea miembro de ambos grupos de usuarios para poder acceder al contenido confidencial de un servidor llamado “project1” (10.1.1.70).

WebUI

1. Dirección

Objects > Addresses > List > New: Introduzca los siguientes datos y haga clic en **OK**:

Address Name: project1

IP Address/Domain Name:

IP/Netmask: (seleccione), 10.1.1.70/32

Zone: Trust

2. Expresión de grupo

Objects > Group Expressions > New: Introduzca los siguientes datos y haga clic en **OK**:

Group Expression: s+m

AND: (seleccione), sales AND marketing

1. Para que una directiva intrazonal funcione correctamente, las direcciones de origen y de destino deben estar en subredes diferentes, conectadas con el dispositivo NetScreen a través de dos interfaces asociadas a la misma zona. No puede haber ningún otro dispositivo de enrutamiento junto a un dispositivo NetScreen capaz de enrutar tráfico entre ambas direcciones. Para obtener más información sobre directivas intrazonales, consulte “Directivas” en la página **2**-305.

3. Directiva

Policies > (From: Trust, To: Trust) New: Introduzca los siguientes datos y haga clic en **OK**:

Source Address:

Address Book Entry: (seleccione), Any

Destination Address:

Address Book Entry: (seleccione), project1

Service: ANY

Action: Permit

Position at Top: (seleccione)

> Advanced: Escriba lo siguiente y haga clic en **Return** para establecer las opciones avanzadas y regresar a la página de configuración básica:

Authentication: (seleccione)

Auth Server: (seleccione)

Use: radius1

Group Expression: (seleccione), External Group Expression - s+m

CLI

1. Dirección

```
set address trust project1 10.1.1.70/32
```

2. Expresión de grupo

```
set group-expression s+m sales and marketing
```

3. Directiva

```
set policy top from trust to trust any project1 any permit auth server radius1
    group-expression s+m
save
```

Ejemplo: Expresiones de grupos (OR)

En este ejemplo creará una expresión de grupo “a/b”, que significa “amy OR basil”. Previamente habrá creado las cuentas de usuario de autenticación “amy” y “basil” en un servidor de autenticación RADIUS externo llamado “radius1”. (Para ver un ejemplo de configuración de un servidor de autenticación RADIUS externo, consulte el “Ejemplo: Servidor de autenticación RADIUS” en la página 34). Luego utilizará esa expresión de grupo en una directiva desde la zona Trust a DMZ. El componente de autenticación de la directiva requiere que el usuario sea “amy” o “basil” para poder acceder al servidor web llamado “web1” en la dirección IP 210.1.1.70.

WebUI

1. Dirección

   Objects > Addresses > List > New: Introduzca los siguientes datos y haga clic en **OK**:

   Address Name: web1

   IP Address/Domain Name

   IP/Netmask: (seleccione), 210.1.1.70/32

   Zone: DMZ

2. Expresión de grupo

   Objects > Group Expressions > New: Introduzca los siguientes datos y haga clic en **OK**:

   Group Expression: a/b

   OR: (seleccione), amy OR basil

3. Directiva

Policies > (From: Trust, To: DMZ) New: Introduzca los siguientes datos y haga clic en **OK**:

Source Address:

Address Book Entry: (seleccione), Any

Destination Address:

Address Book Entry: (seleccione), web1

Service: ANY

Action: Permit

Position at Top: (seleccione)

> Advanced: Escriba lo siguiente y haga clic en **Return** para establecer las opciones avanzadas y regresar a la página de configuración básica:

Authentication: (seleccione)

Auth Server: (seleccione)

Use: radius1

Group Expression: (seleccione), External Group Expression - a/b

CLI

1. Dirección

```
set address trust project1 210.1.1.70/32
```

2. Expresión de grupo

```
set group-expression a/b amy or basil
```

3. Directiva

```
set policy top from trust to dmz any web1 any permit auth server radius1
    group-expression a/b
save
```

Ejemplo: Expresiones de grupos (NOT)

En este ejemplo creará una expresión de grupo “-temp”, que significa “NOT temp”. Previamente habrá creado un grupo de usuarios de autenticación local “temp” en un servidor de autenticación RADIUS externo llamado “radius1”. (Para ver un ejemplo de configuración de un servidor de autenticación RADIUS externo, consulte el “Ejemplo: Servidor de autenticación RADIUS” en la página 34). Luego utilizará esa expresión de grupo en una directiva desde la zona Trust a la zona Untrust que permita el acceso a Internet a todos los empleados fijos, pero no a los temporales. El componente de autenticación de la directiva requerirá que cada usuario de la zona Trust sea autenticado, salvo los usuarios de “temp”, a los que se denegará el acceso a la zona Untrust.

WebUI

1. Expresión de grupo

   Objects > Group Expressions > New: Introduzca los siguientes datos y haga clic en **OK**:

   Group Expression: -temp

   OR: (seleccione), NOT temp

2. Directiva

   Policies > (From: Trust, To: Untrust) New: Introduzca los siguientes datos y haga clic en **OK**:

   Source Address:

   Address Book Entry: (seleccione), Any

   Destination Address:

   Address Book Entry: (seleccione), Any

   Service: HTTP

   Action: Permit

   Position at Top: (seleccione)

   > Advanced: Escriba lo siguiente y haga clic en **Return** para establecer las opciones avanzadas y regresar a la página de configuración básica:

   Authentication: (seleccione)

   Auth Server: (seleccione)

   Use: Local

   Group Expression: (seleccione), External Group Expression -temp

CLI

1. **Expresión de grupo**

```
set group-expression -temp not temp
```

2. **Directiva**

```
set policy top from trust to untrust any any any permit auth server radius1
    group-expression -temp
save
```

PERSONALIZACIÓN DE MENSAJES DE BIENVENIDA

Un mensaje de bienvenida es el mensaje que aparece en pantalla en los siguientes lugares durante los siguientes tipos de inicios de sesión:

- En la parte superior de la pantalla de Telnet o de consola, cuando se conecta un usuario administrador para iniciar una sesión en el dispositivo NetScreen[2]
- En la parte superior de una pantalla del explorador Web, después de que un usuario de autenticación haya iniciado una sesión correctamente en una dirección de WebAuth
- En mensajes de petición de inicio de sesión, mensajes de éxito y mensajes de fallo Telnet, FTP o HTTP para usuarios de autenticación

Todos los mensajes de bienvenida, salvo los de inicio de sesión de la consola, ya disponen de mensajes predeterminados. Puede personalizar los mensajes de bienvenida para adaptarlos al entorno de red en el que esté utilizando el dispositivo NetScreen.

Ejemplo: Personalizar un mensaje de bienvenida de WebAuth

En este ejemplo cambiará el mensaje que aparece en el explorador Web para indicar que un usuario de autenticación se ha autenticado con éxito después de iniciar una sesión con éxito a través de WebAuth. El nuevo mensaje será “Autenticación aprobada”.

WebUI

Configuration > Banners > WebAuth: En el campo Success Banner, escriba **Autenticación aprobada** y haga clic en **Apply**.

CLI

```
set webauth banner success “Autenticación aprobada”
save
```

2. Puede incluir una línea adicional de mensaje de bienvenida debajo de un mensaje de bienvenida de Telnet o de consola. La segunda línea del mensaje de bienvenida sigue siendo igual tanto para el inicio de sesión de Telnet como de la consola, aunque el mensaje de bienvenida de Telnet puede ser distinto del de la consola. Para crear un segundo mensaje de bienvenida, introduzca el siguiente comando: **set admin auth banner secondary** *string*.

2

Servidores de autenticación

Este capítulo comienza examinando diversas clases de servidores de autenticación (la base de datos local incorporada en cada dispositivo NetScreen y los servidores de autenticación externos RADIUS, SecurID y LDAP). Este material se presenta en las siguientes secciones:

TIPOS DE SERVIDORES DE AUTENTICACIÓN

Puede configurar el dispositivo NetScreen de modo que utilice la base de datos local o al menos un servidor de autenticación externo para verificar las identidades de los siguientes tipos de usuarios:

- Auth users (Usuarios Auth (de autenticación))
- IKE users (Usuarios IKE)
- L2TP Users (Usuarios L2TP)
- XAuth users (Usuarios XAuth)
- Admin users (Usuarios Admin (con permisos de administrador))

> ***Nota:*** *Las cuentas de usuarios IKE se deben almacenar en la base de datos local. El único servidor externo que admite asignaciones de configuración remota L2TP y XAuth y asignaciones de privilegios de administrador es RADIUS.*

Además de su propia base de datos local, los dispositivos NetScreen pueden trabajar con servidores externos RADIUS, SecurID y LDAP. Para autenticar usuarios L2TP, usuarios de autenticación, usuarios XAuth y usuarios con permisos de administrador se puede utilizar cualquier clase de servidor de autenticación. NetScreen también es compatible con WebAuth, un esquema de autenticación alternativo para usuarios de autenticación. (Para ver un ejemplo de WebAuth, consulte “Ejemplo: WebAuth + SSL solamente (grupo de usuarios externo)” en la página 72). Cualquier servidor de autenticación que contenga cuentas del tipo “usuarios de autenticación” puede convertirse en el servidor de autenticación predeterminado de WebAuth. La tabla siguiente muestra qué servidores admiten qué tipos de usuarios y funciones de autenticación:

Tipo de servidor	Características y tipos de usuarios admitidos									
	Usuarios de autenticación	Usuarios IKE	Usuarios L2TP		Usuarios XAuth		Usuarios con permisos de administrador		Grupos de usuarios	Expresiones de grupos
			Auth	Ajustes remotos	Auth	Ajustes remotos	Auth	Privilegios		
Local	✓	✓	✓	✓	✓	✓	✓	✓	✓	
RADIUS	✓		✓	✓	✓	✓	✓	✓	✓	✓
SecurID	✓		✓		✓		✓			
LDAP	✓		✓		✓		✓			

En la mayoría de dispositivos NetScreen se pueden utilizar simultáneamente hasta 10 servidores de autenticación principales por cada sistema (raíz o virtual) en cualquier combinación de tipos. Este total incluye la base de datos local y excluye los servidores de autenticación de respaldo. Los servidores RADIUS o LDAP admiten dos servidores de respaldo, mientras que los servidores SecurID admiten uno. Así pues, podrían utilizarse, por ejemplo, la base de datos local y 9 servidores RADIUS principales, cada uno de ellos con dos servidores de respaldo asignados.

Múltiples servidores de autenticación funcionando simultáneamente

El color de cada petición de conexión coincide con el color de la comprobación de autenticación:

Usuario IKE/XAuth (naranja) –> base de datos local

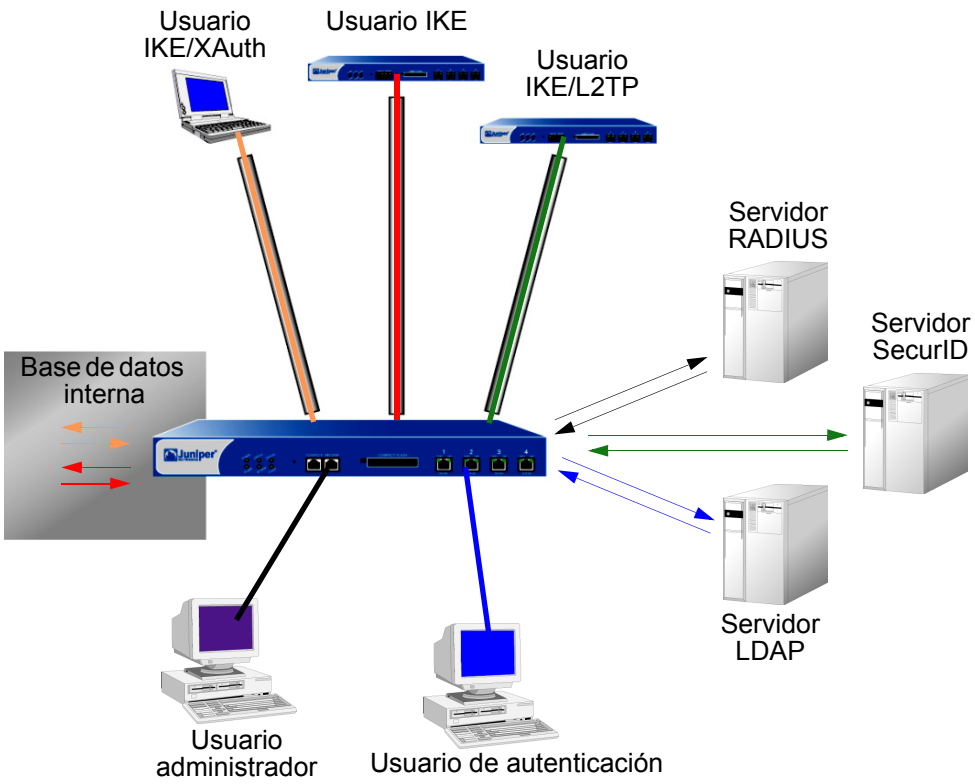
Usuario IKE (rojo) –> base de datos local

Usuario IKE/L2TP (verde) –> servidor SecurID

Usuario administrador (púrpura) –> servidor RADIUS

Usuario de autenticación (azul) –> servidor LDAP

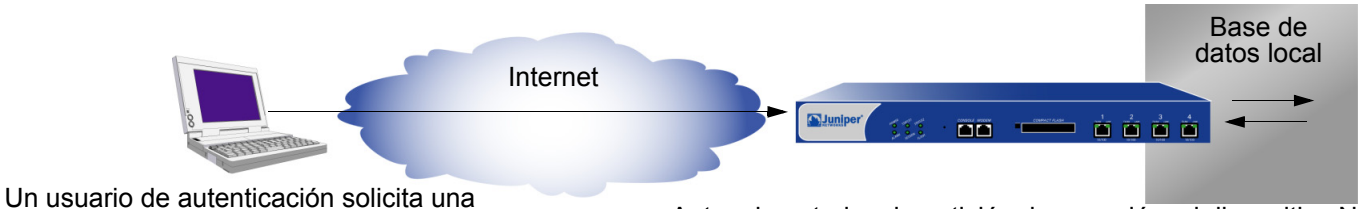
Nota: *Se puede utilizar un solo servidor de autenticación para múltiples tipos de autenticación de usuario. Por ejemplo, un servidor RADIUS puede almacenar simultáneamente datos de usuarios administradores, de autenticación, L2TP y XAuth.*



En las siguientes secciones se analiza en detalle la base de datos local y cada servidor de autenticación.

BASE DE DATOS LOCAL

Todos los dispositivos NetScreen disponen de una base de datos de usuarios integrada para la autenticación. Cuando se define un usuario en el dispositivo NetScreen, éste introduce el nombre y la contraseña del usuario en su base de datos local.



Un usuario de autenticación solicita una conexión a la red protegida.

Antes de autorizar la petición de conexión, el dispositivo NetScreen consulta sus bases de datos internas para autenticar al usuario.

Características y tipos de usuarios admitidos

La base de datos local admite los siguientes tipos de usuarios y características de autenticación:

- Usuarios de autenticación
- Usuarios IKE
- Usuarios L2TP
- Usuarios XAuth
- Usuarios con permisos de administrador
- Privilegios de administrador
- WebAuth
- Grupos de usuarios
- Expresiones de grupos*

* Las expresiones de grupos se definen en el dispositivo NetScreen, pero los usuarios y grupos de usuarios deben almacenarse en un servidor de autenticación RADIUS externo. Para obtener más información sobre expresiones de grupos, consulte “Expresiones de grupos” en la página 6.

La base de datos local es el servidor de autenticación predeterminado (“auth server”) para todos los tipos de autenticación. Para obtener instrucciones sobre cómo agregar usuarios y grupos de usuarios a la base de datos local mediante WebUI y CLI, consulte “Usuarios de autenticación” en la página 43 y “Usuarios IKE, XAuth y L2TP” en la página 77.

Ejemplo: Tiempo de espera de la base de datos local

De forma predeterminada, el tiempo de espera de la base de datos local para autenticaciones de administradores y usuarios de autenticación es de 10 minutos. En este ejemplo, cambiará a que no caduque nunca para los administradores y a que caduque a los 30 minutos para los usuarios de autenticación.

WebUI

Configuration > Admin > Management: Desactive la casilla de verificación Enable Web Management Idle Timeout y haga clic en **Apply**.

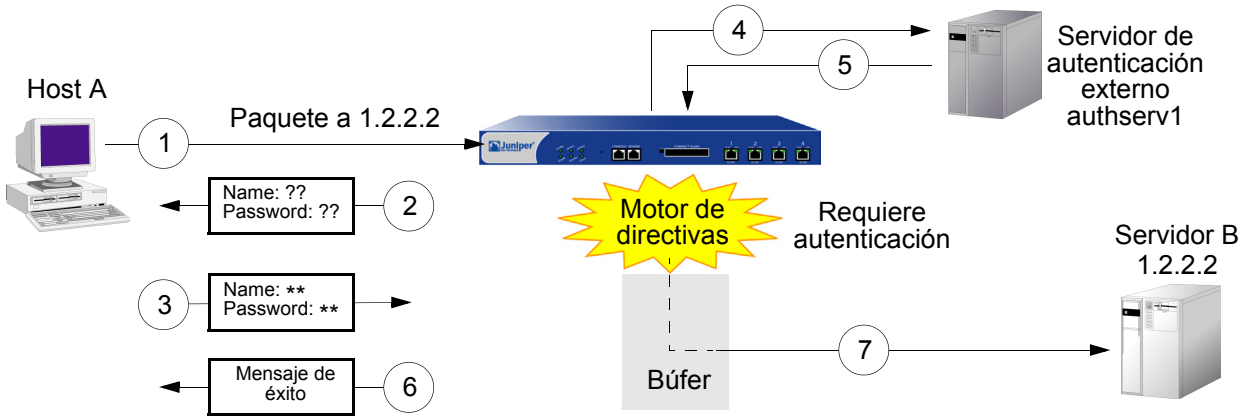
Configuration > Auth > Servers > Edit (para Local): Escriba **30** en el campo Timeout y haga clic en **Apply**.

CLI

```
set admin auth timeout 0
set auth-server Local timeout 30
save
```

SERVIDORES DE AUTENTICACIÓN EXTERNOS

Un dispositivo NetScreen se puede conectar a unos o más servidores de autenticación externos o “servidores auth”, en los que se almacenan cuentas de usuarios. Cuando el dispositivo NetScreen recibe una petición de conexión que requiere una verificación de autenticación, solicita una comprobación de autenticación al servidor de autenticación externo especificado en la directiva, en la configuración del túnel L2TP o en la configuración de la puerta de enlace IKE. El dispositivo NetScreen actúa entonces como retransmisor entre el usuario que solicita la autenticación y el servidor de autenticación que la concede. Una comprobación de autenticación correcta por parte de un servidor de autenticación externo ocurre de la siguiente forma:

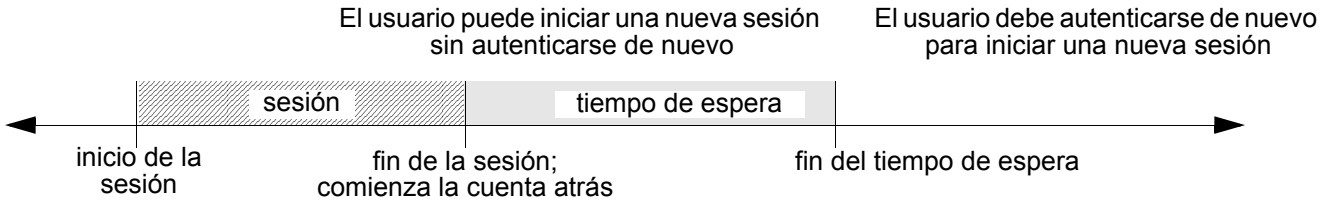


1. El host A envía un paquete FTP, HTTP o Telnet TCP SYN a 1.2.2.2.
2. El dispositivo NetScreen intercepta el paquete, detecta que su directiva correspondiente requiere autenticación por parte de authserv1, guarda el paquete en un búfer y solicita al usuario su nombre y contraseña.
3. El usuario responde con un nombre de usuario y una contraseña.
4. El dispositivo NetScreen retransmite la información de inicio de sesión a authserv1.
5. Authserv1 devuelve una notificación de éxito al dispositivo NetScreen.
6. El dispositivo NetScreen informa el usuario de autenticación sobre el éxito de su inicio de sesión.
7. Seguidamente, el dispositivo NetScreen remite el paquete de su búfer a su destino 1.2.2.2.

Propiedades del objeto “servidor de autenticación”

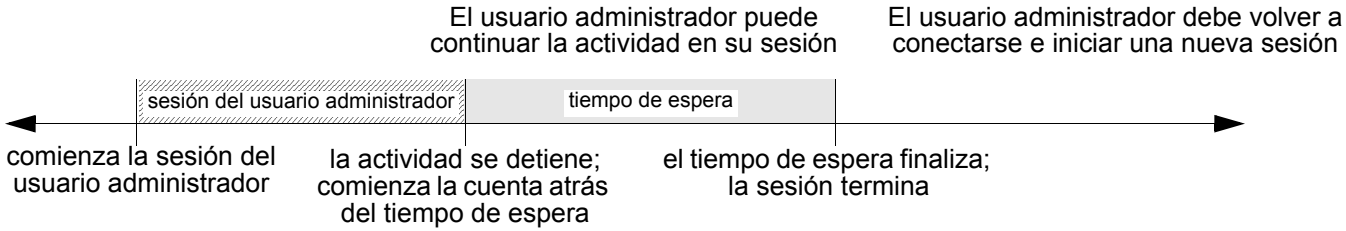
Un dispositivo NetScreen trata cada servidor de autenticación como un objeto al que se puede hacer referencia en directivas, puertas de enlace IKE y túneles L2TP. Las siguientes propiedades definen e identifican de forma inequívoca un objeto de servidor de autenticación:

- Object name: Una cadena de nombre, como “authserv1” (el único servidor de autenticación predefinido es “Local”).
- ID number: Puede establecer el número de identificación o permitir que el dispositivo NetScreen lo haga automáticamente. Si establece un número de identificación, debe elegir uno que aún no se esté utilizando.
- Type: RADIUS, SecurID, LDAP.
- Server name: La dirección IP o el nombre de dominio del servidor
- Backup1: La dirección IP o el nombre de dominio de un servidor de respaldo principal
- Backup2: (RADIUS y LDAP) La dirección IP o nombre de dominio de un servidor de respaldo secundario
- Account Type: Uno o más de los siguientes tipos de usuarios: Auth, L2TP, XAuth o Admin solamente.
- Timeout value: El valor del tiempo de espera cambia dependiendo del tipo de usuario (de autenticación o administrador).
  - Usuario de autenticación: La cuenta atrás del tiempo de espera comienza después de completarse la primera sesión autenticada. Si el usuario inicia una nueva sesión antes de que la cuenta atrás alcance el límite del tiempo de espera, no tendrá que volver a autenticarse y el contador de cuenta atrás se restablecerá. El valor predeterminado del tiempo de espera es de 10 minutos, y el máximo es de 255 minutos. También puede establecer el valor del tiempo de espera en 0 para que el periodo de autenticación nunca caduque.



Nota: *El tiempo de espera para la autenticación de usuarios no es igual que el tiempo de espera de la sesión. Si durante un tiempo predefinido no se produce ninguna actividad en una sesión, el dispositivo NetScreen elimina automáticamente la sesión de su tabla de sesiones.*

– Usuario administrador: Si el tiempo de inactividad alcanza el umbral establecido, el dispositivo NetScreen termina la sesión del usuario administrador. Para continuar administrando el dispositivo NetScreen, el administrador debe volver a conectarse al dispositivo y autenticarse de nuevo. El valor predeterminado del tiempo de espera es de 10 minutos, y el máximo es de 1000 minutos. También puede establecer el valor del tiempo de espera en 0 si desea que una sesión de administrador nunca caduque.



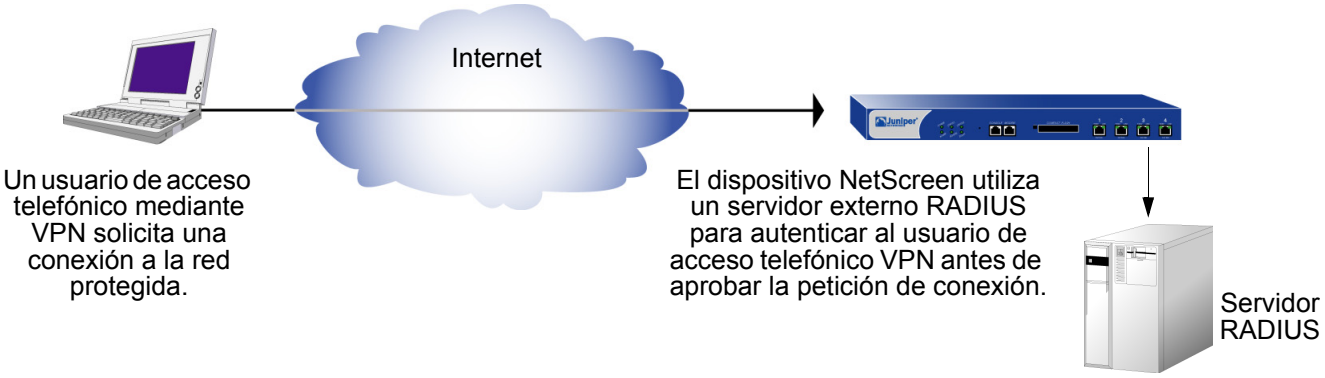
Además de las propiedades antedichas, aplicables a todos los objetos del servidor de autenticación, cada servidor tiene unas cuantas propiedades específicas. Éstas se explican en las siguientes secciones sobre propiedades de los servidores de autenticación RADIUS, SecurID y LDAP.

TIPOS DE SERVIDORES DE AUTENTICACIÓN

Además de las bases de datos internas, los dispositivos NetScreen admiten tres tipos de servidores de autenticación externos: RADIUS, SecurID y LDAP.

RADIUS

El servicio de autenticación remota de usuarios de acceso telefónico “Remote Authentication Dial-In User Service (RADIUS)” es un protocolo para servidores de autenticación que admite decenas de miles de usuarios.



El cliente RADIUS (es decir, el dispositivo NetScreen) autentica a usuarios mediante una serie de comunicaciones entre el cliente y el servidor. Básicamente, RADIUS pide a la persona que se está conectando que introduzca su nombre de usuario y contraseña. Entonces compara estos valores con lo que tiene almacenados en su base de datos y, una vez que el usuario ha sido autenticado, el cliente proporciona al usuario acceso a los correspondientes servicios de red.

Para configurar el dispositivo NetScreen para RADIUS, debe especificar la dirección IP del servidor RADIUS y definir un secreto compartido (“shared secret”), el mismo que haya definido en dicho servidor. El secreto compartido es una contraseña que el servidor RADIUS utiliza para generar una clave con la que encriptar el tráfico entre los dispositivos NetScreen y RADIUS.

Propiedades del objeto servidor de autenticación RADIUS

Además de las propiedades genéricas del servidor de autenticación descritas en “Propiedades del objeto “servidor de autenticación”” en la página 22, un servidor RADIUS también utiliza las propiedades siguientes:

- **Shared Secret:** El secreto (contraseña) compartido entre el dispositivo NetScreen y el servidor RADIUS. Los dispositivos utilizan este secreto para encriptar las contraseñas de usuarios que envían al servidor RADIUS.
- **RADIUS Port:** El número del puerto en el servidor RADIUS al que el dispositivo NetScreen envía las peticiones de autenticación. El número de puerto predeterminado es 1645.
- **RADIUS Retry Timeout:** El intervalo (en segundos) que el dispositivo NetScreen espera antes de enviar otra petición de autenticación al servidor RADIUS si la petición anterior no obtuvo ninguna respuesta. El valor predeterminado es de tres segundos.

Características y tipos de usuarios admitidos

Un servidor RADIUS admite los siguientes tipos de usuarios y características de autenticación:

- Usuarios de autenticación
- Usuarios L2TP (autenticación y ajustes remotos)
- Usuarios XAuth (autenticación y ajustes remotos)
- Usuarios con permisos de administrador (autenticación y asignación de privilegios)
- Grupos de usuarios

Un servidor RADIUS admite los mismos tipos de usuarios y características que la base de datos local, excepto los usuarios IKE. Entre los tres tipos de servidores de autenticación externos, RADIUS es, por el momento, el único con tan amplia compatibilidad. Para que un servidor RADIUS pueda trabajar con atributos tan específicos de NetScreen como los privilegios de administrador, grupos de usuarios y direcciones IP L2TP y XAuth remotas[1], así como con las asignaciones de direcciones de servidores DNS y WINS, es necesario cargar un archivo de diccionario de NetScreen que defina estos atributos en el servidor RADIUS.

1. NetScreen utiliza el atributo estándar de RADIUS para las asignaciones de direcciones IP. Si solamente desea utilizar RADIUS para asignar direcciones IP, no necesita cargar los atributos de NetScreen específicos de cada fabricante (“vendor-specific attributes” o VSAs).

Archivo de diccionario de NetScreen

Un archivo de diccionario contiene las definiciones de los atributos específicos de cada fabricante (VSAs) que se pueden cargar en un servidor RADIUS. Una vez definidos los valores de estos VSAs, NetScreen puede consultarlos cada vez que un usuario se conecta a un dispositivo NetScreen. Los atributos VSA de NetScreen son: privilegios de administrador, grupos de usuarios y dirección IP L2TP y XAuth remota, y asignaciones de direcciones de servidores DNS y WINS. Hay dos archivos de diccionario de NetScreen, uno para servidores RADIUS de Cisco y otro para servidores RADIUS de Funk Software. Los servidores RADIUS de Microsoft no requieren archivos de diccionario. Debe configurarlo como se explica en el documento *Bi-Directional NetScreen Remote VPN using xAuth and Firewall Authentication with Microsoft Internet Authentication Service (IAS)*, que puede descargar en http://ns200-support.netscreen.com/knowbase/root/public/ns10382.pdf.

Cada archivo de diccionario de NetScreen contiene la información específica siguiente:

- **Vendor ID:** La identificación de fabricante (“Vendor ID” o VID, pero también llamada “número IETF”) de NetScreen es 3224. El número VID identifica a un proveedor específico con respecto a un atributo determinado. Algunos tipos de servidores RADIUS requieren introducir el número VID con cada entrada de atributo, mientras que otros tipos solamente requieren introducirlo una vez y luego lo aplican globalmente. Para obtener información adicional, consulte la documentación del servidor RADIUS.
- **Attribute Name:** Los nombres de atributos describen atributos individuales específicos de NetScreen, como NS-Admin-Privilege, NS-User-Group, NS-Primary-DNS-Server, etc.
- **Attribute Number:** El número de atributo identifica un atributo individual específico del fabricante. Los números de atributos específicos de NetScreen se dividen en dos rangos:
  - NetScreen ScreenOS: 1 – 199
  - NetScreen-Global PRO: a partir del 200

  Por ejemplo, el número del atributo ScreenOS para grupos de usuarios es 3. El número de atributo NetScreen-Global PRO para grupos de usuarios es 200.
- **Attribute Type:** El tipo de atributo identifica la forma en la que se representan los datos del mismo (o su “valor”): como cadena, dirección IP o número entero.

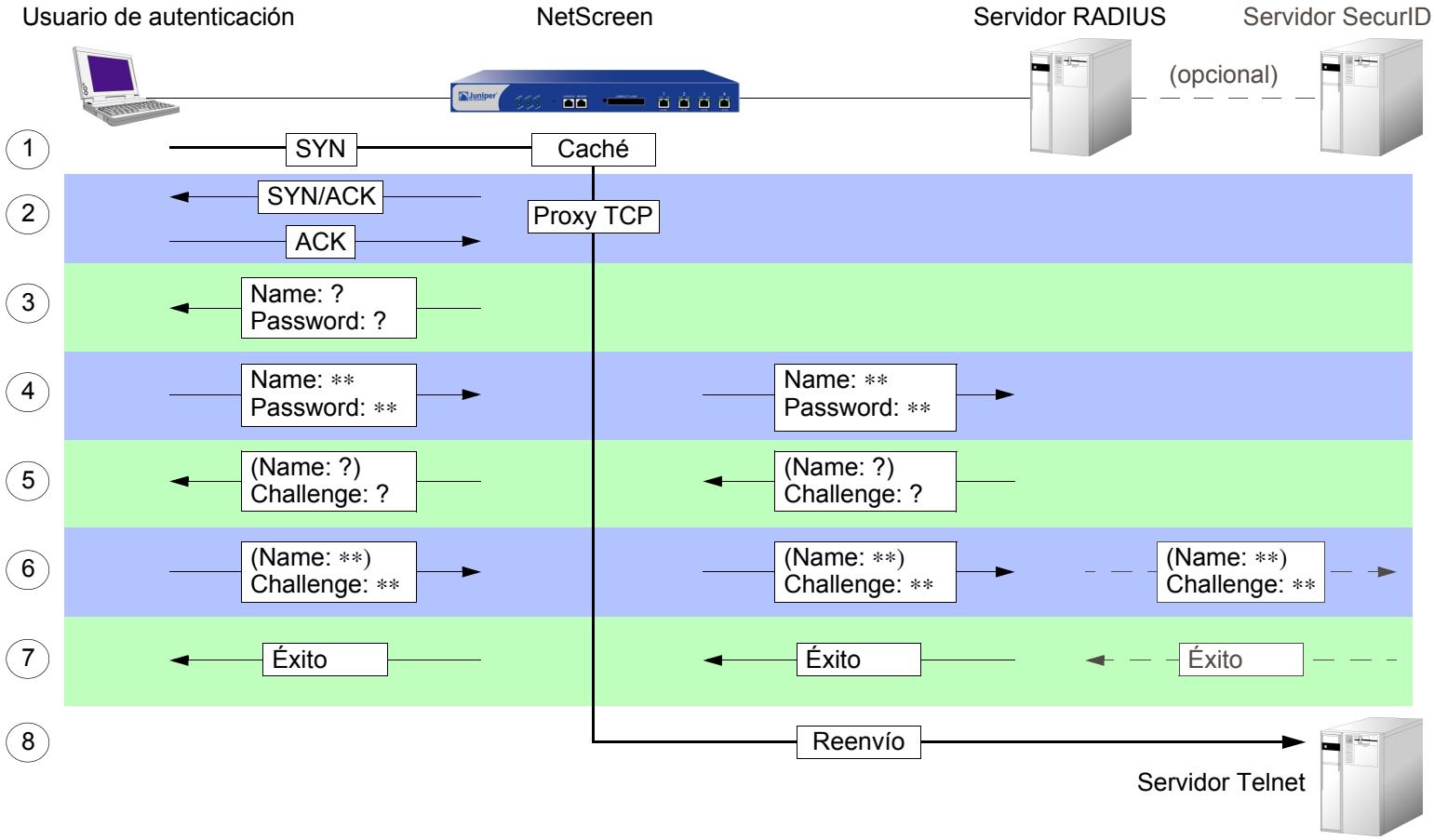
El servidor RADIUS recibe automáticamente la información antedicha cuando se carga el archivo de diccionario de NetScreen en el mismo. Para crear nuevas entradas de datos, debe introducir manualmente un valor en la forma indicada por el tipo de atributo. Por ejemplo, una entrada para un administrador de lectura-escritura aparece como sigue:

VID	Attribute Name	Attribute Number	Attribute Type	Value
3224	NS-Admin-Privileges	1	data=int4 (es decir número entero)	2 (2 = todos los privilegios)

Para descargar un archivo de diccionario, vaya a http://www.juniper.net/customers/csc/research/netscreen_kb/downloads/dictionary/funk_radius.zip o a http://www.juniper.net/customers/csc/research/netscreen_kb/downloads/dictionary/cisco_radius.zip, inicie una sesión y guarde el archivo en una unidad local.

RADIUS Access-Challenge

Ahora, los dispositivos NetScreen pueden procesar paquetes access-challenge de servidores RADIUS externos cuando un usuario de autenticación intenta iniciar una sesión a través de Telnet. Después de aprobar un nombre de usuario y su correspondiente contraseña, access-challenge solicita una comprobación adicional durante el proceso de inicio de sesión. Cuando un usuario de autenticación responde a una petición de inicio de sesión indicando su nombre y contraseña correctos, el servidor RADIUS envía una señal access-challenge al dispositivo NetScreen, que lo remite al usuario. Cuando el usuario contesta, el dispositivo NetScreen envía una nueva petición de acceso al servidor RADIUS con la respuesta del usuario. Si la respuesta del usuario es correcta, el proceso de autenticación concluye con éxito. Observe e el supuesto siguiente, en el cual un usuario de autenticación desea establecer una conexión Telnet con un servidor:



1. Un usuario de autenticación envía un paquete SYN al iniciar una conexión TCP para establecer una sesión Telnet con un servidor Telnet.
2. Un dispositivo NetScreen intercepta el paquete, comprueba su lista de directivas y determina que esta sesión requiere autenticación de usuario. El dispositivo NetScreen coloca el paquete SYN en su memoria caché y registra en su proxy el establecimiento de comunicación TCP de 3 fases (“TCP 3-way handshake”) con el usuario.
3. El dispositivo NetScreen pide al usuario que inicie una sesión con su nombre y contraseña.
4. El usuario de autenticación introduce su nombre y contraseña y los envía al dispositivo NetScreen. Entonces, el dispositivo NetScreen envía una petición de acceso (“access-request”) con la información de inicio de sesión a un servidor RADIUS.
5. Si la información es correcta, el servidor RADIUS envía una señal access-challenge al dispositivo NetScreen con un atributo reply-message que pide al usuario que proporcione una respuesta a un desafío (pregunta de comprobación). (Opcionalmente, access-challenge puede pedir al sistema de autenticación que proporcione de nuevo un nombre de usuario. El segundo nombre de usuario puede ser igual o distinto del primero). El dispositivo NetScreen envía entonces al usuario otro mensaje de petición de inicio de sesión con el contenido del atributo “reply-message”.
6. El usuario de autenticación introduce su respuesta al desafío (y, opcionalmente, un nombre de usuario) y la envía al dispositivo NetScreen. El dispositivo NetScreen envía al servidor RADIUS una segunda petición de acceso, con la respuesta del usuario al desafío.

   Si el servidor RADIUS necesita autenticar la respuesta de desafío por medio de otro servidor de autenticación (por ejemplo, cuando un servidor SecurID necesita autenticar un código token) el servidor RADIUS envía la petición de acceso “access-request” al otro servidor de autenticación.
7. Si el servidor RADIUS reenvió la respuesta al desafío a otro servidor de autenticación y ese servidor necesita una señal “access-accept”, o si el mismo servidor RADIUS aprueba la respuesta, el servidor RADIUS envía un mensaje “access-accept” al dispositivo NetScreen. En ese momento, el dispositivo NetScreen notifica al usuario de autenticación si su inicio de sesión se ha completado correctamente.
8. El dispositivo NetScreen reenvía el paquete SYN inicial a su destino original: el servidor Telnet.

Nota: *En la presente versión, NetScreen no admite “access-challenge” con L2TP.*

SecurID

En lugar de una contraseña fija, SecurID combina dos factores para crear una contraseña que cambia dinámicamente. SecurID produce un dispositivo del tamaño de una tarjeta de crédito llamado authenticator (“autenticador”), que dispone de una pantalla LCD en la que aparece una secuencia de números generada aleatoriamente llamada código token, que cambia cada minuto. El usuario también tiene un número de identificación personal (PIN). Cuando el usuario inicia sesión, introduce un nombre del usuario y su PIN más el código token actual.

El autenticador ejecuta un algoritmo conocido solamente por RSA para generar los valores que aparecen en la ventana LCD. Cuando el usuario a autenticar introduce su PIN y el número de su tarjeta, el servidor ACE, que también ejecuta el mismo algoritmo, compara los valores recibidos con los de su base de datos. Si coinciden, la autenticación es correcta.

La relación del dispositivo NetScreen con el servidor RSA SecurID ACE es similar a la de un dispositivo NetScreen con un servidor RADIUS. Es decir, el dispositivo NetScreen actúa como cliente, reenviando las peticiones de autenticación al servidor externo para su aprobación y retransmitiendo la información del inicio de sesión entre el usuario y el servidor. SecurID se diferencia de RADIUS en que la “contraseña” del usuario está asociada a un código token que cambia continuamente.

Propiedades del objeto servidor de autenticación SecurID

Además de las propiedades genéricas de cualquier servidor de autenticación detalladas en “Propiedades del objeto “servidor de autenticación”” en la página 22, los servidores SecurID también utilizan las propiedades siguientes:

- **Authentication Port:** El número del puerto en el servidor SecurID ACE al que el dispositivo NetScreen envía las peticiones de autenticación. El número de puerto predeterminado es 5500.
- **Encryption Type:** El algoritmo (SDI o DES) utilizado para encriptar la comunicación entre el dispositivo NetScreen y el servidor SecurID ACE.
- **Client Retries:** El número de veces que el cliente SecurID (es decir, el dispositivo NetScreen) intenta establecer comunicación con el servidor SecurID ACE antes de cancelar el intento.
- **Client Timeout:** El tiempo en segundos que el dispositivo NetScreen espera entre sucesivos reintentos de autenticación.
- **Use Duress:** Una opción que impide o permite utilizar otro número PIN. Cuando esta opción está habilitada y un usuario introduce un número PIN de emergencia previamente acordado (“duress PIN”), el dispositivo NetScreen envía una señal al servidor SecurID ACE, indicando que el usuario está realizando el inicio de sesión en contra de su voluntad, es decir, bajo amenaza. El servidor SecurID ACE permite el acceso esa única vez y después rechaza cualquier otro intento de inicio de sesión de ese usuario hasta que se ponga en contacto con el administrador de SecurID. El modo de amenaza solamente está disponible si el servidor SecurID ACE admite esta opción.

Características y tipos de usuarios admitidos

Los servidores SecurID Ace admiten los siguientes tipos de usuarios y características de autenticación:

- Usuarios de autenticación
- Usuarios L2TP (autenticación de usuarios; el usuario L2TP recibe los ajustes L2TP predeterminados del dispositivo NetScreen)
- Usuarios XAuth (autenticación de usuarios; no admite asignaciones de ajustes remotas)
- Usuarios administradores (autenticación de usuarios; el usuario administrador recibe la asignación de privilegios predeterminada: sólo lectura)

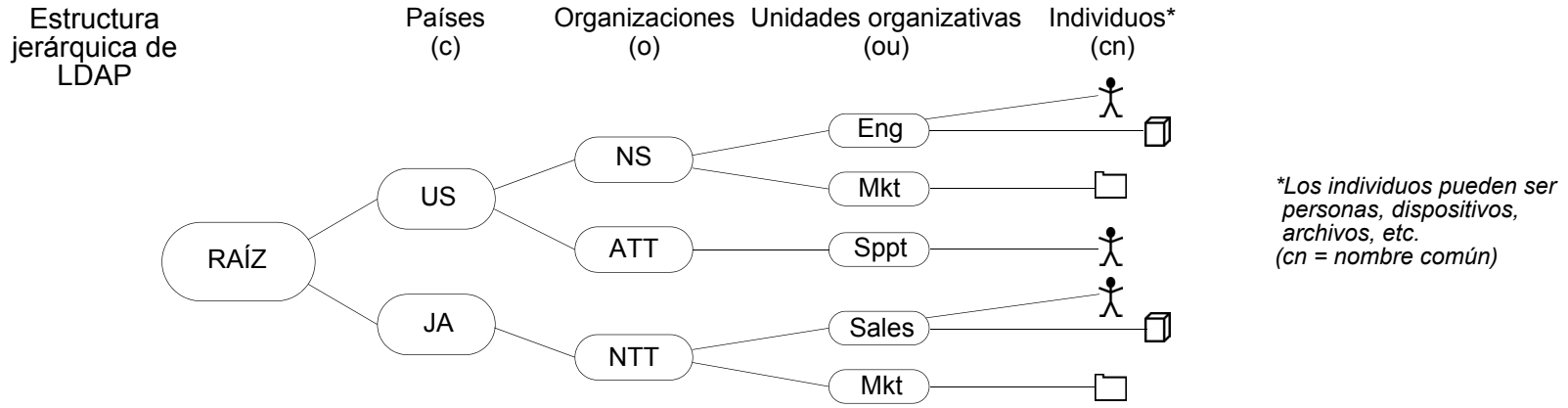
Actualmente, un servidor SecurID ACE no puede asignar ajustes remotos L2TP o XAuth ni privilegios de administrador NetScreen, aunque se puede utilizar un servidor SecurID para almacenar cuentas de usuarios administradores, L2TP y XAuth con fines de autenticación. Asimismo, NetScreen no admite grupos de usuarios cuando se utiliza conjuntamente con SecurID.

LDAP

El protocolo ligero de acceso a directorios (“Lightweight Directory Access Protocol” o LDAP) es un estándar de servidor de directorios desarrollado en la Universidad de Michigan en 1996. LDAP es un protocolo para la organización y acceso a la información dentro de una estructura jerárquica similar a las ramas de un árbol. Su finalidad es doble:

- Para localizar recursos, como organizaciones, individuos y archivos en una red
- Para ayudar a autenticar usuarios que intentan conectarse a redes controladas por servidores de directorios

La estructura básica de LDAP se ramifica desde el nivel de países al de organizaciones, luego unidades organizativas y, por último, individuos. También puede haber otros niveles de ramificación intermedios, como “regiones” y “provincias”. La ilustración siguiente muestra un ejemplo de la estructura de organización ramificada de LDAP.



Nota: *Si desea obtener información sobre LDAP, consulte* RFC-1777 “Lightweight Directory Access Protocol”.

Puede configurar el dispositivo NetScreen para enlazarse con un servidor de protocolo ligero de acceso a directorios (LDAP). Este servidor utiliza la sintaxis jerárquica de LDAP para identificar a cada usuario de forma inequívoca.

Propiedades del objeto servidor de autenticación LDAP

Además de las propiedades genéricas de cualquier servidor de autenticación detalladas en “Propiedades del objeto “servidor de autenticación”” en la página 22, los servidores LDAP también utilizan las propiedades siguientes:

- **LDAP Server Port:** El número del puerto en el servidor LDAP al que el dispositivo NetScreen envía las peticiones de autenticación. El número de puerto predeterminado es 389.

  Nota: *Si cambia el número del puerto de LDAP en el dispositivo NetScreen, cámbielo también en el servidor LDAP.*

- **Common Name Identifier:** El identificador utilizado por el servidor LDAP para identificar al individuo introducido en un servidor LDAP. Por ejemplo, una entrada “uid” significa “user ID” (identificación de usuario) y “cn” significa “nombre común”.
- **Distinguished Name (dn):** La ruta utilizada por el servidor LDAP antes de utilizar el identificador de nombre común para buscar una entrada específica. (Por ejemplo, c=us;o=juniper, donde “c” significa país (“country”) y “o” significa organización (“organization”).

Características y tipos de usuarios admitidos

Un servidor LDAP admite los siguientes tipos de usuarios y características de autenticación:

- Usuarios de autenticación
- Usuarios L2TP (autenticación de usuarios; el usuario L2TP recibe los ajustes L2TP predeterminados del dispositivo NetScreen)
- Usuarios XAuth (autenticación de usuarios; no admite asignaciones de ajustes remotos)
- Usuarios administradores (autenticación de usuarios; el usuario administrador recibe la asignación de privilegios predeterminada: sólo lectura)

Actualmente, un servidor LDAP no puede asignar ajustes remotos L2TP o XAuth ni privilegios de administrador NetScreen, aunque se puede utilizar un servidor LDAP para almacenar cuentas de usuarios administradores, L2TP y XAuth con fines de autenticación. Asimismo, NetScreen no admite grupos de usuarios cuando se utiliza conjuntamente con LDAP.

DEFINICIÓN DE OBJETOS DE SERVIDOR DE AUTENTICACIÓN

Antes de poder referirse a servidores de autenticación externos (servidores auth) en directivas, puertas de enlace IKE y túneles L2TP, primero es necesario definir los objetos del servidor de autenticación. Los ejemplos siguientes ilustran cómo definir los objetos del servidor de autenticación para servidores RADIUS, servidores SecurID y servidores LDAP.

Ejemplo: Servidor de autenticación RADIUS

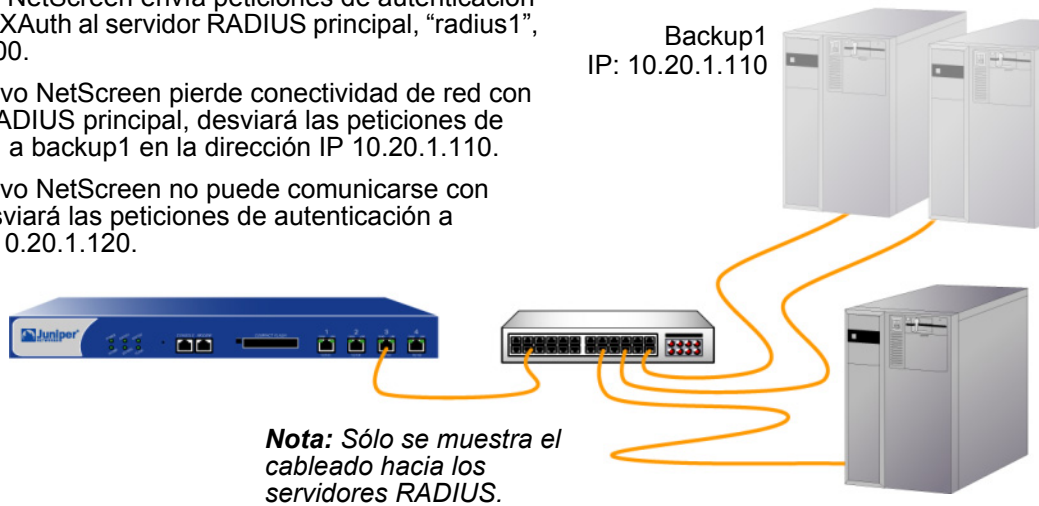
En el siguiente ejemplo definirá un objeto de servidor de autenticación para un servidor RADIUS. Especificará sus tipos de cuentas de usuario como auth (“de autenticación”), L2TP y XAuth. Llamará al servidor RADIUS “radius1” y aceptará el número de identificación que el dispositivo NetScreen le asigne automáticamente. Introducirá su dirección IP, que es 10.20.1.100; y cambiará su número de puerto predeterminado (1645) a 4500. Definirá su secreto compartido como “A56htYY97kl”. Modificará el valor del tiempo de espera predeterminado para la autenticación (10 minutos) a 30 minutos y el tiempo de espera entre reintentos de RADIUS de 3 a 4 segundos. También asignará a sus dos servidores de respaldo las direcciones IP 10.20.1.110 y 10.20.1.120.

También cargará el archivo de diccionario de NetScreen en el servidor RADIUS de modo que admita consultas sobre los siguientes atributos específicos de cada fabricante (VSAs): grupos de usuarios, privilegios de administrador, ajustes remotos L2TP y XAuth.

El dispositivo NetScreen envía peticiones de autenticación auth, L2TP y XAuth al servidor RADIUS principal, “radius1”, en 10.20.1.100.

Si el dispositivo NetScreen pierde conectividad de red con el servidor RADIUS principal, desviará las peticiones de autenticación a backup1 en la dirección IP 10.20.1.110.

Si el dispositivo NetScreen no puede comunicarse con backup1, desviará las peticiones de autenticación a backup2 en 10.20.1.120.



Nota: *Sólo se muestra el cableado hacia los servidores RADIUS.*

WebUI

Configuration > Auth > Servers > New: Introduzca los siguientes datos y haga clic en **OK**:

Name: radius1

IP/Domain Name: 10.20.1.100

Backup1: 10.20.1.110

Backup2: 10.20.1.120

Timeout: 30

Account Type: Auth, L2TP, XAuth

RADIUS: (seleccione)

RADIUS Port: 4500

Retry Timeout: 4 (segundos)

Shared Secret: A56htYY97kl

Cargue el archivo de diccionario de NetScreen en el servidor RADIUS.

Nota: *Para obtener más información sobre el archivo de diccionario de NetScreen, consulte* *"Archivo de diccionario de NetScreen" en la página 26**. Para obtener instrucciones sobre cómo cargar el archivo de diccionario en un servidor RADIUS, consulte la documentación específica de su servidor.*

CLI

```
set auth-server radius1 type radius
set auth-server radius1 account-type auth l2tp xauth[2]
set auth-server radius1 server-name 10.20.1.100
set auth-server radius1 backup1 10.20.1.110
set auth-server radius1 backup2 10.20.1.120
set auth-server radius1 timeout 30
set auth-server radius1 radius port 4500[3]
set auth-server radius1 radius timeout 4
set auth-server radius1 radius secret A56htYY97kl
save
```

Cargue el archivo de diccionario de NetScreen en el servidor RADIUS.

Nota: *Para obtener más información sobre el archivo de diccionario de NetScreen, consulte* *"Archivo de diccionario de NetScreen" en la página 26**. Para obtener instrucciones sobre cómo cargar el archivo de diccionario en un servidor RADIUS, consulte la documentación específica de su servidor.*

2. El orden en el que se introducen los tipos de cuentas es importante. Por ejemplo, si escribe primero **set auth-server radius1 account-type l2tp**, la única opción siguiente posible es **xauth**, porque no se puede escribir **auth** después de **l2tp**. El orden correcto puede recordarse fácilmente porque es alfabético.
3. Cambiando el número de puerto se pueden impedir ataques potenciales dirigidos al número de puerto predeterminado de RADIUS (1645).

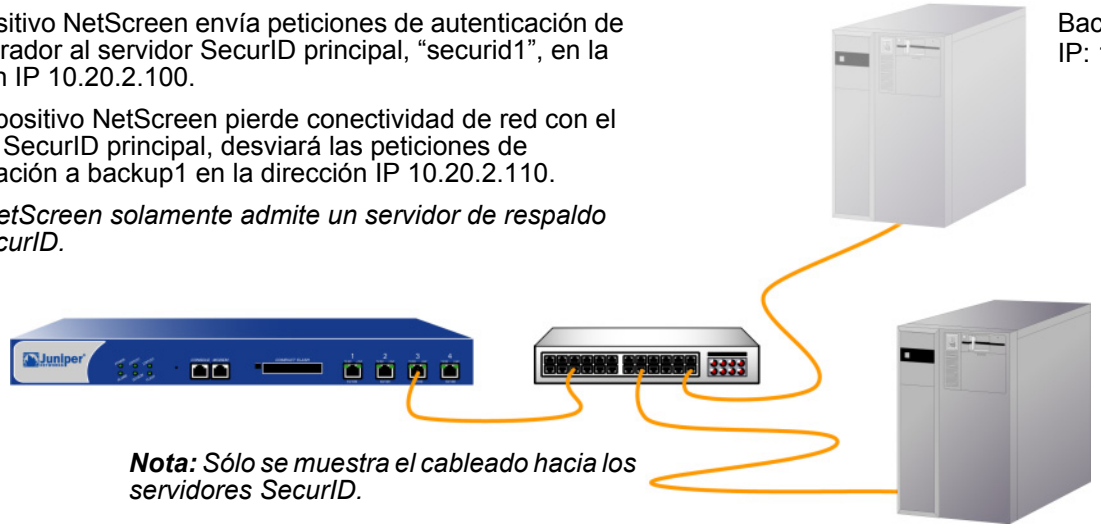
Ejemplo: Servidor de autenticación SecurID

En el ejemplo siguiente configurará un objeto de servidor de autenticación para un servidor SecurID ACE. Especificará su tipo de cuenta de usuario como admin. Llamará al servidor “securid1” y aceptará el número de identificación que el dispositivo NetScreen le asigne automáticamente. Introducirá la dirección IP del servidor principal, que es 10.20.2.100 y la dirección IP de un servidor de respaldo: 10.20.2.110. Cambiará su número de puerto predeterminado (5500) a 15000. El dispositivo NetScreen y el servidor SecurID ACE protegerán la información de autenticación utilizando el algoritmo de encriptación DES. Se admiten hasta tres reintentos y un tiempo de espera del cliente de 10 segundos[4]. Cambiará el tiempo de espera por inactividad predeterminado (10 minutos) a 60 minutos[5]. Desactivará el ajuste **Use Duress**.

El dispositivo NetScreen envía peticiones de autenticación de administrador al servidor SecurID principal, “securid1”, en la dirección IP 10.20.2.100.

Si el dispositivo NetScreen pierde conectividad de red con el servidor SecurID principal, desviará las peticiones de autenticación a backup1 en la dirección IP 10.20.2.110.

Nota: *NetScreen solamente admite un servidor de respaldo para SecurID.*



Nota: *Sólo se muestra el cableado hacia los servidores SecurID.*

4. El tiempo de espera del cliente es el número de segundos que el cliente SecurID (es decir, el dispositivo NetScreen) espera entre sucesivos reintentos de autenticación.

5. El valor del tiempo de espera por inactividad es el número de minutos que pueden transcurrir antes de que el dispositivo NetScreen termine automáticamente una sesión de administrador inactiva. (Para obtener información comparativa entre los tiempos de espera aplicados a usuarios administradores y los aplicados a otros tipos de usuarios, consulte “Propiedades del objeto “servidor de autenticación”” en la página 22).

WebUI

Configuration > Auth > Servers > New: Introduzca los siguientes datos y haga clic en **OK**:

Name: securid1

IP/Domain Name: 10.20.2.100

Backup1: 10.20.2.110

Timeout: 60

Account Type: Admin

SecurID: (seleccione)

Client Retries: 3

Client Timeout: 10 seconds

Authentication Port: 15000

Encryption Type: DES

User Duress: No

CLI

```
set auth-server securid1 type securid
set auth-server securid1 server-name 10.20.2.100
set auth-server securid1 backup1 10.20.2.110
set auth-server securid1 timeout 60
set auth-server securid1 account-type admin
set auth-server securid1 securid retries 3
set auth-server securid1 securid timeout 10
set auth-server securid1 securid auth-port 15000
set auth-server securid1 securid encr 1
set auth-server securid1 securid duress 0
save
```

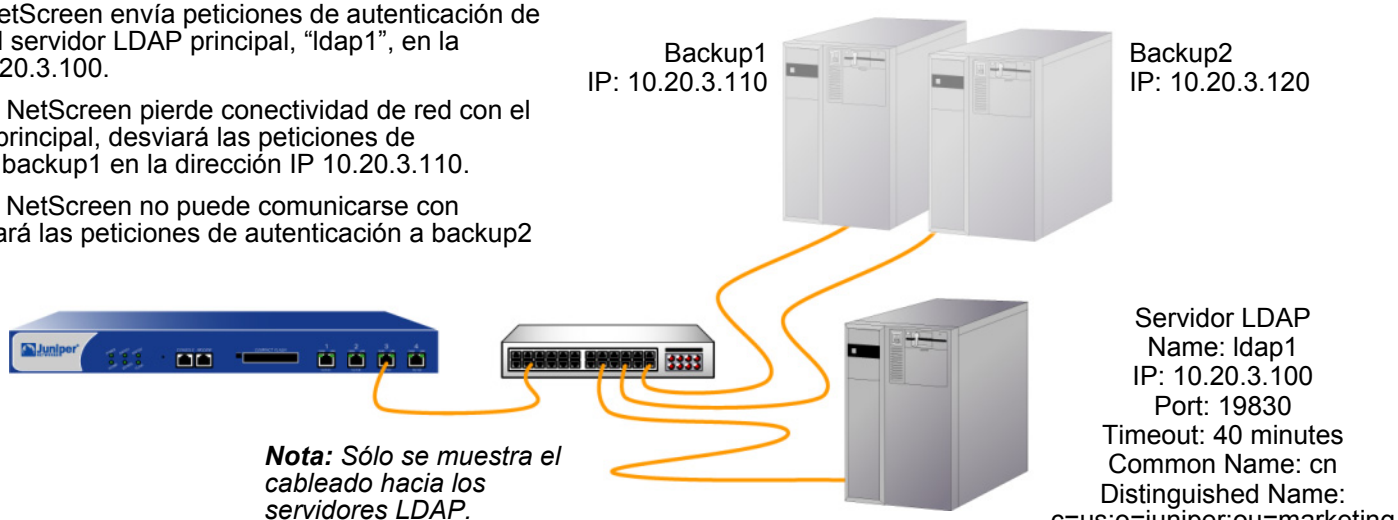
Ejemplo: Servidor de autenticación LDAP

En el ejemplo siguiente configurará un objeto de servidor de autenticación para un servidor LDAP. Especificará su tipo de cuenta de usuario como auth. Denominará al servidor LDAP “ldap1” y aceptará el número de identificación que el dispositivo NetScreen le asigne automáticamente. Introducirá su dirección IP, que es 10.20.3.100 y cambiará su número de puerto predeterminado (389) a 19830. Cambiará el valor del tiempo de espera predeterminado (10 minutos) a 40 minutos. También asignará a sus dos servidores de respaldo las direcciones IP 10.20.3.110 y 10.20.3.120. El identificador de common name (nombre común) LDAP será “cn” y el Distinguished Name (nombre completo) “c=us;o=juniper;ou=marketing”.

El dispositivo NetScreen envía peticiones de autenticación de usuarios auth al servidor LDAP principal, “ldap1”, en la dirección IP 10.20.3.100.

Si el dispositivo NetScreen pierde conectividad de red con el servidor LDAP principal, desviará las peticiones de autenticación a backup1 en la dirección IP 10.20.3.110.

Si el dispositivo NetScreen no puede comunicarse con backup1, desviará las peticiones de autenticación a backup2 en 10.20.3.120.



Nota: *Sólo se muestra el cableado hacia los servidores LDAP.*

WebUI

Configuration > Auth > Servers > New: Introduzca los siguientes datos y haga clic en **OK**:

Name: ldap1

IP/Domain Name: 10.20.3.100

Backup1: 10.20.3.110

Backup2: 10.20.3.120

Timeout: 40

Account Type: Auth

LDAP: (seleccione)

LDAP Port: 4500

Common Name Identifier: cn

Distinguished Name (dn): c=us;o=juniper;ou=marketing

CLI

```
set auth-server ldap1 type ldap
set auth-server ldap1 account-type auth
set auth-server ldap1 server-name 10.20.3.100
set auth-server ldap1 backup1 10.20.3.110
set auth-server ldap1 backup2 10.20.3.120
set auth-server ldap1 timeout 40
set auth-server ldap1 ldap port 15000
set auth-server ldap1 ldap cn cn
set auth-server ldap1 ldap dn c=us;o=juniper;ou=marketing
save
```

DEFINICIÓN DE LOS SERVIDORES DE AUTENTICACIÓN PREDETERMINADOS

De forma predeterminada, la base de datos local es el servidor de autenticación predeterminado para todos los tipos de usuarios. Puede especificar servidores de autenticación externos como servidores predeterminados para la autenticación de al menos uno de los siguientes tipos de usuarios:

- Admin
- Auth
- L2TP
- XAuth

Si posteriormente desea utilizar el servidor de autenticación predeterminado para un tipo de usuario determinado al configurar la autenticación en directivas, túneles L2TP o puertas de enlace IKE, no necesitará especificar un servidor de autenticación en cada configuración. El dispositivo NetScreen establecerá las referencias apropiadas a los correspondientes servidores de autenticación designados previamente como predeterminados.

Ejemplo: Cambiar los servidores de autenticación predeterminados

En este ejemplo se utilizan los objetos de servidores de autenticación RADIUS, SecurID y LDAP creados en los ejemplos anteriores:

- radius1 (“Ejemplo: Servidor de autenticación RADIUS” en la página 34)
- securid1 (“Ejemplo: Servidor de autenticación SecurID” en la página 37)
- ldap1 (“Ejemplo: Servidor de autenticación LDAP” en la página 39)

A continuación asignará la base de datos local, radius1, securid1 y ldap1 como servidores predeterminados para los siguientes tipos de usuarios:

- Local: Servidor de autenticación predeterminado para usuarios XAuth[6]
- radius1: Servidor de autenticación predeterminado para usuarios L2TP
- securid1: Servidor de autenticación predeterminado para usuarios con permisos de administrador
- ldap1: Servidor de autenticación predeterminado para usuarios de autenticación (Auth)

6. De forma predeterminada, la base de datos local es el servidor de autenticación predeterminado para todos los tipos de usuarios. Por lo tanto, a menos que haya asignado previamente un servidor de autenticación externo como servidor predeterminado para los usuarios XAuth, no necesita configurarlo como tal.

WebUI

VPNs > AutoKey Advanced > XAuth Settings: Seleccione **Local** en la lista desplegable Default Authentication Server y haga clic en **Apply**[7].

VPNs > L2TP > Default Settings: Seleccione **radius1** en la lista desplegable Default Authentication Server y haga clic en **Apply**.

Configuration > Admin > Administrators: Seleccione **Local/securid1** en la lista desplegable Admin Auth Server y haga clic en **Apply**.

Configuration > Auth > Firewall: Seleccione **ldap1** en la lista desplegable Default Auth Server y haga clic en **Apply**.

CLI

```
set xauth default auth server Local[7]
set l2tp default auth server radius1
set admin auth server securid1
set auth default auth server ldap1
save
```

7. De forma predeterminada, la base de datos local es el servidor de autenticación predeterminado para todos los tipos de usuarios. Por lo tanto, a menos que haya asignado previamente un servidor de autenticación externo como servidor predeterminado para los usuarios XAuth, no necesita configurarlo como tal.

3

Usuarios de autenticación

Un usuario de autenticación (o “auth user”) es un usuario de red que debe proporcionar un nombre de usuario y la correspondiente contraseña para autenticarse al iniciar una conexión a través del cortafuegos. Las cuentas de usuarios de autenticación se pueden almacenar en la base de datos local o en el servidor RADIUS, SecurID o LDAP externo.

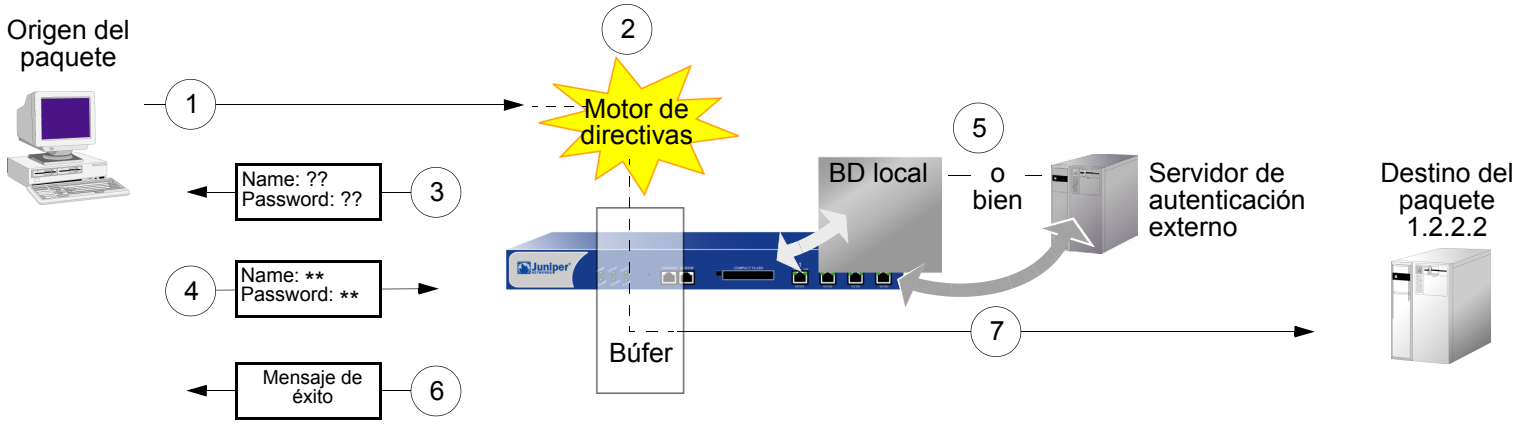
Se pueden agrupar varias cuentas de usuarios de autenticación para crear un grupo de usuarios auth, que se puede guardar en la base de datos local o en un servidor RADIUS. Una sola cuenta de usuario de autenticación puede estar asociada hasta a cuatro grupos de usuarios en la base de datos local o en un servidor RADIUS. Si crea un grupo de usuarios externo en un servidor RADIUS, también debe crear un grupo idéntico (pero vacío) de usuarios en el dispositivo NetScreen. Por ejemplo, si define un grupo de usuarios de autenticación denominado “au_grp1” en un servidor RADIUS llamado “rs1” y agrega 10 miembros al grupo, en el dispositivo NetScreen deberá definir un grupo de usuarios de autenticación denominado también “au_grp1”, identificándolo como grupo externo de usuarios, pero sin agregarle ningún miembro. Al hacer referencia al grupo de usuarios externo “au_grp1” y al servidor de autenticación “rs1” en una directiva, el dispositivo NetScreen podrá consultar correctamente el servidor RADIUS especificado cada vez que el tráfico descrito por la directiva provoque una comprobación de autenticación.

REFERENCIAS A USUARIOS AUTENTICADOS EN DIRECTIVAS

Después de haber definido un usuario de autenticación, podrá crear una directiva que obligue al usuario a autenticarse por medio de uno de los dos esquemas de autenticación. El primer esquema autentica a los usuarios cuando algún tráfico FTP, HTTP o Telnet que coincide con alguna directiva que requiere autenticación alcanza el dispositivo NetScreen. En el segundo esquema, los usuarios se autentican antes de enviar tráfico (de cualquier clase, no sólo FTP, HTTP o Telnet) que coincida con alguna directiva que requiera autenticación.

Autenticación en tiempo de ejecución

Cuando un usuario intenta iniciar una petición de conexión HTTP, FTP o Telnet que coincide con alguna directiva que requiere autenticación, el dispositivo NetScreen intercepta la petición y pide al usuario que introduzca un nombre y una contraseña (consulte "Autenticación de usuarios" en la página **2**-321). Antes de conceder el permiso, el dispositivo NetScreen comprueba el nombre de usuario y la contraseña comparándolos con los almacenados en la base de datos local o en un servidor de autenticación externo.

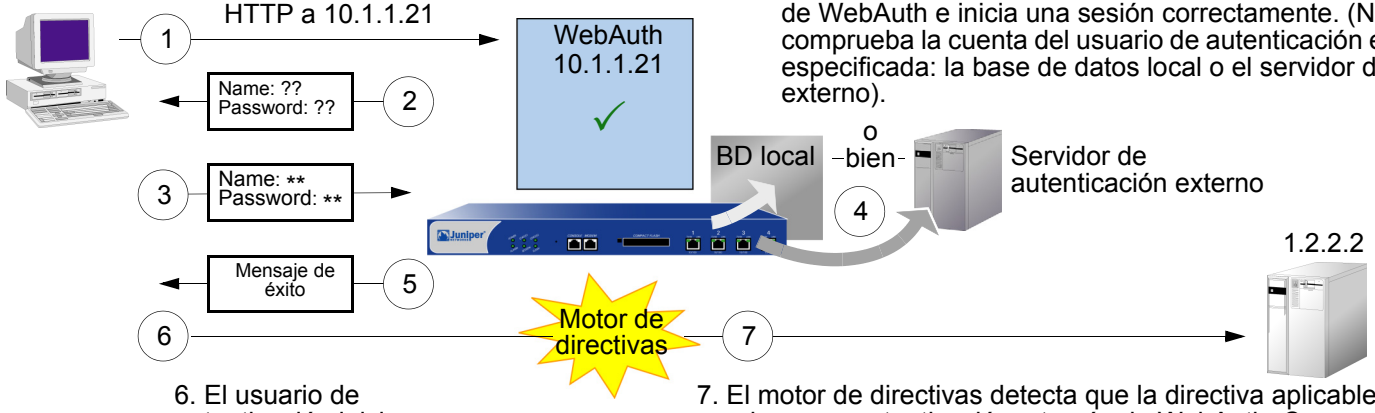


1. El usuario de autenticación envía un paquete FTP, HTTP o Telnet a la dirección 1.2.2.2.
2. El dispositivo NetScreen intercepta el paquete, detecta que su directiva requiere autenticación en la base de datos local o en un servidor externo, y guarda el paquete en un búfer.
3. El dispositivo NetScreen pide al usuario la información de inicio de sesión mediante FTP, HTTP o Telnet.

4. El usuario responde con un nombre de usuario y una contraseña.
5. El dispositivo NetScreen comprueba si en su base de datos local existe la cuenta de usuario de autenticación o envía la información de inicio de sesión al servidor de autenticación externo según lo especificado en la directiva.
6. Si encuentra alguna coincidencia (o recibe un aviso de coincidencia desde el servidor de autenticación externo), el dispositivo NetScreen informa al usuario de que el inicio de sesión ha sido correcto.
7. Seguidamente, el dispositivo NetScreen remite el paquete de su búfer a su destino 1.2.2.2.

Autenticación de comprobación previa a la directiva (WebAuth)

Antes de enviar tráfico al destino previsto, los usuarios de autenticación inician una sesión HTTP en la dirección IP que contiene la característica WebAuth en el dispositivo NetScreen y se autentican. Una vez el dispositivo NetScreen haya autenticado al usuario, éste puede enviar tráfico al destino según lo permitido por una directiva que requiere autenticación mediante WebAuth.



1 – 5. El usuario de autenticación se conecta a la dirección IP 10.1.1.21 de WebAuth e inicia una sesión correctamente. (NetScreen comprueba la cuenta del usuario de autenticación en la base de datos especificada: la base de datos local o el servidor de autenticación externo).

6. El usuario de autenticación inicia una conexión a 1.2.2.2.

7. El motor de directivas detecta que la directiva aplicable a este tráfico requiere una autenticación a través de WebAuth. Comprueba su lista de usuarios autenticados, descubre que el usuario está actualmente autenticado a través de WebAuth y envía el tráfico a su destino.

Algunos detalles sobre WebAuth:

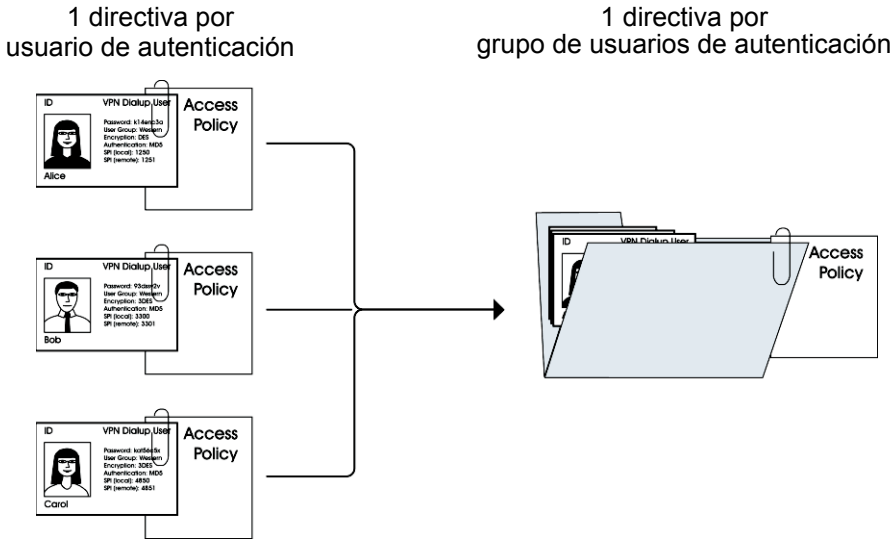
- Puede dejar la base de datos local como servidor de autenticación predeterminado de WebAuth o elegir un servidor de autenticación externo para este papel. El requisito principal para un servidor de autenticación de WebAuth es que, entre sus tipos de cuentas, debe incluir usuarios de autenticación.
- La dirección de WebAuth debe estar en la misma subred que la interfaz que desea utilizar para hospedarlo. Por ejemplo, si desea que los usuarios de autenticación se conecten a WebAuth a través de ethernet3, que tiene la dirección IP 1.1.1.1/24, puede asignar a WebAuth una dirección IP en la subred 1.1.1.0/24.
- Puede poner una dirección de WebAuth en la misma subred que la dirección IP de cualquier interfaz, subinterfaz o interfaz de seguridad virtual (VSI) física. (Si desea obtener información sobre diversos tipos de interfaces, consulte “Interfaces” en la página **2**-53).
- Si desea utilizar WebAuth mientras está en modo transparente, puede poner una dirección de WebAuth en la misma subred que la dirección IP de VLAN1.
- Puede poner direcciones de WebAuth en múltiples interfaces.
- Si tiene varias interfaces asociadas a la misma zona de seguridad, puede poner una dirección de WebAuth en una subred de una interfaz; seguirá recibiendo el tráfico procedente de la misma zona pero a través de otra interfaz.
- Recuerde que después de autenticar a un usuario en una determinada dirección IP de origen, el dispositivo NetScreen permitirá posteriormente el tráfico de cualquier otro usuario en esa misma dirección, según lo especificado en la directiva que exige autenticación a través de WebAuth. Este caso puede darse si los usuarios originan tráfico desde detrás de un dispositivo NAT que cambia todas las direcciones de origen originales a una sola dirección traducida.
- Puede hacer que el dispositivo acepte solamente conexiones SSL (HTTPS) para las sesiones WebAuth.

REFERENCIAS A GRUPOS DE USUARIOS DE AUTENTICACIÓN EN DIRECTIVAS

Para administrar un determinado número de usuarios de autenticación, puede crear grupos de usuarios de autenticación y almacenarlos en el dispositivo NetScreen local o en un servidor RADIUS externo.

Nota: *Si almacena usuarios en grupos en un servidor RADIUS, deberá crear también grupos de usuarios externos vacíos en el dispositivo NetScreen con nombres que correspondan a los de los grupos de usuarios previamente creados en el servidor RADIUS.*

En lugar de administrar cada usuario individualmente, puede agrupar usuarios en un grupo para que cualquier cambio realizado en éste se propague a todos sus miembros. Un usuario de autenticación puede ser miembro de hasta cuatro grupos de usuarios en la base de datos local o en un servidor RADIUS. Un usuario de autenticación perteneciente a más de un grupo deberá indicar un nombre de usuario y una contraseña solamente una vez antes de ser autorizado a acceder a los recursos definidos para cada grupo de los que es miembro.



Ejemplo: Autenticación en tiempo de ejecución (usuario local)

En este ejemplo definirá un usuario de autenticación local llamado “louis” con la contraseña “iDa84rNk” y una dirección denominada “host1” en la libreta de direcciones de la zona Trust. Entonces configurará dos directivas de tráfico saliente: una que rechace todo el tráfico saliente y otra de “host1” pidiendo a “louis” que se autentique. (Louis debe iniciar todo el tráfico saliente desde el host1). El dispositivo NetScreen rechazará el tráfico saliente de cualquier otra dirección, así como el tráfico no autenticado procedente de “host1”.

WebUI

1. Usuario de autenticación y dirección locales

Objects > Users > Local > New: Introduzca los siguientes datos y haga clic en **OK**:

User Name: louis

Status: Enable

Authentication User: (seleccione)

User Password: iDa84rNk

Confirm Password: iDa84rNk

Objects > Addresses > List > New: Introduzca los siguientes datos y haga clic en **OK**:

Address Name: host1

IP Address/Domain Name:

IP/Netmask: (seleccione), 10.1.1.4/32

Zone: Trust

2. Directivas

Policies > (From: Trust, To: Untrust) New: Introduzca los siguientes datos y haga clic en **OK**:

Source Address:

Address Book Entry: (seleccione), Any

Destination Address:

Address Book Entry: (seleccione), Any

Service: ANY

Action: Deny

Policies > (From: Trust, To: Untrust) New: Introduzca los siguientes datos y haga clic en **OK**:

Source Address:

Address Book Entry: (seleccione), host1

Destination Address:

Address Book Entry: (seleccione), Any

Service: ANY

Action: Permit

Position at Top: (seleccione)

> Advanced**:** Escriba lo siguiente y haga clic en **Return** para establecer las opciones avanzadas y regresar a la página de configuración básica:

Authentication: (seleccione)

Auth Server: (seleccione)

Use: Local

User: (seleccione), Local Auth User - louis

CLI

1. Usuario local y dirección

```
set user louis password iDa84rNk[1]
set address trust host1 10.1.1.4/32
```

2. Directivas

```
set policy from trust to untrust any any any deny
set policy top from trust to untrust host1 any any permit auth user louis
save
```

1. De forma predeterminada, todo usuario al que se asigna una contraseña entra en la categoría de usuarios de autenticación.

Ejemplo: Autenticación en tiempo de ejecución (grupo de usuarios locales)

En este ejemplo definirá un grupo de usuarios local llamado “auth_grp1”. Agregará los usuarios de autenticación previamente creados “louis” y “lara” al grupo[2]. Después configurará una directiva que haga referencia a “auth_grp1”. La directiva otorgará los privilegios FTP-GET y FTP-PUT a “auth_grp1”, con el nombre de dirección “auth_grp1” (dirección IP 10.1.8.0/24) en la zona Trust para acceder a un servidor FTP llamado “ftp1” (dirección IP 1.2.2.3/32) de la zona DMZ.

WebUI

1. Grupo de usuarios local y miembros

Objects > Users > Local Groups > New: Escriba **auth_grp1** en el campo Group Name, haga lo siguiente, y luego haga clic en **OK**:

Seleccione **louis** y utilice el botón **<<** para trasladarlo de la columna “Available Members” a la columna “Group Members”.

Seleccione **lara** y utilice el botón **<<** para trasladarla de la columna “Available Members” a la columna “Group Members”.

2. Dirección

Objects > Addresses > List > New: Introduzca los siguientes datos y haga clic en **OK**:

Address Name: auth_grp1

IP Address/Domain Name:

IP/Netmask: (seleccione), 10.1.8.0/24

Zone: Trust

2. Cuando se crea un grupo de usuarios en la base de datos local, su tipo de usuario permanece sin definir hasta que se le agrega un usuario. En ese momento, el grupo de usuarios asume el tipo o los tipos de usuarios que se le agreguen. Se pueden crear grupos de usuarios de múltiples tipos agregando los tipos de usuarios Auth, IKE, L2TP y XAuth. Los usuarios administradores no se pueden combinar con ningún otro tipo de usuarios.

Objects > Addresses > List > New: Introduzca los siguientes datos y haga clic en **OK**:

Address Name: ftp1

IP Address/Domain Name:

IP/Netmask: (seleccione), 1.2.2.3/32

Zone: DMZ

3. Directiva

Policies > (From: Trust, To: DMZ) New: Introduzca los siguientes datos y haga clic en **OK**:

Source Address:

Address Book Entry: (seleccione), auth_grp1

Destination Address:

Address Book Entry: (seleccione), ftp1

Service: FTP

Action: Permit

Position at Top: (seleccione)

> Advanced: Escriba lo siguiente y haga clic en **Return** para establecer las opciones avanzadas y regresar a la página de configuración básica:

Authentication: (seleccione)

Auth Server: (seleccione)

Use: Local

User Group: (seleccione), Local Auth Group - auth_grp1

CLI

1. Grupo de usuarios local y miembros

```
set user-group auth_grp1 location local
set user-group auth_grp1 user louis
set user-group auth_grp1 user lara
```

2. Dirección

```
set address trust auth_grp1 10.1.8.0/24
set address dmz ftp1 1.2.2.3/32
```

3. Directiva

```
set policy top from trust to dmz auth_grp1 ftp1 ftp permit auth user-group
    auth_grp1
save
```

Ejemplo: Autenticación en tiempo de ejecución (usuario externo)

En este ejemplo definirá un servidor de autenticación externo LDAP llamado “x_srv1” con los atributos siguientes:

- Account type: auth
- IP address: 10.1.1.100
- Backup1 IP address: 10.1.1.110
- Backup2 IP address: 10.1.1.120
- Authentication timeout: 60 minutes
- LDAP port number: 14500
- Common Name Identifier: cn
- Distinguished name: c=us;o=netscreen

Asignará al usuario de autenticación “euclid” la contraseña eTcS114u en el servidor de autenticación externo. Después configurará una directiva saliente que requiera autenticación en el servidor de autenticación “x_srv1” para el usuario externo “euclid”.

WebUI

1. Servidor de autenticación

Configuration > Auth > Servers > New: Introduzca los siguientes datos y haga clic en **OK**:

Name: x_srv1

IP/Domain Name: 10.1.1.100

Backup1: 10.1.1.110

Backup2: 10.1.1.120

Timeout: 60

Account Type: Auth

LDAP: (seleccione)

LDAP Port: 14500

Common Name Identifier: cn

Distinguished Name (dn): c=us;o=netscreen

2. Usuario externo

Defina el usuario de autenticación “euclid” con la contraseña eTcS114u en el servidor de autenticación LDAP externo “x_serv1”.

3. Dirección

Objects > Addresses > List > New: Introduzca los siguientes datos y haga clic en **OK**:

Address Name: euc_host

IP Address/Domain Name:

IP/Netmask: (seleccione), 10.1.1.20/32

Zone: Trust

4. Directiva

Policies > (From: Trust, To: Untrust) New: Introduzca los siguientes datos y haga clic en **OK**:

Source Address:

Address Book Entry: (seleccione), Any

Destination Address:

Address Book Entry: (seleccione), Any

Service: ANY

Action: Permit

Position at Top: (seleccione)

> Advanced: Escriba lo siguiente y haga clic en **Return** para establecer las opciones avanzadas y regresar a la página de configuración básica:

Authentication: (seleccione)

Auth Server: (seleccione)

Use: x_srv1

User: (seleccione), External User

External User: euclid

CLI

1. Servidor de autenticación

```
set auth-server x_srv1
set auth-server x_srv1 type ldap
set auth-server x_srv1 account-type auth
set auth-server x_srv1 server-name 10.1.1.100
set auth-server x_srv1 backup1 10.1.1.110
set auth-server x_srv1 backup2 10.1.1.120
set auth-server x_srv1 timeout 60
set auth-server x_srv1 ldap port 14500
set auth-server x_srv1 ldap cn cn
set auth-server x_srv1 ldap dn c=us;o=netscreen
```

2. Usuario externo

Defina el usuario de autenticación “euclid” con la contraseña eTcS114u en el servidor de autenticación LDAP externo “x_srv1”.

3. Dirección

```
set address trust euc_host 10.1.1.20/32
```

4. Directiva

```
set policy top from trust to untrust euc_host any any auth server x_srv1 user
    euclid
save
```

Ejemplo: Autenticación en tiempo de ejecución (grupo de usuarios externo)

En este ejemplo se configura un servidor de autenticación RADIUS externo denominado “radius1”[3] y se define un grupo de usuarios de autenticación externo llamado “auth_grp2”. También se define el grupo de usuarios de autenticación externo “auth_grp2” en dos sitios:

1. Servidor de autenticación RADIUS externo “radius1”
2. Dispositivo NetScreen

Alimentará el grupo de usuarios de autenticación “auth_grp2” solamente con los usuarios de autenticación del servidor RADIUS, dejando el grupo vacío en el dispositivo NetScreen. Los miembros de este grupo son contables que requieren acceso exclusivo a un servidor en la dirección IP 10.1.1.80. Creará una entrada en la libreta de direcciones para el servidor y llamará a la dirección “midas”. Luego configurará una directiva intrazonal que sólo permitirá tráfico autenticado de “auth_grp2” a “midas”, ambos en la zona Trust. (Para obtener más información sobre directivas intrazonales, consulte el “Directivas” en la página **2**-305).

Servidor RADIUS

1. Cargue el archivo de diccionario de NetScreen en el servidor RADIUS[4].

   Nota: *Para obtener más información sobre el archivo de diccionario de NetScreen, consulte el “Archivo de diccionario de NetScreen” en la página 26. Para obtener instrucciones sobre cómo cargar el archivo de diccionario en un servidor RADIUS, consulte la documentación del servidor RADIUS.*

2. Después de definir las cuentas de los usuarios de autenticación en el servidor RADIUS, utilice la VSA del grupo de usuarios NetScreen para crear el grupo de usuarios “auth_grp2” y aplíquelo a las cuentas de usuarios de autenticación que desee agregar a dicho grupo.

3. La configuración del servidor de autenticación de RADIUS es casi idéntica a la descrita en el “Ejemplo: Servidor de autenticación RADIUS” en la página 34, salvo que en este ejemplo solamente se especificará “auth” como tipo de cuenta de usuario.

4. Si está utilizando un servidor IAS RADIUS de Microsoft, no hay que cargar ningún archivo de diccionario. En lugar de ello hay que definir los atributos correctos específicos de cada fabricante (VSAs) en el servidor.

WebUI

1. Servidor de autenticación

   Configuration > Auth > Servers > New: Introduzca los siguientes datos y haga clic en **OK**:

   Name: radius1

   IP/Domain Name: 10.20.1.100

   Backup1: 10.20.1.110

   Backup2: 10.20.1.120

   Timeout: 30

   Account Type: Auth

   RADIUS: (seleccione)

   RADIUS Port: 4500

   Shared Secret: A56htYY97kl

2. Grupo de usuarios externo

   Objects > Users > External Groups > New: Introduzca los siguientes datos y haga clic en **OK**:

   Group Name: auth_grp2

   Group Type: Auth

3. Dirección

   Objects > Addresses > List > New: Introduzca los siguientes datos y haga clic en **OK**:

   Address Name: midas

   IP Address/Domain Name:

   IP/Netmask: (seleccione), 10.1.1.80/32

   Zone: Trust

4. Directiva

Policies > (From: Trust, To: Trust) New: Introduzca los siguientes datos y haga clic en **OK**:

Source Address:

Address Book Entry: (seleccione), Any

Destination Address:

Address Book Entry: (seleccione), midas

Service: ANY

Action: Permit

Position at Top: (seleccione)

> Advanced: Escriba lo siguiente y haga clic en **Return** para establecer las opciones avanzadas y regresar a la página de configuración básica:

Authentication: (seleccione)

Auth Server: (seleccione)

Use: radius1

User Group: (seleccione), External Auth Group - auth_grp2

CLI

1. Servidor de autenticación

```
set auth-server radius1 type radius
set auth-server radius1 account-type auth
set auth-server radius1 server-name 10.20.1.100
set auth-server radius1 backup1 10.20.1.110
set auth-server radius1 backup2 10.20.1.120
set auth-server radius1 timeout 30
set auth-server radius1 radius port 4500
set auth-server radius1 radius secret A56htYY97kl
```

2. Grupo de usuarios externo

```
set user-group auth_grp2 location external
set user-group auth_grp2 type auth
```

3. Dirección

```
set address trust midas 10.1.1.80/32
```

4. Directiva

```
set policy top from trust to trust any midas any permit auth server radius1
    user-group auth_grp2
save
```

Ejemplo: Usuario de autenticación local en múltiples grupos

En este ejemplo definirá una usuaria de autenticación local llamada “Mary”. Mary es jefa de ventas y necesita acceso a dos servidores: el servidor A, dedicado al equipo de agentes comerciales (grupo “sales_reps”) y el servidor B, dedicado a los jefes de ventas (grupo “sales_mgrs”). Para proporcionarle acceso a ambos, agregará a Mary a ambos grupos de usuarios. Luego creará dos directivas, uno para cada grupo.

Nota: *Este ejemplo no muestra la configuración de los otros miembros del grupo.*

WebUI

1. Usuario local

Objects > Users > Local > New: Introduzca los siguientes datos y haga clic en **OK**:

User Name: mary

Status: Enable

Authentication User: (seleccione)

User Password: iFa8rBd

Confirm Password: iFa8rBd

2. Grupos de usuarios locales y miembros

Objects > Users > Local Groups > New: Escriba **sales_mgrs** en el campo Group Name, haga lo siguiente, y luego haga clic en **OK**:

Seleccione **mary** y utilice el botón **<<** para trasladarla de la columna “Available Members” a la columna “Group Members”.

Objects > Users > Local Groups > New: Escriba **sales_reps** en el campo Group Name, haga lo siguiente, y luego haga clic en **OK**:

Seleccione **mary** y utilice el botón **<<** para trasladarla de la columna “Available Members” a la columna “Group Members”.

3. Direcciones

Objects > Addresses > List > New: Introduzca los siguientes datos y haga clic en **OK**:

Address Name: sales
IP Address/Domain Name:
IP/Netmask: (seleccione), 10.1.8.0/24
Zone: Trust

Objects > Addresses > List > New: Introduzca los siguientes datos y haga clic en **OK**:

Address Name: server_a
IP Address/Domain Name:
IP/Netmask: (seleccione), 1.1.1.5/32
Zone: Untrust

Objects > Addresses > List > New: Introduzca los siguientes datos y haga clic en **OK**:

Address Name: server_b
IP Address/Domain Name:
IP/Netmask: (seleccione), 1.1.1.6/32
Zone: Untrust

4. Directivas

Policies > (From: Trust, To: Untrust) > New: Introduzca los siguientes datos y haga clic en **OK**:

Source Address:
Address Book Entry: (seleccione), sales
Destination Address:
Address Book Entry: (seleccione), server_a
Service: FTP
Action: Permit

Position at Top: (seleccione)

> Advanced: Escriba lo siguiente y haga clic en **Return** para establecer las opciones avanzadas y regresar a la página de configuración básica:

Authentication: (seleccione)

Auth Server: (seleccione)

Use: Local

User Group: (seleccione), Local Auth Group - sales_reps

Policies > (From: Trust, To: Untrust) > New: Introduzca los siguientes datos y haga clic en **OK**:

Source Address:

Address Book Entry: (seleccione), sales

Destination Address:

Address Book Entry: (seleccione), server_b

Service: FTP

Action: Permit

Position at Top: (seleccione)

> Advanced: Escriba lo siguiente y haga clic en **Return** para establecer las opciones avanzadas y regresar a la página de configuración básica:

Authentication: (seleccione)

Auth Server: (seleccione)

Use: Local

User Group: (seleccione), Local Auth Group - sales_mgrs

CLI

1. **Usuario local**

```
set user mary password iFa8rBd
```

2. **Grupos de usuarios locales y miembros**

```
set user-group sales_mgrs location local
set user-group sales_mgrs user mary
set user-group sales_reps location local
set user-group sales_reps user mary
```

3. **Direcciones**

```
set address trust sales 10.1.8.0/24
set address untrust server_a 1.1.1.5/32
set address untrust server_b 1.1.1.6/32
```

4. **Directiva**

```
set policy top from trust to untrust sales server_a ftp permit auth user-group
    sales_reps
set policy top from trust to untrust sales server_b ftp permit auth user-group
    sales_mgrs
save
```

Ejemplo: WebAuth (grupo de usuarios local)

En este ejemplo se requiere de los usuarios una autenticación previa utilizando el método de WebAuth antes de iniciar un tráfico saliente hacia Internet. Creará un grupo de usuarios denominado “auth_grp3” en la base de datos local del dispositivo NetScreen. Después creará las cuentas de usuarios de autenticación para cada miembro en la zona Trust y las agregará a “auth_grp3”.

La interfaz de la zona Trust utiliza ethernet1 y tiene la dirección IP 10.1.1.1/24. Le asignará 10.1.1.50 como dirección IP de WebAuth y seguirá utilizando la base de datos local como servidor predeterminado de WebAuth. Por lo tanto, antes de que un usuario pueda iniciar un tráfico hacia Internet, primero deberá establecer una conexión HTTP a 10.1.1.50 e iniciar una sesión con un nombre de usuario y contraseña. Seguidamente, el dispositivo NetScreen comparará el nombre de usuario y la contraseña introducidos con los de su base de datos y aprobará o rechazará la petición de autenticación. Si aprueba la petición, el usuario autenticado dispondrá de 30 minutos para iniciar el tráfico hacia Internet. Después de terminar la sesión inicial, el usuario tendrá otros 30 minutos para iniciar otra sesión antes de que el dispositivo NetScreen le exija autenticarse de nuevo.

WebUI

1. WebAuth

Configuration > Auth > WebAuth: Seleccione **Local** en la lista desplegable WebAuth Server y haga clic en **Apply**.

Network > Interfaces > Edit (para ethernet1): Seleccione **WebAuth** y, en el campo WebAuth IP, escriba **10.1.1.50**.

Configuration > Auth > Servers > Edit (para Local): Escriba **30** en el campo Timeout y haga clic en **Apply**.

2. Grupo de usuarios

Objects > Users > Local Groups > New: Escriba **auth_grp3** en el campo Group Name, haga lo siguiente, y luego haga clic en **OK**:

Seleccione el ***nombre de usuario*** y utilice el botón **<<** para trasladarlo de la columna “Available Members” a la columna “Group Members”.

Repita el proceso de selección, agregando usuarios de autenticación hasta que el grupo esté completo.

3. Directiva

Policies > (From: Trust, To: Untrust) New: Introduzca los siguientes datos y haga clic en **OK**:

Source Address:

Address Book Entry: (seleccione), Any

Destination Address:

Address Book Entry: (seleccione), Any

Service: ANY

Action: Permit

> Advanced: Escriba lo siguiente y haga clic en **Return** para establecer las opciones avanzadas y regresar a la página de configuración básica:

Authentication: (seleccione)

WebAuth: (seleccione)

User Group: (seleccione), Local Auth Group - auth_grp3

CLI

1. WebAuth

```
set webauth server Local
set interface ethernet1 webauth-ip 10.1.1.50
set interface ethernet1 webauth
set auth-server Local timeout 30
```

2. Grupo de usuarios

```
set user-group auth_grp3 location local
```

Nota: *El dispositivo NetScreen determinará el tipo del grupo de usuarios local según el tipo de miembros que le agregue. Para hacer que "auth_grp3" sea un grupo de usuarios de autenticación, agréguele un usuario de autenticación.*

Utilice el comando siguiente para agregar usuarios de autenticación al grupo del usuarios recién creado:

```
set user-group auth_grp3 user name_str
```

3. Directiva

```
set policy top from trust to untrust any any any permit webauth user-group
    auth_grp3
save
```

Ejemplo: WebAuth (grupo de usuarios externo)

WebAuth es un método de autenticación previa de usuarios que se ejecuta antes de que éstos puedan iniciar tráfico a través de un cortafuegos. En este ejemplo creará una directiva que requiere autenticación para todo el tráfico saliente utilizando el método de WebAuth.

Creará el grupo de usuarios de autenticación “auth_grp4” denominado “auth_grp4” tanto en el servidor RADIUS “radius1” como en el dispositivo NetScreen. En el servidor RADIUS, creará las cuentas de usuario para cada miembro en la zona Trust y las agregará a “auth_grp4”.

Nota: *En este ejemplo se utilizan prácticamente los mismos ajustes del servidor RADIUS que en el “Ejemplo: Servidor de autenticación RADIUS” en la página 34, salvo que aquí sólo se especifica “auth” como tipo de cuenta de usuario.*

La interfaz de la zona Trust utilizará ethernet1 y tendrá la dirección IP 10.1.1.1/24. Usted asignará 10.1.1.50 como dirección IP de WebAuth y utilizará el servidor de autenticación RADIUS externo “radius1” como servidor predeterminado de WebAuth. Por lo tanto, antes de que un usuario pueda iniciar un tráfico hacia Internet, primero deberá establecer una conexión HTTP a 10.1.1.50 e iniciar una sesión con un nombre de usuario y contraseña. Entonces, el dispositivo NetScreen reenviará todas las peticiones y respuestas de autenticación de usuarios de WebAuth entre “radius1” y los usuarios que intenten iniciar una sesión.

Servidor RADIUS

1. Cargue el archivo de diccionario de NetScreen en el servidor RADIUS.

   Nota: *Para obtener más información sobre el archivo de diccionario de NetScreen, consulte el “Archivo de diccionario de NetScreen” en la página 26. Para obtener instrucciones sobre cómo cargar el archivo de diccionario en un servidor RADIUS, consulte la documentación del servidor RADIUS.*

2. Cree el grupo de usuarios “auth_grp4” en el servidor de autenticación “radius1” y agréguele cuentas de usuarios de autenticación.

WebUI

1. Servidor de autenticación

   Configuration > Auth > Servers > New: Introduzca los siguientes datos y haga clic en **OK**:

   Name: radius1

   IP/Domain Name: 10.20.1.100

   Backup1: 10.20.1.110

   Backup2: 10.20.1.120

   Timeout: 30

   Account Type: Auth

   RADIUS: (seleccione)

   RADIUS Port: 4500

   Shared Secret: A56htYY97k

2. WebAuth

   Configuration > Auth > WebAuth: Seleccione **radius1** en la lista desplegable WebAuth Server y haga clic en **Apply**.

   Network > Interfaces > Edit (para ethernet1): Seleccione **WebAuth**; en el campo WebAuth IP, escriba **10.10.1.50**, y haga clic en **OK**.

3. Grupo de usuarios

   Objects > Users > External Groups > New: Introduzca los siguientes datos y haga clic en **OK**:

   Group Name: auth_grp4

   Group Type: Auth

4. Directiva

Policies > (From: Trust, To: Untrust) New: Introduzca los siguientes datos y haga clic en **OK**:

Source Address:

Address Book Entry: (seleccione), Any

Destination Address:

Address Book Entry: (seleccione), Any

Service: ANY

Action: Permit

> Advanced: Escriba lo siguiente y haga clic en **Return** para establecer las opciones avanzadas y regresar a la página de configuración básica:

Authentication: (seleccione)

WebAuth: (seleccione)

User Group: (seleccione), External Auth Group - auth_grp4

CLI

1. Servidor de autenticación

```
set auth-server radius1 type radius
set auth-server radius1 account-type auth
set auth-server radius1 server-name 10.20.1.100
set auth-server radius1 backup1 10.20.1.110
set auth-server radius1 backup2 10.20.1.120
set auth-server radius1 timeout 30
set auth-server radius1 radius port 4500
set auth-server radius1 radius secret A56htYY97kl
```

2. WebAuth

```
set webauth server radius1
set interface ethernet1 webauth-ip 10.1.1.50
set interface ethernet1 webauth
```

3. Grupo de usuarios

```
set user-group auth_grp4 location external
set user-group auth_grp4 type auth
```

4. Directiva

```
set policy top from trust to untrust any any any permit webauth user-group
    auth_grp4
save
```

Ejemplo: WebAuth + SSL solamente (grupo de usuarios externo)

En este ejemplo se combina WebAuth con tecnologías Secure Sockets Layer (SSL) para permitir la transmisión segura de los nombres de usuarios y contraseñas enviados por los usuarios para iniciar una sesión. WebAuth utiliza el mismo certificado que asegura el tráfico administrativo hacia el dispositivo NetScreen para la administración a través de WebUI. (Para obtener más información sobre SSL, consulte “Secure Sockets Layer” en la página **3**-8).

La configuración para que utilice un servidor de autenticación externo WebAuth con SSL implica los pasos siguientes:

- Definir un servidor de autenticación RADIUS externo denominado “radius1” y crear un grupo de usuarios de autenticación llamado “auth_grp5” tanto en el servidor RADIUS como en el dispositivo NetScreen. En el servidor RADIUS, crear cuentas de usuario para todos los usuarios de autenticación de la zona Untrust y agregarlos a “auth_grp5”.

  Nota: *En este ejemplo se utilizan prácticamente los mismos ajustes del servidor RADIUS que en el “Ejemplo: Servidor de autenticación RADIUS” en la página 34, salvo que aquí sólo se especifica “auth” como tipo de cuenta de usuario.*

- La interfaz de la zona Untrust utilizará ethernet3 y tendrá la dirección IP 1.1.1.1/24. Usted asignará 1.1.1.50 como dirección IP de WebAuth, indicará al dispositivo que sólo acepte conexiones SSL para las peticiones de autenticación WebAuth y utilizará el servidor de autenticación RADIUS externo “radius1” como servidor predeterminado de WebAuth.
- Especificará los siguientes ajustes de SSL:
  - Número IDX (1 en este ejemplo) de un certificado cargado previamente en el dispositivo NetScreen[5]
  - Cifrados DES_SHA-1
  - Puerto SSL número 2020
- Luego configurará una directiva de tráfico entrante que exija autenticación mediante el método WebAuth + SSL para todo el tráfico que pase de la zona Untrust a la zona Trust.

Por lo tanto, para que un usuario pueda iniciar tráfico hacia la red interna, primero deberá establecer una conexión HTTPS a https://1.1.1.50:2020 e iniciar una sesión con un nombre de usuario y contraseña. Desde ese momento, el dispositivo NetScreen reenviará todas las peticiones y respuestas de autenticación de usuarios de WebAuth entre “radius1” y el usuario que intente iniciar una sesión.

5. Si desea información sobre cómo obtener y cargar certificados digitales en un dispositivo NetScreen, consulte “Criptografía de claves públicas” en la página **5**-23.

Servidor RADIUS

1. Cargue el archivo de diccionario de NetScreen en el servidor RADIUS.

   Nota: *Para obtener más información sobre el archivo de diccionario de NetScreen, consulte la sección "Archivo de diccionario de NetScreen" en la página 26. Para obtener instrucciones sobre cómo cargar el archivo de diccionario en un servidor RADIUS, consulte la documentación del servidor RADIUS.*

2. Cree el grupo de usuarios "auth_grp5" en el servidor de autenticación "radius1" y agréguele cuentas de usuarios de autenticación.

WebUI

1. Servidor de autenticación

Configuration > Auth > Servers > New: Introduzca los siguientes datos y haga clic en **OK**:

Name: radius1

IP/Domain Name: 10.20.1.100

Backup1: 10.20.1.110

Backup2: 10.20.1.120

Timeout: 30

Account Type: Auth

RADIUS: (seleccione)

RADIUS Port: 4500

Shared Secret: A56htYY97k

2. WebAuth

Configuration > Auth > WebAuth: Seleccione **radius1** en la lista desplegable WebAuth Server y haga clic en **Apply**.

Network > Interfaces > Edit (para ethernet3): Introduzca los siguientes datos y haga clic en **OK**:

WebAuth: (seleccione)

IP: 1.1.1.50

SSL Only: (seleccione)

3. SSL

Configuration > Admin > Management: Introduzca los siguientes datos y haga clic en **OK**:

HTTPS (SSL) Port: 2020

Certificate: (seleccione el certificado previamente cargado)

Cipher: DES_SHA-1

4. Grupo de usuarios

Objects > Users > External Groups > New: Introduzca los siguientes datos y haga clic en **OK**:

Group Name: auth_grp5

Group Type: Auth

5. Directiva

Policies > (From: Untrust, To: Trust) New: Introduzca los siguientes datos y haga clic en **OK**:

Source Address:

Address Book Entry: (seleccione), Any

Destination Address:

Address Book Entry: (seleccione), Any

Service: ANY

Action: Permit

> Advanced: Escriba lo siguiente y haga clic en **Return** para establecer las opciones avanzadas y regresar a la página de configuración básica:

Authentication: (seleccione)

WebAuth: (seleccione)

User Group: (seleccione), External Auth Group - auth_grp5

CLI

1. Servidor de autenticación

```
set auth-server radius1 type radius
set auth-server radius1 account-type auth
set auth-server radius1 server-name 10.20.1.100
set auth-server radius1 backup1 10.20.1.110
set auth-server radius1 backup2 10.20.1.120
set auth-server radius1 timeout 30
set auth-server radius1 radius port 4500
set auth-server radius1 radius secret A56htYY97kl
```

Cargue el archivo de diccionario de NetScreen en el servidor RADIUS.

Nota: *Para obtener más información sobre el archivo de diccionario de NetScreen, consulte el* *"Archivo de diccionario de NetScreen" en la página 26**. Para obtener instrucciones sobre cómo cargar el archivo de diccionario en un servidor RADIUS, consulte la documentación del servidor RADIUS.*

2. WebAuth

```
set webauth server radius1
set interface ethernet3 webauth-ip 1.1.1.50
set interface ethernet3 webauth ssl-only
```

3. SSL

```
set ssl port 2020
set ssl cert 1
set ssl encrypt des sha-1
set ssl enable
```

4. Grupo de usuarios

```
set user-group auth_grp5 location external
set user-group auth_grp5 type auth
```

5. Directiva

```
set policy top from untrust to trust any any any permit webauth user-group
    auth_grp5
save
```

4

Usuarios IKE, XAuth y L2TP

Este capítulo trata de los tres tipos de usuarios implicados en los protocolos de encapsulamiento: usuarios Internet Key Exchange (IKE), usuarios XAuth y usuarios Layer 2 Transport Protocol (L2TP):

Nota: *Para ver más información de conceptos y ejemplos de configuración de IKE y L2TP, consulte el Volumen 5, "VPNs".*

USUARIOS Y GRUPOS DE USUARIOS IKE

Un usuario IKE es un usuario de VPN remoto con una dirección IP asignada dinámicamente. El usuario (en realidad, el dispositivo del usuario) se autentica enviando un certificado o clave previamente compartida junto con una identificación IKE durante la negociación de Fase 1 con el dispositivo NetScreen.

La identificación IKE puede ser una dirección de correo electrónico, una dirección IP, un nombre de dominio o una cadena ASN1-DN[1]. El dispositivo NetScreen autenticará al usuario IKE si éste envía cualquiera de los siguientes datos:

- Un **certificado** en el cual uno o más de los valores que aparecen en los campos del nombre completo (DN) o en el campo SubAltName coincida con la identificación del usuario IKE configurada en el dispositivo NetScreen
- Una **clave previamente compartida** y una **identificación IKE** con la que el dispositivo NetScreen pueda generar correctamente una clave precompartida idéntica a partir de la identificación IKE recibida y de un valor inicial de clave precompartida almacenado en el dispositivo NetScreen

Hará referencia a un usuario o grupo de usuarios IKE en una configuración de puerta de enlace AutoKey IKE. Reuniendo en un grupo a los usuarios IKE que requieran configuraciones similares de puerta de enlace y de túnel, solamente necesitará definir una puerta de enlace que haga referencia al grupo (y a un túnel VPN que haga referencia a esa puerta de enlace), en lugar de establecer una puerta de enlace y un túnel para cada usuario IKE.

A menudo resulta poco práctico crear cuentas de usuario separadas para cada host. En tales casos, puede crear un grupo de usuarios IKE que solamente tenga un miembro, al que se hará referencia como usuario del grupo con identificación IKE. La identificación IKE de ese usuario contendrá un conjunto de valores que deben estar presentes en las definiciones de identificación IKE de los usuarios IKE de acceso telefónico. Si la identificación IKE de un usuario remoto de acceso telefónico coincide con la identificación IKE del usuario del grupo con esa misma identificación, NetScreen autentica a ese usuario remoto. Para obtener más información, consulte “Identificación IKE de grupo” en la página **5**-275.

Nota: *Las cuentas de usuarios IKE y de grupos de usuarios IKE sólo se pueden almacenar en la base de datos local.*

1. Como ejemplo de identificación IKE utilizando la versión 1 de la notación de sintaxis abstracta (“Abstract Syntax Notation” o ASN), el formato del nombre completo (ASN1-DN) sería CN=joe,OU=it,O=netscreen,L=sunnyvale,ST=ca,C=us,E=joe@ns.com.

Ejemplo: Definir usuarios IKE

En este ejemplo definirá cuatro usuarios IKE, “Amy”, “Basil”, “Clara” y “Desmond”, cada uno con un tipo distinto de identificación IKE.

- Amy: dirección de correo electrónico (nombre de dominio completo para el usuario o U-FQDN): amy@ns.com
- Basil: dirección IP: 3.3.1.1
- Clara: nombre de dominio completo (FQDN): www.netscreen.com
- Desmond: cadena ASN1-DN: CN=des,OU=art,O=netscreen,L=sunnyvale,ST=ca,C=us,E=des@ns.com

WebUI

Objects > Users > Local > New: Introduzca los siguientes datos y haga clic en **OK**:

User Name: Amy

Status: Enable

IKE User: (seleccione)

Simple Identity: (seleccione)

IKE ID Type: AUTO

IKE Identity: amy@ns.com

Objects > Users > Local > New: Introduzca los siguientes datos y haga clic en **OK**:

User Name: Basil

Status: Enable

IKE User: (seleccione)

Simple Identity: (seleccione)

IKE ID Type: AUTO

IKE Identity: 3.3.1.1

Objects > Users > Local > New: Introduzca los siguientes datos y haga clic en **OK**:

User Name: Clara

Status: Enable

IKE User: (seleccione)

Simple Identity: (seleccione)

IKE ID Type: AUTO

IKE Identity: www.netscreen.com

Objects > Users > Local > New: Introduzca los siguientes datos y haga clic en **OK**:

User Name: Desmond

Status: Enable

IKE User: (seleccione)

Use Distinguished Name for ID: (seleccione)

CN: des

OU: art

Organization: netscreen

Location: sunnyvale

State: ca

Country: us

E-mail: des@ns.com

CLI

```
set user Amy ike-id u-fqdn amy@ns.com
set user Basil ike-id ip 3.3.1.1
set user Clara ike-id fqdn www.netscreen.com
set user Desmond ike-id wildcard
    CN=des,OU=art,O=netscreen,L=sunnyvale,ST=ca,C=us,E=des@ns.com
save
```

Ejemplo: Crear un grupo de usuarios IKE

En este ejemplo creará un grupo de usuarios denominado “ike_grp1”. En el momento de agregarle el usuario IKE “Amy”, el grupo se convertirá en un grupo de usuarios IKE. Seguidamente, agregará los otros tres usuarios IKE que definió en el ejemplo anterior, “Ejemplo: Definir usuarios IKE” en la página 79.

WebUI

Objects > Users > Local Groups > New: Escriba **ike_grp1** en el campo Group Name, haga lo siguiente, y luego haga clic en **OK**:

Seleccione **Amy** y utilice el botón **<<** para trasladarla de la columna “Available Members” a la columna “Group Members”.

Seleccione **Basil** y utilice el botón **<<** para trasladarlo de la columna “Available Members” a la columna “Group Members”.

Seleccione **Clara** y utilice el botón **<<** para trasladarla de la columna “Available Members” a la columna “Group Members”.

Seleccione **Desmond** y utilice el botón **<<** para trasladarlo de la columna “Available Members” a la columna “Group Members”.

CLI

```
set user-group ike_grp1 location local
set user-group ike_grp1 user amy
set user-group ike_grp1 user basil
set user-group ike_grp1 user clara
set user-group ike_grp1 user desmond
save
```

Referencias a usuarios IKE en puertas de enlace

Una vez definido un usuario IKE o un grupo de usuarios IKE, podrá referirse a él en una configuración de puerta de enlace IKE cuando la puerta de enlace IKE remota sea un usuario de acceso telefónico o un grupo de usuarios de acceso telefónico.

Para ver ejemplos en los que se hace referencia a usuarios IKE en configuraciones de puerta de enlace, consulte los ejemplos siguientes:

- “Ejemplo: VPN de acceso telefónico basada en directivas, AutoKey IKE” en la página **5**-235
- “Ejemplo: Identificación IKE de grupo (certificados)” en la página **5**-281
- “Ejemplo: ID IKE de grupo (claves previamente compartidas)” en la página **5**-290

USUARIOS Y GRUPOS DE USUARIOS XAUTH

El protocolo XAuth consta de dos componentes: autenticación de usuarios VPN remotos (nombre del usuario y contraseña) y asignaciones de direcciones TCP/IP (dirección IP, máscara de red[2] y asignaciones de servidores DNS y servidores WINS). NetScreen admite la aplicación individual o conjunta de ambos componentes.

Un usuario o grupo de usuarios XAuth es uno o varios usuarios remotos que se autentican al conectarse al dispositivo NetScreen a través de un túnel VPN de AutoKey IKE y, opcionalmente, pueden recibir ajustes TCP/IP del dispositivo NetScreen. Mientras que la autenticación de los usuarios IKE es en realidad una autenticación de puertas de enlace o clientes VPN, la autenticación de los usuarios XAuth consiste en autenticar a los individuos mismos. Los usuarios XAuth deben introducir información que supuestamente sólo ellos conocen, es decir, su nombre de usuario y contraseña.

El cliente NetScreen-Remote puede utilizar los ajustes TCP/IP que recibe para crear un adaptador virtual[3] y enviar tráfico VPN, mientras que para el tráfico no VPN utilizará los ajustes del adaptador de red TCP/IP proporcionados por el proveedor de servicios de Internet o por el administrador de red. Asignando direcciones IP conocidas a los usuarios remotos, se pueden definir rutas en el dispositivo NetScreen hacia esas direcciones a través de interfaces de túnel específicas. Desde ese momento, el dispositivo NetScreen puede garantizar que el enrutamiento de retorno llegue a la dirección IP del usuario remoto a través del túnel VPN, no de la puerta de enlace predeterminada. Las asignaciones de direcciones también permiten a un cortafuegos de bajada referirse a esas direcciones al crear directivas. El ajuste “XAuth lifetime” permite controlar cuánto tiempo puede permanecer una dirección IP asociada a un determinado usuario XAuth.

2. La máscara de red asignada es siempre 255.255.255.255 y no puede ser modificada.
3. Un adaptador virtual consta de los ajustes TCP/IP (dirección IP, direcciones de servidores DNS, direcciones de servidores WINS) que el dispositivo NetScreen asigna a un usuario remoto durante la permanencia de una conexión de túnel VPN. Sólo los clientes NetScreen-Remote disponen de la funcionalidad de adaptador virtual. Las plataformas NetScreen no.

ScreenOS es compatible con los siguientes aspectos de XAuth:

- Autenticación de usuarios XAuth locales y de usuarios XAuth externos
- Autenticación de grupos de usuarios XAuth locales y de grupos de usuarios XAuth externos si están almacenados en un servidor de autenticación RADIUS
- Asignaciones de las direcciones IP propia, de los servidores DNS y de los servidores WINS a partir de un conjunto de direcciones IP para usuarios XAuth locales y usuarios XAuth externos almacenado en un servidor de autenticación RADIUS

  Para configurar el dispositivo NetScreen con el fin de utilizar los ajustes XAuth predeterminados almacenados en un servidor RADIUS externo, ejecute cualquiera de los siguientes procedimientos:

  – WebUI: En la página VPNs > AutoKey Advanced > XAuth Settings, seleccione **Query Client Settings on Default Server**.
  – CLI: Introduzca el comando **set xauth default auth server** *name_str* **query-config**.

  El dispositivo NetScreen también puede utilizar los ajustes XAuth específicos de la puerta de enlace almacenados en un servidor RADIUS externo. Para configurar una puerta de enlace IKE específica, ejecute cualquiera de los siguientes procedimientos:

  – WebUI: En la página VPNs > AutoKey Advanced > Gateway > New > Advanced, seleccione el nombre del servidor RADIUS en la lista desplegable External Authentication y seleccione **Query Remote Setting**.
  – CLI: Introduzca el comando **set ike gateway** *name_str* **xauth server** *name_str* **query-config**.
- Autenticación sólo sin asignaciones de direcciones, asignaciones de direcciones sólo sin autenticación (**set ike gateway** *name_str* **xauth bypass-auth**), y tanto autenticación como asignaciones de direcciones combinadas

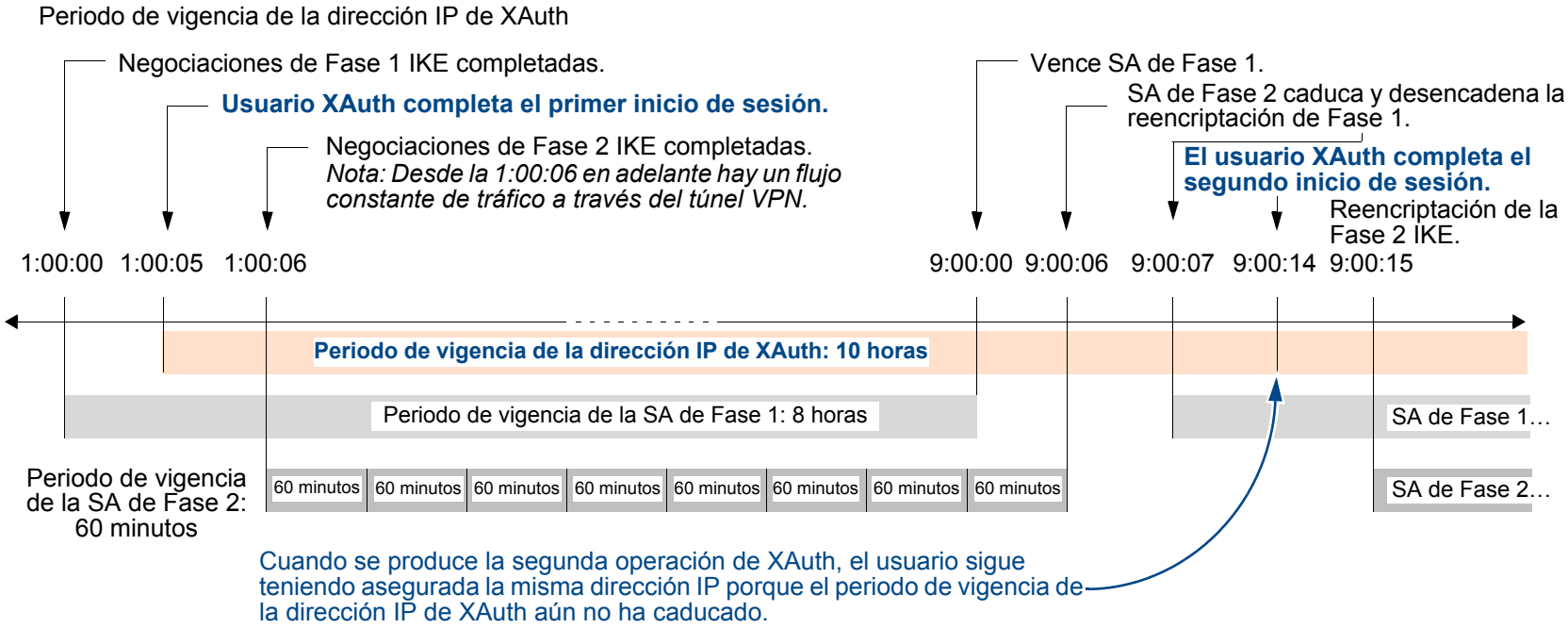
Usuarios XAuth en negociaciones IKE

NetScreen es compatible con XAuth, versión 6 (v6). Para confirmar que ambos interlocutores participantes en las negociaciones de la Fase 1 de IKE admiten XAuth v6, intercambian entre sí la siguiente identificación de fabricante en los dos primeros mensajes de dicha fase: 0x09002689DFD6B712. Este número de identificación del fabricante está especificado en el borrador de XAuth Internet, “draft-beaulieu-ike-xauth-02.txt”.

Finalizadas las negociaciones de la Fase 1, el dispositivo NetScreen envía un mensaje de petición de inicio de sesión al usuario XAuth que se encuentra en el sitio remoto. Si el usuario XAuth inicia una sesión con éxito indicando la combinación correcta de nombre de usuario y contraseña, el dispositivo NetScreen asigna al usuario una dirección IP propia, una máscara de red de 32 bits, las direcciones de los servidores DNS y de los servidores WINS, y ambos interlocutores continúan con las negociaciones de la Fase 2.

El usuario XAuth tiene 60 segundos para completar el proceso de inicio de sesión. Si el primer intento de inicio de sesión falla, el usuario XAuth puede hacer hasta cuatro intentos más, disponiendo de 60 segundos para cada uno. Si el usuario falla al cabo de cinco intentos consecutivos, el dispositivo NetScreen deja de generar la petición de inicio de sesión y anula la sesión.

Como mínimo, la dirección IP asignada por XAuth a un usuario sigue perteneciendo a éste durante el tiempo especificado como periodo de vigencia de la dirección XAuth (“XAuth address lifetime”). La dirección IP puede pertenecer más tiempo al usuario XAuth, dependiendo de cuándo se vuelvan a introducir las asociaciones de seguridad (SAs) de Fase 1 y Fase 2. El ejemplo siguiente ilustra la relación entre las operaciones de reencriptación de Fase 1 y Fase 2 y el periodo de vigencia de la dirección IP de XAuth.



1. La SA de Fase 1 se establece con un periodo de vigencia de ocho horas y caduca después de las primeras 8 horas.
2. El periodo de vigencia de la SA de Fase 2 se establece en 60 minutos. Debido al retardo de 5 segundos que se produce durante las negociaciones iniciales de IKE mientras el usuario XAuth introduce su nombre de usuario y contraseña, la octava SA de Fase 2 caduca 8 horas y 6 segundos después de finalizar las negociaciones de la Fase 1 (5 segundos para el inicio de sesión de XAuth + 1 segundo para las negociaciones de la Fase 2).

3. Dado que hay tráfico VPN activo, al caducar la octava SA de la Fase 2 se provoca la reencriptación de la SA de Fase 1, caducada 6 segundos antes; es decir, se producen las negociaciones (o “renegociaciones”) de la Fase 1 de IKE.
4. Una vez completadas las renegociaciones de la Fase 1 de IKE, el dispositivo NetScreen solicita al usuario XAuth que vuelva a iniciar una sesión.

   Nota: *Para evitar la repetición de inicios de sesión después del inicial, configure el túnel VPN con cualquier tiempo de inactividad distinto de 0 utilizando el comando CLI:* ***set vpn*** *name* ***gateway*** *name* ***idletime*** *number (en minutos). Si hay actividad de VPN al completarse las renegociaciones de la Fase 1 de IKE, el dispositivo NetScreen no pide al usuario XAuth que vuelva a iniciar una sesión. Esta opción permite al usuario descargar archivos de gran tamaño, enviar o recibir secuencias multimedia (“streams”), así como participar en conferencias Web sin interrupciones.*

5. Debido a que el periodo de vigencia de la dirección XAuth (10 horas) es superior al de la SA de Fase 1, el usuario conserva la misma dirección IP, aunque después de la siguiente reencriptación de Fase 1 puede que se le asigne una dirección diferente.

   Si el periodo de vigencia de la dirección XAuth fuese inferior al de la SA de Fase 1, el dispositivo NetScreen asignaría al usuario otra dirección IP, que podría ser igual o diferente a la dirección[4] previamente asignada.

   Nota: *Para cambiar el periodo de vigencia de la dirección, ejecute cualquiera de los siguientes procedimientos:*

   - *(WebUI) VPNs > AutoKey Advanced > XAuth Settings: Introduzca un número (en minutos) en el campo Reserve Private IP for XAuth User y haga clic en* ***Apply****.*
   - *(CLI) set xauth lifetime* number

   Para desactivar la característica de periodo de vigencia de la dirección, introduzca el valor 1, que es el valor mínimo permitido.

4. Si es crucial que siempre se asigne la misma dirección IP a un usuario, puede especificarla en la configuración del usuario. El dispositivo NetScreen le asignará entonces esa dirección en lugar de tomar otra al azar del conjunto de direcciones IP disponibles. Tenga en cuenta que la dirección elegida no debe pertenecer al conjunto de direcciones IP (“IP pool”), ya que el sistema podría asignarla a otro usuario, por lo que no estaría disponible cuando se necesitase.

Ejemplo: Autenticación XAuth (usuario local)

En este ejemplo definirá un usuario XAuth llamado “x1” con la contraseña “aGgb80L0ws” en la base de datos local.

Después establecerá una referencia en una configuración de puerta de enlace IKE remota desde este usuario hacia un interlocutor en la IP 2.2.2.2. Asignará el nombre “gw1” a la puerta de enlace remota, especificará el modo principal y la propuesta pre-g2-3des-sha para las negociaciones de Fase 1 y utilizará la clave previamente compartida “netscreen1”. Asignará el nombre “vpn1” al túnel VPN y especificará el conjunto de propuestas “Compatible” para las negociaciones de Fase 2. Elegirá la interfaz “ethernet3” de la zona Untrust como interfaz de salida.

WebUI

1. Usuario XAuth

   Objects > Users > Local > New: Introduzca los siguientes datos y haga clic en **OK**:

   User Name: x1

   Status: Enable

   XAuth User: (seleccione)

   User Password: iDa84rNk

   Confirm Password: iDa84rNk

2. VPN

   VPNs > AutoKey Advanced > Gateway > New: Introduzca los siguientes datos y haga clic en **OK**:

   Gateway Name: gw1

   Security Level: Custom

   Remote Gateway Type:

   Static IP Address: (seleccione), Address/Hostname: 2.2.2.2

   Preshared Key: netscreen1

   Outgoing Interface: ethernet3

> Advanced: Introduzca los siguientes ajustes avanzados y haga clic en **Return** para regresar a la página de configuración básica de Gateway:

Security Level: Custom: (seleccione)

Phase 1 Proposal: pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

XAuth Server: (seleccione)

Local Authentication: (seleccione)

User: (seleccione), x1

VPNs > AutoKey IKE > New: Introduzca los siguientes datos y haga clic en **OK**:

VPN Name: vpn1

Security Level: Compatible

Remote Gateway Tunnel: gw1

CLI

1. Usuario XAuth

```
set user x1 password aGgb80L0ws
set user x1 type xauth
unset user x1 type auth[5]
```

2. VPN

```
set ike gate gw1 ip 2.2.2.2 main outgoing-interface ethernet3 preshare
    netscreen1 proposal pre-g2-3des-sha
set ike gateway gw1 xauth server Local user x1
set vpn vpn1 gateway gw1 sec-level compatible
save
```

5. El comando CLI **set user** *name_str* **password** *pswd_str* crea un usuario de autenticación. Para crear un usuario de sólo XAuth, debe definirlo como usuario XAuth (**set user** *name_str* **type xauth**) y eliminar la definición de usuario de autenticación (**unset user** *name_str* **type auth**).

Ejemplo: Autenticación de XAuth (grupo de usuarios local)

En este ejemplo creará un grupo de usuarios llamado “xa-grp1” en la base de datos local y le agregará el usuario XAuth “x1” creado en el ejemplo anterior, “Ejemplo: Autenticación XAuth (usuario local)” en la página 87. Cuando agregue dicho usuario al grupo, éste se convertirá automáticamente en grupo de usuarios XAuth.

Después establecerá una referencia en una configuración de puerta de enlace IKE remota desde este grupo hacia un interlocutor en la IP 2.2.2.2. Asignará el nombre “gw2” a la puerta de enlace remota, especificará el modo principal y la propuesta pre-g2-3des-sha para las negociaciones de Fase 1 y utilizará la clave previamente compartida “netscreen2”. Asignará el nombre “vpn2” al túnel VPN y especificará el conjunto de propuestas “Compatible” para las negociaciones de Fase 2. Elegirá la interfaz “ethernet3” de la zona Untrust como interfaz de salida.

WebUI

1. Grupo de usuarios XAuth

Objects > Users > Local Groups > New: Escriba **xa-grp1** en el campo Group Name, haga lo siguiente, y luego haga clic en **OK**:

Seleccione **x1** y utilice el botón **<<** para trasladarlo de la columna “Available Members” a la columna “Group Members”.

2. VPN

VPNs > AutoKey Advanced > Gateway > New: Introduzca los siguientes datos y haga clic en **OK**:

Gateway Name: gw2

Security Level: Custom

Remote Gateway Type:

Static IP Address: (seleccione), Address/Hostname: 2.2.2.2

Preshared Key: netscreen2

Outgoing Interface: ethernet3

> Advanced: Introduzca los siguientes ajustes avanzados y haga clic en **Return** para regresar a la página de configuración básica de Gateway:

Phase 1 Proposal: pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

XAuth Server: (seleccione)

Local Authentication: (seleccione)

User Group: (seleccione), xa-grp1

VPNs > AutoKey IKE > New: Introduzca los siguientes datos y haga clic en **OK**:

VPN Name: vpn2

Security Level: Compatible

Remote Gateway Tunnel:

Predefined: (seleccione), gw2

CLI

1. Grupo de usuarios XAuth

```
set user-group xa-grp1 location local
set user-group xa-grp1 user x1
```

2. VPN

```
set ike gate gw2 ip 2.2.2.2 main outgoing-interface ethernet3 preshare
    netscreen2 proposal pre-g2-3des-sha
set ike gateway gw2 xauth server Local user-group xa-grp1
set vpn vpn2 gateway gw2 sec-level compatible
save
```

Ejemplo: Autenticación XAuth (usuario externo)

A este ejemplo establecerá una referencia a un usuario XAuth llamado “xa-1” con la contraseña “iNWw10bd01” que habrá cargado previamente en un servidor de autenticación SecurID externo. Este ejemplo utiliza casi la misma configuración de servidor de autenticación SecurID que el definido en el “Ejemplo: Servidor de autenticación SecurID” en la página 37, salvo que en este caso el tipo de cuenta se definirá como XAuth.

Establecerá una referencia al usuario XAuth “xa-1” en una configuración de puerta de enlace IKE remota hacia un interlocutor con la dirección IP 2.2.2.2. Asignará el nombre “gw3” a la puerta de enlace remota, especificará el modo principal y la propuesta pre-g2-3des-sha para las negociaciones de Fase 1 y utilizará la clave previamente compartida “netscreen3”. Asignará al túnel VPN el nombre “vpn3” y especificará la propuesta g2-esp-3des-sha para las negociaciones de la Fase 2. Elegirá la interfaz “ethernet3” de la zona Untrust como interfaz de salida.

WebUI

1. Servidor de autenticación SecurID externo

Configuration > Auth > Servers > New: Introduzca los siguientes datos y haga clic en **OK**:

Name: securid1

IP/Domain Name: 10.20.2.100

Backup1: 10.20.2.110

Timeout: 60

Account Type: XAuth

SecurID: (seleccione)

Client Retries: 3

Client Timeout: 10 segundos

Authentication Port: 15000

Encryption Type: DES

User Duress: No

2. Usuario XAuth

Defina el usuario de autenticación “xa-1” con la contraseña “iNWw10bd01” en el servidor de autenticación SecurID externo “securid1”.

3. VPN

VPNs > AutoKey Advanced > Gateway > New: Introduzca los siguientes datos y haga clic en **OK**:

Gateway Name: gw3

Security Level: Custom

Remote Gateway Type:

Static IP Address: (seleccione), Address/Hostname: 2.2.2.2

Preshared Key: netscreen3

Outgoing Interface: ethernet3

> Advanced: Introduzca los siguientes ajustes avanzados y haga clic en **Return** para regresar a la página de configuración básica de Gateway:

Phase 1 Proposal: pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

XAuth Server: (seleccione)

External Authentication: (seleccione), securid1

User: (seleccione)

Name: xa-1

VPNs > AutoKey IKE > New: Introduzca los siguientes datos y haga clic en **OK**:

VPN Name: vpn3

Security Level: Compatible

Remote Gateway Tunnel:

Predefined: (seleccione), gw3

CLI

1. Servidor de autenticación SecurID externo

```
set auth-server securid1 type securid
set auth-server securid1 server-name 10.20.2.100
set auth-server securid1 backup1 10.20.2.110
set auth-server securid1 timeout 60
set auth-server securid1 account-type xauth
set auth-server securid1 securid retries 3
set auth-server securid1 securid timeout 10
set auth-server securid1 securid auth-port 15000
set auth-server securid1 securid encr 1
set auth-server securid1 securid duress 0
```

2. Usuario XAuth

Defina el usuario de autenticación “xa-1” con la contraseña “iNWw10bd01” en el servidor de autenticación SecurID externo “securid1”.

3. VPN

```
set ike gate gw3 ip 2.2.2.2 main outgoing-interface ethernet3 preshare
    netscreen3 proposal pre-g2-3des-sha
set ike gateway gw3 xauth server securid1 user xa-1
set vpn vpn3 gateway gw3 sec-level compatible
save
```

Ejemplo: Autenticación XAuth (grupo de usuarios externo)

En este ejemplo configurará un servidor de autenticación RADIUS externo llamado “radius1”[6] y definirá un grupo de usuarios de autenticación externo llamado “xa-grp2”. Definirá un grupo de usuarios XAuth externo “xa-grp2” en dos sitios:

1. Servidor de autenticación RADIUS externo “radius1”
2. Dispositivo NetScreen

Alimentará el grupo de usuarios XAuth llamado “xa-grp2” solamente con los usuarios XAuth del servidor RADIUS, dejando el grupo vacío en el dispositivo NetScreen. Los miembros de este grupo son distribuidores en una oficina remota que necesitan acceso a los servidores FTP de la LAN corporativa. Agregará una entrada en la libreta de direcciones de la zona Untrust para el sitio remoto con la dirección IP 10.2.2.0/24 y lo llamará “reseller1”. También introducirá una dirección en la libreta de direcciones de la zona Trust para el servidor FTP “rsl-srv1” con la dirección IP 10.1.1.5/32.

Configurará un túnel VPN hacia 2.2.2.2 para autenticar a los usuarios XAuth del grupo de usuarios “xa-grp2”. Asignará el nombre “gw4” a la puerta de enlace remota, especificará el modo principal y la propuesta pre-g2-3des-sha para las negociaciones de Fase 1 y utilizará la clave previamente compartida “netscreen4”. Asignará el nombre “vpn4” al túnel VPN y especificará el conjunto de propuestas “Compatible” para las negociaciones de Fase 2. Elegirá la interfaz “ethernet3” de la zona Untrust como interfaz de salida.

Finalmente, creará una directiva que permita el tráfico FTP desde el usuario “reseller1” de la zona Untrust a través de “vpn4” hacia “rsl-svr1” en la zona Trust.

Servidor RADIUS

1. Cargue el archivo de diccionario de NetScreen en el servidor RADIUS.

   Nota: *Para obtener más información sobre el archivo de diccionario de NetScreen, consulte el “Archivo de diccionario de NetScreen” en la página 26. Para obtener instrucciones sobre cómo cargar el archivo de diccionario en un servidor RADIUS, consulte la documentación del servidor RADIUS.*

2. Introduzca el grupo de usuarios de autenticación “xa-grp2” en el servidor de autenticación externo “radius1” y aliméntelo con cuentas de usuarios XAuth.

6. La configuración del servidor de autenticación de RADIUS es casi idéntica a la descrita en el “Ejemplo: Servidor de autenticación RADIUS” en la página 34, salvo que en este ejemplo solamente se especificar “xauth” como tipo de cuenta de usuario.

WebUI

1. **Servidor de autenticación**

   Configuration > Auth > Servers > New: Introduzca los siguientes datos y haga clic en **OK**:

   Name: radius1
   IP/Domain Name: 10.20.1.100
   Backup1: 10.20.1.110
   Backup2: 10.20.1.120
   Timeout: 30
   Account Type: XAuth
   RADIUS: (seleccione)
   RADIUS Port: 4500
   Shared Secret: A56htYY97kl

2. **Grupo de usuarios externo**

   Objects > Users > External Groups > New: Introduzca los siguientes datos y haga clic en **OK**:

   Group Name: xa-grp2
   Group Type: XAuth

3. **Dirección**

   Objects > Addresses > List > New: Introduzca los siguientes datos y haga clic en **OK**:

   Address Name: reseller1
   IP Address/Domain Name:
   IP/Netmask: (seleccione), 10.2.2.0/24
   Zone: Untrust

Objects > Addresses > List > New: Introduzca los siguientes datos y haga clic en **OK**:

Address Name: rsl-svr1

IP Address/Domain Name:

IP/Netmask: (seleccione), 10.1.1.5/32

Zone: Trust

4. VPN

VPNs > AutoKey Advanced > Gateway > New: Introduzca los siguientes datos y haga clic en **OK**:

Gateway Name: gw4

Security Level: Custom

Remote Gateway Type:

Static IP Address: (seleccione), Address/Hostname: 2.2.2.2

Preshared Key: netscreen4

Outgoing Interface: ethernet3

> Advanced: Introduzca los siguientes ajustes avanzados y haga clic en **Return** para regresar a la página de configuración básica de Gateway:

Phase 1 Proposal: pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

XAuth Server: (seleccione)

External Authentication: (seleccione), securid1

User Group: (seleccione)

Name: xa-grp2

VPNs > AutoKey IKE > New: Introduzca los siguientes datos y haga clic en **OK**:

VPN Name: vpn4

Security Level: Compatible

Remote Gateway:

Predefined: (seleccione), gw4

5. Directiva

Policies > (From: Untrust, To: Trust) New: Introduzca los siguientes datos y haga clic en **OK**:

Source Address:

Address Book Entry: (seleccione), reseller1

Destination Address:

Address Book Entry: (seleccione), rsl-svr1

Service: FTP-Get

Action: Tunnel

Tunnel VPN: vpn4

Modify matching bidirectional VPN policy: (anule la selección)

Position at Top: (seleccione)

CLI

1. Servidor de autenticación

```
set auth-server radius1 type radius
set auth-server radius1 account-type xauth
set auth-server radius1 server-name 10.20.1.100
set auth-server radius1 backup1 10.20.1.110
set auth-server radius1 backup2 10.20.1.120
set auth-server radius1 timeout 30
set auth-server radius1 radius port 4500
set auth-server radius1 radius secret A56htYY97kl
```

2. Grupo de usuarios externo

```
set user-group xa-grp2 location external
set user-group xa-grp2 type xauth
```

3. Dirección

```
set address untrust reseller1 10.2.2.0/24
set address trust rsl-svr1 10.1.1.5/32
```

4. VPN

```
set ike gate gw4 ip 2.2.2.2 main outgoing-interface ethernet3 preshare
    netscreen4 proposal pre-g2-3des-sha
set ike gateway gw4 xauth server radius1 user-group xa-grp2
set vpn vpn4 gateway gw4 sec-level compatible
```

5. Directiva

```
set policy top from untrust to trust reseller1 rsl-svr1 ftp-get tunnel vpn vpn4
save
```

Ejemplo: Autenticación y asignación de direcciones XAuth (grupo de usuarios local)

En este ejemplo configurará tanto la autenticación como las asignaciones de las direcciones IP propia, de los servidores DNS y de los servidores WINS para un grupo de usuarios IKE/XAuth almacenado en la base de datos local[7]. Cuando un usuario IKE/XAuth establece una conexión VPN de acceso telefónico al dispositivo NetScreen, éste autentica al usuario IKE (es decir, al dispositivo cliente) que utilice una identificación IKE y un certificado RSA durante las negociaciones de la Fase 1. A continuación, el dispositivo NetScreen autentica al usuario XAuth (es decir, a la persona que esté utilizando el dispositivo) utilizando un nombre de usuario y una contraseña y le asigna las direcciones IP propia, de los servidores DNS y de los servidores WINS entre las negociaciones de la Fase 1 y de la Fase 2.

Creará un grupo de usuarios local “ixa-grp1”. Luego definirá dos usuarios IKE/XAuth llamados “ixa-u1” (contraseña: “ccF1m84s”) e “ixa-u2” (contraseña: “C113g1tw”) y los agregará al grupo, definiendo de este modo el tipo de grupo como IKE/XAuth. (La inclusión de otros usuarios IKE/XAuth en el grupo no se incluye en este ejemplo).

Creará un conjunto de direcciones IP dinámicas (DIP) llamado “xa-pool1” con el rango de direcciones 10.2.2.1 a 10.2.2.100. Éste será el conjunto de direcciones de las que el dispositivo NetScreen tomará una dirección IP para asignarla a cada usuario XAuth.

Nota: *Para evitar problemas de enrutamiento y duplicaciones en la asignación de direcciones, el conjunto DIP debe encontrarse en un espacio de direcciones distinto del de la zona a la que el usuario XAuth dirige el tráfico.*

7. También puede utilizar un servidor de autenticación RADIUS externo para la autenticación de usuarios XAuth y la asignación de direcciones. Puede utilizar un servidor de autenticación SecurID o LDAP externo sólo para la autenticación XAuth (no para la asignación de direcciones). Para la autenticación de usuarios IKE solamente se puede utilizar la base de datos local.

Configurará los siguientes ajustes predeterminados de XAuth:

- Establezca el tiempo de espera de la dirección XAUTH en 480 minutos.
- Seleccione la base de datos local como servidor de autenticación predeterminado.
- Habilite el protocolo de autenticación de establecimiento de conexión por desafío (“Challenge Handshake Authentication Protocol” o CHAP), en el cual el dispositivo NetScreen envía un desafío (clave de encriptación) al cliente remoto, que utiliza la clave para encriptar su nombre de inicio de sesión y contraseña.
- Seleccione “xa-pool1” como conjunto de DIP predeterminado.
- Defina las direcciones IP de los servidores DNS principal y secundario como 10.1.1.150 y 10.1.1.151, respectivamente.
- Defina las direcciones IP de los servidores WINS principal y secundario como 10.1.1.160 y 10.1.1.161, respectivamente.

Configurará una puerta de enlace IKE llamada “ixa-gw1”, haciendo referencia al grupo de usuarios “ixa-grp1” y utilizando los ajustes predeterminados del servidor de autenticación XAuth. Luego configurará un túnel VPN con el nombre “ixa-tun1” y una directiva que permita el tráfico desde “ixa-grp1” a la zona Trust (dirección IP 10.1.1.0/24) a través del túnel VPN “ixa-tun1”.

WebUI

1. Usuarios y grupo de usuarios IKE/XAuth

Objects > Users > Local > New: Introduzca los siguientes datos y haga clic en **OK**:

User Name: ixa-u1
Status: Enable
IKE User: (seleccione)
Simple Identity: (seleccione)
IKE ID Type: AUTO
IKE Identity: u1@ns.com
XAuth User: (seleccione)
User Password: ccF1m84s
Confirm Password: ccF1m84s

Objects > Users > Local > New: Introduzca los siguientes datos y haga clic en **OK**:

User Name: ixa-u2

Status: Enable

IKE User: (seleccione)

Simple Identity: (seleccione)

IKE ID Type: AUTO

IKE Identity: u2@ns.com

XAuth User: (seleccione)

User Password: C113g1tw

Confirm Password: C113g1tw

Objects > Users > Local Groups > New: Escriba **ixa-grp1** en el campo Group Name, haga lo siguiente, y luego haga clic en **OK**:

Seleccione **ixa-u1** y utilice el botón **<<** para trasladarlo de la columna "Available Members" a la columna "Group Members".

Seleccione **ixa-u2** y utilice el botón **<<** para trasladarlo de la columna "Available Members" a la columna "Group Members".

2. Conjunto de direcciones IP

Objects > IP Pools > New: Introduzca los siguientes datos y haga clic en **OK**:

IP Pool Name: xa-pool1

Start IP: 10.2.2.1

End IP: 10.2.2.100

3. Servidor de autenticación XAuth predeterminado

VPNs > AutoKey Advanced > XAuth Settings: Introduzca los siguientes datos y haga clic en **Apply**:

Reserve Private IP for XAuth User: 480 minutos
Default Authentication Server: Local
Query Client Settings on Default Server: (anule la selección)
CHAP: (seleccione)
IP Pool Name: xa-pool1
DNS Primary Server IP: 10.1.1.150
DNS Secondary Server IP: 10.1.1.151
WINS Primary Server IP: 10.1.1.160
WINS Secondary Server IP: 10.1.1.161

4. Dirección

Objects > Addresses > List > New: Introduzca los siguientes datos y haga clic en **OK**:

Address Name: Trust_Zone
IP Address/Domain Name:
  IP/Netmask: (seleccione), 10.1.1.0/24
Zone: Trust

5. VPN

VPNs > AutoKey Advanced > Gateway > New: Introduzca los siguientes datos y haga clic en **OK**:

Gateway Name: ixa-gw1
Security Level: Custom
Remote Gateway Type:
  Dialup User Group: (seleccione)
    Group: ixa-grp1

> Advanced: Introduzca los siguientes ajustes avanzados y haga clic en **Return** para regresar a la página de configuración básica de Gateway:

Phase 1 Proposal: rsa-g2-3des-sha

Mode (Initiator): Aggressive

Outgoing Interface: ethernet3

XAuth Server: (seleccione)

Use Default: (seleccione)

User Group: (seleccione), ixa-grp1

VPNs > AutoKey IKE > New: Introduzca los siguientes datos y haga clic en **OK**:

VPN Name: ixa-vpn1

Security Level: Compatible

Remote Gateway:

Predefined: (seleccione), ixa-gw1

6. Directiva

Policies > (From: Untrust, To: Trust) New: Introduzca los siguientes datos y haga clic en **OK**:

Source Address:

Address Book Entry: (seleccione), Dial-Up VPN

Destination Address:

Address Book Entry: (seleccione), Trust_Zone

Service: ANY

Action: Tunnel

Tunnel VPN: ixa-vpn1

Modify matching bidirectional VPN policy: (anule la selección)

Position at Top: (seleccione)

CLI

1. Usuarios y grupo de usuarios IKE/XAuth

```
set user-group ixa-grp1 location local
set user ixa-u1 type ike xauth
set user ixa-u1 ike-id u-fqdn u1@ns.com
set user ixa-u1 password ccF1m84s
unset user ixa-u1 type auth
set user ixa-u2 type ike xauth
set user ixa-u2 ike-id u-fqdn u2@ns.com
set user ixa-u2 password C113g1tw
unset user ixa-u2 type auth
```

2. Conjunto de direcciones IP

```
set ippool xa-pool1 10.2.2.1 10.2.2.100
```

3. Servidor de autenticación XAuth predeterminado

```
set xauth lifetime 480
set xauth default auth server Local chap
set xauth default ippool xa-pool1
set xauth default dns1 10.1.1.150
set xauth default dns2 10.1.1.151
set xauth default wins1 10.1.1.160
set xauth default wins2 10.1.1.161
```

4. Dirección

```
set address trust Trust_zone 10.1.1.0/24
```

5. VPN

```
set ike gateway ixa-gw1 dialup ixa-grp1 aggressive outgoing-interface ethernet3
    proposal rsa-g2-3des-sha
set ike gateway ixa-gw1 xauth server Local user-group ixa-grp1
set vpn ixa-vpn1 gateway ixa-gw1 sec-level compatible
```

6. Directiva

```
set policy top from untrust to trust "Dial-Up VPN" Trust_zone any tunnel vpn
    ixa-vpn1
save
```

Cliente XAuth

Un cliente XAuth es un usuario o dispositivo remoto que se conecta a un servidor XAuth a través de un túnel VPN de AutoKey IKE. Un dispositivo NetScreen puede actuar como cliente XAuth, respondiendo a las peticiones de autenticación de un servidor XAuth remoto. Finalizadas las negociaciones de la Fase 1, el servidor XAuth remoto envía un mensaje de petición de inicio de sesión al dispositivo NetScreen. Si el dispositivo NetScreen que actúa como cliente XAuth inicia una sesión con éxito indicando el nombre de usuario y la contraseña correctos, comienzan las negociaciones de la Fase 2.

Para configurar el dispositivo NetScreen como cliente XAuth, debe especificar lo siguiente:

- Nombre de la puerta de enlace IKE
- Nombre de usuario y contraseña XAuth

Puede configurar los siguientes tipos de autenticación XAuth:

- Any: Permite el protocolo de autenticación de establecimiento de conexión por desafío (CHAP) o el protocolo de autenticación mediante contraseña (PAP)
- CHAP: Permite solamente CHAP

Ejemplo: Dispositivo NetScreen como cliente XAuth

En este ejemplo, primero configurará una puerta de enlace IKE remota “*gw1*” con la dirección IP 2.2.2.2. Especificará el nivel de seguridad estándar y utilizará la clave previamente compartida “*netscreen1*”. Luego configurará un cliente XAuth para la puerta de enlace IKE con el nombre de usuario “*beluga9*” y la contraseña “*1234567*”. También requerirá la autenticación CHAP para el cliente.

WebUI

VPN > AutoKey Advanced > Gateway > New: Introduzca los siguientes datos y haga clic en **OK**:

Gateway Name: gw1

Security Level: Standard (seleccione)

Remote Gateway Type:

Static IP Address: (seleccione), Address/Hostname: 2.2.2.2

Preshared Key: netscreen1

Outgoing Interface: Untrust

> Advanced: Introduzca los siguientes ajustes avanzados y haga clic en **Return** para regresar a la página de configuración básica de Gateway:

XAuth Client: (seleccione)

User Name: beluga9

Password: 1234567

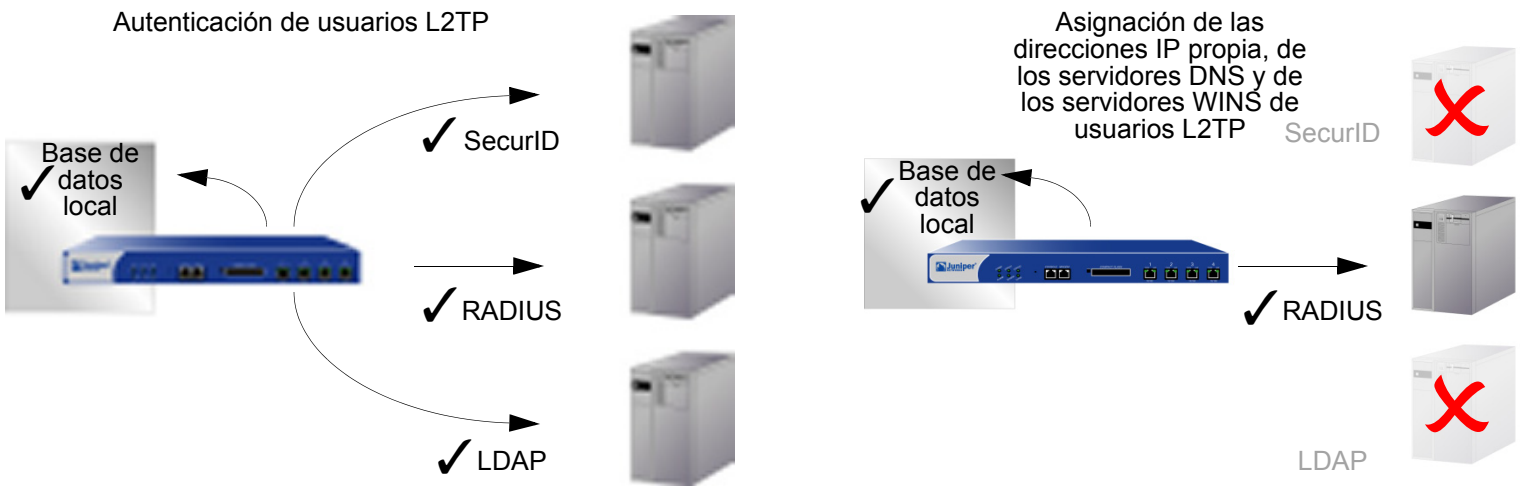
Allowed Authentication Type: (seleccione), CHAP Only

CLI

```
set ike gateway gw1 ip 2.2.2.2 Main outgoing-interface untrust preshare
    netscreen1 sec-level standard
set ike gateway gw1 xauth client chap username beluga1 password 1234567
save
```

USUARIOS Y GRUPOS DE USUARIOS L2TP

El protocolo de túnel de la capa 2 (“Layer 2 Tunneling Protocol” o L2TP) proporciona los medios para autenticar usuarios remotos y asignarles las direcciones IP propia, de los servidores DNS y de los servidores WINS. Puede configurar el dispositivo NetScreen para que utilice la base de datos local o un servidor de autenticación externo para autenticar usuarios L2TP. Para realizar asignaciones de las direcciones IP propia, de los servidores DNS y de los servidores WINS, puede configurar el dispositivo NetScreen de modo que utilice la base de datos local o un servidor RADIUS (cargado con el archivo de diccionario de NetScreen; consulte “Archivo de diccionario de NetScreen” en la página 26).



Puede incluso utilizar una combinación de servidores de autenticación, uno diferente por cada uno de los dos aspectos de L2TP. Por ejemplo, puede utilizar un servidor SecurID para autenticar a un usuario L2TP, pero realizar las asignaciones de direcciones desde la base de datos local. El ejemplo siguiente ilustra la aplicación de dos servidores de autenticación para procesar ambos componentes de L2TP. Para ver otros ejemplos junto con un análisis detallado de L2TP, consulte “L2TP” en la página **5** -307.

Ejemplo: Servidores de autenticación L2TP locales y externos

En este ejemplo configurará un servidor de autenticación SecurID externo para autenticar usuarios L2TP y utilizará la base de datos local para asignar a usuarios L2TP sus direcciones IP propia, de los servidores DNS y de los servidores WINS.

El servidor de autenticación SecurID externo es “securid1”. Es casi idéntico a la configuración de servidor de autenticación descrita en el “Ejemplo: Servidor de autenticación SecurID” en la página 37, salvo que el tipo de cuenta es L2TP. Los parámetros del servidor de autenticación SecurID son los siguientes:

- Name: securid1
- IP Address 10.20.2.100
- Backup1 IP Address: 10.20.2.110
- Port: 15000
- Encryption: DES
- Client Retries: 3
- Client Timeout: 10 segundos
- Idle Timeout: 60 minutes
- Account Type: L2TP

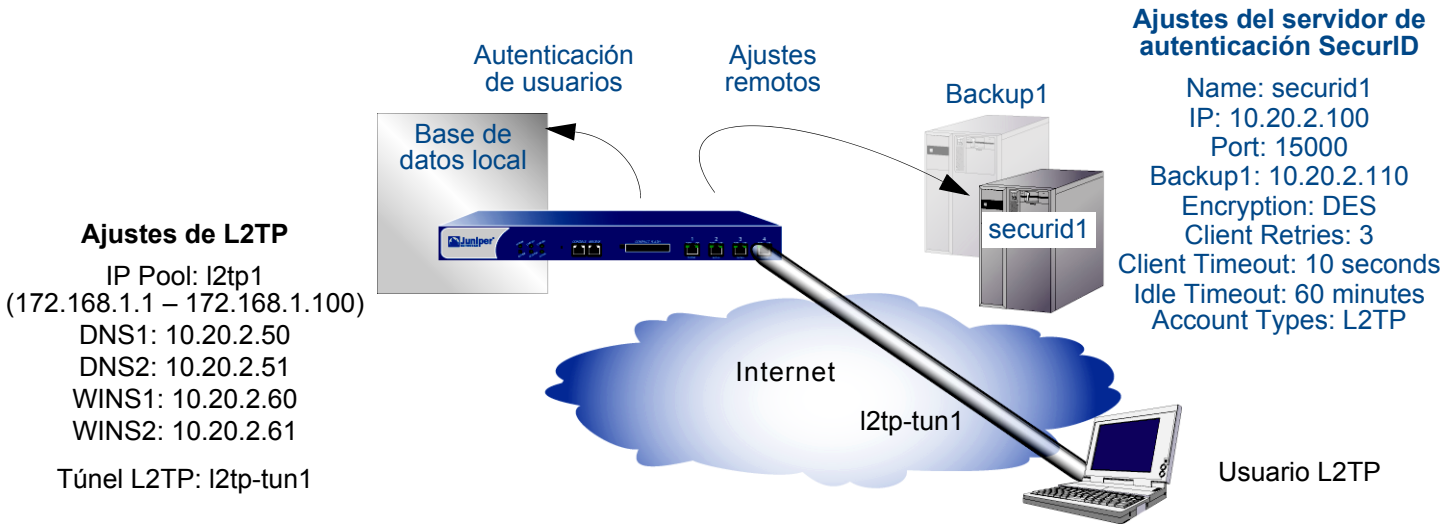
Los ajustes predeterminados de L2TP son los siguientes:

- IP Pool: l2tp1 (172.168.1.1 – 172.168.1.100)
- DNS Primary Server IP: 10.20.2.50
- DNS Secondary Server IP: 10.20.2.51
- PPP Authentication: CHAP
- WINS Primary Server IP: 10.20.2.60
- WINS Primary Server IP: 10.20.2.61

Después de configurar el dispositivo NetScreen con los ajustes descritos, creará un túnel L2TP llamado “l2tp-tun1” que hará referencia a “securid1” para la autenticación y utilizará los ajustes predeterminados para la asignación de direcciones.

También deberá configurar el servidor SecurID según lo mostrado arriba y alimentarlo con los usuarios L2TP.

Nota: *Una configuración con sólo L2TP no es segura. Para agregar seguridad a un túnel L2TP, se recomienda combinarlo con un túnel IPSec, que debe estar en modo de transporte, según se describe en el “Ejemplo: Configuración de L2TP sobre IPSec” en la página* ***5*** *-326.*



WebUI

1. Servidor de autenticación

Configuration > Auth > Servers > New: Introduzca los siguientes datos y haga clic en **OK**:

Name: securid1
IP/Domain Name: 10.20.2.100
Backup1: 10.20.2.110
Timeout: 60
Account Type: L2TP
SecurID: (seleccione)
  Client Retries: 3
  Client Timeout: 10 segundos
  Authentication Port: 15000
  Encryption Type: DES
  Use Duress: No

2. Conjunto de direcciones IP

Objects > IP Pools > New: Introduzca los siguientes datos y haga clic en **OK**:

IP Pool Name: l2tp1

Start IP: 172.168.1.1

End IP: 172.168.1.100

3. Ajustes predeterminados de L2TP

VPNs > L2TP > Default Settings: Introduzca los siguientes datos y haga clic en **Apply**:

Default Authentication Server: Local

IP Pool Name: l2tp1

PPP Authentication: CHAP

DNS Primary Server IP: 10.20.2.50

DNS Secondary Server IP: 10.20.2.51

WINS Primary Server IP: 10.20.2.60

WINS Secondary Server IP: 10.20.2.61

4. Túnel L2TP

VPNs > L2TP > Tunnel > New: Introduzca los siguientes datos y haga clic en **OK**:

Name: l2tp-tun1

Use Custom Settings: (seleccione)

Authentication Server: securid1

Query Remote Settings: (anule la selección)

Dialup User: (seleccione), Allow Any

CLI

1. Servidor de autenticación

```
set auth-server securid1 type securid
set auth-server securid1 server-name 10.20.2.100
set auth-server securid1 backup1 10.20.2.110
set auth-server securid1 timeout 60
set auth-server securid1 account-type l2tp
set auth-server securid1 securid retries 3
set auth-server securid1 securid timeout 10
set auth-server securid1 securid auth-port 15000
set auth-server securid1 securid encr 1
set auth-server securid1 securid duress 0
```

2. Conjunto de direcciones IP

```
set ippool l2tp1 172.168.1.1 172.168.1.100
```

3. Ajustes predeterminados de L2TP

```
set l2tp default auth server Local
set l2tp default ippool l2tp1
set l2tp default ppp-auth chap
set l2tp dns1 10.20.2.50
set l2tp dns1 10.20.2.51
set l2tp wins1 10.20.2.60
set l2tp wins2 10.20.2.61
```

4. Túnel L2TP

```
set l2tp l2tp-tun1
set l2tp l2tp-tun1 auth server securid1
save
```

Índice

T

U

V

W

X