

PIX, TACACS+, y configuraciones de ejemplo de RADIUS: 4.4.x

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Autenticación vs. Autorización](#)

[Qué ve el usuario con la autenticación/autorización activada](#)

[Configuración del servidor de seguridad utilizado para todos los escenarios](#)

[Configuración de servidor CiscoSecure UNIX TACACS](#)

[Configuración de servidor de RADIUS UNIX CiscoSecure](#)

[CiscoSecure NT 2.x RADIUS](#)

[EasyACS TACACS+](#)

[CiscoSecure 2.x TACACS+](#)

['Configuración del servidor Livingston RADIUS'](#)

[Configuración del servidor Merit RADIUS](#)

[Configuración del servidor freeware TACACS+](#)

[Pasos de depuración](#)

[Diagrama de la red](#)

[Ejemplos de PIX del comando authentication debug](#)

[Agregado de autorización](#)

[Ejemplos de Depuración de Autenticación y Autorización de PIX](#)

[Incorporación de contabilidad](#)

[TACACS+](#)

[RADIUS](#)

[Utilización del comando Except](#)

[Establecer el número máximo de sesiones y ver a los usuarios conectados](#)

[Autenticación y activación en el PIX mismo](#)

[Autenticación en la consola serie](#)

[Modificación de la línea de comando que ven los usuarios](#)

[Personalizar el mensaje que ven los usuarios en Éxito/Fracaso](#)

[Tiempos de Espera Absolutos e Inactivos por Usuario](#)

[HTTP virtual](#)

[Virtual telnet](#)

[Desconexión de Virtual Telnet](#)

['Autorización del puerto](#)

[Información Relacionada](#)

Introducción

El RADIUS y autenticación de TACACS+ se puede hacer para el FTP, Telnet, y las conexiones HTTP. La autenticación para otros menos protocolos comunes TCP se puede hacer generalmente para trabajar.

Autorización TACACS+ se soporta; La autorización de RADIUS no. Los cambios en el Authentication, Authorization, and Accounting (AAA) PIX 4.4.1 sobre la versión anterior incluyen: Los Grupos de servidores AAA y la Conmutación por falla, autenticación para el acceso del permiso y de la consola en serie, y validan y rechazan los prompts de petición.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las [Convenciones de Consejos Técnicos de Cisco](#).

Autenticación vs. Autorización

- La autenticación es quién es el usuario.
- La autorización es lo que puede hacer el usuario.
- La autenticación es válida sin autorización.
- La autorización no es válida sin autenticación.

Suponga usted tiene 100 usuarios interiores y usted querer quisiera solamente que 6 de estos usuarios pudieran hacer el FTP, Telnet, o el HTTP fuera de la red. Usted diría el PIX autenticar el tráfico saliente y dar los 6 ID de los usuarios en el servidor de seguridad TACACS+/RADIUS. Con la autenticación simple, estos 6 usuarios podrían ser autenticados con el nombre de usuario y contraseña, después salen. Los otros 94 usuarios no podrían salir. El PIX indica a los usuarios para el nombre de usuario/la contraseña, después pasa su nombre de usuario y contraseña al servidor de seguridad TACACS+/RADIUS, y dependiendo de la respuesta, abre o niega la conexión. Estos 6 usuarios podrían hacer el FTP, Telnet, o el HTTP.

Pero suponga a uno de estos tres usuarios, "Terry," no es ser confiado en. Usted quisiera permitir que Terry hagan el FTP, pero no el HTTP o Telnet al exterior. Esto significa tener que agregar la autorización, es decir, autorizando lo que pueden hacer los usuarios además de autenticar quién son. Cuando agregamos la autorización al PIX, el PIX primero enviaría el nombre de usuario y contraseña de Terry al servidor de seguridad, después envía un pedido de autorización que dice al servidor de seguridad lo que está intentando el "comando" Terry hacer. Con la configuración de

servidor correctamente, Terry se podía permitir a "FTP 1.2.3.4" pero negó la capacidad al HTTP o a Telnet dondequiera.

Qué ve el usuario con la autenticación/autorización activada

Cuando intenta ir desde adentro hacia afuera (o viceversa) con autenticación/autorización activada:

- **Telnet** - El usuario ve una pantalla de prompt de nombre de usuario, seguida por una petición para la contraseña. Si la autenticación (y autorización) resulta exitosa en el PIX/servidor, el siguiente host de destino le pide al usuario el nombre de usuario y contraseña.
- **FTP** - El usuario ve un prompt de nombre de usuario subir. El usuario debe ingresar "nombredeusuario_local@nombredeusuario_remoto" para el nombre de usuario y "contraseña_local@contraseña_remota" para la contraseña. El PIX envía el "nombredeusuario_local" y "contraseña_local" al servidor de seguridad local y si la autenticación (y autorización) resulta exitosa en el PIX/servidor, el "nombredeusuario_remoto" y "contraseña_remota" se envían al servidor FTP de destino posterior.
- **HTTP** - Una ventana se visualiza en el nombre de usuario del buscador requerido y la contraseña. Si la autenticación (y la autorización) se realiza con éxito, el usuario accederá al sitio Web siguiente. Tenga presente que los **navegadores ocultan los nombres de usuario y contraseña**. Si aparentemente el PIX debería interrumpir una conexión HTTP pero no lo hace, es posible que se esté realizando una reautenticación en la que el explorador "lanza" el nombre de usuario y la contraseña en memoria caché hacia el PIX, que luego reenvía estos datos al servidor de autenticación. La depuración del servidor y/o registro del sistema de PIX mostrará este fenómeno. Si Telnet y FTP parecen funcionar "con normalidad", pero las conexiones HTTP no, éste es el motivo.

Configuración del servidor de seguridad utilizado para todos los escenarios

Configuración de servidor CiscoSecure UNIX TACACS

Asegúrese que usted tiene la dirección IP o nombre y clave de dominio completamente calificar PIX en el archivo CSU.cfg.

```
user = ddunlap {  
password = clear "rtp"  
default service = permit  
}
```

```
user = can_only_do_telnet {  
password = clear "telnetonly"  
service = shell {  
cmd = telnet {  
permit .*  
}  
}  
}
```

```
user = can_only_do_ftp {  
password = clear "ftponly"
```

```

service = shell {
cmd = ftp {
permit .*
}
}
}

user = httponly {
password = clear "httponly"
service = shell {
cmd = http {
permit .*
}
}
}

```

[Configuración de servidor de RADIUS UNIX CiscoSecure](#)

Utilice la interfaz del usuario gráfica avanzada (GUI) para agregar el IP PIX y la clave a la lista del servidor de acceso a la red (NAS).

```

user=adminuser {
radius=Cisco {
check_items= {
2="all"
}
reply_attributes= {
6=6
}
}
}

```

[CiscoSecure NT 2.x RADIUS](#)

Complete estos pasos.

1. Obtenga una contraseña en la sección de la GUI de configuración de usuario.
2. De la sección GUI de la configuración de grupo, fije el atributo 6 (tipo de servicio) para iniciar sesión o administrativo.
3. Agregue el IP PIX en la Configuración de NAS GUI.

[EasyACS TACACS+](#)

La documentación de EasyACS describe la configuración.

1. En la sección de grupo, haga clic en el **ejecutivo del shell** (dar los privilegios exec).
2. A para agregar la autorización al PIX, haga clic los **comandos deny unmatched ios** en la parte inferior de la configuración de grupo.
3. Seleccione el **comando add/edit new** para cada comando que usted quiere permitir (por ejemplo, Telnet).
4. Si usted quiere permitir el telnet a los sitios específicos, ingrese el IP en la sección de argumento en la forma "permiso #.#.#.#". Para permitir Telnet a todos los sitios, el tecleo **permite todos los argumentos no enumerados**.
5. **Comando editing** del clic en Finalizar.
6. Realice los pasos 1 a 5 para cada uno de los comandos permitidos (por ejemplo, Telnet, HTTP y/o FTP).

7. Agregue el IP PIX en la sección GUI de la Configuración de NAS.

CiscoSecure 2.x TACACS+

El usuario obtiene una contraseña en la sección de configuración de usuario del GUI.

1. En la sección de grupo, **ejecutivo del shell del teclado** (dar los privilegios exec).
2. Para agregar la autorización al PIX, **comandos deny unmatched ios del teclado** en la parte inferior de la configuración de grupo.
3. Selecto **agregue/edite** para cada comando que usted quiere permitir (por ejemplo, Telnet).
4. Si usted quiere permitir el telnet a los sitios específicos, ingrese el IP del permiso en el rectángulo de argumento (por ejemplo, el "permiso el 1.2.3.4"). Para permitir Telnet a todos los sitios, el teclado **permite todos los argumentos no enumerados**.
5. **Comando editing del clic** en Finalizar.
6. Realice los pasos 1 a 5 para cada uno de los comandos permitidos (por ejemplo, Telnet, HTTP o FTP).
7. Agregue el IP PIX en la sección GUI de la Configuración de NAS.

'Configuración del servidor Livingston RADIUS'

Agregue el IP PIX y la clave a los clientes clasifian.

```
adminuser Password="all"  
User-Service-Type = Shell-User
```

Configuración del servidor Merit RADIUS

Agregue el IP PIX y la clave a los clientes clasifian.

```
adminuser Password="all"  
Service-Type = Shell-User
```

Configuración del servidor freeware TACACS+

```
key = "cisco"
```

```
user = adminuser {  
login = cleartext "all"  
default service = permit  
}
```

```
user = can_only_do_telnet {  
login = cleartext "telnetonly"  
cmd = telnet {  
permit .*  
}  
}
```

```
user = httponly {  
login = cleartext "httponly"  
cmd = http {  
permit .*  
}  
}
```

```
user = can_only_do_ftp {
```

```
login = cleartext "ftponly"  
cmd = ftp {  
  permit .*  
}  
}
```

Pasos de depuración

- Asegúrese que las configuraciones PIX están trabajando antes de agregar el Authentication, Authorization, and Accounting (AAA). Si no puede pasar tráfico antes de iniciar la autenticación y autorización, no podrá realizarlo luego.
- Permiso que abre una sesión el PIX: **El comando logging console debugging** no debe ser utilizado en pesadamente un sistema cargado. Puede usarse el comando logging buffered debugging (depuración guardada en la memoria intermedia del registro). La salida de los **comandos show logging o logging** puede ser enviada a un servidor de Syslog y ser examinada.
- Asegúrese que el hacer el debug de está prendido para el TACACS+ o los servidores de RADIUS. Todos los servidores tienen esta opción.

Diagrama de la red

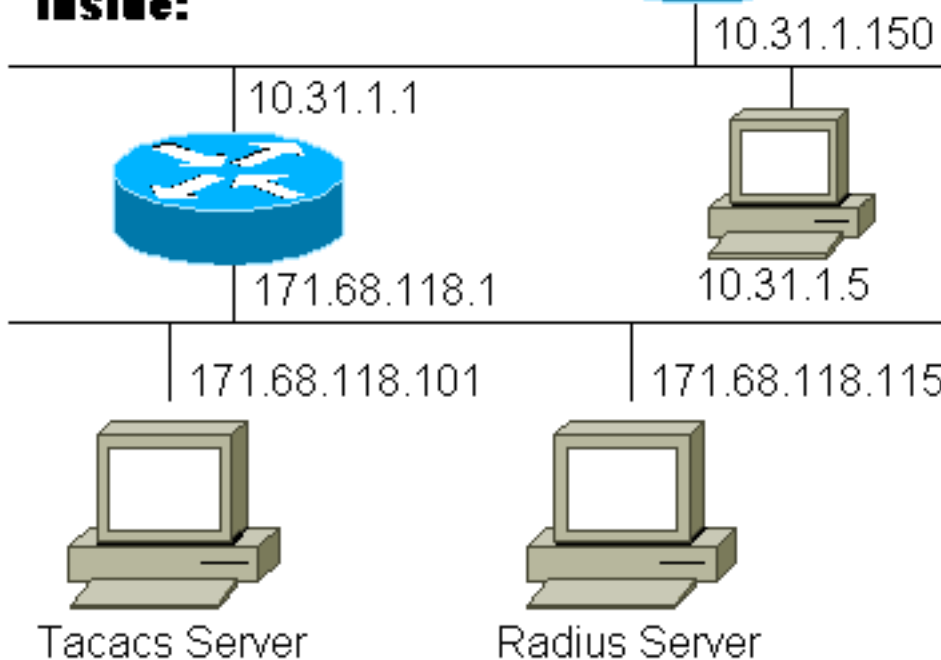
Outside:



11.11.11.15



Inside:



Configuración de PIX

```
pix-5# write terminal Building configuration... : Saved
: PIX Version 4.4(1) nameif ethernet0 outside security0
nameif ethernet1 inside security100 nameif ethernet2
pix/intf2 security10 nameif ethernet3 pix/intf3
security15 enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted hostname pix-5 fixup
protocol ftp 21 fixup protocol http 80 fixup protocol
smtp 25 fixup protocol h323 1720 fixup protocol rsh 514
fixup protocol sqlnet 1521 names pager lines 24 no
logging timestamp logging console debugging no logging
monitor no logging buffered logging trap debugging
logging facility 20 interface ethernet0 auto interface
ethernet1 auto interface ethernet2 auto interface
ethernet3 auto mtu outside 1500 mtu inside 1500 mtu
pix/intf2 1500 mtu pix/intf3 1500 ip address outside
11.11.11.1 255.255.255.0 ip address inside 10.31.1.150
255.255.255.0 ip address pix/intf2 127.0.0.1
```

```

255.255.255.255 ip address pix/intf3 127.0.0.1
255.255.255.255 no failover failover timeout 0:00:00
failover ip address outside 0.0.0.0 failover ip address
inside 0.0.0.0 failover ip address pix/intf2 0.0.0.0
failover ip address pix/intf3 0.0.0.0 arp timeout 14400
global (outside) 1 11.11.11.10-11.11.11.14 netmask
255.255.255.0 static (inside,outside) 11.11.11.20
171.68.118.115 netmask 255.255.255.255 0 0 static
(inside,outside) 11.11.11.21 171.68.118.101 netmask
255.255.255.255 0 0 static (inside,outside) 11.11.11.22
10.31.1.5 netmask 255.255.255.255 0 0 conduit permit
icmp any any conduit permit tcp any any no rip outside
passive no rip outside default no rip inside passive no
rip inside default no rip pix/intf2 passive no rip
pix/intf2 default no rip pix/intf3 passive no rip
pix/intf3 default route inside 0.0.0.0 0.0.0.0 10.31.1.1
1 timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00
udp 0:02:00 timeout rpc 0:10:00 h323 0:05:00 timeout
uauth 0:00:00 absolute aaa-server TACACS+ protocol
tacacs+ aaa-server RADIUS protocol radius ! !--- For any
given list, multiple AAA servers can !--- be configured.
They will be !--- tried sequentially if any one of them
is down. ! aaa-server Outgoing protocol tacacs+ aaa-
server Outgoing (inside) host 171.68.118.101 cisco
timeout 10 aaa-server Incoming protocol radius aaa-
server Incoming (inside) host 171.68.118.115 cisco
timeout 10 aaa authentication ftp outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa authentication http
outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa
authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 Outgoing aaa authentication ftp inbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa authentication http
inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa
authentication telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 Incoming no snmp-server location no snmp-server
contact snmp-server community public no snmp-server
enable traps telnet timeout 5 terminal width 80
Cryptochecksum:b287a37a676262275a4201cac52399ca : end

```

[Ejemplos de PIX del comando authentication debug](#)

En estos ejemplos del debug:

Saliente

El usuario interior en 10.31.1.5 inicia el tráfico a 11.11.11.15 exterior y se autentica con el TACACS+ (el tráfico saliente utiliza la lista de servidores “saliente” que incluye al servidor TACACS 171.68.118.101).

Entrante

El usuario externo en 11.11.11.15 inicia el tráfico a 10.31.1.5 interior (11.11.11.22) y se autentica con el RADIUS (el tráfico entrante utiliza la lista de servidores “entrante” que incluye al servidor de RADIUS 171.68.118.115).

[PIX debug - Buena autenticación - TACACS+](#)

El ejemplo debajo del PIX debug de las demostraciones con la buena autenticación:


```
109001: Auth start for user '???' from 10.31.1.5/11004 to 11.11.11.15/23
109011: Authen Session Start: user 'ddunlap', sid 3
109005: Authentication succeeded for user 'ddunlap'
from 10.31.1.5/11004 to 11.11.11.15/23
109012: Authen Session End: user 'ddunlap', sid 3, elapsed 1 seconds
302001: Built outbound TCP connection 4 for faddr 11.11.11.15/23 gaddr
11.11.11.22/11004 laddr 10.31.1.5/11004
```

[PIX debug - Autentificación que resultó mal \(nombre de usuario o contraseña\) - TACACS+](#)

El ejemplo debajo del PIX debug de las demostraciones con la autentificación que resultó mal (nombre de usuario o contraseña). El usuario ve cuatro nombres de usuario/contraseñas definidas. Las visualizaciones de siguiente mensaje: "Error: Número máximo de intentos excedidos".

```
109001: Auth start for user '???' from 10.31.1.5/11005 to 11.11.11.15/23
109006: Authentication failed for user '' from 10.31.1.5/11005 to 11.11.11.15/23
```

[PIX debug - Puede hacer ping, solamente ninguna respuesta - TACACS+](#)

El ejemplo debajo del PIX debug de las demostraciones para un servidor al que se le puede hacer ping que no está hablando al PIX. El usuario ve el nombre de usuario una vez, y el PIX nunca pide una contraseña (éste está en Telnet).

```
'Error: Max number of tries exceeded'
109001: Auth start for user '???' from 10.31.1.5/11006 to 11.11.11.15/23
109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
(server 171.68.118.101 failed)
109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
(server 171.68.118.101 failed)
304006: URL Server 171.68.118.101 not responding, trying 171.68.118.101
109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
(server 171.68.118.101 failed)
109006: Authentication failed for user '' from 10.31.1.5/11006 to 11.11.11.15/23
```

[PIX debug - No puede hacer ping el servidor - TACACS+](#)

El ejemplo debajo del PIX debug de las demostraciones para un servidor que no es pingable. El usuario ve el nombre de usuario una vez. El PIX nunca pide una contraseña (éste está en Telnet). Las visualizaciones de siguiente mensaje: "Descanso al servidor TACACS+" y al "error: Número máximo de intentos excedidos" (la configuración en este ejemplo refleja a un servidor ficticio).

```
109001: Auth start for user '???' from 10.31.1.5/11007 to 11.11.11.15/23
109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
(server 171.68.118.199 failed)
109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
(server 171.68.118.199 failed)
304006: URL Server 171.68.118.199 not responding, trying 171.68.118.199
109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
(server 171.68.118.199 failed)
109006: Authentication failed for user '' from 10.31.1.5/11007 to 11.11.11.15/23
```

[PIX debug - Buena autentificación - RADIUS](#)

El ejemplo debajo del PIX debug de la demostración con la buena autentificación:

```
109001: Auth start for user '???' from 11.11.11.15/11003 to 10.31.1.5/23
109011: Authen Session Start: user 'adminuser', sid 4
109005: Authentication succeeded for user 'adminuser'
from 10.31.1.5/23 to 11.11.11.15/11003
```

```
109012: Authen Session End: user 'adminuser', sid 4, elapsed 1 seconds
302001: Built inbound TCP connection 5 for faddr
11.11.11.15/11003 gaddr 11.11.11.22/23 laddr 10.31.1.5/23
```

[PIX debug - Autentificación que resultó mal \(nombre de usuario o contraseña\) - RADIUS](#)

El ejemplo debajo del PIX debug de las demostraciones con la autentificación que resultó mal (nombre de usuario o contraseña). El usuario ve una petición para el nombre de usuario y contraseña. Si cualquiera es incorrecto, el mensaje “contraseña incorrecta” visualiza cuatro veces. Entonces, el usuario es disconnected. Este problema se ha asignado el ID de bug #CSCdm46934.

```
'Error: Max number of tries exceeded'
109001: Auth start for user '???' from 11.11.11.15/11007 to 10.31.1.5/23
109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11007
```

[PIX debug - Daemon abajo, no comunicará con el PIX - RADIUS](#)

El ejemplo debajo del PIX debug de las demostraciones con un servidor al que se le puede hacer ping, pero la daemon está abajo. El servidor no comunicará con el PIX. El usuario ve el nombre de usuario, seguido por la contraseña. La visualización de siguientes mensajes: “Servidor de RADIUS fallado” y “error: Número máximo de intentos excedidos”.

```
109001: Auth start for user '???' from 11.11.11.15/11008 to 10.31.1.5/23
109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
(server 171.68.118.115 failed)
109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
(server 171.68.118.115 failed)
304006: URL Server 171.68.118.115 not responding, trying 171.68.118.115
109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
(server 171.68.118.115 failed)
109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11008
```

[PIX debug - No puede hacer ping el servidor o la discrepancia de clave/cliente - RADIUS](#)

Está una discrepancia de clave/cliente el ejemplo debajo del PIX debug de las demostraciones para un servidor que no sea pingable o donde allí. El usuario ve el nombre de usuario y contraseña. La visualización de siguientes mensajes: “Descanso al servidor de RADIUS” y al “error: Número máximo de intentos excedidos” (el servidor en la configuración es por ejemplo propósitos solamente).

```
109001: Auth start for user '???' from 11.11.11.15/11009 to 10.31.1.5/23
109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
(server 171.68.118.199 failed)
109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
(server 171.68.118.199 failed)
304006: URL Server 171.68.118.199 not responding, trying 171.68.118.199
109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
(server 171.68.118.199 failed)
109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11009
```

[Agregado de autorización](#)

Pues la autorización es inválida sin la autentificación, requeriremos la autorización para el mismo rango de origen y de destino:

```
aaa authorization ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 aaa authorization http outbound
```

```
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 aaa authorization telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0
```

Saliente

Observe que no agregamos la autorización para “entrante” porque el tráfico entrante se autentica con el RADIUS, y la autorización de RADIUS es inválida

Ejemplos de Depuración de Autenticación y Autorización de PIX

PIX debug con la buena autenticación y la autorización exitosa - TACACS+

El ejemplo debajo del PIX debug de la demostración con la buena autenticación y la autorización exitosa:

```
109001: Auth start for user '???' from 10.31.1.5/11002 to 11.11.11.15/23
109011: Authen Session Start: user 'can_only_do_telnet', sid 7
109005: Authentication succeeded for user 'can_only_do_telnet'
from 10.31.1.5/11002 to 11.11.11.15/23
109011: Authen Session Start: user 'can_only_do_telnet', sid 7
109007: Authorization permitted for user 'can_only_do_telnet'
from 10.31.1.5/11002 to 11.11.11.15/23
109012: Authen Session End: user 'can_only_do_telnet', sid 7,
elapsed 1 seconds
302001: Built outbound TCP connection 6 for faddr 11.11.11.15/23
gaddr 11.11.11.22/11002 laddr 10.31.1.5/11002 (can_only_do_telnet)
```

PIX debug - Buena autenticación, autorización fallida - TACACS+

El ejemplo debajo del PIX debug de las demostraciones con la buena autenticación, pero autorización fallida:

Aquí el usuario también ve error del mensaje “: Autorización negada”

```
109001: Auth start for user '???' from 10.31.1.5/11000 to 11.11.11.15/23
109011: Authen Session Start: user 'can_only_do_ftp', sid 5
109005: Authentication succeeded for user 'can_only_do_ftp'
from 10.31.1.5/11000 to 11.11.11.15/23
109008: Authorization denied for user 'can_only_do_ftp' from
10.31.1.5/11000 to 11.11.11.15/23
109012: Authen Session End: user 'can_only_do_ftp', sid 5, elapsed 33 seconds
```

Incorporación de contabilidad

TACACS+

```
aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
```

El debug mirará lo mismo si el considerar es con./desc. Sin embargo, a la hora “construido”, habrá del registro de contabilidad del “comienzo” enviado. A la hora “desmontaje”, habrá del registro de contabilidad de la “parada” enviado.

Los registros de contabilidad TACACS+ parecen el siguiente (éstos son de CiscoSecure UNIX; las que está en el CiscoSecure NT pueden ser coma delimitada en lugar de otro):

```
Thu Jun 3 10:41:50 1999 10.31.1.150 can_only_do_telnet
```

```
PIX 10.31.1.5 start task_id=0x7 foreign_ip=11.11.11.15
local_ip=10.31.1.5 cmd=telnet
Thu Jun 3 10:41:55 1999 10.31.1.150 can_only_do_telnet PIX 10.31.1.5
stop task_id=0x7 foreign_ip=11.11.11.15
local_ip=10.31.1.5 cmd=telnet elapsed_time=4 bytes_in=74 bytes_out=27
```

RADIUS

```
aaa accounting any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming
```

El debug mirará lo mismo si el considerar es con./desc. Sin embargo, a la hora “construyó”, del registro de contabilidad del “comienzo” se envía. A la hora se envía el “desmontaje”, del registro de contabilidad de la “parada”:

Los registros de contabilidad RADIUS parecen el siguiente: (éstos son de CiscoSecure UNIX; las que está en el CiscoSecure NT pueden ser coma delimitada en lugar de otro):

```
10.31.1.150adminuser -- start server=rtp-evergreen.rtp.cisco.com
time=14:53:11 date=06/3/1999 task_id=0x00000008
Thu Jun 3 15:53:11 1999
    Acct-Status-Type = Start
    Client-Id = 10.31.1.150
    Login-Host = 10.31.1.5
    Login-TCP-Port = 23
    Acct-Session-Id = "0x00000008"
    User-Name = "adminuser"
10.31.1.150 adminuser -- stop server=rtp-evergreen.rtp.cisco.com
time=14:54:24 date=06/ 3/1999 task_id=0x00000008
Thu Jun 3 15:54:24 1999
    Acct-Status-Type = Stop
    Client-Id = 10.31.1.150
    Login-Host = 10.31.1.5
    Login-TCP-Port = 23
    Acct-Session-Id = "0x00000008"
    User-Name = "adminuser"
    Acct-Session-Time = 73
    Acct-Input-Octets = 27
    Acct-Output-Octets = 73
```

Utilización del comando Except

En nuestra red, si decidimos que una fuente particular y/o un destino no necesita la autenticación, la autorización, o considerar, podemos hacer algo como el siguiente:

```
aaa authentication except outbound 10.31.1.60 255.255.255.255 11.11.11.15 255.255.255.255
Outgoing aaa authorization except outbound 10.31.1.60 255.255.255.255 11.11.11.15
255.255.255.255 Outgoing
```

¡Si usted está “excepto” los IP Addresses de la autenticación y tiene autorización encendido, usted debe también exceptuarlos de la autorización!

Establecer el número máximo de sesiones y ver a los usuarios conectados

Algunos servidores TACACS+ y RADIUS tienen funciones que permiten establecer un número máximo de sesiones o ver a los usuarios conectados. La posibilidad de establecer un número máximo de sesiones o verificar los usuarios conectados depende de los registros de contabilidad.

Cuando hay un expediente del “comienzo” de las estadísticas generado pero ningún expediente de la “parada”, el TACACS+ o el servidor de RADIUS asume que todavía abren una sesión a la persona (es decir, tiene una sesión con el PIX).

Esto funciona bien en conexiones Telnet y FTP debido a la naturaleza de las conexiones. Esto no funciona bien para HTTP debido a la naturaleza de la conexión. En el siguiente ejemplo, se utiliza una diversa configuración de red pero los conceptos son lo mismo.

Las telnets del usuario con el PIX, autenticando en la manera:

```
(pix) 109001: Auth start for user '???' from 171.68.118.100/1200
to 9.9.9.25 /23
(pix) 109011: Authen Session Start: user 'cse', sid 3
(pix) 109005: Authentication succeeded for user 'cse' from
171.68.118.100/12 00 to 9.9.9.25/23
(pix) 302001: Built TCP connection 5 for faddr 9.9.9.25/23
gaddr 9.9.9.10/12 00 laddr 171.68.118.100/1200 (cse)
(server start account) Sun Nov 8 16:31:10 1998 rtp-pinecone.rtp.cisco.com cse
PIX 171.68.118.100 start task_id=0x3 foreign_ip=9.9.9.25
local_ip=171.68.118.100 cmd=telnet
```

Porque el servidor ha visto un expediente del “comienzo” pero ningún expediente de la “parada” (en este momento), el servidor mostrará que abren una sesión al usuario de “Telnet”. Si el usuario intenta otra conexión que requiera la autenticación (quizás de otro PC) y si fijan a las sesiones máximas hasta el “1” en el servidor para este usuario (si se asume que las sesiones máximas de los soportes de servidor), la conexión será rechazada por el servidor.

El usuario continúa con su Telnet o negocio FTP en el host de destino, después las salidas (pasa 10 minutos allí):

```
(pix) 302002: Teardown TCP connection 5 faddr 9.9.9.25/80 gaddr
9.9.9.10/128 1 laddr 171.68.118.100/1281 duration 0:00:00 bytes 1907 (cse)

(server stop account) Sun Nov 8 16:41:17 1998 rtp-pinecone.rtp.cisco.com cse

PIX 171.68.118.100 stop task_id=0x3 foreign_ip=9.9.9.25 local_ip=171.68.118.100
cmd=telnet elapsed_time=5 bytes_in=98 bytes_out=36
```

Si el uauth es 0 (autentique cada vez) o más (autentique una vez y no otra vez durante el período uauth), un registro de contabilidad se corta para cada sitio accedido.

Sin embargo, el HTTP trabaja diverso debido a la naturaleza del protocolo. Abajo está un ejemplo de HTTP.

El usuario hojea de 171.68.118.100 a 9.9.9.25 con el PIX:

```
(pix) 109001: Auth start for user '???' from 171.68.118.100/1281
to 9.9.9.25 /80
(pix) 109011: Authen Session Start: user 'cse', sid 5
(pix) 109005: Authentication succeeded for user 'cse' from
171.68.118.100/12 81 to 9.9.9.25/80
(pix) 302001: Built TCP connection 5 for faddr 9.9.9.25/80 gaddr
9.9.9.10/12 81 laddr 171.68.118.100/1281 (cse)
(server start account) Sun Nov 8 16:35:34 1998 rtp-pinecone.rtp.cisco.com cse
PIX 171.68.118.100 start task_id=0x9 foreign_ip=9.9.9.25
local_ip=171.68.118.100 cmd=http
(pix) 302002: Teardown TCP connection 5 faddr 9.9.9.25/80 gaddr
9.9.9.10/128 1 laddr 171.68.118.100/1281 duration 0:00:00 bytes 1907 (cse)
(server stop account) Sun Nov 8 16:35:35 1998 rtp-pinecone.rtp.cisco .com
cse PIX 171.68.118.100 stop task_id=0x9 foreign_ip =9.9.9.25
```

```
local_ip=171.68.118.100 cmd=http elapsed_time=0 bytes_in=1907 bytes_out=223
```

El usuario lee la página web descargada.

El registro de comienzo fijado en 16:35:34, y el expediente de la parada fijado en 16:35:35. Esta descarga tardó al segundo (que es; había menos que el segundo entre el comienzo y el expediente de la parada). ¿Todavía todavía abren una sesión al usuario al sitio web y a la conexión abiertos cuando están leyendo la página web? No. ¿Se utilizarán aquí las funciones que permiten establecer un número máximo de sesiones y ver a los usuarios conectados? No, porque el tiempo de conexión (el tiempo entre la 'conexión' y la 'desconexión') en HTTP es demasiado corto. El registro "iniciar" y "detener" es subsegundo. No habrá un expediente del "comienzo" sin un expediente de la "parada", puesto que los expedientes ocurren en virtualmente el mismo instante. Todavía habrá "comienzo" y "pare" el expediente enviado al servidor para cada transacción, si el uauth está fijado para 0 o algo más grande. Sin embargo, las funciones número máximo de sesiones y ver usuarios conectados no funcionarán debido a la índole de las conexiones HTTP.

Autenticación y activación en el PIX mismo

La explicación anterior estaba de autenticar el tráfico de Telnet (y HTTP, FTP) con el PIX. En el ejemplo abajo, nos aseguramos que Telnet al pix trabaja sin la autenticación encendido:

```
telnet 10.31.1.5 255.255.255.255 passwd ww
```

Entonces, agregamos el comando de autenticar el Telnetting de los usuarios al PIX:

```
aaa authentication telnet console Outgoing
```

Cuando indican al usuario de telnet al PIX, él para la contraseña de Telnet ("ww"). El PIX también pide el TACACS+ en este caso (puesto que se utiliza la lista de servidores "saliente") o nombre de usuario de RADIUS y contraseña.

```
aaa authentication enable console Outgoing
```

Con este comando, indican al usuario para un nombre de usuario y contraseña que se envíe al TACACS o al servidor de RADIUS. En este caso, puesto que se utiliza la lista de servidores "saliente", la petición va al servidor TACACS. Puesto que el paquete de autenticación para el permiso es lo mismo que el paquete de autenticación para el login, el usuario puede habilitar con el TACACS o el RADIUS con el mismo nombre de usuario/la contraseña, si se asume que al usuario puede iniciar sesión al PIX con el TACACS o el RADIUS. Este problema se ha asignado el ID de bug #CSCdm47044.

En caso que el servidor esté abajo, el usuario puede acceder al enable mode PIX ingresando el "PIX" para el nombre de usuario y la contraseña habilitada normal del PIX ("contraseña habilitada sea cual sea"). Si la "contraseña habilitada sea cual sea" no está en la configuración PIX, el usuario ingresa el "PIX" para el nombre de usuario y presiona tecla Enter (Intro). Si se fija pero no se sabe la contraseña habilitada, un disco de recuperación de contraseña será requerido para reajustar.

Autenticación en la consola serie

El comando `aaa authentication serial console` requiere la verificación de autenticación para acceder la consola en serie del PIX. Cuando cortarán a los comandos `user performs configuration`

de la consola, los mensajes de Syslog (si el PIX se configura para enviar el Syslog en el nivel de debug a un syslog host). Abajo está un ejemplo del servidor de Syslog:

```
Jun  5 07:24:09 [10.31.1.150.2.2] %PIX-5-111008: User 'cse' executed
the 'hostname' command.
```

Modificación de la línea de comando que ven los usuarios

Si tenemos el comando:

```
auth-prompt THIS_IS_PIX_5
```

los usuarios que pasan con el PIX ven la secuencia:

```
THIS_IS_PIX_5 [at which point one would enter the username]
Password:[at which point one would enter the password]
```

y entonces, en la llegada en la casilla de destino final, el “nombre de usuario: ” y “contraseña: ” indique el cuadro de destino se presenta.

Este prompt afecta solamente a los usuarios que van con el PIX, no al PIX.

Nota: No hay registros de contabilidad cortados para el acceso al PIX.

Personalizar el mensaje que ven los usuarios en Éxito/Fracaso

Si tenemos los comandos:

```
auth-prompt accept "You're allowed through the pix" auth-prompt reject "You blew it"
```

Los usuarios verán el siguiente en un registro fallido/exitoso con el PIX:

```
THIS_IS_PIX_5
Username: asjdkl
Password:
"You blew it"
"THIS_IS_PIX_5"
Username: cse
Password:
"You're allowed through the pix"
```

Tiempos de Espera Absolutos e Inactivos por Usuario

La marcha lenta y los tiempos de espera uauth absoluto se pueden enviar abajo del servidor TACACS+ sobre por usuario una base. ¡Si todos los usuarios en su red deben tener el mismo “timeout uauth,” entonces no implemente esto! Pero, si usted necesita diversos uauths por usuario, siga leyendo.

En nuestro ejemplo en el PIX, utilizamos el **comando timeout uauth 3:00:00**. Esto significa que una vez que una persona autentica, no tendrán que reauthenticate por 3 horas. Pero si configuramos a un usuario con el perfil siguiente y tenemos autorización AAA TACACS encendido en el PIX, la marcha lenta y los tiempos de espera absolutos en el perfil del usuario reemplazan el timeout uauth en el PIX para ese usuario. Esto no significa que la sesión telnet con el PIX consigue disconnected después de la marcha lenta/del tiempo de espera absoluto. Apenas controla independientemente de si ocurre la reautenticación.

```
user = timeout {
default service = permit
login = cleartext "timeout"
service = exec {
timeout = 2
idletime = 1
}
}
```

Después de la autenticación, publique un **comando show uauth** en el PIX:

```
pix-5# show uauth Current Most Seen Authenticated Users 1 1 Authen In Progress 0 1 user
'timeout' at 10.31.1.5, authorized to: port 11.11.11.15/telnet absolute timeout: 0:02:00
inactivity timeout: 0:01:00
```

Después de que el usuario siente la marcha lenta para un minuto, el debug en el PIX muestra:

```
109012: Authen Session End: user 'timeout', sid 19, elapsed 91 seconds
```

El usuario tendrá que reautenticar al volver al mismo host de destino o a un diverso host.

[HTTP virtual](#)

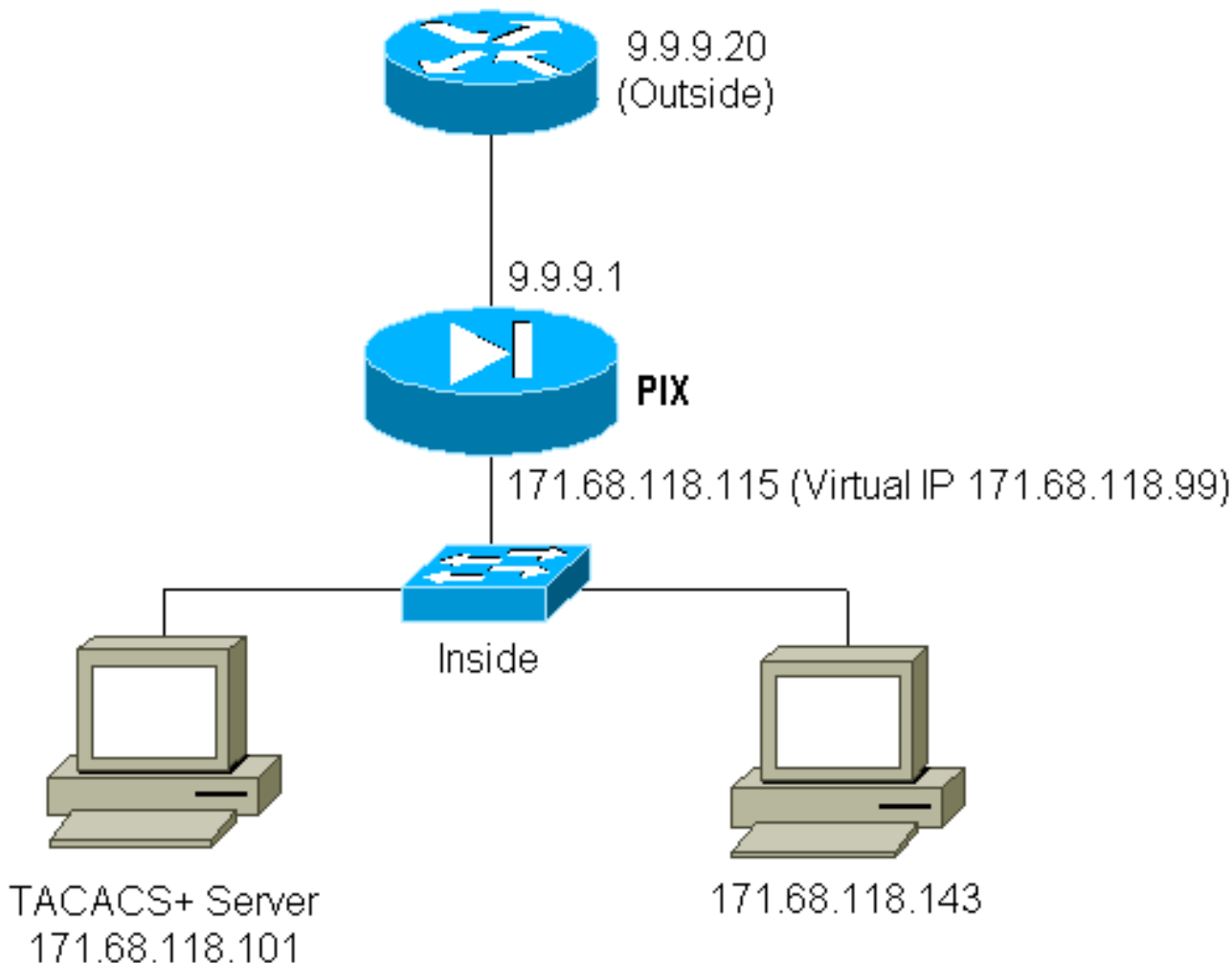
Si la autenticación se requiere en los sitios fuera del PIX, así como en el PIX sí mismo, la conducta inusual del buscador puede ser observada a veces puesto que los navegadores ocultan el nombre de usuario y contraseña.

Para evitar esto, usted puede implementar el HTTP virtual agregando un direccionamiento del [RFC 1918](#) (es decir, un direccionamiento que es unroutable en el Internet, pero válido y único para la red interna PIX) a la configuración PIX usando el siguiente comando:

```
virtual http #.#.#.# [warn]
```

Cuando el usuario intente salir de PIX, se le pedirá autenticación. Si está el parámetro de advertencia, el usuario recibe un mensaje de redirección. La autenticación sirve durante el período de tiempo en uauth. Como se indica en la documentación, no fije la duración del **comando timeout uauth a los segundos 0** con el HTTP virtual; esto impide que se realicen conexiones HTTP al servidor Web real.

Ejemplo de salida de HTTP virtual:



Configuración PIX HTTP de salida virtual:

```
ip address outside 9.9.9.1 255.255.255.0
ip address inside 171.68.118.115 255.255.255.0
global (outside) 1 9.9.9.5-9.9.9.9 netmask 255.0.0.0
timeout uauth 01:00:00
aaa-server TACACS+ protocol tacacs+
aaa-server Outgoing protocol tacacs+
aaa-server Outgoing (inside) host 171.68.118.101 cisco timeout 10
aaa authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
virtual http 171.68.118.99
auth-prompt THIS_IS_PIX_5
```

Virtual telnet

Configurar el PIX para autenticar todo el tráfico entrante y saliente no es una buena idea porque algunos protocolos, tales como "correo," no se autentican fácilmente. Cuando un mail server y un cliente intentan comunicarse con el PIX cuando todo el tráfico con el PIX se está autenticando, el syslog PIX para los protocolos no autenticables mostrará los mensajes por ejemplo:

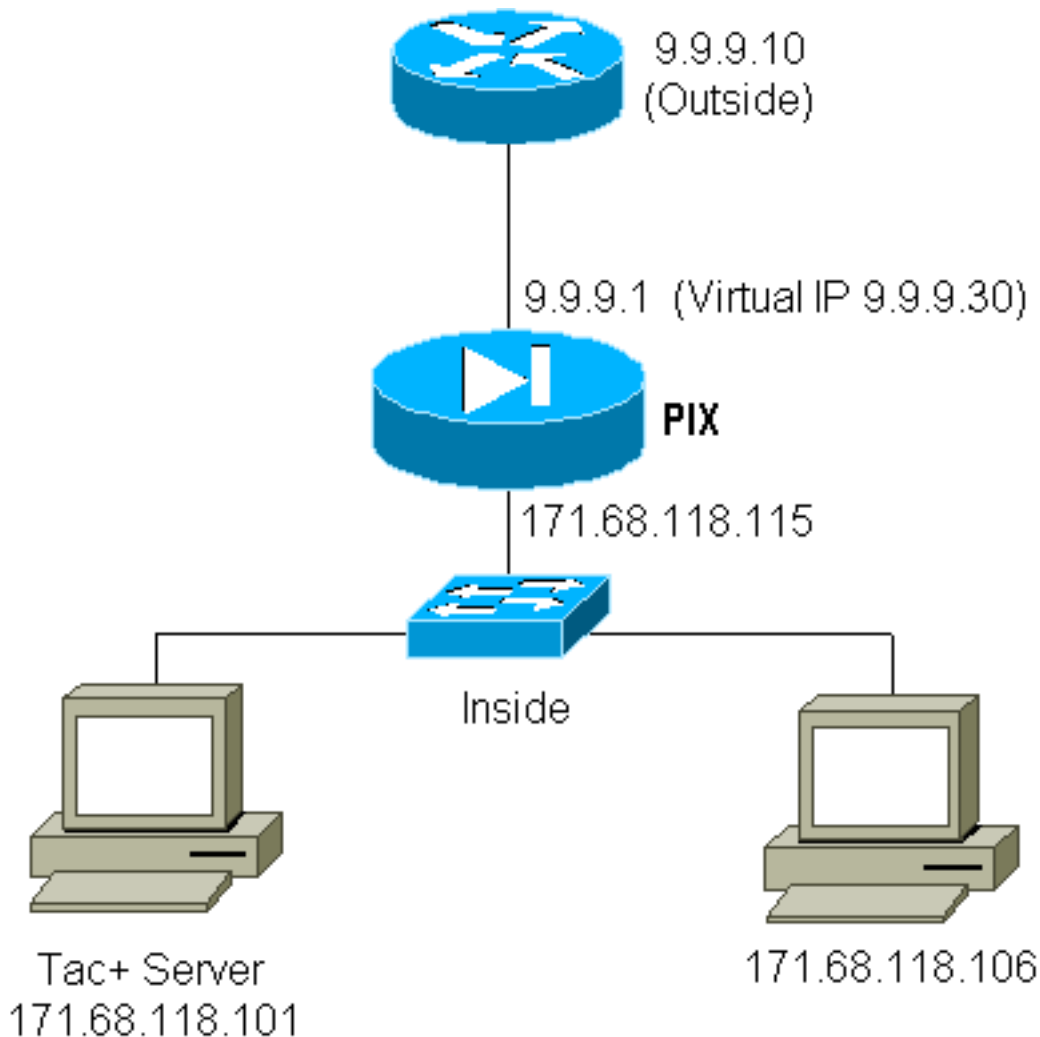
```
109001: Auth start for user '???' from 9.9.9.10/11094 to 171.68.118.106/25
109009: Authorization denied from 171.68.118.106/49 to 9.9.9.10/11094
(not authenticated)
```

Puesto que el correo y algunos otros servicios no son bastante interactivos autenticar, una solución es utilizar el **comando except** para la autenticación/la autorización (autentique todos a excepción de la fuente/del destino del mail server/del cliente).

Pero si hay realmente una necesidad de autenticar una cierta clase de servicio inusual, esto se puede hacer por medio del **comando virtual telnet**. Este comando permite que la autenticación ocurra al IP de Telnet virtual. Después de esta autenticación, el tráfico para el servicio inusual puede ir al servidor real que se ata al IP virtual.

En nuestro ejemplo, queremos permitir que el tráfico del puerto TCP 49 fluya del host exterior 9.9.9.10 al host interior 171.68.118.106. Pues este tráfico no es realmente authenticatable, configuramos la Telnet virtual.

Entrada Telnet virtual:



Entrada Telnet virtual de la configuración PIX:

```
ip address outside 9.9.9.1 255.255.255.0
ip address inside 171.68.118.115 255.255.255.0
static (inside,outside) 9.9.9.30 171.68.118.106 netmask 255.255.255.255 0 0
conduit permit tcp host 9.9.9.30 host 9.9.9.10
aaa-server TACACS+ protocol tacacs+
aaa-server Incoming protocol tacacs+
aaa-server Incoming (inside) host 171.68.118.101 cisco timeout 5
aaa authentication any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming
virtual telnet 9.9.9.30
```

TACACS+ Telnet virtual de configuración del usuario del servidor entrante:

```
user = pinecone {
default service = permit
```

```
login = cleartext "pinecone"
service = exec {
    timeout = 10
    idletime = 10
}
}
```

Entrada Telnet virtual del PIX debug:

El usuario en 9.9.9.10 debe primero autenticar telnetting al direccionamiento de 9.9.9.30 en el PIX:

```
pixfirewall# 109001: Auth start for user '???' from 9.9.9.10/11099
to 171.68.118.106/23
109011: Authen Session Start: user 'pinecone', sid 13
109005: Authentication succeeded for user 'pinecone' from
171.68.118.106/23 to 9.9.9.10/11099
```

Después de la autenticación satisfactoria, el **comando show uauth** muestra que el usuario tiene “tiempo en el contador”:

```
pixfirewall# show uauth Current Most Seen Authenticated Users 1 1 Authen In Progress 0 1 user
'pinecone' at 9.9.9.10, authenticated absolute timeout: 0:10:00 inactivity timeout: 0:10:00
```

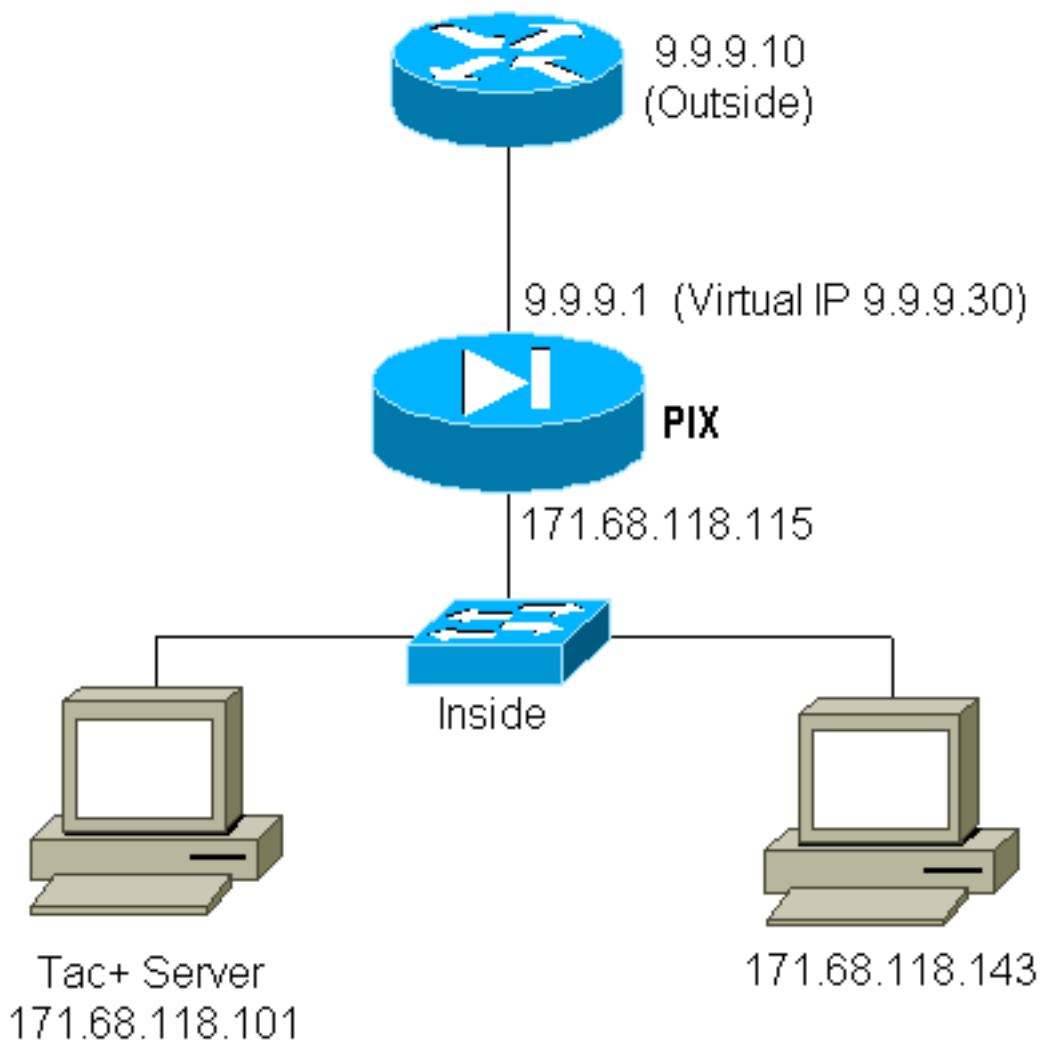
Y cuando el dispositivo en 9.9.9.10 quiere enviar el tráfico TCP/49 al dispositivo en 171.68.118.106:

```
pixfirewall# 109001: Auth start for user 'pinecone'
from 9.9.9.10/11104 to 171.68.118.106/49
109011: Authen Session Start: user 'pinecone', sid 14
109007: Authorization permitted for user 'pinecone' from 9.9.9.10/11104
to 171.68.118.106/49
302001: Built TCP connection 23 for faddr 9.9.9.10/11104 gaddr
9.9.9.30/49 laddr 171.68.118.106/49 (pinecone)
302002: Teardown TCP connection 23 faddr 9.9.9.10/11104 gaddr 9.9.9.30/49
laddr 171.68.118.106/49 duration 0:00:10 bytes 179 (pinecone)
```

Telnet virtual saliente:

Puesto que el tráfico saliente se permite por abandono, no estático se requiere para el uso de la Telnet virtual saliente. En el siguiente ejemplo, el usuario interior en 171.68.118.143 quiere Telnet a 9.9.9.30 virtual y lo autentica. La conexión Telnet se cae inmediatamente.

Una vez que está autenticado, tráfico TCP se permite de 171.68.118.143 al servidor en 9.9.9.10:



Telnet virtual saliente de la configuración PIX:

```
ip address outside 9.9.9.1 255.255.255.0
ip address inside 171.68.118.115 255.255.255.0
global (outside) 1 9.9.9.5-9.9.9.9 netmask 255.0.0.0
timeout uauth 00:05:00
aaa-server TACACS+ protocol tacacs+
aaa-server Outgoing protocol tacacs+
aaa-server Outgoing (inside) host 171.68.118.101 cisco timeout 10
aaa authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
virtual telnet 9.9.9.30
```

Telnet virtual saliente del PIX debug:

```
109001: Auth start for user '???' from 171.68.118.143/1536 to 9.9.9.30/23
109011: Authen Session Start: user 'timeout_143', sid 25
109005: Authentication succeeded for user 'timeout_143' from
171.68.118.143/1536 to 9.9.9.30/23
302001: Built TCP connection 46 for faddr 9.9.9.10/80 gaddr 9.9.9.30/1537
laddr 171.68 .118.143/1537 (timeout_143)
304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
302001: Built TCP connection 47 for faddr 9.9.9.10/80 gaddr 9.9.9.30/1538
laddr 171.68 .118.143/1538 (timeout_143)
302002: Teardown TCP connection 46 faddr 9.9.9.10/80 gaddr 9.9.9.30/1537
laddr 171.68. 118.143/1537 duration 0:00:03 bytes 625 (timeout_143)
304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
302002: Teardown TCP connection 47 faddr 9.9.9.10/80 gaddr 9.9.9.30/1538
laddr 171.68. 118.143/1538 duration 0:00:01 bytes 2281 (timeout_143)
302009: 0 in use, 1 most used
```

Desconexión de Virtual Telnet

Cuando las telnets del usuario al IP de Telnet virtual, el comando `show uauth` muestran su uauth. Si el usuario quiere evitar que vaya el tráfico a través después de que se acabe su sesión (cuando hay tiempo dejado en el uauth), él necesita Telnet al IP de Telnet virtual otra vez. Esto finaliza la sesión.

'Autorización del puerto

Usted puede requerir la autorización en un rango de puertos. En el siguiente ejemplo, la autenticación todavía fue requerida para todo el saliente, pero la autorización se requiere solamente para los puertos TCP 23-49.

Configuración PIX:

```
aaa authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa authorization
tcp/23-49 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
```

Así pues, cuando Telnet de 171.68.118.143 a 9.9.9.10, autenticación y autorización ocurrimos porque el puerto 23 de Telnet está en el rango 23-49. Cuando hacemos HTTP session de 171.68.118.143 a 9.9.9.10, todavía tenemos que autenticar, pero el PIX no pide el servidor TACACS+ para autorizar el HTTP porque 80 no está en el rango 23-49.

Configuración del servidor freeware TACACS+

```
user = telnetrange {
    login = cleartext "telnetrange"
    cmd = tcp/23-49 {
        permit 9.9.9.10
    }
}
```

Observe que el PIX está enviando el "cmd=tcp/23-49" y el "cmd-arg=9.9.9.10" al servidor TACACS+.

Debug en el PIX:

```
109001: Auth start for user '???' from 171.68.118.143/1051 to 9.9.9.10/23
109011: Authen Session Start: user 'telnetrange', sid 0
109005: Authentication succeeded for user 'telnetrange' from
171.68.118.143/1051 to 9.9.9.10/23
109011: Authen Session Start: user 'telnetrange', sid 0
109007: Authorization permitted for user 'telnetrange' from
171.68.118.143/1051 to 9.9.9.10/23
302001: Built TCP connection 0 for faddr 9.9.9.10/23 gaddr 9.9.9.5/1051
laddr 171.68.1 18.143/1051 (telnetrange)
109001: Auth start for user '???' from 171.68.118.143/1105 to 9.9.9.10/80
109001: Auth start for user '???' from 171.68.118.143/1110 to 9.9.9.10/80
109011: Authen Session Start: user 'telnetrange', sid 1
109005: Authentication succeeded for user 'telnetrange' from
171.68.118.143/1110 to 9.9.9.10/80
302001: Built TCP connection 1 for faddr 9.9.9.10/80 gaddr 9.9.9.5/1110
laddr 171.68.1 18.143/1110 (telnetrange)
302001: Built TCP connection 2 for faddr 9.9.9.10/80 gaddr 9.9.9.5/1111
laddr 171.68.1 18.143/1111 (telnetrange)
302002: Teardown TCP connection 1 faddr 9.9.9.10/80 gaddr 9.9.9.5/1110
laddr 171.68.11 8.143/1110 duration 0:00:08 bytes 338 (telnetrange)
```

304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
302002: Teardown TCP connection 2 faddr 9.9.9.10/80 gaddr 9.9.9.5/1111 laddr
171.68.11 8.143/1111 duration 0:00:01 bytes 2329 (telnetrange)

[Información Relacionada](#)

- [Soporte de productos del Software Cisco PIX Firewall](#)
- [Referencias de Comandos de Cisco Secure PIX Firewall](#)
- [Solicitudes de Comentarios \(RFC\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)