

Configurar PIX 5.0.x: TACACS+ y RADIUS

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 TACACS segura de Cisco UNIX](#)

[Cisco asegura la Configuración del servidor del UNIX RADIUS](#)

[Cisco Windows seguro 2.x RADIUS](#)

[EasyACS TACACS+](#)

[Cisco 2.x seguro TACACS+](#)

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

[Configuración del servidor Merit RADIUS](#)

[Pasos de depuración](#)

[Diagrama de la red](#)

[Ejemplos del debug de la autenticación de los ejemplos del debug de PIXAuthentication del PIX](#)

[Saliente](#)

[Entrante](#)

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

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

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

[PIX debug - Incapaz de hacer ping el servidor - TACACS+](#)

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

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

[Debug del ping - Puede hacer ping el servidor, la daemon abajo - RADIUS](#)

[PIX debug - Incapaz de hacer ping el servidor o la discrepancia de clave/cliente - RADIUS](#)

[Agregue la autorización](#)

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

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

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

[Agregar 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](#)

[Cambie el prompt que los usuarios ven](#)

[Personalice a los usuarios del mensaje ven en el éxito/el error](#)

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

[HTTP virtual](#)

[HTTP de salida virtual diagrama](#)

[Configuración PIX HTTP de salida virtual](#)

[Virtual telnet](#)

[Diagrama de la entrada Telnet virtual](#)

[Entrada Telnet virtual de la configuración PIX](#)

[TACACS+ Telnet virtual de configuración del usuario del servidor entrante](#)

[Entrada Telnet virtual del PIX debug](#)

[Virtual Telnet de salida](#)

[Telnet virtual saliente de la configuración PIX](#)

[Telnet virtual saliente del PIX debug](#)

[Desconexión de Virtual Telnet](#)

[Autorización del puerto](#)

[Configuración de PIX](#)

[Configuración del servidor freeware TACACS+](#)

[Debug en el PIX](#)

[Contabilización AAA para cualquier otro tráfico que no sea HTTP, FTP y Telnet](#)

[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 5.0 sobre la versión anterior incluyen el tráfico que explica AAA con excepción del HTTP, del FTP, y de Telnet.

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.

Como un ejemplo, asuma usted tiene cientos usuarios interiores y usted querer quisiera solamente que seis de estos usuarios pudieran hacer el FTP, Telnet, o el HTTP fuera de la red. Diga el PIX autenticar el tráfico saliente y dar los seis ID de los usuarios en el servidor de seguridad TACACS+/RADIUS. Con la autenticación simple, estos seis usuarios pueden ser autenticados con el nombre de usuario y contraseña, después salen. Los otros noventa y cuatro usuarios no pueden 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. Dependiendo de la respuesta, abre o niega la conexión. Estos seis usuarios pueden hacer el FTP, Telnet, o el HTTP.

Por otra parte, asuma 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 le significa necesidad de agregar la *autorización*. Es decir, autorizando *lo que* pueden hacer los usuarios además de autenticar *quién* son. Cuando usted agrega la *autorización al PIX*, el PIX primero envía 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 puede permitir a "FTP 1.2.3.4" pero se niega la capacidad al "HTTP" o a "Telnet" dondequiera.

Qué ve el usuario con la autenticación/autorización activada

Cuando usted intenta ir desde adentro al exterior (o vice versa) con la autenticación/la autorización encendido:

- **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 visualizada en el navegador que pide el nombre de usuario y 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 el FTP parecen trabajar normalmente, pero no lo hacen las conexiones HTTP, esta es la razón por la cual.

Configuración del servidor de seguridad utilizado para todos los escenarios

Configuración de servidor TACACS segura de Cisco UNIX

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 .*
}
}
}
```

Cisco asegura la Configuración del servidor del UNIX RADIUS

Utilice el Interfaz gráfica del usuario (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
}
}
```

Cisco Windows seguro 2.x RADIUS

Siga 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, **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. **Comando add/edit new** selecto para cada comando que usted desea 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 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.

[Cisco 2.x seguro TACACS+](#)

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

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. **Comando add/edit new** selecto 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 final del teclado**.
6. Realice los pasos anteriores 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.

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

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

```
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 key = "cisco"
```

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

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

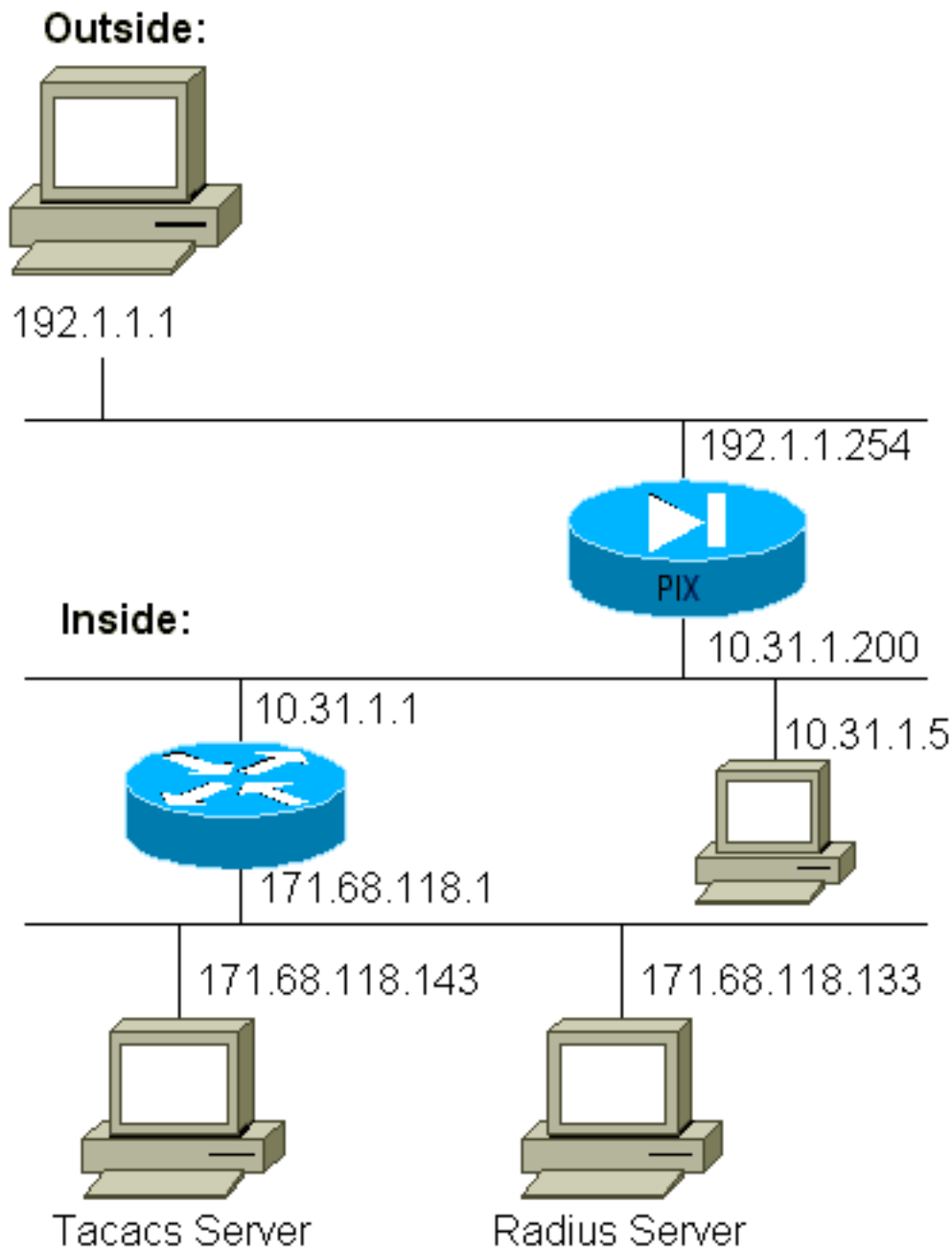
```
user = httponly {  
login = cleartext "httponly"  
cmd = http {  
permit .*  
}  
}
```

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

Pasos de depuración

- Asegúrese que las configuraciones PIX trabajan antes de que usted agregue el 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 un sistema muy 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



Configuración de PIX

```

pix-5# write terminal nameif ethernet0 outside security0
nameif ethernet1 inside security100 enable password
8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU
encrypted hostname pixfirewall 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 name 1.1.1.1 abcd name 1.1.1.2
a123456789 name 1.1.1.3 a123456789123456 pager lines 24
logging timestamp no logging standby logging console
debugging no logging monitor logging buffered debugging
no logging trap logging facility 20 logging queue 512
interface ethernet0 auto interface ethernet1 auto mtu
outside 1500 mtu inside 1500 ip address outside
192.1.1.254 255.255.255.0 ip address inside 10.31.1.200
255.255.255.0 no failover failover timeout 0:00:00
failover ip address outside 0.0.0.0 failover ip address
inside 0.0.0.0 arp timeout 14400 global (outside) 1
192.1.1.10-192.1.1.20 netmask 255.255.255.0 static
(inside,outside) 192.1.1.25 171.68.118.143 netmask
255.255.255.255 0 0 static (inside,outside) 192.1.1.30

```

```
10.31.1.5 netmask 255.255.255.255 0 0 conduit permit tcp
any any conduit permit icmp any any conduit permit udp
any any no rip outside passive no rip outside default no
rip inside passive no rip inside default route inside
171.68.118.0 255.255.255.0 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 aaa-server AuthInbound protocol
tacacs+ aaa-server AuthInbound (inside) host
171.68.118.143 cisco timeout 5 aaa-server AuthOutbound
protocol radius aaa-server AuthOutbound (inside) host
171.68.118.133 cisco timeout 5 aaa authentication telnet
outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication telnet inbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthInbound aaa authentication http
outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication http inbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 AuthInbound aaa authentication ftp outbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound aaa
authentication ftp inbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 AuthInbound no snmp-server location no snmp-
server contact snmp-server community public no snmp-
server enable traps telnet timeout 5 terminal width 80
Cryptochecksum:fef4bfc9801d7692dce0cf227fe7859b : end
```

Ejemplos del debug de la autenticación de los ejemplos del debug de PIXAuthentication del PIX

En estos ejemplos del debug:

Saliente

El usuario interior en 10.31.1.5 inicia el tráfico a 192.1.1.1 exterior y se autentica con el TACACS+. El tráfico saliente utiliza la lista de servidores "AuthOutbound" que incluye al servidor de RADIUS 171.68.118.133.

Entrante

El usuario externo en 192.1.1.1 inicia el tráfico a 10.31.1.5 interior (192.1.1.30) y se autentica con el TACACS. El tráfico entrante utiliza la lista de servidores "AuthInbound" que incluye al servidor TACACS 171.68.118.143).

PIX debug - Buena autenticación - TACACS+

Este ejemplo muestra un PIX debug con la buena autenticación:

```
pixfirewall# 109001: Auth start for user "???" from 192.1.1.1/13155
to 10.31.1.5/23
109011: Authen Session Start: user 'pixuser', sid 6
109005: Authentication succeeded for user 'pixuser' from 10.31.1.5/23
to 192.1.1.1/13155
109012: Authen Session End: user 'pixuser', Sid 6, elapsed 1 seconds
302001: Built inbound TCP connection 6 for faddr 192.1.1.1/13155
gaddr 192.1.1.30/23 laddr 10.31.1.5/23 (pixuser)
```


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

Este ejemplo muestra el PIX debug con la autenticación que resultó mal (nombre de usuario o contraseña). El usuario ve cuatro nombres de usuario/contraseñas definidas y errores del mensaje “: Número máximo de intentos excedidos.”

```
pixfirewall# 109001: Auth start for user '???' from 192.1.1.1/13157
to 10.31.1.5/23
109006: Authentication failed for user '' from 10.31.1.5/23
to 192.1.1.1/13157
```

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

Este ejemplo muestra el PIX debug donde el servidor puede ser hecho ping pero no está hablando al PIX. El usuario ve el nombre de usuario una vez, pero el PIX nunca pide una contraseña (éste está en Telnet). El usuario ve el “error: Número máximo de intentos excedidos.”

```
Auth start for user '???' from 192.1.1.1/13159 to
10.31.1.5/23
pixfirewall# 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13159
failed (server 171.68.118.143 failed)
109002: Auth from 10.31.1.5/23 to 192.1.1.1/13159 failed
(server 171.68.118.143 failed)
109002: Auth from 10.31.1.5/23 to 192.1.1.1/13159 failed
(server 171.68.118.143 failed)
109006: Authentication failed for user '' from 10.31.1.5/23
to 192.1.1.1/13159
```

[PIX debug - Incapaz de hacer ping el servidor - TACACS+](#)

Este ejemplo muestra a PIX debug donde no está pingable el servidor. El usuario ve el nombre de usuario una vez, pero el PIX nunca pide una contraseña (éste está en Telnet). Se visualizan estos mensajes: “Descanso al servidor TACACS+” y al “error: Número máximo de intentos excedidos” (intercambiamos adentro a un servidor ficticio en la configuración).

```
109001: Auth start for user '???' from 192.1.1.1/13158
to 10.31.1.5/23
109002: Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed
(server 171.68.118.143 failed)
109002: Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed
(server 171.68.118.143 failed)
109002: Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed
(server 171.68.118.143 failed)
109006: Authentication failed for user '' from 10.31.1.5/23
to 192.1.1.1/13158
```

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

Este ejemplo muestra un PIX debug con la buena autenticación:

```
109001: Auth start for user '???' from 10.31.1.5/11074
to 192.1.1.1/23
109011: Authen Session Start: user 'pixuser', Sid 7
109005: Authentication succeeded for user 'pixuser'
from 10.31.1.5/11074 to 192.1.1.1/23
109012: Authen Session End: user 'pixuser', Sid 7,
elapsed 1 seconds
302001: Built outbound TCP connection 7 for faddr 192.1.1.1/23
```

```
gaddr 192.1.1.30/11074 laddr 10.31.1.5/11074 (pixuser)
```

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

Este ejemplo muestra un PIX debug con la autenticación que resultó mal (nombre de usuario o contraseña). El usuario ve una petición para el nombre de usuario y contraseña. El usuario tiene tres oportunidades para un nombre de usuario exitoso/entrada de contraseña.

```
- 'Error: max number of tries exceeded'
pixfirewall# 109001: Auth start for user '???' from
 192.1.1.1/13157 to 10.31.1.5/23
109001: Auth start for user '???' from 10.31.1.5/11075
 to 192.1.1.1/23
109002: Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed
 (server 171.68.118.133 failed)
109002: Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed
 (server 171.68.118.133 failed)
109002: Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed
 (server 171.68.118.133 failed)
109006: Authentication failed for user '' from 10.31.1.5/11075
 to 192.1.1.1/23
```

[Debug del ping - Puede hacer ping el servidor, la daemon abajo - RADIUS](#)

Este ejemplo muestra a PIX debug donde está pingable el servidor, pero la daemon está abajo y no comunicará con el PIX. El usuario ve el nombre de usuario, la contraseña, y servidor de RADIUS de los mensajes el “fallado” y el “error: Número máximo de intentos excedidos.”

```
pixfirewall# 109001: Auth start for user '???'
 from 10.31.1.5/11076 to 192.1.1.1/23
109002: Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed
 (server 171.68.118.133 failed)
109002: Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed
 (server 171.68.118.133 failed)
109002: Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed
 (server 171.68.118.133 failed)
109006: Authentication failed for user '' from 10.31.1.5/11076
 to 192.1.1.1/23
```

[PIX debug - Incapaz de hacer ping el servidor o la discrepancia de clave/cliente - RADIUS](#)

Este ejemplo calza un PIX debug donde no está pingable el servidor o hay una discrepancia de clave/cliente. El usuario ve el nombre de usuario, la contraseña, y descanso de los mensajes el “al servidor de RADIUS” y al “error: Número máximo de intentos excedidos” (intercambiaron a un servidor ficticio adentro la configuración).

```
109001: Auth start for user '???' from 10.31.1.5/11077
 to 192.1.1.1/23
109002: Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed
 (server 100.100.100.100 failed)
109002: Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed
 (server 100.100.100.100 failed)
109002: Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed
 (server 100.100.100.100 failed)
109006: Authentication failed for user '' from 10.31.1.5/11077
 to 192.1.1.1/23
```

[Agregue la autorización](#)

Si usted decide agregar la autorización, usted requerirá la autorización para el mismo rango de origen y de destino (puesto que la autorización es inválida sin la autenticación):

```
aaa authorization telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa authorization
HTTP inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa authorization ftp inbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

Observe que la autorización no está agregada para “saliente” porque el tráfico saliente se autentica con el RADIUS, y la autorización de RADIUS es inválida.

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

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

Este ejemplo muestra un PIX debug con la buena autenticación y la autorización exitosa:

```
109011: Authen Session Start: user 'pixuser', Sid 8
109007: Authorization permitted for user 'pixuser'
      from 192.1.1.1/13160 to 10.31.1.5/23
109012: Authen Session End: user 'pixuser', Sid 8,
      elapsed 1 seconds
302001: Built inbound TCP connection 8 for faddr 192.1.1.1/13160
      gaddr 192.1.1.30/23 laddr 10.31.1.5/23 (pixuser)
```

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

Este ejemplo muestra un PIX debug con la buena autenticación pero con la autorización fallida. Aquí el usuario también ve error del mensaje “: Autorización negada.”

```
109001: Auth start for user '???' from 192.1.1.1/13162
      to 10.31.1.5/23
109011: Authen Session Start: user 'userhttp', Sid 10
109005: Authentication succeeded for user 'userhttp'
      from 10.31.1.5/23 to 192.1.1.1/13162
109008: Authorization denied for user 'userhttp'
      from 10.31.1.5/23 to 192.1.1.1/13162
109012: Authen Session End: user 'userhttp', Sid 10,
      elapsed 1 seconds
302010: 0 in use, 2 most used
```

[Agregar contabilidad](#)

[TACACS+](#)

```
aaa accounting any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

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

Los registros de contabilidad TACACS+ parecen esta salida (éstos son de Cisco Secure NT, por lo tanto del formato de la coma delimitada):

```
04/26/2000,01:31:22,pixuser,Default Group,192.1.1.1,
start,,,,,,,,0x2a,,PIX,10.31.1.200,telnet,6,
Login,1,,,1,,,,,,,,,,,,,local_ip=10.31.1.5 foreign_ip=192.1.1.1,
```

```

, , , , , , , , , , zekie , , , , , ^
04/26/2000,01:31:26,pixuser,Default Group,192.1.1.1,stop,4,
,36,82,,,0x2a,,PIX,10.31.1.200,telnet,6,
Login,1,,,1,,,,,,local_ip=10.31.1.5 foreign_ip=192.1.1. 1,
, , , , , , , , , , zekie , , , , ,

```

RADIUS

```
aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
```

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

Los registros de contabilidad RADIUS parecen esta salida (éstos son de Cisco UNIX seguro; unas en el Cisco Secure NT pueden ser coma delimitada en lugar de otro):

```
radrecv: Request from host alf01c8 code=4, id=18, length=65
Acct-Status-Type = Start
Client-Id = 10.31.1.200
Login-Host = 10.31.1.5
Login-TCP-Port = 23
Acct-Session-Id = "0x0000002f"
User-Name = "pixuser"
Sending Accounting Ack of id 18 to alf01c8 (10.31.1.200)
radrecv: Request from host alf01c8 code=4, id=19, length=83
Acct-Status-Type = Stop
Client-Id = 10.31.1.200
Login-Host = 10.31.1.5
Login-TCP-Port = 23
Acct-Session-Id = "0x0000002f"
Username = "pixuser"
Acct-Session-Time = 7

```

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 similar hecha salir:

```
aaa authentication except inbound 192.1.1.1 255.255.255.255 0.0.0.0 0.0.0.0 AuthInbound
```

Si usted está “excepto” un cuadro de la autenticación y tiene autorización encendido, usted debe también exceptuar el cuadro 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 (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 esta salida de 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
```

Puesto que el servidor ha visto un expediente del “comienzo” pero ningún expediente de la “parada” (en este momento), el servidor muestra 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 es rechazada por el servidor.

El usuario continúa con Telnet o el 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.

HTTP funciona de manera distinta debido a la naturaleza del protocolo. Esta salida muestra 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 sólo un segundo (es decir, hubo menos de un segundo entre el registro de inicio y de detención). ¿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 sesiones máximas y los usuarios conectados al sistema de la visión no trabajan debido a las naturalezas de la conexión HTTP.

Autenticación y activación en el PIX mismo

La explicación anterior describió el autenticar del tráfico de Telnet (y HTTP, FTP) *con el PIX*. Nos aseguramos Telnet a los trabajos PIX *sin la autenticación encendido*:

```
telnet 10.31.1.5 255.255.255.255 passwd ww
aaa authentication telnet console AuthInbound
```

Cuando indican al usuario de telnet al PIX, él para la contraseña de Telnet (**ww**). Entonces el PIX también pide el TACACS+ (en este caso, puesto que se utiliza la lista de servidores del "AuthInbound") o nombre de usuario de RADIUS y contraseña. Si el servidor está abajo, usted puede conseguir en el PIX ingresando el **pix** para el nombre de usuario, y entonces la contraseña habilitada (**contraseña habilitada sea cual sea**) para acceder.

Con este comando:

```
aaa authentication enable console AuthInbound
```

indican al usuario para un nombre de usuario y contraseña, que se envía al TACACS (en este caso, puesto que se utiliza la lista de servidores del "AuthInbound", la petición va al servidor TACACS) o al servidor de RADIUS. Puesto que el paquete de autenticación para el permiso es lo mismo que el paquete de autenticación para el login, si el usuario puede iniciar sesión al PIX con el TACACS o el RADIUS, pueden habilitar con el TACACS o el RADIUS con el mismo nombre de usuario/la contraseña. Este problema se ha asignado el Id. de bug Cisco [CSCdm47044](#) ([clientes registrados solamente](#)).

Autenticación en la consola serie

El comando **aaa authentication serial console AuthInbound** requiere la verificación de autenticación para acceder la consola en serie del PIX.

Cuando cortan a los comandos user performs configuration de la consola, los mensajes de Syslog (asumiendo el PIX se configura para enviar el Syslog en el nivel de debug a un syslog host). Éste es un ejemplo de qué se visualiza en el servidor de Syslog:

```
logmsg: pri 245, flags 0, from [10.31.1.200.2.2], msg Nov 01 1999
03:21:14: %PIX-5-111008: User 'pixuser' executed the 'logging' command.
```

Cambie el prompt que los usuarios ven

Si usted tiene el comando `auth-prompt PIX_PIX_PIX`, los usuarios que pasan con el PIX ven esta secuencia:

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

Sobre la llegada en la casilla de destino final, el “nombre de usuario:” y “contraseña: se visualiza el” prompt. 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.

Personalice a los usuarios del mensaje ven en el éxito/el error

Si usted tiene los comandos:

```
auth-prompt accept "GOOD_AUTH" auth-prompt reject "BAD_AUTH"
```

los usuarios ven esta secuencia en un registro fallido/exitoso con el PIX:

```
PIX_PIX_PIX
Username: asjdkl
Password:
"BAD_AUTH"
"PIX_PIX_PIX"
Username: cse
Password:
"GOOD_AUTH"
```

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`,” no implemente esto! Pero si usted necesita diversos `uauths` por usuario, continúe leyendo.

En este ejemplo, utilizan al comando `timeout uauth 3:00:00`. Una vez que una persona autentica, no tienen que reautenticar por tres horas. Sin embargo, si usted configura a un usuario con este perfil y tiene 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 es disconnected después de la marcha lenta/del tiempo de espera absoluto. Apenas controla si ocurre la reautenticación.

Este perfil viene del freeware TACACS+:

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

Después de la autenticación, ejecute 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 tiene que reautenticar cuando vuelve al mismo host de destino o a un diverso host.

[HTTP virtual](#)

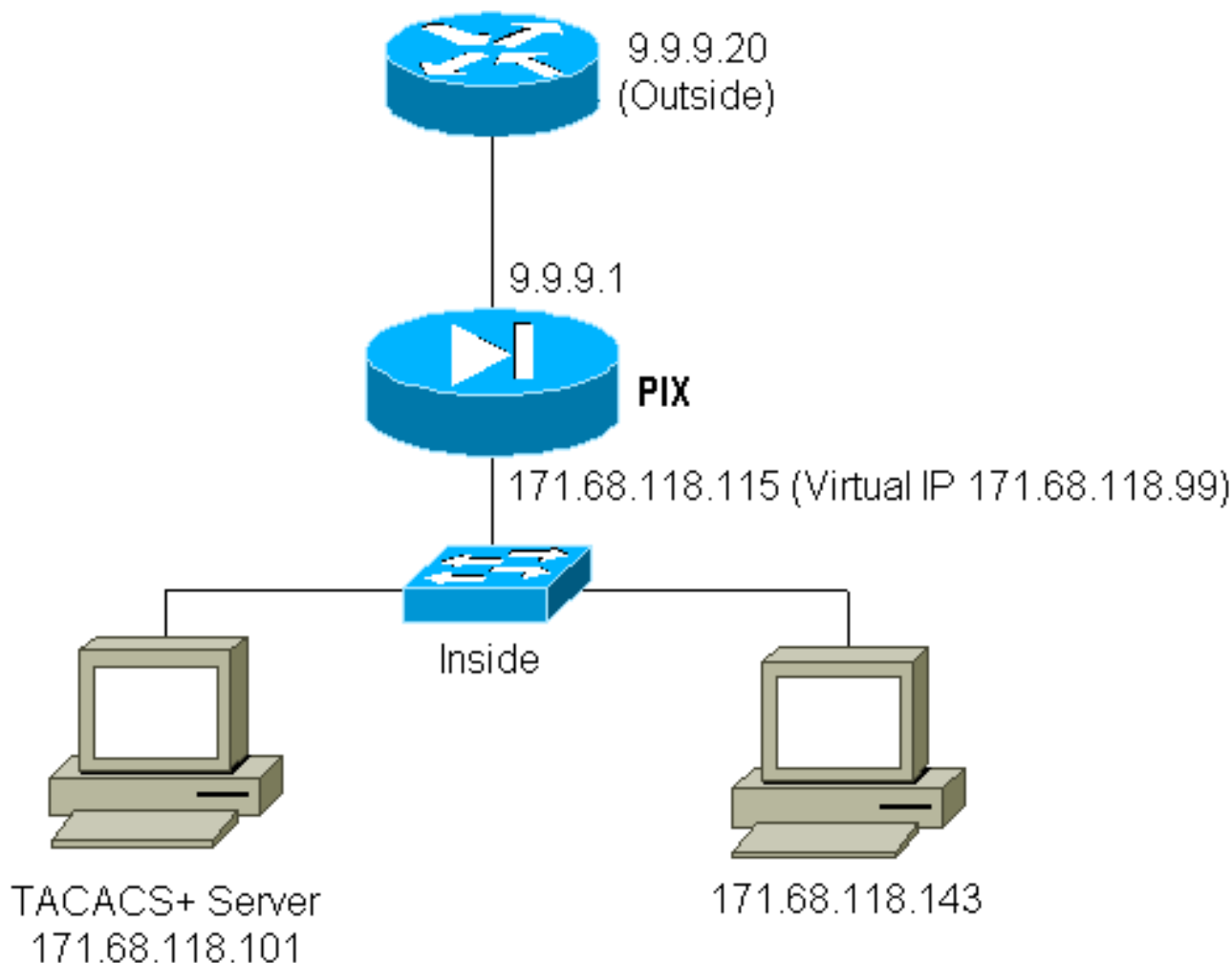
Si la autenticación se requiere en los sitios fuera del PIX, así como en el PIX sí mismo, la conducta inusual del buscador puede ser observada a veces puesto que los navegadores ocultan el nombre de usuario y contraseña.

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

[HTTP de salida virtual diagrama](#)



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 AuthOutbound protocol tacacs+
aaa-server AuthOutbound (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 AuthOutbound
virtual http 171.68.118.99
auth-prompt THIS_IS_PIX_5
```

Virtual telnet

Es posible configurar el PIX para autenticar todo el tráfico entrante y saliente, pero no es una buena idea hacer tan. Esto es 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, syslog PIX para los mensajes unautenticables de la demostración de los protocolos 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)
```

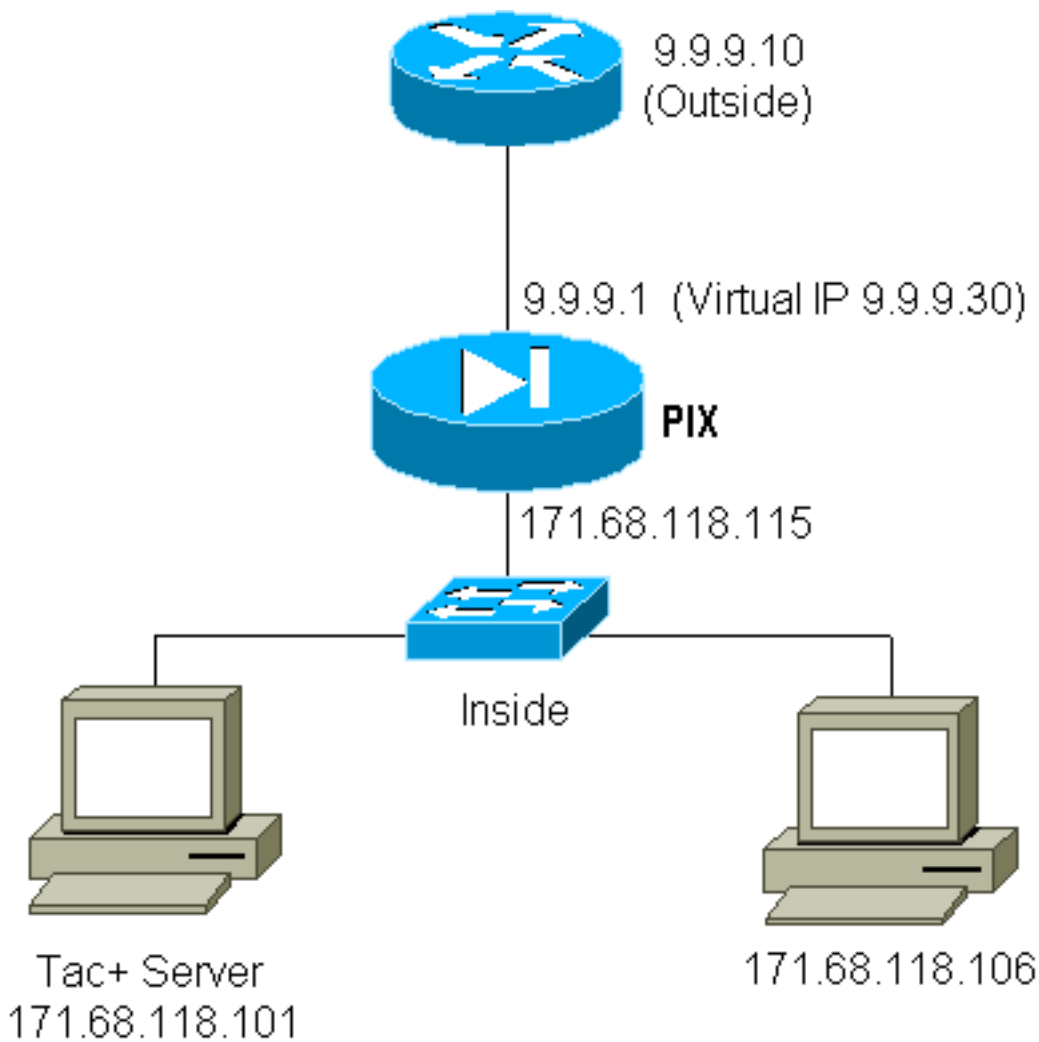
Puesto que el correo y algunos otros servicios no son bastante interactivos autenticar, una solución es utilizar el **comando except** para la autenticación/la autorización (autentique todos a

excepción de la fuente/del destino del mail server/del cliente).

Si hay una necesidad real 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.

En este ejemplo, quisiéramos que el tráfico del puerto TCP 49 fluyera del host exterior 9.9.9.10 al host interior 171.68.118.106. Puesto que este tráfico no es realmente authenticatable, configuramos una Telnet virtual. Para la Telnet virtual entrante, debe haber parásitos atmosféricos asociados. Aquí, 9.9.9.20 y 171.68.118.20 son direcciones virtuales.

Diagrama de la 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) 9.9.9.20 171.68.118.20 netmask 255.255.255.255 0 0
static (inside,outside) 9.9.9.30 171.68.118.106 netmask 255.255.255.255 0 0
conduit permit tcp host 9.9.9.20 eq telnet any
conduit permit tcp host 9.9.9.30 eq tacacs any
aaa-server TACACS+ protocol tacacs+
aaa-server AuthInbound protocol tacacs+
aaa-server AuthInbound (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 AuthInbound
virtual telnet 9.9.9.20
```

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 por el Telnetting al direccionamiento de 9.9.9.20 en el PIX:

```
pixfirewall# 109001: Auth start for user '???' from 9.9.9.10/11099
to 171.68.118.20/23
109011: Authen Session Start: user 'pinecone', Sid 13
109005: Authentication succeeded for user 'pinecone'
from 171.68.118.20/23 to 9.9.9.10/1470
```

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

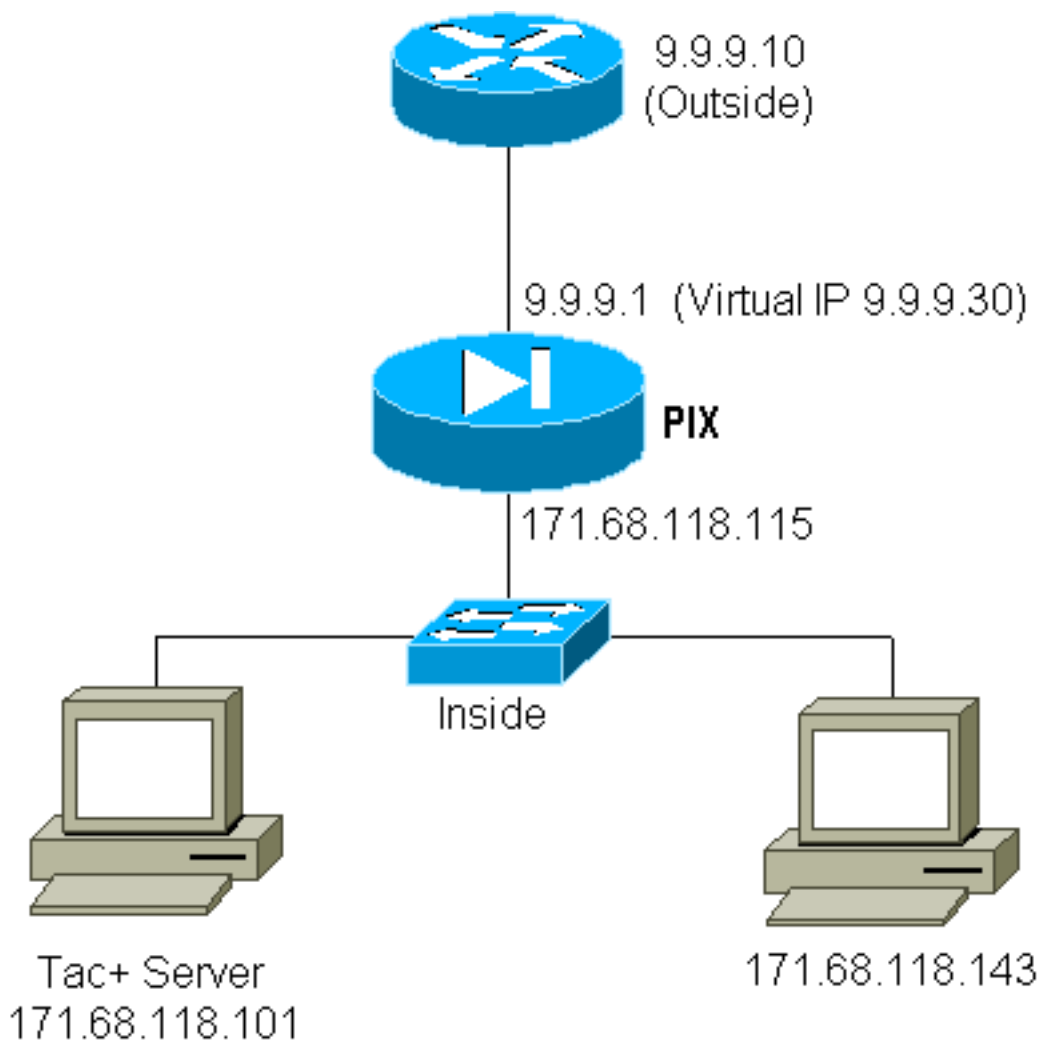
```
pixfirewall# show uauth Current Most Seen Authenticated Users 1 1 Authen In Progress 0 1 user
'pinecone' at 9.9.9.10, authenticated absolute timeout: 0:10:00 inactivity timeout: 0:10:00
```

Aquí, 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 171.68.118.20/23
109011: Authen Session Start: user 'pinecone', Sid 14
109005: Authentication succeeded for user 'pinecone' from 171.68.118.20/23
to 9.9.9.10/1470
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)
```

Virtual Telnet de salida

Puesto que el tráfico saliente se permite por abandono, no estático se requiere para el uso de la Telnet virtual saliente. En este ejemplo, el usuario interior en el Telnets de 171.68.118.143 a 9.9.9.30 virtual y 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 AuthOutbound protocol tacacs+
aaa-server AuthOutbound (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 AuthOutbound
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 el uauth.

Si el usuario quiere evitar que vaya el tráfico a través después de que se acabe la sesión (cuando hay tiempo dejado en el uauth), el usuario 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 este ejemplo, la autenticación todavía fue requerida para todo saliente, pero solamente la autorización fue requerida para los puertos TCP 23-49.

Configuración de PIX

```
AAA authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound AAA authorization
tcp/23-49 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
```

Cuando Telnet fue hecho de 171.68.118.143 a 9.9.9.10, la autenticación y autorización ocurrió porque el puerto 23 de Telnet está en el rango 23-49.

Cuando HTTP session se hace de 171.68.118.143 a 9.9.9.10, usted todavía tiene 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 envía 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 171.68.118.143/1051 (telnetrange)
109001: Auth start for user '???' from 171.68.118.143/1105
to 9.9.9.10/80
```

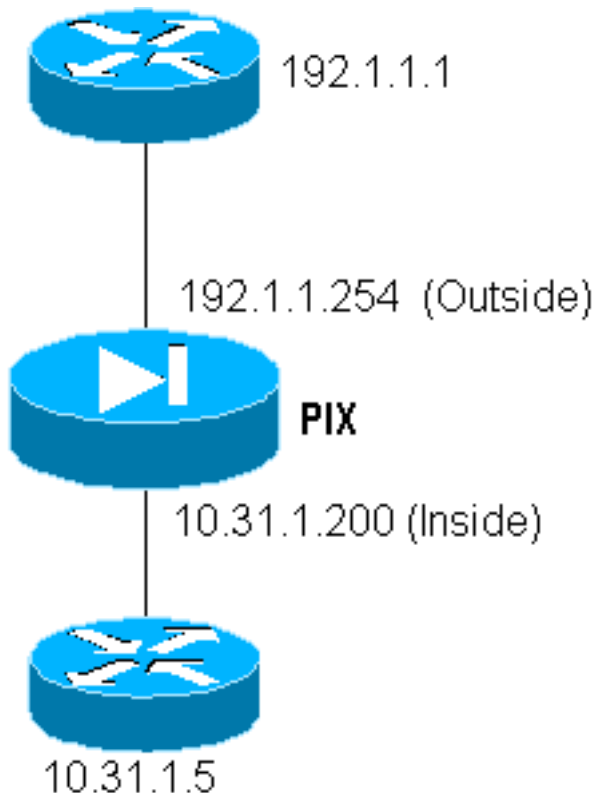
```

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)

```

Contabilización AAA para cualquier otro tráfico que no sea HTTP, FTP y Telnet

La versión de software PIX 5.0 cambia las funciones de las estadísticas del tráfico. Los registros de contabilidad se pueden ahora cortar para el tráfico con excepción del HTTP, del FTP, y de Telnet, una vez que se completa la autenticación.



Para la TFTP-copia un archivo del router externo (192.1.1.1) al router interno (10.31.1.5), agrega la Telnet virtual para abrir un agujero para el proceso TFTP:

```

virtual telnet 192.1.1.30 static (inside,outside) 192.1.1.30 10.31.1.5 netmask 255.255.255.255 0
0 conduit permit udp any any AAA authentication udp/69 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthInbound AAA authorization udp/69 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound AAA
accounting udp/0 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound

```

Después, Telnet del router externo en 192.1.1.1 IP virtual a 192.1.1.30 y autentica a la dirección virtual que permite que el UDP atraviese el PIX. En este ejemplo, el proceso del **flash de tftp de la copia** fue comenzado del exterior al interior:

```
302006: Teardown UDP connection for faddr 192.1.1.1/7680
      gaddr 192.1.1.30/69 laddr 10.31.1.5/69
```

Para cada **flash de tftp de la copia** en el PIX (había tres durante esta copia IOS), un registro de contabilidad se corta y se envía al servidor de autenticación. Lo que sigue es un ejemplo de un expediente TACACS en Cisco asegura Windows):

```
Date,Time,Username,Group-Name,Caller-Id,Acct-Flags,elapsed_time,
service,bytes_in,bytes_out,paks_in,paks_out,
task_id,addr,NAS-Portname,NAS-IP-Address,cmd
04/28/2000,03:08:26,pixuser,Default Group,192.1.1.1,start,,,,,,,,
0x3c,,PIX,10.31.1.200,udp/69
```

[Información Relacionada](#)

- [Referencia de Comandos PIX](#)
- [Página de soporte de producto PIX](#)
- [Solicitudes de Comentarios \(RFC\)](#)
- [Soporte Técnico - Cisco Systems](#)