Configuración de PIX 5.0.x: TACACS+ y RADIUS

Contenido

Introducción

La autenticación RADIUS y TACACS+ se puede realizar para conexiones FTP, Telnet y HTTP. La autenticación para otros protocolos TCP menos comunes normalmente se puede hacer para funcionar.

Se admite la autorización TACACS+. La autorización de RADIUS no. Los cambios en la autenticación, autorización y contabilidad (AAA) de PIX 5.0 con respecto a la versión anterior incluyen la contabilización AAA para el tráfico que no sea HTTP, FTP y Telnet.

Prerequisites

Requirements

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

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Autenticación vs. Autorización

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

A modo de ejemplo, suponga que tiene cien usuarios dentro y que sólo desea que seis de estos usuarios puedan realizar FTP, Telnet o HTTP fuera de la red. Dígale al PIX que autentique el tráfico saliente y proporcione los seis ID de usuario en el servidor de seguridad TACACS+/RADIUS. Con *autenticación* simple, estos seis usuarios pueden autenticarse con nombre de usuario y contraseña y luego salir. Los otros noventa y cuatro usuarios no pueden salir. El PIX solicita a los usuarios el nombre de usuario/la contraseña y luego pasa su nombre de usuario y contraseña al servidor de seguridad TACACS+/RADIUS. Dependiendo de la respuesta, se abre o se niega la conexión. Estos seis usuarios pueden hacer FTP, Telnet o HTTP.

Por otro lado, supongamos que *uno* de estos tres usuarios, "Terry", no es de confianza. Le gustaría permitir a Terry hacer FTP, pero no HTTP o Telnet al exterior. Esto significa que necesita agregar *autorización*. Es decir, autorizar *lo que* los usuarios pueden hacer además de autenticar *quiénes* son. Cuando agrega *autorización* al PIX, el PIX primero envía el nombre de usuario y la contraseña de Terry al servidor de seguridad y luego envía una solicitud de autorización informándole al servidor de seguridad qué "*comando*" intenta hacer Terry. Con el servidor configurado correctamente, a Terry se le puede permitir "FTP 1.2.3.4" pero se le niega la capacidad de "HTTP" o "Telnet" en cualquier lugar.

Qué ve el usuario con la autenticación/autorización activada

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

- **Telnet** - El usuario ve una visualización de solicitud de nombre de usuario, seguida de una solicitud de 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 aparecer un mensaje de nombre de usuario** 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**: ventana que se muestra en el explorador y que solicita el nombre de usuario y la contraseña. Si la autenticación (y la autorización) se realiza con éxito, el usuario accederá al sitio Web siguiente. Tenga en cuenta que **los navegadores almacenan nombres de usuario y contraseñas.**. 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 normalmente, pero las conexiones HTTP no, es por eso que.

Configuración del servidor de seguridad utilizado para todos los escenarios

Configuración del servidor TACACS de Cisco Secure UNIX

Asegúrese de que tiene la dirección IP PIX o el nombre de dominio completo y la clave 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 del servidor RADIUS de Cisco Secure UNIX

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

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

```
}
```

Cisco Secure Windows 2.x RADIUS

Siga estos pasos:

1. Obtenga una contraseña en la sección User Setup GUI (Configuración de usuario).
2. En la sección Group Setup GUI (Configuración de grupo), establezca el atributo 6 (Tipo de servicio) en Login (Inicio de sesión) o Administrative (Administración).
3. Agregue la IP PIX en la GUI de configuración de NAS.

EasyACS TACACS+

La documentación de EasyACS describe la configuración.

1. En la sección de grupo, haga clic en **Shell exec** (para otorgar privilegios exec).
2. Para agregar autorización al PIX, haga clic en **Denegar comandos IOS no coincidentes** en la parte inferior de la configuración del grupo.
3. Seleccione **Add/Edit new command** para cada comando que desee permitir (por ejemplo, Telnet).
4. Si desea permitir que Telnet acceda a sitios específicos, introduzca las IP en la sección de argumentos con el formato "permit #.#.#.#". Para permitir Telnet a todos los sitios, haga clic en **Permitir todos los argumentos no enumerados**.
5. Haga clic en el **comando Finalizar edición**.
6. Realice los pasos del 1 al 5 para cada uno de los comandos permitidos (por ejemplo, Telnet, HTTP o FTP).
7. Agregue el PIX IP en la sección NAS Configuration GUI.

Cisco Secure 2.x TACACS+

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

1. En la sección de grupo, haga clic en **Shell exec** (para otorgar privilegios exec).
2. Para agregar autorización al PIX, haga clic en **Denegar comandos IOS no coincidentes** en la parte inferior de la configuración del grupo.
3. Seleccione **Add/Edit new command** para cada comando que desee permitir (por ejemplo, Telnet).
4. Si desea permitir Telnet a sitios específicos, introduzca permit IP en el rectángulo del argumento (por ejemplo, "permit 1.2.3.4"). Para permitir Telnet a todos los sitios, haga clic en **Permitir todos los argumentos no enumerados**.
5. Haga clic en **finalizar el comando de edición**.
6. Realice los pasos anteriores para cada uno de los comandos permitidos (por ejemplo, Telnet, HTTP o FTP).
7. Agregue el PIX IP en la sección NAS Configuration GUI.

'Configuración del servidor Livingston RADIUS'

Agregue la IP PIX y la clave al archivo de clientes.

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

Configuración del servidor Merit RADIUS

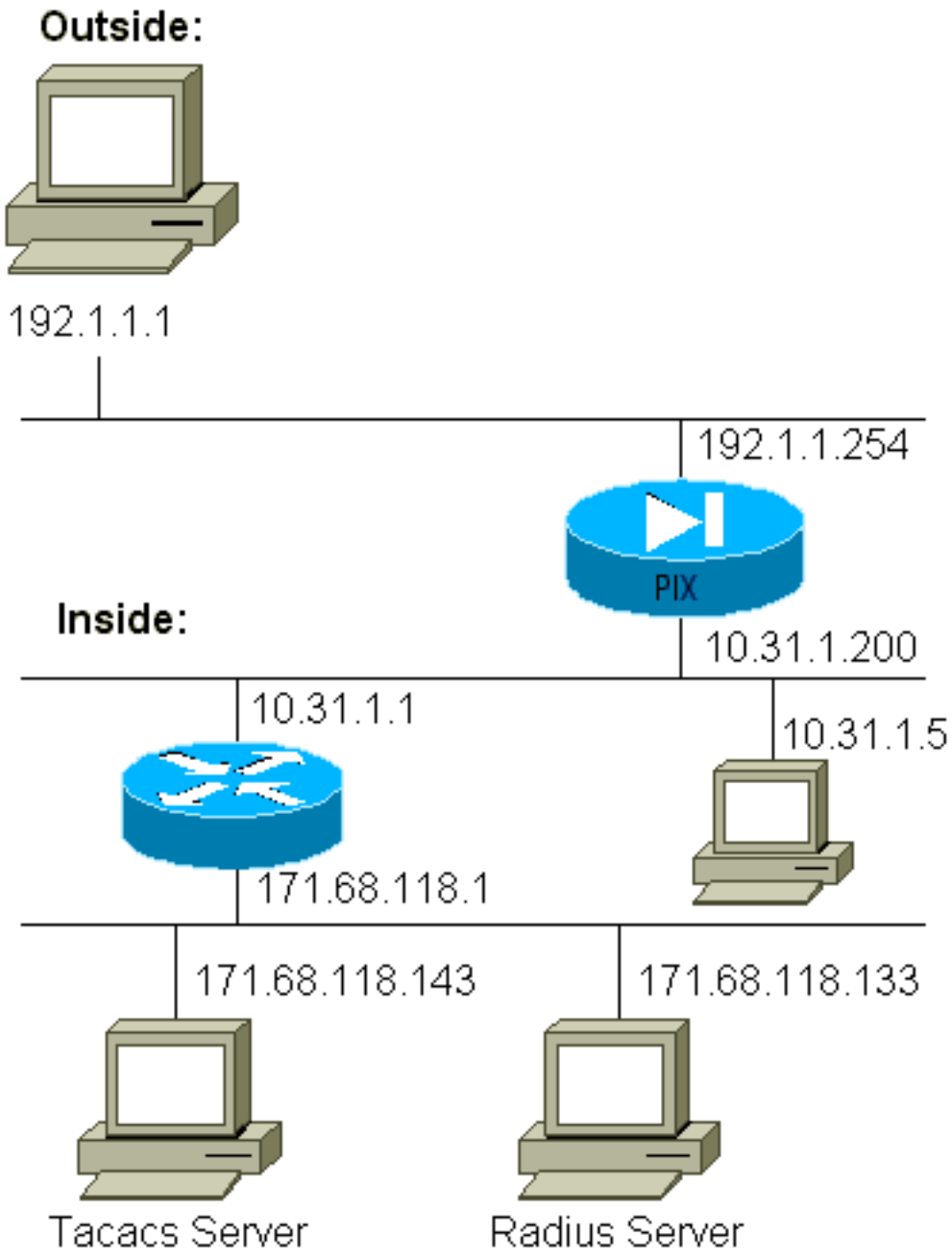
Agregue la IP PIX y la clave al archivo de clientes.

```
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 de que las configuraciones PIX funcionen antes de agregar AAA.Si no puede pasar tráfico antes de iniciar la autenticación y autorización, no podrá realizarlo luego.
- Habilite el inicio de sesión en el PIXEl 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** se puede enviar a un servidor syslog y examinarla.
- Asegúrese de que la depuración esté activada para los servidores TACACS+ o 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 de Depuración de Autenticación de PIXAuthauthentication Debug de PIX

En estos ejemplos de depuración:

Salientes

El usuario interno en 10.31.1.5 inicia el tráfico hacia afuera 192.1.1.1 y se autentica a través de TACACS+. El tráfico saliente utiliza la lista de servidores "AuthOutbound" que incluye el servidor RADIUS 171.68.118.133.

Entrante

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

Depuración de PIX - Buena autenticación - TACACS+

Este ejemplo muestra un debug PIX con una 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)
```

Depuración PIX - Autenticación incorrecta (nombre de usuario o contraseña) - TACACS+

Este ejemplo muestra la depuración PIX con autenticación incorrecta (nombre de usuario o contraseña). El usuario ve cuatro conjuntos de nombre de usuario/contraseña y el mensaje "`Error: 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 - Servidor Can Ping, Sin Respuesta - TACACS+

Este ejemplo muestra la depuración PIX donde se puede hacer ping al servidor pero no está hablando con el PIX. El usuario ve el nombre de usuario una vez, pero el PIX nunca pide una contraseña (esto está en Telnet). El usuario ve "`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
```

Depuración PIX - No se puede hacer ping al servidor - TACACS+

Este ejemplo muestra una depuración PIX donde el servidor no puede hacer ping. El usuario ve el nombre de usuario una vez, pero el PIX nunca solicita una contraseña (esto está en Telnet). Se muestran estos mensajes: "`Tiempo de espera para el servidor TACACS+`" y "`Error: Número máximo de intentos excedidos`" (intercambiamos en un servidor falso 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
```

Depuración PIX - Autenticación correcta - RADIUS

Este ejemplo muestra un debug PIX con una 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)
```

Depuración de PIX - Autenticación incorrecta (nombre de usuario o contraseña) - RADIUS

Este ejemplo muestra una depuración PIX con autenticación incorrecta (nombre de usuario o contraseña). El usuario ve una solicitud de nombre de usuario y contraseña. El usuario tiene tres oportunidades para introducir correctamente el nombre de usuario/la 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
```

Depuración de ping: servidor Can Ping, Daemon Down - RADIUS

Este ejemplo muestra un debug PIX donde el servidor es ping, pero el demonio está caído y no se comunicará con el PIX. El usuario ve el nombre de usuario, la contraseña y los mensajes "`El servidor RADIUS falló`" y "`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
```

Depuración de PIX - No se puede hacer ping al servidor o a la discordancia de clave/cliente - RADIUS

En este ejemplo se inicia una depuración PIX donde el servidor no puede hacer ping o hay una discordancia de clave/cliente. El usuario ve el nombre de usuario, la contraseña y los mensajes "`Timeout to RADIUS server`" y "`Error: Número máximo de intentos excedidos`" (se intercambió un servidor falso en 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
```

Agregar autorización

Si decide agregar autorización, necesitará autorización para el mismo rango de origen y destino (ya que la autorización no es válida sin 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
```

Tenga en cuenta que la autorización no se agrega para "saliente" porque el tráfico saliente se autentica con RADIUS y la autorización RADIUS no es válida.

Ejemplos de Depuración de Autenticación y Autorización de PIX

Depuración PIX - Autenticación correcta y autorización exitosa - TACACS+

Este ejemplo muestra un debug PIX con una buena autenticación y 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)
```

Depuración PIX - Autenticación correcta, Autorización fallida - TACACS+

Este ejemplo muestra un debug PIX con una buena autenticación pero con una autorización fallida. Aquí el usuario también ve el mensaje "`Error: Autorización denegada.`"

```
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
```

La depuración se ve igual si la contabilización está activada o desactivada. Sin embargo, en el momento de la creación, se envía un registro contable de "inicio". En el momento de la "Teardown", se envía un registro contable de "stop".

Los registros de contabilidad TACACS+ se asemejan a este resultado (estos son de Cisco Secure NT, por lo que el formato delimitado por comas):

```
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
```

La depuración se muestra igual si la contabilización está activada o desactivada. Sin embargo, en el momento de la creación, se envía un registro contable de "inicio". En el momento de la "Teardown", se envía un registro contable de "stop".

Los registros de contabilidad RADIUS se asemejan a este resultado (estos son de Cisco Secure UNIX; los de Cisco Secure NT pueden estar delimitados por comas en su lugar):

```
radrecv: Request from host a1f01c8 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 a1f01c8 (10.31.1.200)
radrecv: Request from host a1f01c8 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 un origen o destino en particular no necesita autenticación, autorización o contabilidad, podemos hacer algo como este resultado:

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

Si está "exceptuando" una casilla de la autenticación y tiene autorización activada, también debe excepto la casilla 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 se genera un registro de "inicio" de contabilización pero no se "detiene", el servidor TACACS+ o RADIUS asume que la persona aún está conectada (tiene una sesión a través del 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 este resultado de ejemplo, se

utiliza una configuración de red diferente, pero los conceptos son los mismos.

El usuario Telnet a través del PIX, autenticándose en el camino:

```
(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
```

Dado que el servidor ha visto un registro de "inicio" pero no un registro de "detención" (en este momento), el servidor muestra que el usuario "Telnet" ha iniciado sesión. Si el usuario intenta otra conexión que requiere autenticación (tal vez desde otro PC) y si max-sessions se establece en "1" en el servidor para este usuario (suponiendo que el servidor admita el número máximo de sesiones), el servidor rechaza la conexión.

El usuario continúa con el negocio de Telnet o FTP en el host de destino y luego sale (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 uauth es 0 (autentificar cada vez) o más (autenticar una vez y no de nuevo durante el período uauth), se corta un registro contable para cada sitio al que se accede.

HTTP funciona de manera distinta debido a la naturaleza del protocolo. Este resultado muestra un ejemplo de HTTP:

El usuario navega de 171.68.118.100 a 9.9.9.25 a través del 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 inicio se publicó a las 16:35:34, y el registro de parada se publicó a las 16:35:35. Esta descarga tardó sólo un segundo (es decir, hubo menos de un segundo entre el registro de inicio y de detención). ¿El usuario aún ha iniciado sesión en el sitio web y la conexión sigue abierta cuando está leyendo la página web? No. ¿Funcionarán aquí las sesiones máximas o los usuarios registrados? 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 registro de "inicio" sin un registro de "parada", ya que los registros ocurren prácticamente en el mismo instante. Seguirá habiendo un registro "start" y "stop" enviado al servidor para cada transacción, ya sea que uauth esté configurado para 0 o algo más grande. Sin embargo, el número máximo de sesiones y los usuarios de la vista conectados no funcionan debido a la naturaleza de las conexiones HTTP.

Autenticación y activación en el PIX mismo

La discusión anterior describió la autenticación del tráfico Telnet (y HTTP, FTP) *a través* del PIX. Nos aseguramos de que Telnet *al* PIX funcione *sin* autenticación en:

```
telnet 10.31.1.5 255.255.255.255 passwd ww
```

```
aaa authentication telnet console AuthInbound
```

Cuando los usuarios se conectan mediante Telnet al PIX, se les solicita la contraseña de Telnet (**ww**). Luego el PIX también solicita el TACACS+ (en este caso, ya que se utiliza la lista de servidores "AuthInbound") o el nombre de usuario y la contraseña RADIUS. Si el servidor no funciona, puede ingresar al PIX ingresando **pix** para el nombre de usuario y luego la contraseña de habilitación (**habilitar contraseña *lo que sea***) para obtener acceso.

Con este comando:

```
aaa authentication enable console AuthInbound
```

se le solicita al usuario un nombre de usuario y una contraseña, que se envía al TACACS (en este caso, dado que se utiliza la lista de servidores "AuthInbound", la solicitud va al servidor TACACS) o al servidor RADIUS. Dado que el paquete de autenticación para habilitar es el mismo que el paquete de autenticación para el login, si el usuario puede iniciar sesión en el PIX con TACACS o RADIUS, pueden habilitar a través de TACACS o RADIUS con el mismo nombre de usuario/contraseña. Este problema se ha asignado a Cisco bug ID CSCdm4704 (sólo clientes registrados) .

Autenticación en la consola serie

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

Cuando el usuario ejecuta comandos de configuración desde la consola, se cortan los mensajes de syslog (suponiendo que el PIX esté configurado para enviar syslog en el nivel de depuración a un host de syslog). Este es un ejemplo de lo que se muestra en el servidor 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.
```

Cambiar el mensaje que ven los usuarios

Si tiene el comando **auth-prompt PIX_PIX_PIX**, los usuarios que pasan a través del PIX verán esta secuencia:

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

Al llegar al cuadro de destino final, se muestra el mensaje "Nombre de usuario:" y "Contraseña:". Este mensaje afecta solamente a los usuarios que pasan *a través* del PIX, no *al* PIX.

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

Personalización del mensaje que los usuarios ven sobre éxito/fallo

Si tiene los comandos:

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

los usuarios ven esta secuencia en un login fallido/exitoso a través del 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

Los tiempos de espera de espera inactivos y absolutos se pueden enviar desde el servidor TACACS+ por usuario. Si todos los usuarios de su red han de tener el mismo "timeout uauth", ¡no lo implemente! Pero si necesita diferentes usuarios por usuario, continúe leyendo.

En este ejemplo, se utiliza el comando **timeout uauth 3:00:00**. Una vez que una persona se

autentica, no tiene que volver a autenticarse durante tres horas. Sin embargo, si configura un usuario con este perfil y tiene *autorización* TACACS AAA en el PIX, los tiempos de espera inactivos y absolutos en el perfil de usuario invalidan el tiempo de espera uauth en el PIX para ese usuario. Esto no significa que la sesión Telnet a través del PIX se desconecte después del tiempo de espera inactivo/absoluto. Sólo controla si se realiza la reautenticación.

Este perfil viene de TACACS+ freeware:

```
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 permanezca inactivo durante un minuto, el debug en el PIX muestra:

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

El usuario debe volver a autenticarse cuando vuelve al mismo host de destino o a un host diferente.

HTTP virtual

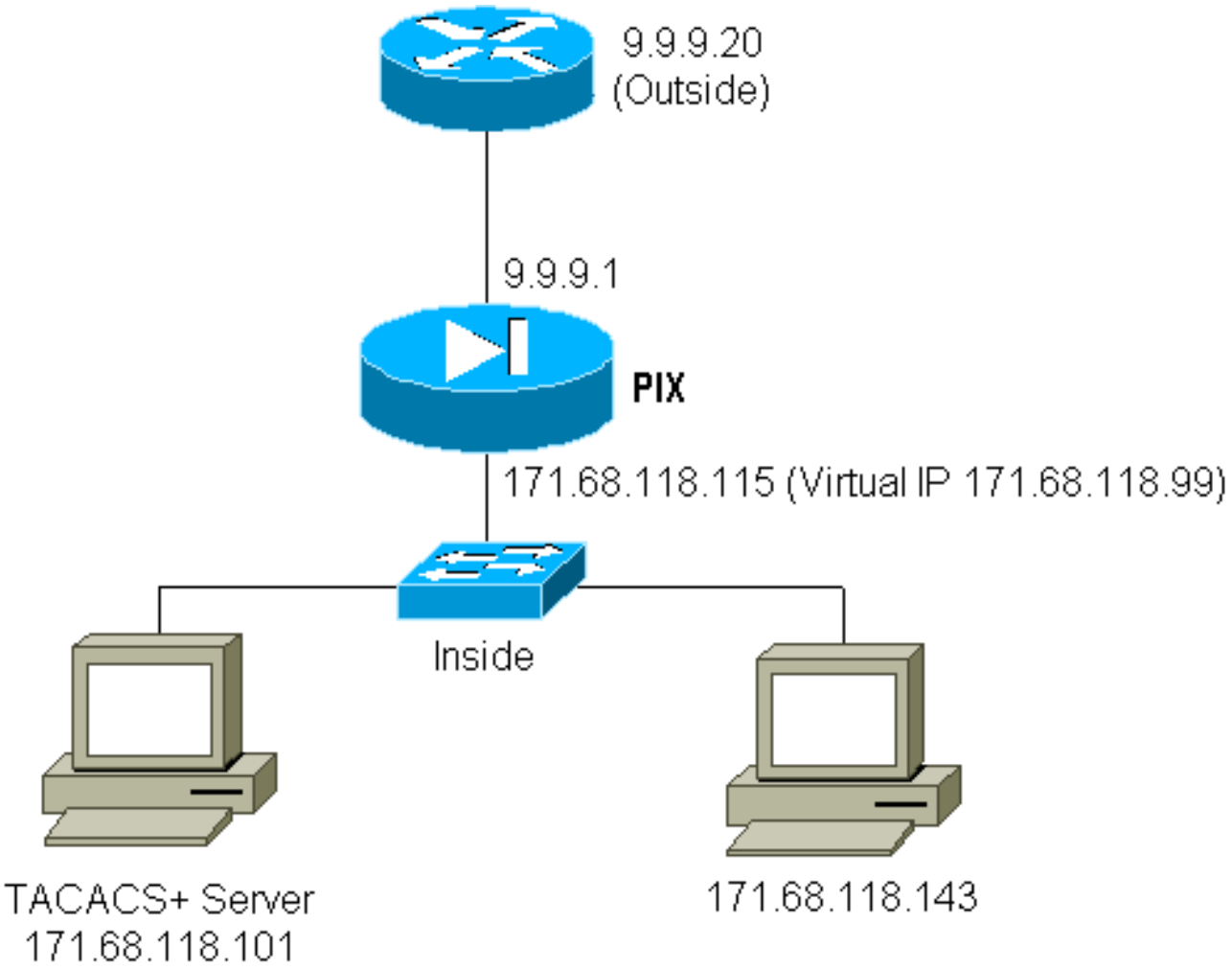
Si se requiere autenticación en sitios fuera del PIX, así como en el propio PIX, a veces se puede observar un comportamiento inusual del navegador, ya que los exploradores almacenan el nombre de usuario y la contraseña.

Para evitar esto, puede implementar HTTP virtual agregando una dirección RFC 1918 (una dirección que no se puede rutear en Internet, pero que es válida y única 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 establezca la duración del comando **timeout uauth** en 0 segundos con HTTP virtual. esto impide que se realicen conexiones HTTP al servidor Web real.

Diagrama HTTP saliente virtual



Configuración de PIX HTTP virtual saliente

```
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 hacerlo. Esto se debe a que algunos protocolos, como "correo", no se autentican fácilmente. Cuando un servidor de correo y un cliente tratan de comunicarse a través del PIX cuando todo el tráfico a través del PIX está siendo autenticado, PIX syslog para protocolos no autenticables muestra mensajes como:

```
109001: Auth start for user '???' from 9.9.9.10/11094
    to 171.68.118.106/25
```

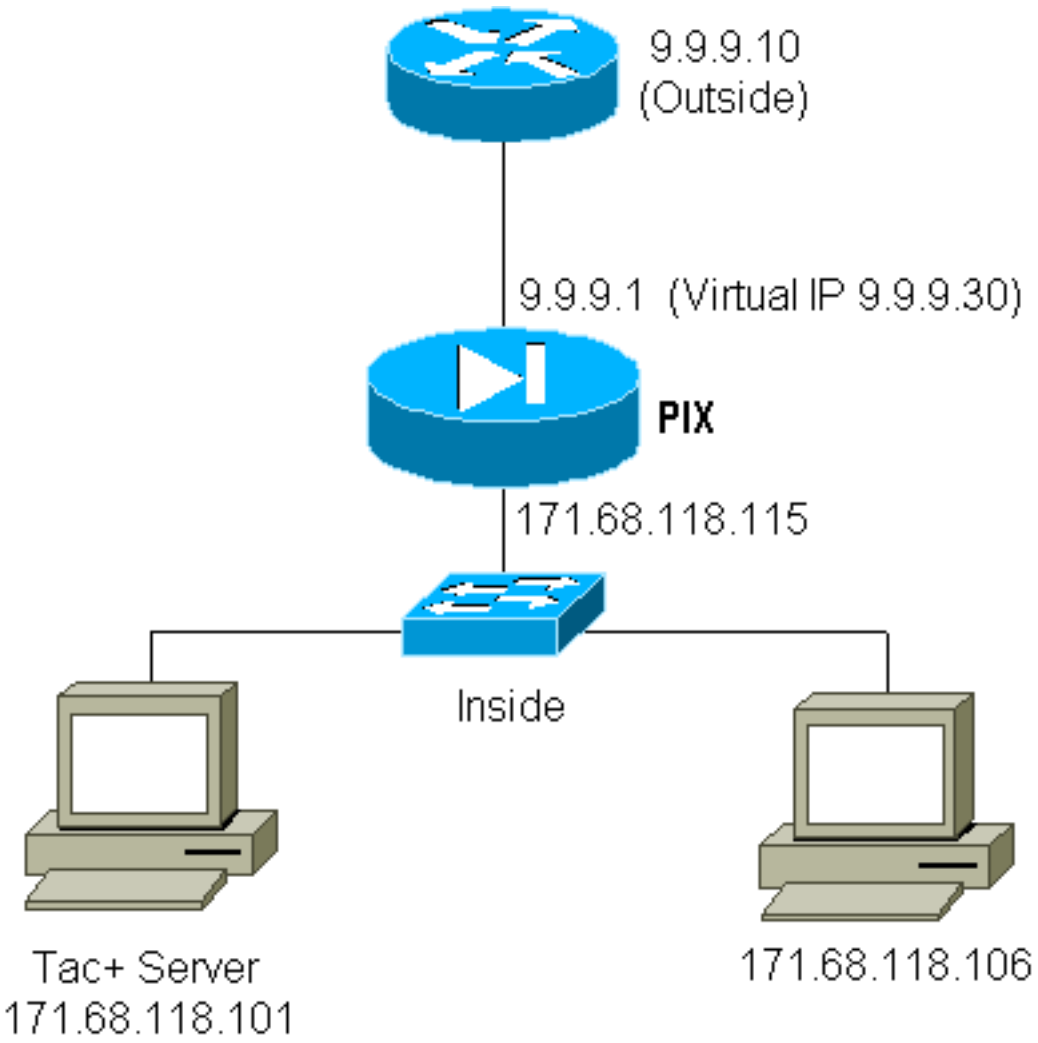
```
109009: Authorization denied from 171.68.118.106/49 to
   9.9.9.10/11094 (not authenticated
```

Dado que el correo y algunos otros servicios no son lo suficientemente interactivos como para autenticarse, una solución es utilizar el comando **excepto** para la autenticación/autorización (autentique todo excepto el origen/destino del servidor/cliente de correo).

Si hay una necesidad real de autenticar algún tipo de servicio inusual, esto puede hacerse mediante el uso del comando **virtual telnet**. Este comando permite que la autenticación se produzca en la IP de Telnet virtual. Después de esta autenticación, el tráfico para el servicio inusual puede ir al servidor real.

En este ejemplo, queremos que el tráfico del puerto TCP 49 fluya desde el host exterior 9.9.9.10 al host interno 171.68.118.106. Dado que este tráfico no es realmente autenticable, configuramos un Telnet virtual. Para Telnet virtual entrante, debe haber una estática asociada. Aquí, tanto 9.9.9.20 como 171.68.118.20 son direcciones virtuales.

Diagrama entrante de Telnet virtual



Configuración de PIX Virtual Telnet Inbound

```
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
```

Configuración del usuario del servidor TACACS+ Virtual Telnet Inbound

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

PIX Debug Virtual Telnet Inbound

El usuario en 9.9.9.10 primero debe autenticarse mediante Telnet a la dirección 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 exitosa, el comando **show uauth** muestra que el usuario tiene "tiempo en el medidor":

```
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
```

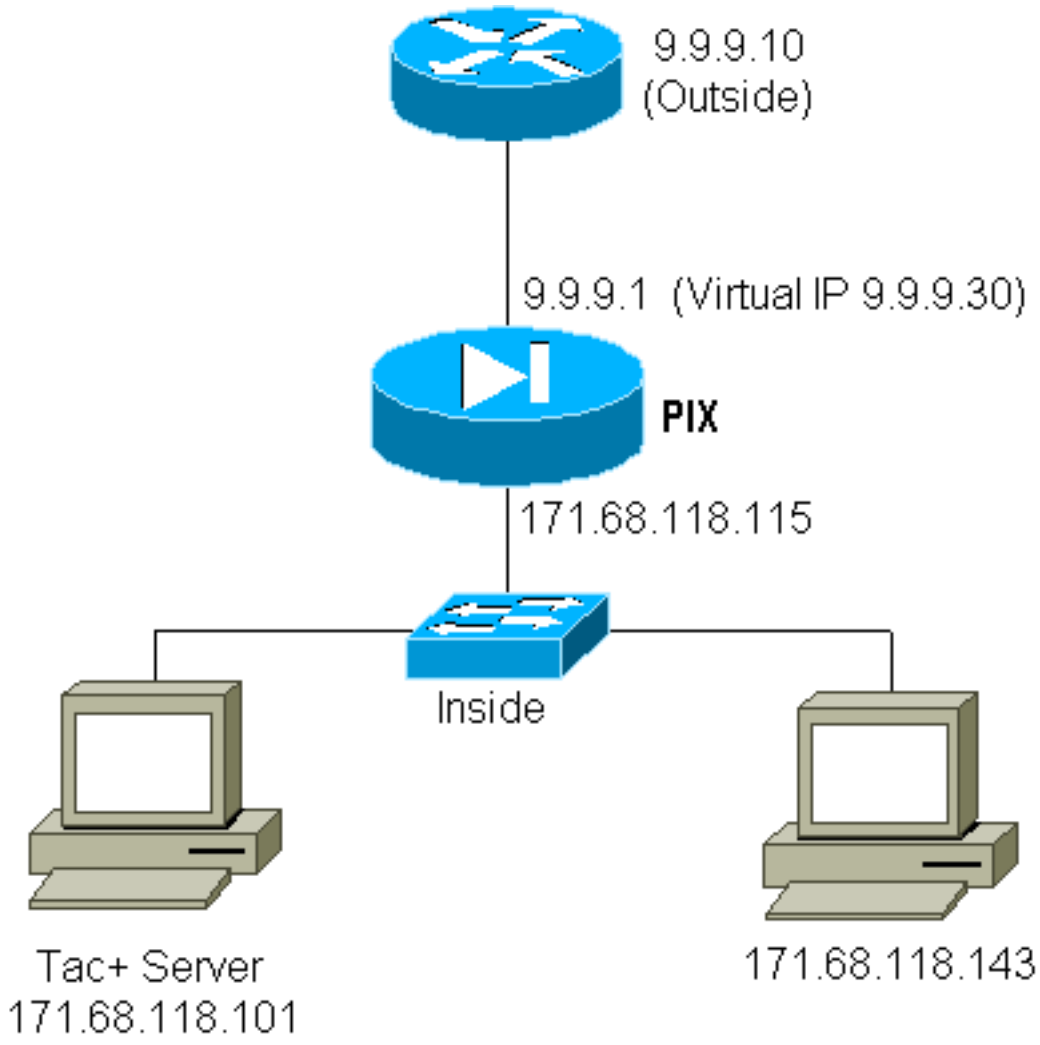
Aquí, el dispositivo 9.9.9.10 desea enviar tráfico TCP/49 al dispositivo en 171.68.118.106:

```
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

Dado que el tráfico saliente se permite de forma predeterminada, no se requiere ninguna estática para el uso de Telnet saliente virtual. En este ejemplo, el usuario interno en 171.68.118.143 Telnet a virtual 9.9.9.30 y se autentica. La conexión Telnet se interrumpe inmediatamente. Una

vez autenticado, el tráfico TCP se permite desde 171.68.118.143 al servidor en 9.9.9.10:



Configuración de PIX Virtual Telnet Saliente

```
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
```

PIX Debug Virtual Telnet Outbound

```
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 el usuario se conecta mediante Telnet a la IP de Telnet virtual, el comando **show uauth** muestra el uauth.

Si el usuario desea evitar que el tráfico pase después de que la sesión haya finalizado (cuando queda tiempo en la autenticación), el usuario necesita volver a conectarse a Telnet con la IP de Telnet virtual. Esto finaliza la sesión.

'Autorización del puerto

Puede requerir autorización en un rango de puertos. En este ejemplo, la autenticación aún era necesaria para todos los salientes, pero sólo se requería autorización 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 se realizó de 171.68.118.143 a 9.9.9.10, se produjo autenticación y autorización porque el puerto Telnet 23 está en el rango 23-49.

Cuando se realiza una sesión HTTP de 171.68.118.143 a 9.9.9.10, todavía tiene que autenticarse, pero el PIX no le pide al servidor TACACS+ que autorice 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
        }
        }
```

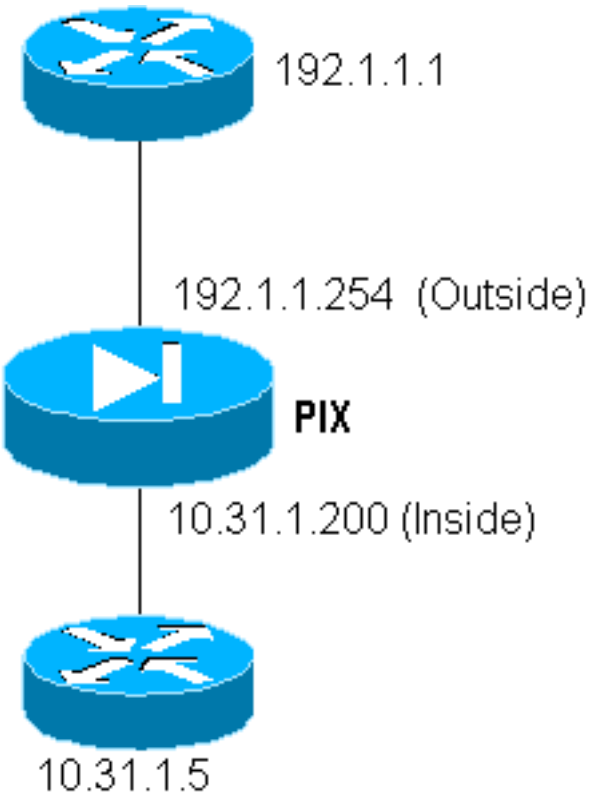
Observe que el PIX envía "`cmd=tcp/23-49`" y "`cmd-arg=9.9.9.10`" al servidor TACACS+.

Depuración en 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)
```

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

La versión 5.0 del software PIX cambia la funcionalidad de contabilización del tráfico. Los registros contables se pueden cortar para el tráfico que no sea HTTP, FTP y Telnet, una vez que se haya completado la autenticación.



Para TFTP-copiar un archivo desde el router externo (192.1.1.1) al router interno (10.31.1.5), agregue 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
```

Luego, Telnet del router externo en 192.1.1.1 a la IP virtual 192.1.1.30 y autentique a la dirección virtual que permite a UDP atravesar el PIX. En este ejemplo, el proceso **copy tftp flash** se inició de afuera hacia adentro:

```
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 **copy tftp flash** en el PIX (hubo tres durante esta copia del IOS), se corta un registro de contabilización y se envía al servidor de autenticación. A continuación se muestra un ejemplo de un registro TACACS en Cisco Secure 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