Configuraciones de Ejemplo de PIX, TACACS+ y RADIUS: 4.4.x

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 4.4.1 con respecto a la versión anterior incluyen: El servidor AAA agrupa y falla, autentica para habilitar y acceso a la consola serial, y acepta y rechaza los mensajes de solicitud.

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.

Suponga que tiene 100 usuarios dentro y que solo desea que 6 de estos usuarios puedan realizar FTP, Telnet o HTTP fuera de la red. Usted le diría al PIX que autentique el tráfico saliente y dé a los 6 ID de usuarios en el servidor de seguridad TACACS+/RADIUS. Con una autenticación simple, estos 6 usuarios podrían autenticarse con el nombre de usuario y la contraseña y luego salir. Los otros 94 usuarios no pudieron salir. El PIX solicita a los usuarios el nombre de usuario/contraseña, luego 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 pueden hacer FTP, Telnet o HTTP.

Pero supongamos que uno de estos tres usuarios, "Terry", no es de fiar. Le gustaría permitir a Terry hacer FTP, pero no HTTP o Telnet al exterior. Esto significa tener que agregar autorización, es decir, autorizar lo que los usuarios pueden hacer además de autenticar quiénes son. Cuando agregamos autorización al PIX, el PIX primero enviaría el nombre de usuario y la contraseña de Terry al servidor de seguridad y luego enviaría una solicitud de autorización informándole al servidor de seguridad qué "comando" Terry está tratando de hacer. Con el servidor configurado correctamente, a Terry se le podría permitir "FTP 1.2.3.4" pero se le negaría 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 activada:

- **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 – Se muestra una ventana en el navegador, 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. ¡Recuerde los nombres de usuario y contraseñas de la memoria caché del explorador. 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 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 de servidor de RADIUS UNIX CiscoSecure

Utilice la interfaz gráfica de usuario (GUI) avanzada 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
}
}
```

CiscoSecure NT 2.x RADIUS

Complete los siguientes pasos.

1. Obtenga una contraseña en la sección User Setup GUI (Configuración de usuario).
2. En la sección GUI de configuración de grupo, establezca el atributo 6 (Tipo de servicio) en Inicio de sesión o 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 el nuevo comando **Add/Edit** 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.

CiscoSecure 2.x TACACS+

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

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** para cada comando que desee permitir (por ejemplo, Telnet).
4. Si desea permitir Telnet a sitios específicos, introduzca las IP de permiso 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 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.

'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
```

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 .*
```

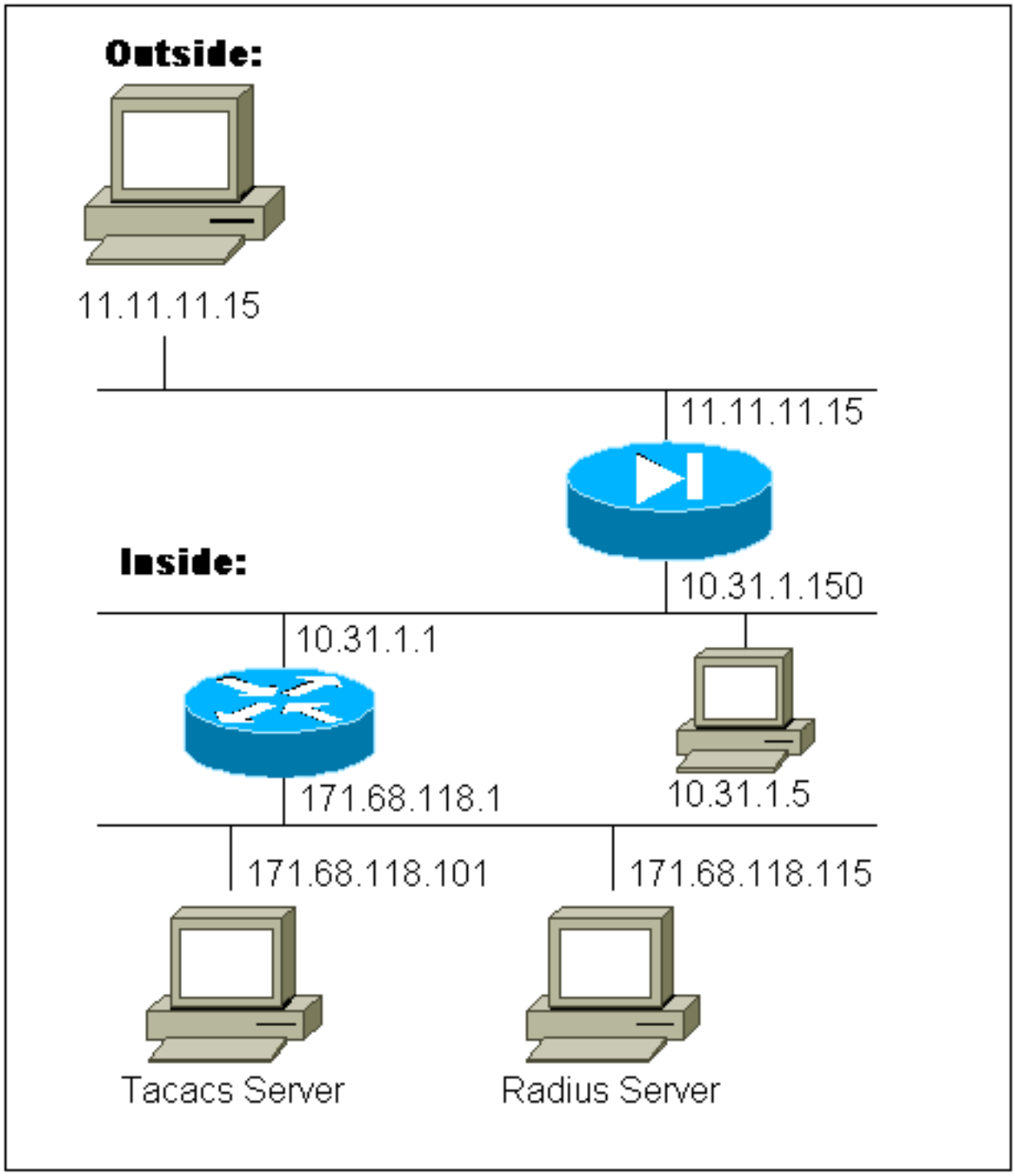
```
}
}

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

Pasos de depuración

- Asegúrese de que las configuraciones de PIX estén funcionando antes de agregar autenticación, autorización y contabilidad (AAA).Si no puede pasar tráfico antes de iniciar la autenticación y autorización, no podrá realizarlo luego.
- Habilite el registro en el PIX:El comando **logging console debugging** no se debe utilizar en un sistema con una carga excesiva.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
 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 de depuración:

Salientes

El usuario interno 10.31.1.5 inicia el tráfico hacia afuera 11.11.11.15 y se autentica a través de TACACS+ (el tráfico saliente utiliza la lista de servidores "Saliente" que incluye el servidor TACACS 171.68.118.101).

Entrante

El usuario externo en 11.11.11.15 inicia el tráfico hacia el interior 10.31.1.5 (11.11.11.22) y se autentica a través de RADIUS (el tráfico entrante utiliza la lista de servidores "Entrantes" que incluye el servidor RADIUS 171.68.118.15).

Depuración de PIX - Buena autenticación - TACACS+

El siguiente ejemplo muestra la depuración PIX con una 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 - Autenticación incorrecta (nombre de usuario o contraseña) - TACACS+

El siguiente ejemplo muestra la depuración PIX con autenticación incorrecta (nombre de usuario o contraseña). El usuario ve cuatro conjuntos de nombre de usuario/contraseña. Se muestra el 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 - Can Ping pero no Response - TACACS+

El siguiente ejemplo muestra la depuración PIX para un servidor que hace ping y que no habla con el PIX. El usuario ve el nombre de usuario una vez y el PIX nunca solicita una contraseña (esto 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
```

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

El siguiente ejemplo muestra la depuración PIX para un servidor que no es susceptible de ping. El usuario verá el nombre de usuario una vez. PIX nunca solicita una contraseña (esto está en Telnet). Se muestra el siguiente mensaje: "Tiempo de espera para el servidor TACACS+" y "Error: Número máximo de intentos excedidos" (la configuración en este ejemplo refleja un servidor falso).

```
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
```

Depuración PIX - Autenticación correcta - RADIUS

El siguiente ejemplo muestra el debug PIX con una buena autenticación:

```
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
```

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

El siguiente ejemplo muestra la depuración PIX con autenticación incorrecta (nombre de usuario o contraseña). El usuario ve una solicitud de nombre de usuario y contraseña. Si uno de los dos está equivocado, el mensaje "Contraseña incorrecta" se muestra cuatro veces. A continuación, se desconecta al usuario. Este problema se ha asignado al 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
```

Depuración de PIX - Deamon Down, no se comunicará con PIX - RADIUS

El siguiente ejemplo muestra la depuración PIX con un servidor que puede hacer ping, pero el

demonio está inactivo. El servidor no se comunicará con PIX. El usuario ve el nombre de usuario seguido de la contraseña. Se muestran los siguientes mensajes: "Error en el servidor RADIUS" y "Error: Se ha superado el número máximo de intentos".

```
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
```

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

El siguiente ejemplo muestra la depuración de PIX para un servidor que no puede hacer ping o donde hay una discordancia de clave/cliente. El usuario ve el nombre de usuario y la contraseña. Se muestran los siguientes mensajes: "Timeout to RADIUS server" y "Error: Se ha superado el número máximo de intentos" (el servidor de la configuración es sólo para fines de ejemplo).

```
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

Como la autorización no es válida sin autenticación, requeriremos autorización para el mismo rango de origen y 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 autorización para "entrante" porque el tráfico entrante se autentica con RADIUS y la autorización RADIUS no es válida

Ejemplos de Depuración de Autenticación y Autorización de PIX

Depuración PIX con autenticación correcta y autorización exitosa - TACACS+

El siguiente ejemplo muestra el debug PIX con una buena autenticación y 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)
```

Depuración PIX - Autenticación correcta, Autorización fallida - TACACS+

El siguiente ejemplo muestra la depuración PIX con una autenticación correcta, pero con una autorización fallida:

Aquí el usuario también ve el mensaje "Error: Autorización denegada"

```
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
```

La depuración se mostrará igual si la contabilización está activada o desactivada. Sin embargo, en el momento del "Construido", se enviará un registro contable de "inicio". En el momento de la "Teardown", se enviará un registro contable "stop".

Los registros contables TACACS+ son similares a los siguientes (estos son de CiscoSecure UNIX; los de CiscoSecure NT pueden estar delimitados por comas en su lugar):

```
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
```

La depuración se mostrará 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 contabilización RADIUS son similares a los siguientes: (son de CiscoSecure UNIX; los de CiscoSecure NT pueden estar delimitados por comas en su lugar):

```
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 un origen o destino en particular no necesita autenticación, autorización o contabilidad, podemos hacer algo como lo 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 está "exceptuando" las direcciones ip de la autenticación y tiene autorización activada, también debe exceptuarlas 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 sigue conectada (es decir, 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 el siguiente ejemplo, se utiliza una configuración de red diferente pero los conceptos son los mismos.

El usuario envía telnets 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 mostrará 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 rechazará la conexión.

El usuario continúa con su 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.

Sin embargo, HTTP funciona de manera diferente debido a la naturaleza del protocolo. A continuación se 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 un segundo (es decir: hubo menos de un segundo entre el registro inicial y el registro de parada). ¿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, 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 discusión anterior se refería a la autenticación del tráfico Telnet (y HTTP, FTP) a través del PIX. En el siguiente ejemplo, nos aseguramos de que Telnet to the pix funcione sin autenticación en:

```
telnet 10.31.1.5 255.255.255.255
passwd ww
```

Luego, agregamos el comando para autenticar a los usuarios de Telnet al PIX:

```
aaa authentication telnet console Outgoing
```

Cuando los usuarios se conectan mediante Telnet al PIX, se les solicita la contraseña de Telnet ("ww"). El PIX también solicita el TACACS+ en este caso (ya que se utiliza la lista de servidores "salientes") o el nombre de usuario y la contraseña RADIUS.

```
aaa authentication enable console Outgoing
```

Con este comando, se le solicita al usuario un nombre de usuario y una contraseña que se envía al servidor TACACS o RADIUS. En este caso, dado que se utiliza la lista de servidores "salientes", la solicitud va al servidor TACACS. Dado que el paquete de autenticación para habilitar es el mismo que el paquete de autenticación para el login, el usuario puede habilitar a través de TACACS o RADIUS con el mismo nombre de usuario/contraseña, suponiendo que el usuario pueda iniciar sesión en el PIX con TACACS o RADIUS. Este problema se ha asignado al ID de bug #CSCdm47044.

En el caso de que el servidor esté inactivo, el usuario puede obtener acceso al modo de habilitación PIX ingresando "PIX" para el nombre de usuario y la contraseña de habilitación normal desde el PIX ("habilitar contraseña cualquiera"). Si "habilitar contraseña lo que sea" no está en la configuración de PIX, el usuario debe ingresar "PIX" para el nombre de usuario y presionar la tecla Intro. Si se establece la contraseña de activación pero no se conoce, se necesitará un disco de recuperación de contraseña para restablecer.

Autenticación en la consola serie

El comando **aaa authentication serial console** requiere verificación de autenticación para acceder a la consola serial del PIX. Cuando el usuario ejecuta comandos de configuración desde la consola, se cortarán los mensajes de syslog (si el PIX está configurado para enviar syslog en el nivel de depuración a un host de syslog). A continuación se muestra un ejemplo del servidor 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 atraviesan 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, a continuación, al llegar al cuadro de destino final, se muestra el mensaje "Nombre de usuario:" y "Contraseña:" en el cuadro de destino.

Este mensaje sólo afecta a los usuarios que pasan a través del PIX, no al PIX.

Nota: No hay registros contables 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 lo siguiente en un login fallido/exitoso a través del 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

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 deben tener el mismo "timeout uauth", ¡entonces no implemente esto! Pero, si necesita distintos usuarios 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 se autentica, no tendrá que volver a autenticarse durante 3 horas. Pero si configuramos un usuario con el siguiente perfil y tenemos 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 o no la reautenticación.

```
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 tendrá que volver a autenticarse cuando regrese 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.

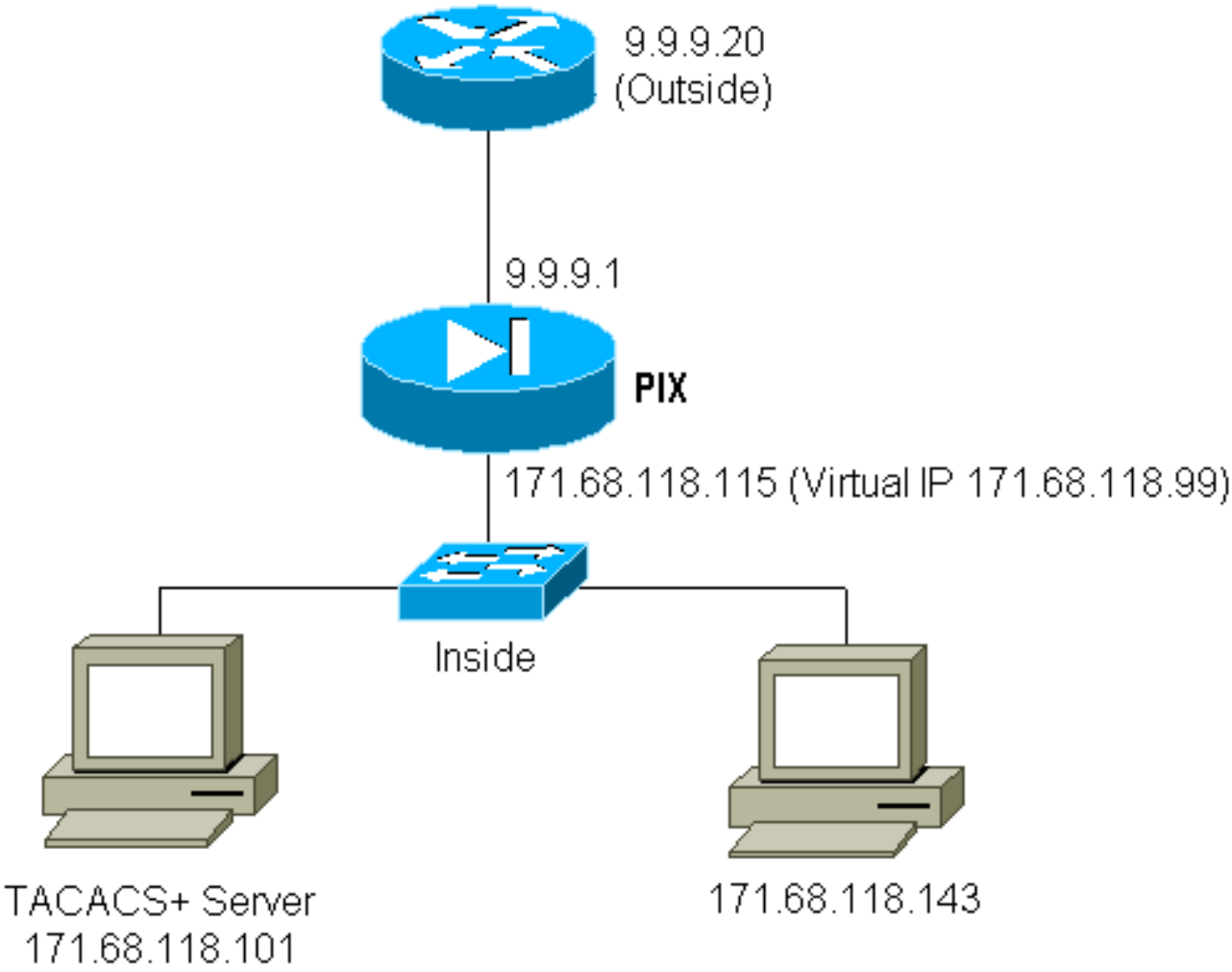
Para evitar esto, puede implementar HTTP virtual agregando una dirección RFC 1918 (es decir, una dirección que no se puede rutear en Internet, pero que es válida y única para la red interna PIX) a la configuración PIX usando el siguiente comando:

```
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 establezca la duración del comando **timeout uauth** en 0 segundos con HTTP virtual; esto impide que se realicen conexiones HTTP al servidor Web real.

Ejemplo de HTTP saliente virtual:



Salida HTTP virtual de 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 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, 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, el syslog PIX para protocolos no autenticables mostrará mensajes como:

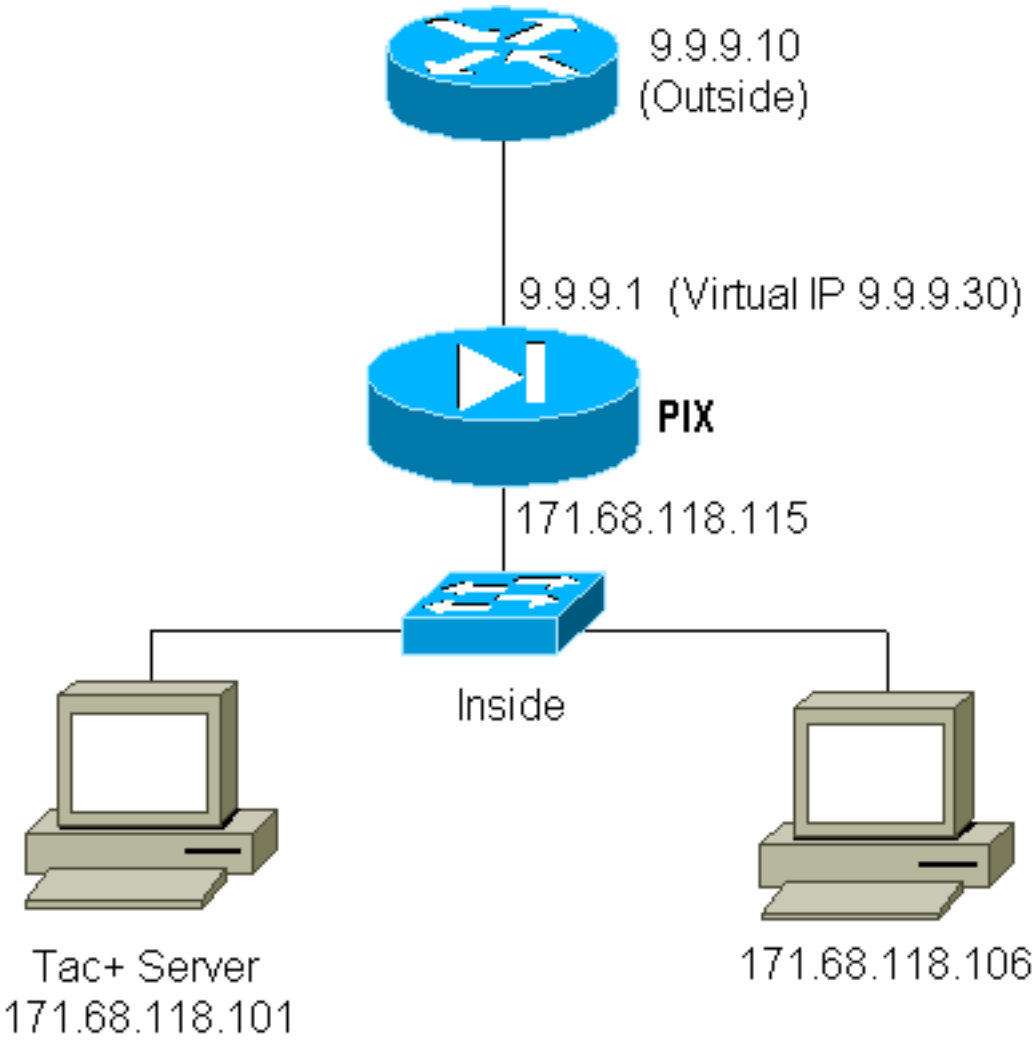
```
109001: Auth start for user '???' from 9.9.9.10/11094 to 171.68.118.106/25
109009: Authorization denied from 171.68.118.106/49 to 9.9.9.10/11094
(not authenticated
```

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).

Pero si realmente hay una necesidad 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 que está asociado a la IP virtual.

En nuestro ejemplo, queremos permitir que el tráfico del puerto TCP 49 fluya desde el host externo 9.9.9.10 al host interno 171.68.118.106. Dado que este tráfico no es realmente autenticable, configuramos Telnet virtual.

Entrada 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) 9.9.9.30 171.68.118.106 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
```

Configuración del usuario del servidor TACACS+ Virtual Telnet entrante:

```
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 9.9.9.30 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 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
```

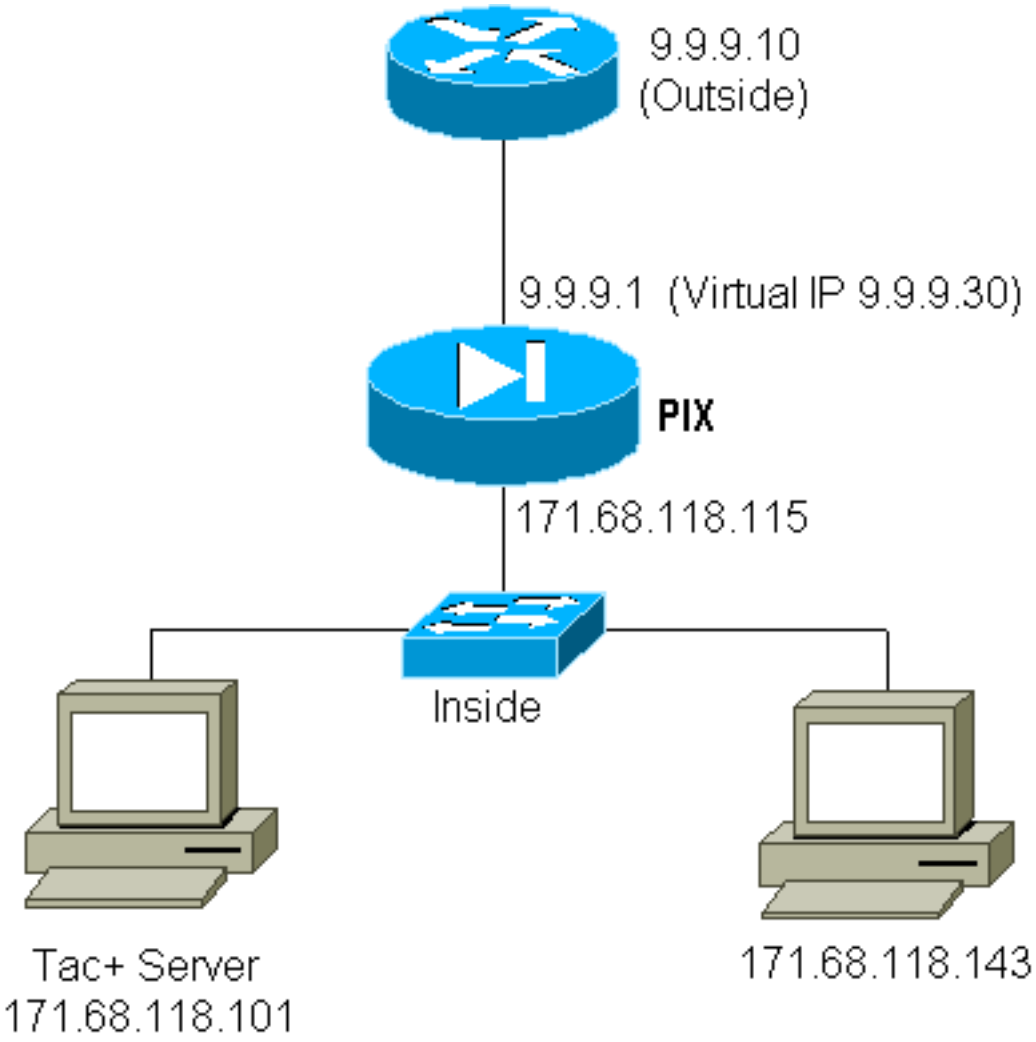
Y cuando el dispositivo 9.9.9.10 desea enviar tráfico TCP/49 al dispositivo en 171.68.118.106:

```
pixfirewall# 109001: Auth start for user 'pinecone'
 from 9.9.9.10/11104 to 171.68.118.106/49
 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)
```

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 el siguiente ejemplo, el usuario interno en 171.68.118.143 realizará Telnet a virtual 9.9.9.30 y se autenticará. 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 Telnet 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 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
```

Salida de Telnet Virtual de Debug PIX:

```
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 su uauth. Si el usuario desea evitar que el tráfico pase después de que finalice la sesión (cuando queda tiempo en la autenticación), 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 el siguiente ejemplo, la autenticación aún era necesaria para todos los salientes, pero la autorización sólo se requiere 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 Outgoing
aaa authorization tcp/23-49 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
```

Por lo tanto, cuando realizamos Telnet desde 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 hacemos una sesión HTTP de 171.68.118.143 a 9.9.9.10, todavía tenemos que autenticarnos, 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 está enviando "cmd=tcp/23-49" y "cmd-arg=9.9.9.10" al servidor TACACS+.

Depuración 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