Realización de autenticación, autorización y contabilidad de usuarios por medio de las versiones 5.2 y posteriores de PIX.

Contenido

Introducción

La autenticación RADIUS y TACACS+ se puede realizar para conexiones FTP, Telnet y HTTP a través de Cisco Secure PIX Firewall. La autenticación para otros protocolos menos comunes generalmente se hace para funcionar. Se admite la autorización TACACS+. No se admite la autorización RADIUS. Los cambios en la autenticación, autorización y contabilidad (AAA) de PIX 5.2 con respecto a la versión anterior incluyen el soporte de la lista de acceso AAA para controlar quién está autenticado y a qué recursos accede el usuario. En PIX 5.3 y versiones posteriores, el cambio de autenticación, autorización y contabilidad (AAA) con respecto a las versiones anteriores del código es que los puertos RADIUS son configurables.

Nota: PIX 6.x puede realizar la contabilización del tráfico de paso pero no del tráfico destinado al PIX.

Prerequisites

Requirements

No hay requisitos previos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Versiones 5.2.0.205 y 5.2.0.207 del software de Cisco Secure PIX Firewall

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Nota: Si ejecuta el software PIX/ASA versión 7.x y posteriores, consulte Configuración de los Servidores AAA y la Base de Datos Local.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Autenticación, autorización y contabilidad

A continuación se ofrece una explicación de Autenticación, Autorización y Contabilización:

- La autenticación es quién es el usuario.
- La autorización es lo que hace el usuario.
- La autenticación es válida sin autorización.
- La autorización no es válida sin autenticación.
- Contabilización es lo que hizo el usuario.

Qué ve el usuario con la autenticación/autorización activada

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

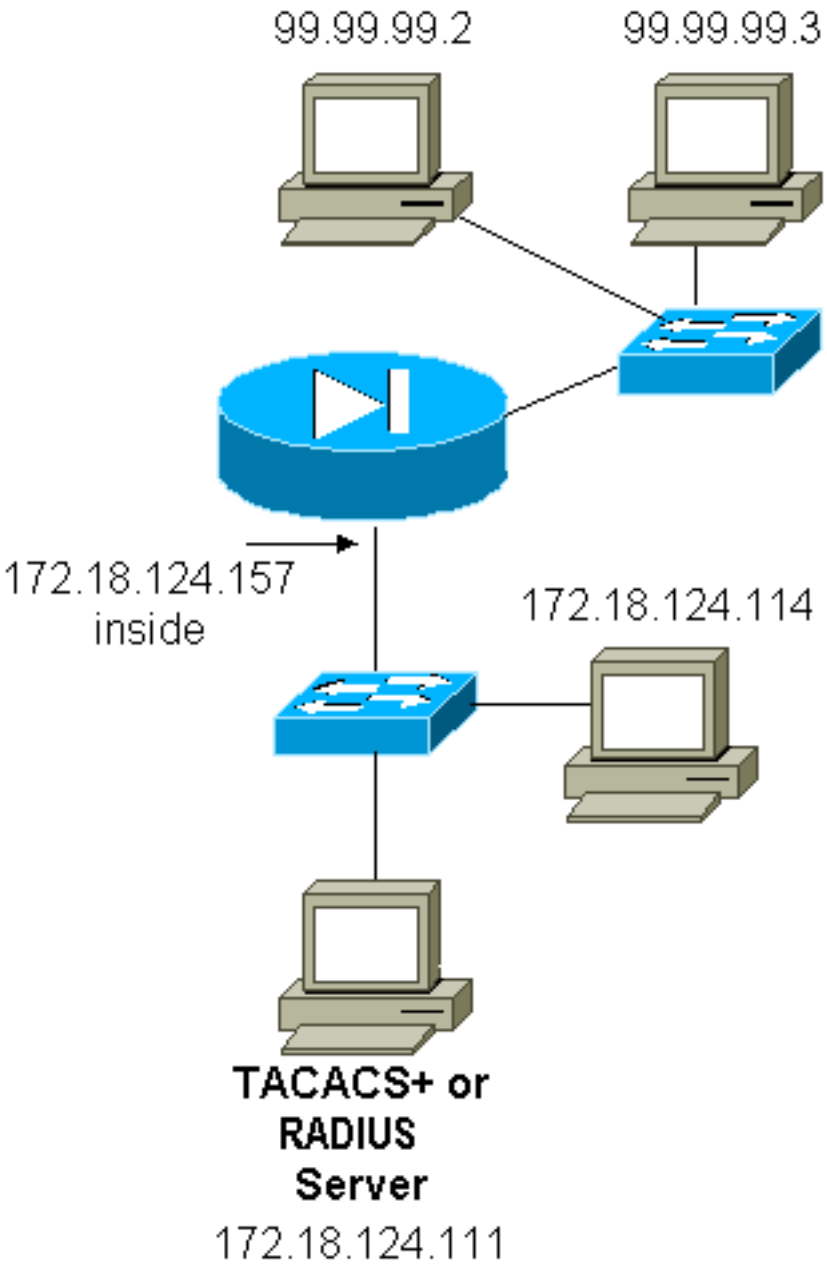
- **Telnet**: el usuario ve que aparece un mensaje de nombre de usuario y luego una solicitud de contraseña. Si la autenticación (y autorización) resulta exitosa en el PIX/servidor, el siguiente host de destino le pide al usuario el nombre de usuario y contraseña.
- **FTP**: el usuario ve que aparece 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 "local_username" y la "local_password" al servidor de seguridad local. Si la autenticación (y autorización) se realiza correctamente en el PIX/servidor, el "remote_username" y "remote_password" se pasan al servidor FTP de destino más allá.
- **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 parece que el PIX debería agotar el tiempo de una conexión HTTP pero no lo hace, es probable que la reautenticación se lleve a cabo realmente con el navegador "disparando" el nombre de usuario y la contraseña almacenados en la memoria caché al PIX. El PIX reenvía esto al servidor de autenticación. PIX syslog y/o server debug muestran este fenómeno. Si Telnet y FTP parecen funcionar "normalmente", pero las conexiones HTTP no, esta es la razón.

Pasos de depuración

- Asegúrese de que la configuración PIX funcione antes de agregar autenticación y autorización AAA. Si no puede pasar tráfico antes de iniciar la autenticación y autorización, no podrá hacerlo después.
- Habilite algún tipo de registro en el PIX.Ejecute el comando **logging console debug** para activar el debugging de la consola de registro.**Nota:** No utilice el debugging de consola de registro en un sistema cargado con fuerza.Utilice el comando logging monitor debug para iniciar una sesión Telnet.Se puede utilizar la depuración guardada en la memoria intermedia del registro y luego ejecutar el comando show logging.El registro también se puede enviar a un servidor syslog y ser examinado allí.
- Activar la depuración en los servidores TACACS+ o RADIUS.

Sólo autenticación

Diagrama de la red



Configuración del servidor – Sólo autenticación

Configuración del servidor TACACS de Cisco Secure UNIX

```
User = cse {
password = clear "cse"
default service = permit
}
```

Configuración del servidor RADIUS de Cisco Secure UNIX

Nota: Agregue la dirección IP y la clave PIX a la lista Servidor de acceso a la red (NAS) con la

ayuda de la GUI avanzada.

```
user=bill {
radius=Cisco {
check_items= {
2="foo"
}
reply_attributes= {
6=6
}
}
}
```

Cisco Secure Windows RADIUS

Utilice estos pasos para configurar un servidor RADIUS de Cisco Secure Windows.

1. Obtenga una contraseña en la sección **Configuración del usuario**.
2. Desde la sección de Group Setup (Configuración de grupo), establezca el atributo 6 (Tipo de servicio) a Login (Ingreso) o Administrative (Administrativo).
3. Agregue la dirección IP del PIX en la sección de Configuración del GUI.

Cisco Secure Windows TACACS+

El usuario obtiene una contraseña en la sección User Setup (Configuración de usuario)

'Configuración del servidor Livingston RADIUS'

Nota: Agregue la dirección IP y la clave PIX al archivo *de clientes*.

- bill Password="foo" User-Service-Type = Shell-User

Configuración del servidor Merit RADIUS

Nota: Agregue la dirección IP y la clave PIX al archivo *de clientes*.

- contraseña de facturación = "foo" tipo de servicio = usuario de shell

Configuración del servidor freeware TACACS+

```
key = "cisco"
user = cse {
login = cleartext "cse"
default service = permit
}
```

Configuración inicial de PIX – Sólo autenticación

Configuración inicial de PIX – Sólo autenticación
`PIX Version 5.2(0)205`

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd OnTrBUG1Tp0edmkr encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
!
!--- These lines are necessary !--- if the new feature
in 5.2 is used to define which !--- target/source IP
addresses are to be authenticated. access-list 101
permit tcp any any eq telnet
access-list 101 permit tcp any any eq ftp
access-list 101 permit tcp any any eq www
!
pager lines 24
logging on
no logging timestamp
no logging standby
logging console debugging
no logging monitor
no logging buffered
logging trap debugging
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 10baset
mtu outside 1500
mtu inside 1500
ip address outside 99.99.99.1 255.255.255.0
ip address inside 172.18.124.157 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
global (outside) 1 99.99.99.10-99.99.99.20 netmask
255.255.255.0
nat (inside) 1 172.18.124.0 255.255.255.0 0 0
static (inside,outside) 99.99.99.99 172.18.124.114
netmask 255.255.255.255 0 0
conduit permit tcp any any
conduit permit udp any any
conduit permit icmp any any
route inside 172.18.0.0 255.255.0.0 172.18.124.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h323 0:05:00
si p 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
!
!--- For the purposes of illustration, the TACACS+
process is used !--- to authenticate inbound users and
RADIUS is used to authenticate outbound users. aaa-
```

```
server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server AuthInbound protocol tacacs+
aaa-server AuthInbound (inside) host 172.18.124.111
cisco timeout 5
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 172.18.124.111
cisco timeout 5
!
!--- The next six statements are used to authenticate
all inbound !--- and outbound FTP, Telnet, and HTTP
traffic. aaa authentication include ftp outside 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authentication include telnet outside 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authentication include http outside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0
   AuthInbound
aaa authentication include http inside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0
   AuthOutbound
aaa authentication include telnet inside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0
   AuthOutbound
aaa authentication include ftp inside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0
   AuthOutbound
!
!--- OR the new 5.2 feature allows these two statements
in !--- conjunction with access-list 101 to replace the
previous six statements. !--- Note: Do not mix the old
and new verbiage.

aaa authentication match 101 outside AuthInbound
aaa authentication match 101 inside AuthOutbound
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
no sysopt route dnat
isakmp identity hostname
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:5882f514247589d784a0d74c800907b8
: end
```

Puertos RADIUS configurables (5.3 y posteriores)

Algunos servidores RADIUS utilizan puertos RADIUS diferentes a 1645/1646 (generalmente 1812/1813). En PIX 5.3 y posteriores, los puertos de autenticación y contabilización RADIUS se pueden cambiar a algo distinto del 1645/1646 predeterminado con estos comandos:

```
aaa-server radius-authport #
aaa-server radius-acctport #
```

Ejemplos de errores de depuración de autenticación PIX

Consulte Pasos de depuración para obtener información sobre cómo activar la depuración. Estos son ejemplos de un usuario en 99.99.99.2 que inicia el tráfico al interior 172.18.124.114 (99.99.99.99) y viceversa. El tráfico entrante es autenticado por TACACS y el saliente es autenticado por RADIUS.

Autenticación exitosa - TACACS+ (entrante)

```
109001: Auth start for user '???' from 99.99.99.2/11003 to 172.18.124.114/23
109011: Authen Session Start: user 'cse', sid 2
109005: Authentication succeeded for user 'cse' from 172.18.124.114/23
  to 99.99. 99.2/11003 on interface outside
302001: Built inbound TCP connection 4 for faddr 99.99.99.2/11003
  gaddr 99.99.99 .99/23 laddr 172.18.124.114/23 (cse)
```

Falló la autenticación debido a nombre de usuario/contraseña incorrecto - TACACS+ (entrante). El usuario ve "Error: Se ha superado el número máximo de intentos".

```
109001: Auth start for user '???' from 99.99.99.2/11004 to 172.18.1 24.114/23
109006: Authentication failed for user '' from 172.18.124.114/23
  to 99.99.99.2/1 1004 on interface outside
```

El servidor no se está comunicando con PIX - TACACS+ (entrante). El usuario ve el nombre de usuario una vez y el PIX nunca pide una contraseña (esto pasa en Telnet). El usuario ve "Error: Se ha superado el número máximo de intentos".

```
109001: Auth start for user '???' from 99.99.99.2/11005 to 172.18.124.114/23
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
  (server 172.18.12 4.111 failed) on interface outside
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
  (server 172.18.12 4.111 failed) on interface outside
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
  (server 172.18.12 4.111 failed) on interface outside
109006: Authentication failed for user '' from 172.18.124.114/23
  to 99.99.99.2/1 1005 on interface outside
```

Autenticación correcta - RADIUS (saliente)

```
109001: Auth start for user '???' from 172.18.124.114/35931 to 99.99.99.2/23
109011: Authen Session Start: user 'bill', Sid 0
109005: Authentication succeeded for user 'bill' from 172.18.124.114/35931
  to 99 .99.99.2/23 on interface inside
```

Autenticación errónea (nombre de usuario o contraseña) - RADIUS (salida). El usuario ve la solicitud de nombre de usuario y, a continuación, la contraseña, tiene tres oportunidades para introducirlas y, si no se realiza correctamente, consulte "Error: Se ha superado el número máximo de intentos".

```
109001: Auth start for user '???' from 172.18.124.114/35932 to 99.99.99.2/23
109002: Auth from 172.18.124.114/35932 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109006: Authentication failed for user '' from 172.18.124.114/35932
  to 99.99.99. 2/23 on interface inside
```

Se puede hacer ping al servidor pero el demonio no responde, no se puede hacer ping al servidor o la clave y el cliente no coinciden; no se establecerá la comunicación con PIX - RADIUS (saliente). El usuario ve Username, luego password, luego "el servidor RADIUS falló" y, finalmente, "Error: Se ha superado el número máximo de intentos".

```
109001: Auth start for user '???' from 172.18.124.114/35933 to 99.99.99.2/23
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109006: Authentication failed for user '' from 172.18.124.114/35933
  to 99.99.99. 2/23 on interface inside
```

Autenticación más autorización

Si desea permitir que todos los usuarios autenticados realicen todas las operaciones (HTTP, FTP y Telnet) a través del PIX, la autenticación es suficiente y no se necesita autorización. Sin embargo, si desea permitir algunos subconjuntos de servicios a determinados usuarios o limitar el acceso de los usuarios a determinados sitios, se necesita autorización. La autorización RADIUS no es válida para el tráfico a través del PIX. La autorización TACACS+ es válida en este caso.

Si la autenticación pasa y la autorización está activada, el PIX envía el comando que el usuario está haciendo al servidor. Por ejemplo, "http 1.2.3.4." En la versión 5.2 de PIX, la autorización TACACS+ se utiliza junto con las listas de acceso para controlar a dónde van los usuarios.

Si desea implementar la autorización para HTTP (sitios web visitados), utilice software como Websense, ya que un solo sitio web puede tener un gran número de direcciones IP asociadas.

Configuración del servidor – Autenticación más autorización

Configuración del servidor TACACS de Cisco Secure UNIX

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

  user = can_only_do_ftp {
  password = clear "*******"
  service = shell {
  cmd = ftp {
  permit .*
  }
  }
  }

  user = httponly {
  password = clear "********"
  service = shell {
```

```
  cmd = http {
  permit .*
  }
  }
  }
```

Cisco Secure Windows TACACS+

Complete estos pasos para configurar un servidor Cisco Secure Windows TACACS+.

1. Haga clic en **Denegar comandos IOS no coincidentes** en la parte inferior de Group Setup.
2. Haga clic en **Add/Edit New Command (FTP, HTTP, Telnet)**.Por ejemplo, si desea permitir Telnet a un sitio específico ("telnet 1.2.3.4"), el comando es **telnet**. El argumento es *1.2.3.4* . Luego de completar "command=telnet," complete la dirección IP "permit" (permitidas) en el rectángulo Argument (Argumento) (por ejemplo, "permit 1.2.3.4"). Si se llegasen a permitir todos los Telnets, el comando todavía es telnet, pero haga clic en Allow all unlisted arguments (Permitir todos los argumentos no detallados). A continuación, haga clic en **Finalizar el comando de edición**.
3. Realice el paso 2 para cada uno de los comandos permitidos (por ejemplo, Telnet, HTTP y FTP).
4. Agregue la dirección IP de PIX en la sección Configuración de NAS con la ayuda de la GUI.

Configuración del servidor freeware TACACS+

```
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 .*
   }
   }
```

Configuración de PIX - Adición de autorización

Agregar comandos para solicitar autorización:

```
aaa authorization include telnet outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authorization include http outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authorization include ftp outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

```
AuthInbound
```

La nueva función 5.2 permite que esta instrucción junto con la lista de acceso 101 definida previamente reemplace las tres sentencias anteriores. No deberían mezclarse la verbiage anterior y la nueva.

```
aaa authorization match 101 outside AuthInbound
```

Ejemplos de depuración de autorización y autenticación PIX

Autenticación y autorización correctas - TACACS+

```
109001: Auth start for user '???' from
   99.99.99.2/11010 to 172.18.124.114/23
109011: Authen Session Start: user 'cse', Sid 3
109005: Authentication succeeded for user
   'cse' from 172.18.124.114/23 to 99.99.99.2/11010
   on interface outside
109011: Authen Session Start: user 'cse', Sid 3
109007: Authorization permitted for user 'cse'
   from 99.99.99.2/11010 to 172.18.1  24.114/23
   on interface outside
302001: Built inbound TCP connection 2 for faddr
   99.99.99.2/11010 gaddr 99.99.99.99/23 laddr
   172.18.124.114/23 (cse)
```

Buena autenticación, pero hay una falla de autorización TACACS+ El usuario también ve el mensaje "Error: Autorización denegada".

```
109001: Auth start for user '???' from
   99.99.99.2/11011 to 172.18.124.114/23
109011: Authen Session Start: user 'httponly', Sid 4
109005: Authentication succeeded for user 'httponly'
   from 172.18.124.114/23 to  9 9.99.99.2/11011
   on interface outside
109008: Authorization denied for user 'httponly'
   from 172.18.124.114/23 to 99.99.99.2/11011
   on interface outside
```

Nueva función Access List (Lista de accesos)

En la versión 5.2 y posteriores del software PIX, defina las listas de acceso en el PIX. Aplíquelas por usuario en función del perfil de usuario del servidor. TACACS+ requiere autenticación y autorización. RADIUS sólo requiere autenticación. En este ejemplo, se cambia la autenticación y autorización de salida a TACACS+ . Se configura una lista de acceso en el PIX.

Nota: En la versión 6.0.1 y posteriores de PIX, si utiliza RADIUS, las listas de acceso se implementan ingresando la lista en el atributo estándar RADIUS 11 (Filter-Id) [CSCdt50422] de IETF. En este ejemplo, el atributo 11 se establece en 115 en lugar de hacer la versión específica del proveedor "acl=115".

Configuración de PIX

```
access-list 115 permit tcp any host 99.99.99.2 eq telnet
access-list 115 permit tcp any host 99.99.99.2 eq www
access-list 115 permit tcp any host 99.99.99.2 eq ftp
access-list 115 deny tcp any host 99.99.99.3 eq www
access-list 115 deny tcp any host 99.99.99.3 eq ftp
access-list 115 deny tcp any host 99.99.99.3 eq telnet
```

Perfiles del servidor

Nota: La versión 2.1 del software gratuito TACACS+ no reconoce el verbiage "acl".

Configuración del servidor Cisco Secure UNIX TACACS+

```
user = pixa{
  password = clear "*********"
  service=shell {
  set acl=115
  }
  }
```

Cisco Secure Windows TACACS+

Para agregar autorización al PIX para controlar dónde el usuario va con las listas de acceso, verifique **shell/exec**, marque la **lista de control de acceso** y complete el número (coincide con el número de lista de acceso en el PIX).

Cisco Secure UNIX RADIUS

```
user = pixa{
  password = clear "*********"
  radius=Cisco {
  reply_attributes= {
  9,1="acl=115"
  }
  }
  }
```

Cisco Secure Windows RADIUS

El tipo de dispositivo es RADIUS/Cisco El usuario "pixa" necesita un nombre de usuario, una contraseña y una marca y "acl=115" en el cuadro rectangular de Cisco/RADIUS donde dice 009\001 AV-Pair (específico del proveedor).

Resultado

El usuario saliente "pixa" con "acl=115" en el perfil autentica y autoriza. El servidor pasa el acl=115 al PIX, y el PIX muestra lo siguiente:

```
pixfirewall#show uauth
                        Current    Most Seen
```

```
Authenticated Users       1          2
Authen In Progress        0          2
user 'pixa' at 172.18.124.114, authenticated
   access-list 115
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

Cuando el usuario "pixa" intenta ir a 99.99.99.3 (o cualquier dirección IP excepto 99.99.99.2, porque hay una negación implícita), el usuario ve lo siguiente:

```
Error: acl authorization denied
```

Nueva lista de acceso por usuario descargable con versión 6.2

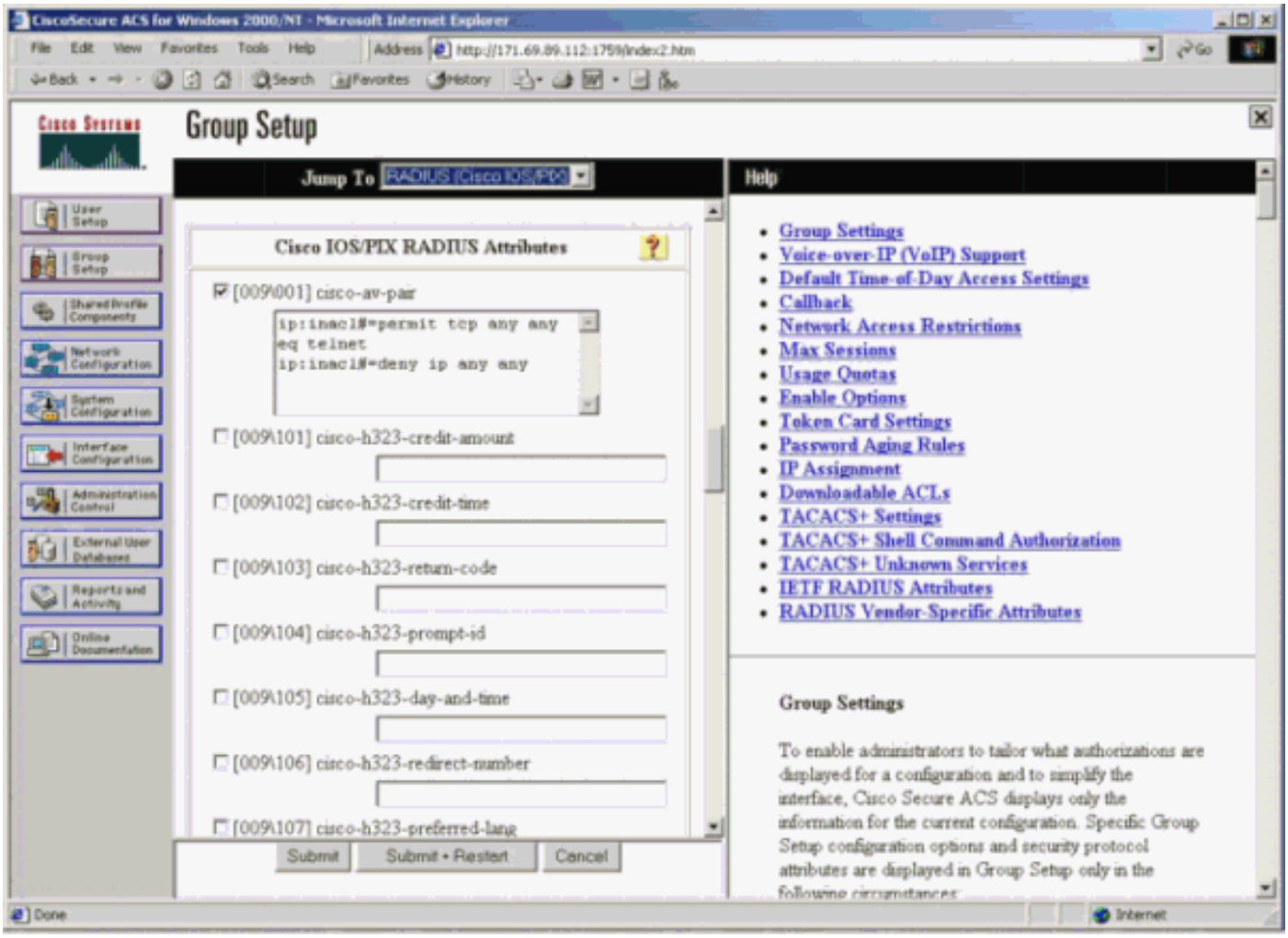
En la versión de software 6.2 y posteriores del Firewall PIX, las listas de acceso se definen en un servidor de control de acceso (ACS) para descargar al PIX después de la autenticación. Esto sólo funciona con el protocolo RADIUS. No es necesario configurar la lista de acceso en el PIX. Se aplica una plantilla de grupo a varios usuarios.

En versiones anteriores, la lista de acceso se define en el PIX. Después de la autenticación, el ACS empujó el nombre de la lista de acceso al PIX. La nueva versión permite al ACS enviar la lista de acceso directamente al PIX.

Nota: Si se produce una conmutación por fallas, la tabla uauth no se copia. Los usuarios se vuelven a autenticar. La lista de acceso se descarga de nuevo.

Configuración de ACS

Haga clic en **Group Setup** y seleccione el tipo de dispositivo **RADIUS (Cisco IOS/PIX)** para configurar una cuenta de usuario. Asigne un nombre de usuario ("cse", en este ejemplo) y una contraseña para el usuario. En la lista Atributos, seleccione la opción para configurar **[009\001]** ***proveedor-av*-par**. Defina la lista de acceso como se muestra en este ejemplo:



Depuración de PIX: Autenticación válida y lista de acceso descargada

- Permite sólo Telnet y niega otro tráfico.

```
pix# 305011: Built dynamic TCP translation from inside:
  172.16.171.33/11063 to outside:172.16.171.201/1049
109001: Auth start for user '???' from 172.16.171.33/11063
   to 172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 10
109005: Authentication succeeded for user 'cse'
   from 172.16.171.33/11063
   to 172.16.171.202/23 on interface inside

302013: Built outbound TCP connection 123 for outside:
   172.16.171.202/23 (172.16.171.202/23) to inside:
   172.16.171.33/11063 (172.16.171.201/1049) (cse)
```

Salida del comando **show uauth**.

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list AAA-user-cse
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
```

Salida del comando **show access-list**.

```
pix#show access-list
access-list AAA-user-cse; 2 elements
access-list AAA-user-cse permit tcp any any eq telnet (hitcnt=1)
access-list AAA-user-cse deny ip any any (hitcnt=0)
```

- Niega solo Telnet y permite otro tráfico.

```
pix# 305011: Built dynamic TCP translation from inside:
   172.16.171.33/11064 to outside:172.16.171.201/1050
109001: Auth start for user '???' from 172.16.171.33/11064 to
   172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 11
109005: Authentication succeeded for user 'cse'
   from 172.16.171.33/11064
   to 172.16.171.202/23 on interface inside
109015: Authorization denied (acl= AAA-user-cse) for user 'cse'
  from 172.16.171.33/11064 to 172.16.171.202/23 on interface inside
```

Salida del comando **show uauth**.

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list AAA-user-cse
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
```

Salida del comando **show access-list**.

```
pix#show access-list
access-list AAA-user-cse; 2 elements
access-list AAA-user-cse deny tcp any any eq telnet (hitcnt=1)
access-list AAA-user-cse permit ip any any (hitcnt=0)
```

Nueva lista de acceso descargable por usuario mediante ACS 3.0

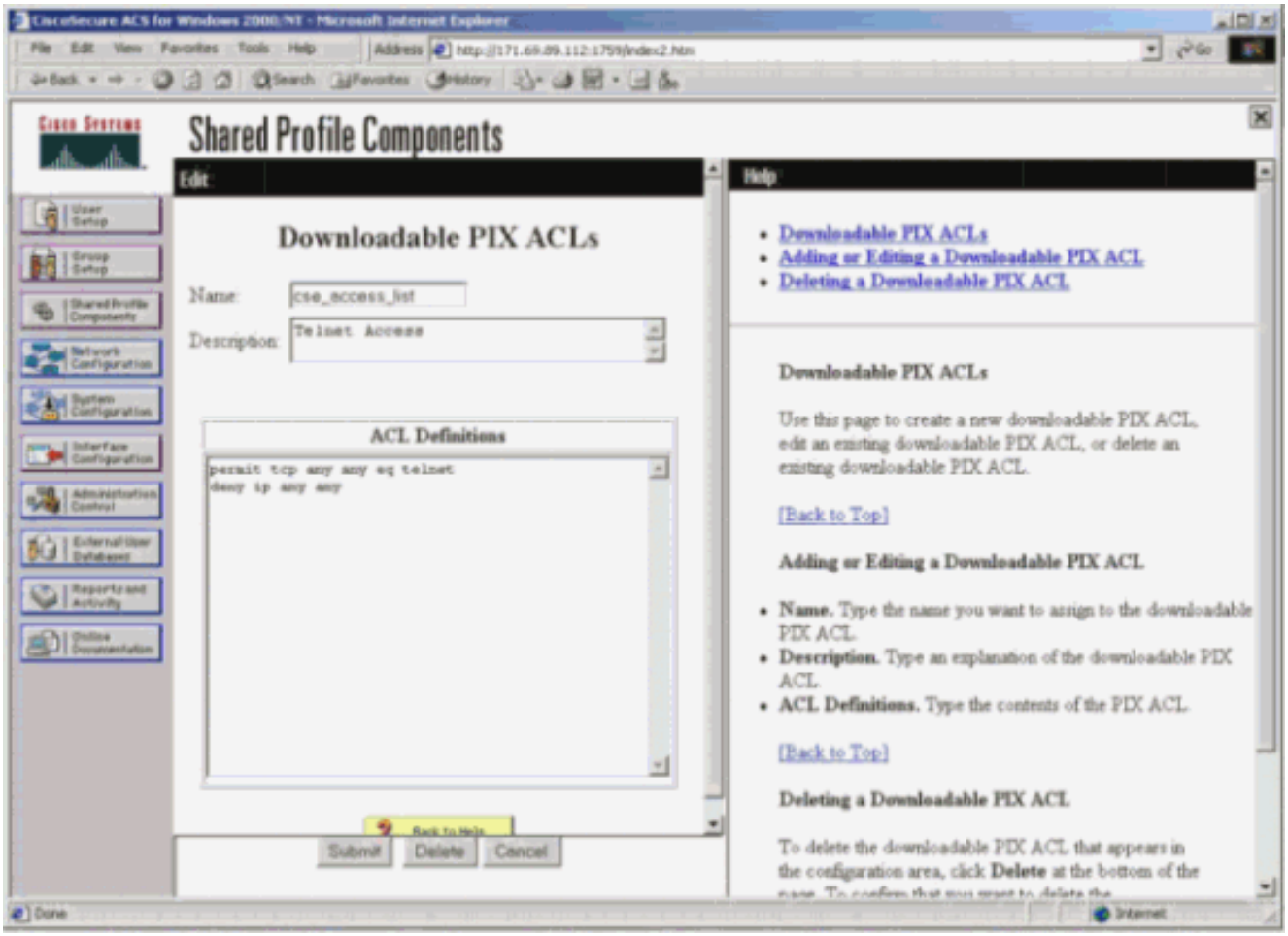
En la versión 3.0, el componente del perfil compartido le permite al usuario crear una plantilla de lista de accesos y definir el nombre de la plantilla para usuarios o grupos específicos. El nombre de la plantilla se puede utilizar con tantos usuarios o grupos como sea necesario. Esto elimina la necesidad de configurar listas de acceso idénticas para cada usuario.

Nota: Si se produce un failover, uauth no se copia en el PIX secundario. En el stateful failover, la sesión se mantiene. Sin embargo, la nueva conexión se debe volver a autenticar y la lista de acceso se debe descargar de nuevo.

Uso de perfiles compartidos

Complete estos pasos cuando utilice perfiles compartidos.

1. Haga clic en Interface Configuration (Configuración de interfaz).
2. Verifique **ACL descargables a nivel de usuario** y/o **ACL descargables a nivel de grupo**.
3. Haga clic en **Componentes del perfil compartido**. Haga clic en **ACL descargables de nivel de usuario**.
4. Defina las ACL descargables.
5. Haga clic en **Group Setup**. En ACL descargables, asigne la lista de acceso PIX a la lista de acceso creada
   anteriormente.



[Depuración de PIX: Autenticación válida y lista de acceso descargada mediante perfiles compartidos]

- Permite sólo Telnet y niega otro tráfico.

```
pix# 305011: Built dynamic TCP translation from inside:
   172.16.171.33/11065 to outside:172.16.171.201/1051
109001: Auth start for user '???' from 172.16.171.33/11065 to
   172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 12
109005: Authentication succeeded for user 'cse' from
   172.16.171.33/11065 to 172.16.171.202/23 on interface inside
302013: Built outbound TCP connection 124 for outside:
   172.16.171.202/23 (172.16.171.202/23) to inside:
   172.16.171.33/11065 (172.16.171.201/1051) (cse)
```

Salida del comando **show uauth**.

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
pix# 111009: User 'enable_15' executed cmd: show uauth
pix#
```

Salida del comando **show access-list**.

```
pix#show access-list
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3; 2 elements
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3
   permit tcp any any eq telnet (hitcnt=1)
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3
```

```
   deny ip any any (hitcnt=0)
pix# 111009: User 'enable_15' executed cmd: show access-list
```

- Niega solo Telnet y permite otro tráfico.

```
pix# 305011: Built dynamic TCP translation from inside:
   172.16.171.33/11066 to outside:172.16.171.201/1052
109001: Auth start for user '???' from 172.16.171.33/11066 to
   172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 13
109005: Authentication succeeded for user 'cse'
   from 172.16.171.33/11066
   to 172.16.171.202/23 on interface inside
109015: Authorization denied (acl=#ACSACL#-PIX-cse_access_list-3cff1dd6)
   for user 'cse' from 172.16.171.33/11066
   to 172.16.171.202/23 on interface inside
```

Salida del comando **show uauth**.

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
pix# 111009: User 'enable_15' executed cmd: show uauth
```

Salida del comando **show access-list**.

```
pix#show access-list
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6; 2 elements
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6
   deny tcp any any eq telnet (hitcnt=1)
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6
   permit ip any any (hitcnt=0)
pix# 111009: User 'enable_15' executed cmd: show access-listpix#
```

Agregar contabilidad

Configuración de PIX - Agregar contabilidad

TACACS (AuthInbound=tacacs)

Agregue este comando.

```
aaa accounting include any inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthInbound
```

O bien, utilice la nueva función de 5.2 para definir lo que se va a contabilizar en las listas de acceso.

```
aaa accounting match 101 outside AuthInbound
```

Nota: La lista de acceso 101 se define por separado.

RADIUS (AuthOutbound=radius)

Agregue este comando.

```
aaa accounting include any inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthOutbound
```

O bien, utilice la nueva función de 5.2 para definir lo que se va a contabilizar en las listas de acceso.

```
aaa accounting match 101 outside AuthOutbound
```

Nota: La lista de acceso 101 se define por separado.

Nota: Los registros contables se pueden generar para las sesiones administrativas en el PIX a partir del código PIX 7.0.

Ejemplos de contabilidad

- Ejemplo de contabilidad TACACS para Telnet desde 99.99.99.2 fuera a 172.18.124.114 dentro (99.99.99.99).

```
172.18.124.157 pixuser PIX 99.99.99.2 start server=rtp-cherry
   time=10:36:16 date=08/23/2000 task_id=0x0 foreign_ip=99.99.99.2
   local_ip=172.18.124.114 cmd=telnet
172.18.124.157 pixuser PIX 99.99.99.2 stop server=rtp-cherry
   time=10:37:50 date=08/23/2000 task_id=0x0 foreign_ip=99.99.99.2
   local_ip=172.18.124.114
   cmd=telnet elapsed_time=94 bytes_in=61 bytes_out=254
```

- Ejemplo de contabilidad RADIUS para la conexión desde 172.18.124.114 dentro a 99.99.99.2 afuera (Telnet) y 99.99.99.3 afuera (HTTP).

```
Sun Aug  6 03:59:28 2000
        Acct-Status-Type = Start
        NAS-IP-Address = 172.18.124.157
        Login-IP-Host = 172.18.124.114
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000004
        User-Name = cse
        Vendor-Specific = Source-IP=172.18.124.114
        Vendor-Specific = Source-Port=35937
        Vendor-Specific = Destination-IP=99.99.99.2
        Vendor-Specific = Destination-Port=23

Sun Aug  6 03:59:32 2000
        Acct-Status-Type = Stop
        NAS-IP-Address = 172.18.124.157
        Login-IP-Host = 172.18.124.114
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000004
         Username = cse
        Acct-Session-Time = 4
        Acct-Input-Octets = 101
        Acct-Output-Octets = 143
        Vendor-Specific = Source-IP=172.18.124.114
        Vendor-Specific = Source-Port=35937
        Vendor-Specific = Destination-IP=99.99.99.2
        Vendor-Specific = Destination-Port=23
```

```
    Sun Aug  6 04:05:02 2000
            Acct-Status-Type = Start
            NAS-IP-Address = 172.18.124.157
            Login-IP-Host = 172.18.124.114
            Login-TCP-Port = 80
            Username = cse
            Vendor-Specific = Source-IP=172.18.124.114
            Vendor-Specific = Source-Port=35949
            Vendor-Specific = Destination-IP=99.99.99.3
            Vendor-Specific = Destination-Port=80

    Sun Aug  6 04:05:02 2000
            Acct-Status-Type = Stop
            NAS-IP-Address = 172.18.124.157
            Login-IP-Host = 172.18.124.114
            Login-TCP-Port = 80
            Acct-Session-Id = 0x0000000a
            Username = cse
            Acct-Session-Time = 0
            Acct-Input-Octets = 1277
            Acct-Output-Octets = 310
            Vendor-Specific = Source-IP=172.18.124.114
            Vendor-Specific = Source-Port=35949
            Vendor-Specific = Destination-IP=99.99.99.3
            Vendor-Specific = Destination-Port=80
```

Utilización del comando exclude

En esta red, si decide que un origen o destino determinado no necesita autenticación, autorización o contabilidad, ejecute estos comandos.

```
aaa authentication exclude telnet outside 172.18.124.114 255.255.255.255
  99.99.99.3 255.255.255.255 AuthInbound
aaa authorization exclude telnet outside 172.18.124.114 255.255.255.255
  99.99.99.3 255.255.255.255 AuthInbound
aaa accounting exclude telnet outside 172.18.124.114 255.255.255.255
  99.99.99.3 255.255.255.255 AuthInbound
```

Nota: Ya tiene los comandos **include**.

```
aaa authentication|authorization|accounting include http|ftp|telnet
```

O bien, con la nueva función en 5.2, defina lo que desea excluir.

```
access-list 101 deny tcp host 99.99.99.3 host 172.18.124.114 eq telnet
access-list 101 deny tcp host 99.99.99.3 host 172.18.124.114 eq ftp
access-list 101 deny tcp host 99.99.99.3 host 172.18.124.114 eq www
access-list 101 permit tcp any any eq telnet
access-list 101 permit tcp any any eq www
access-list 101 permit tcp any any eq ftp
aaa authentication match 101 outside AuthInbound
aaa authorization match 101 outside AuthInbound
```

```
aaa accounting match 101 outside AuthInbound
```

Nota: Si excluye un cuadro de la autenticación y tiene autorización en, también debe excluir el cuadro de la autorización.

Número máximo de sesiones y visualización de 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 informe de control de "inicio" pero ningún informe de "detención", el servidor TACACS+ o RADIUS asume que la persona se encuentra todavía conectada (es decir, el usuario tiene una sesión abierta a través de PIX). Esto funciona bien en conexiones Telnet y FTP debido a la naturaleza de las conexiones. Sin embargo, esto no funciona bien para HTTP. En este ejemplo, se utiliza una configuración de red diferente, pero los conceptos son los mismos.

El usuario utiliza 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 171.68.118.100/1200 to 9.9.9.25/23
    (pix) 302001: Built TCP connection 5 for
        faddr 9.9.9.25/23 gaddr 9.9.9.10/1200 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
```

Como el servidor ha visto un registro de "inicio" pero no un registro de "detención", en este momento, el servidor muestra que el usuario "Telnet" está conectado. 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 realiza su negocio de Telnet o FTP en el host de destino y luego sale (pasa diez 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
```

Ya sea que uauth sea 0 (es decir, autenticar cada vez) o mayor (autenticar una vez y no de nuevo durante un período uauth), un registro contable se divide para cada sitio accedido.

HTTP funciona de manera distinta debido a la naturaleza del protocolo. Este es un ejemplo de

HTTP donde 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 está fijado a las 16:35:34 y el registro de detención 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 no ha iniciado sesión en el sitio web. La conexión no se abre cuando el usuario lee la página web. El número máximo de sesiones o de usuarios que han iniciado sesión no funcionan aquí. Esto se debe a que el tiempo de conexión (el tiempo entre "Construido" y "Desplegado") en HTTP es demasiado corto. El registro "iniciar" y "detener" es subsegundo. No existe un registro de "inicio" sin un registro de "parada", ya que los registros se producen prácticamente en el mismo instante. Todavía hay un registro "start" y "stop" enviado al servidor para cada transacción, independientemente de si uauth está 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.

Interfaz del usuario

Cambiar el mensaje que ven los usuarios

Si tiene el comando:

auth-prompt prompt PIX515B

luego, los usuarios que pasan por el PIX ven este mensaje.

```
PIX515B
```

Personalizar el mensaje que ven los usuarios

Si tiene los comandos:

auth-prompt accept "GOOD_AUTHENTICATION"

```
auth-prompt reject "BAD_AUTHENTICATION"
```

luego, los usuarios ven un mensaje sobre el estado de autenticación en un login fallido/exitoso.

```
  PIX515B
  Username: junk
  Password:
  "BAD_AUTHENTICATION"

  PIX515B
  Username: cse
  Password:
  "GOOD_AUTHENTICATION"
```

Tiempos de Espera Absolutos e Inactivos por Usuario

El comando PIX timeout uauth controla con cuánta frecuencia es necesaria una reautenticación. Si la autenticación/autorización TACACS+ está activada, esto se controla por usuario. Este perfil de usuario se configura para controlar el tiempo de espera (esto se encuentra en el servidor freeware TACACS+ y los tiempos de espera se encuentran en minutos).

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

Luego de la autenticación/autorización:

```
show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
user 'cse' at 99.99.99.3, authorized to:
   port 172.18.124.114/telnet
   absolute   timeout: 0:02:00
   inactivity timeout: 0:01:00
```

Al cabo de dos minutos:

Tiempo de espera absoluto: la sesión se desactiva:

```
109012: Authen Session End: user 'cse', Sid 20, elapsed 122 seconds
302002: Teardown TCP connection 32 faddr 99.99.99.3/11025
   gaddr 99.99.99.99/23 l addr 172.18.124.114/23 duration 0:02:26
   bytes 7547 (TCP FINs)
```

Salida de HTTP virtual

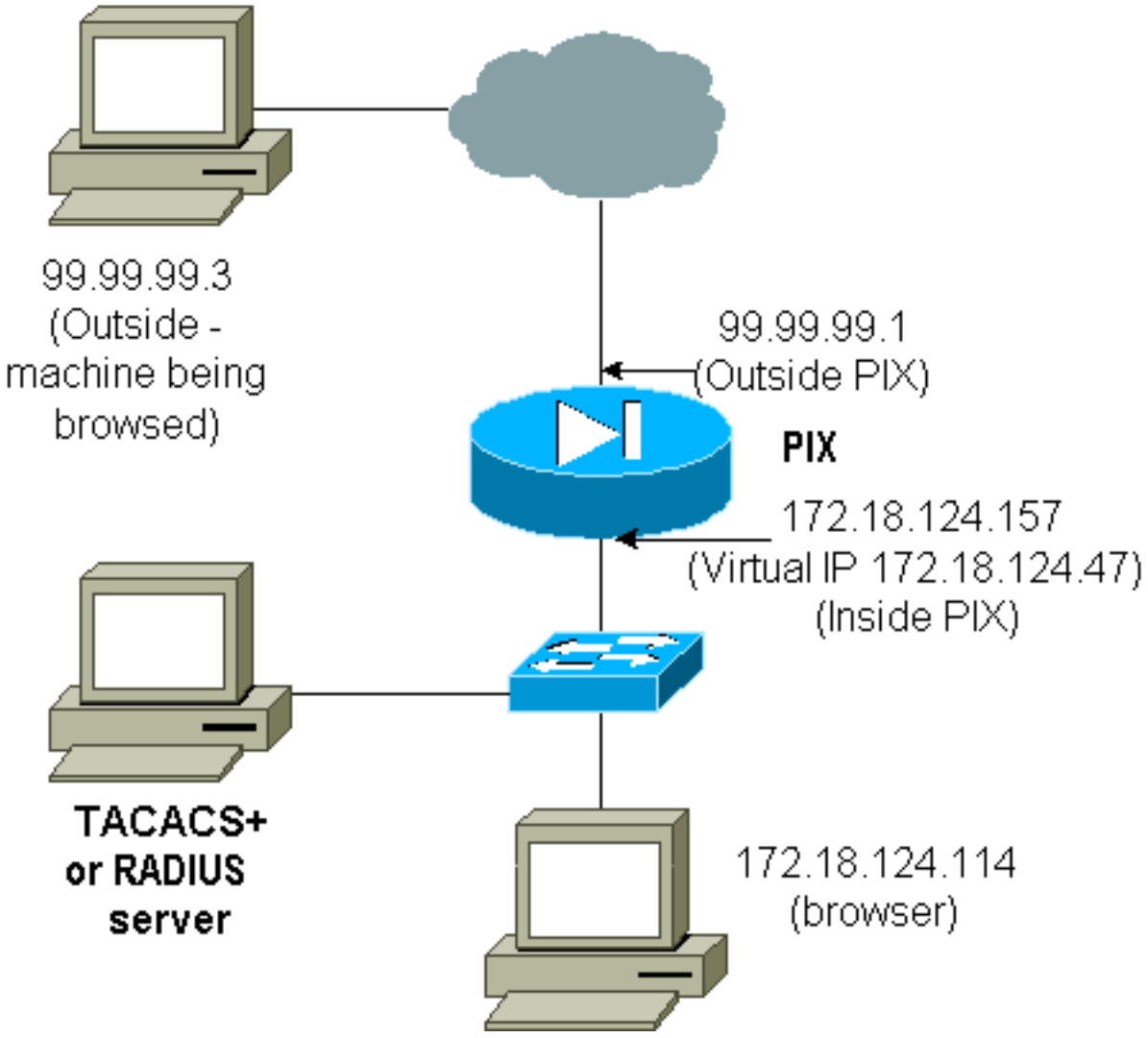
Si se requiere autenticación en sitios fuera del PIX así como en el propio PIX, a veces se observa un comportamiento inusual del navegador, ya que los exploradores almacenan el nombre de usuario y la contraseña.

Para evitar esto, implemente HTTP virtual agregando una dirección RFC 1918 (una dirección no enrutable en Internet, pero válida y única para la red interna PIX) a la configuración PIX en el formato.

```
virtual http #.#.#.#
```

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.

Nota: Las direcciones IP virtuales de Telnet y HTTP se deben incluir en las instrucciones de **autenticación aaa**. En este ejemplo, al especificar 0.0.0.0 se incluyen estas direcciones.



En la configuración PIX, agregue este comando.

```
virtual http 172.18.124.47
```

El usuario señala el navegador a 99.99.99.3. Se muestra este mensaje.

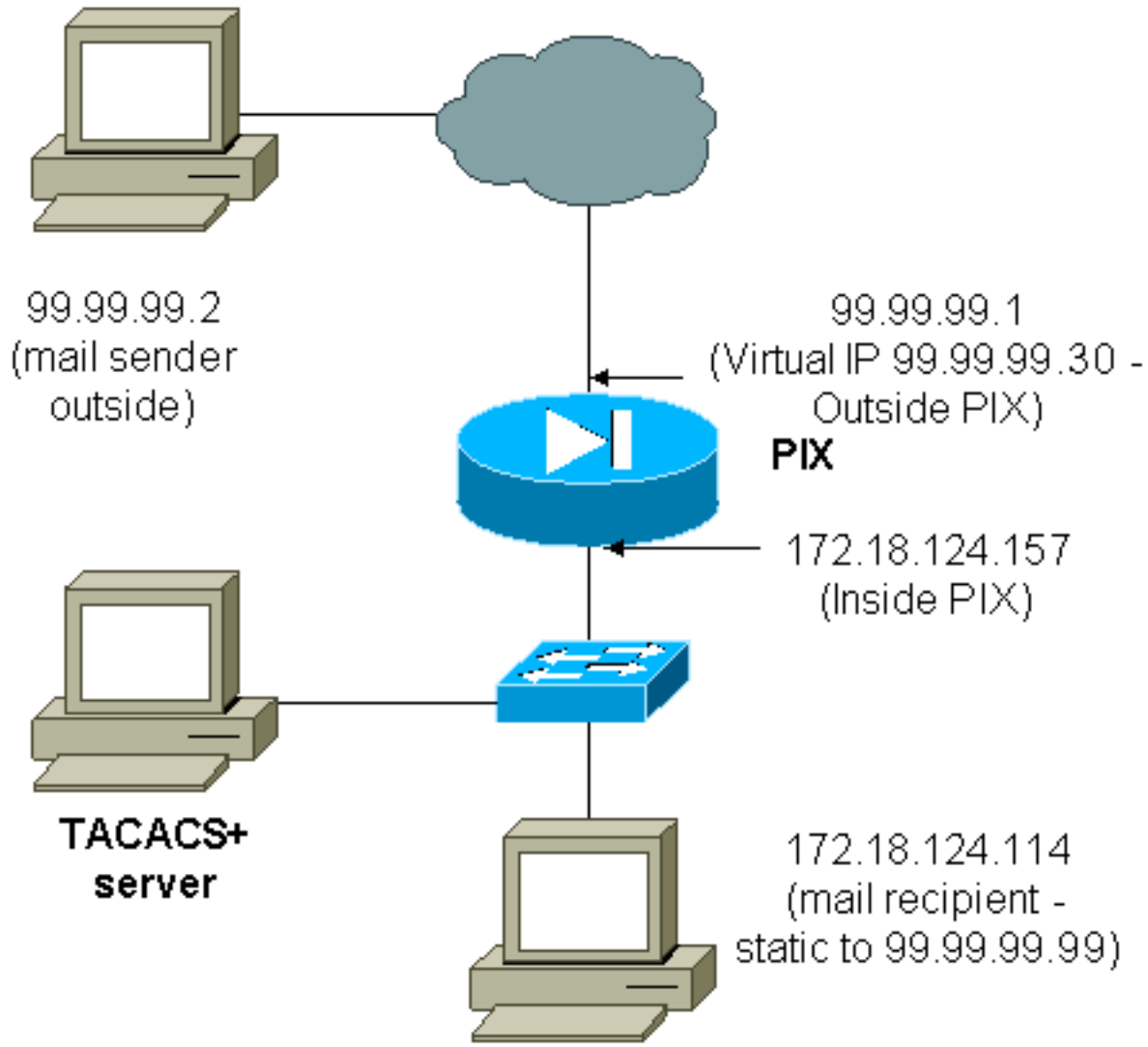
```
Enter username for PIX515B (IDXXX) at 172.18.124.47
```

Después de la autenticación, el tráfico se redirige a 99.99.99.3.

Virtual telnet

Nota: Las direcciones IP virtuales de Telnet y HTTP se deben incluir en las instrucciones de **autenticación aaa**. En este ejemplo, al especificar 0.0.0.0 se incluyen estas direcciones.

Entrada de Telnet virtual



No es una gran idea autenticar correo entrante ya que no se muestra una ventana para que el correo se envíe entrante. Utilice el comando **exclude** en su lugar. Pero a modo de ilustración, se agregan estos comandos.

```
aaa authentication include tcp/25 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authorization include tcp/25 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
!--- OR the new 5.2 feature allows these !--- four statements to perform the same function. !---
Note: The old and new verbiage should not be mixed.

access-list 101 permit tcp any any eq smtp
!--- The "mail" was a Telnet to port 25. access-list 101 permit tcp any any eq telnet
aaa authentication match 101 outside AuthInbound
aaa authorization match 101 outside AuthInbound
!
!--- plus ! virtual telnet 99.99.99.30
static (inside,outside) 99.99.99.30 172.18.124.30
   netmask 255.255.255.255 0 0
static (inside,outside) 99.99.99.99 172.18.124.114
   netmask 255.255.255.255 0 0
conduit permit tcp host 99.99.99.30 eq telnet any
conduit permit tcp host 99.99.99.99 eq telnet any
conduit permit tcp host 99.99.99.99 eq smtp any
```

Los usuarios (esto es TACACS+ freeware):

```
  user = cse {
  default service = permit
  login = cleartext "csecse"
  }


  user = pixuser {
  login = cleartext "pixuser"
  service = exec {
  }
  cmd = telnet {
  permit .*
  }
  }
```

Si sólo la autenticación está activada, ambos usuarios envían correo entrante después de la autenticación en Telnet a la dirección IP 99.99.99.30. Si la autorización está habilitada, el usuario "cse" Telnet a 99.99.99.30 e ingresa el nombre de usuario/contraseña TACACS+. La conexión Telnet se interrumpe. El usuario "cse" envía el correo a 99.99.99.99 (172.18.124.114). La autenticación se realiza correctamente para el usuario "pixuser". Sin embargo, cuando el PIX envía la solicitud de autorización para cmd=tcp/25 y cmd-arg=172.18.124.114, la solicitud falla, como se muestra en este resultado.

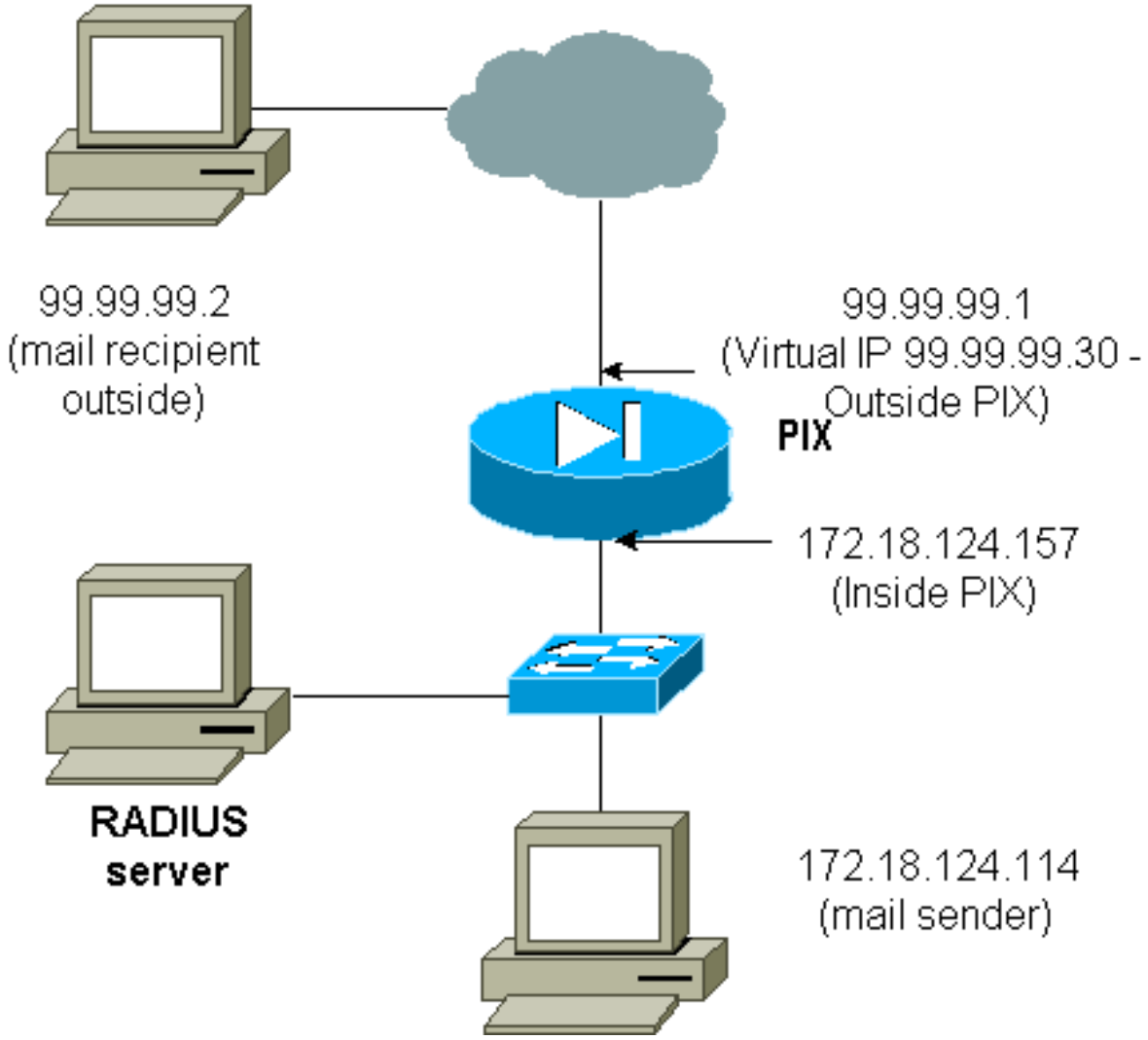
```
109001: Auth start for user '???' from
   99.99.99.2/11036 to 172.18.124.114/23
109005: Authentication succeeded for user
   'cse' from 172.18.124.114/23 to
   99.99.99.2/11036 on interface outside

pixfirewall#show uauth
                        Current    Most Seen
Authenticated Users       1          1
Authen In Progress        0          1
user 'cse' at 99.99.99.2, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

```
pixfirewall# 109001: Auth start for user '???' from
    99.99.99.2/11173 to 172.18.124.30/23
109011: Authen Session Start: user 'cse', sid 10
109005: Authentication succeeded for user 'cse' from 99.99.99.2/23
    to 172.18.124.30/11173 on interface outside
109011: Authen Session Start: user 'cse', sid 10
109007: Authorization permitted for user 'cse' from 99.99.99.2/11173
    to 172.18.124.30/23 on interface outside
109001: Auth start for user 'cse' from 99.99.99.2/11174 to
    172.18.124.114/25
109011: Authen Session Start: user 'cse', sid 10
109007: Authorization permitted for user 'cse' from 99.99.99.2/11174
    to 172.18.124.114/25 on interface outside
302001: Built inbound TCP connection 5 for faddr 99.99.99.2/11174
    gaddr 99.99.99.99/25 laddr 172.18.124.114/25 (cse)

pixfirewall# 109001: Auth start for user '???' from 99.99.99.2/11175
    to 172.18.124.30/23
109011: Authen Session Start: user 'pixuser', sid 11
109005: Authentication succeeded for user 'pixuser' from 99.99.99.2/23
    to 172.18.124.30/11175 on interface outside
109011: Authen Session Start: user 'pixuser', sid 11
109007: Authorization permitted for user 'pixuser' from 99.99.99.2/11175
    to 172.18.124.30/23 on interface outside
109001: Auth start for user 'pixuser' from 99.99.99.2/11176
    to 172.18.124.114/25
109008: Authorization denied for user 'pixuser' from 99.99.99.2/25
    to 172.18.124.114/11176 on interface outside
```

Virtual Telnet de salida



No es una gran idea autenticar correo entrante ya que no se muestra una ventana para que el correo se envíe entrante. Utilice el comando **exclude** en su lugar. Pero a modo de ilustración, se agregan estos comandos.

No es una gran idea autenticar el correo saliente, ya que no se muestra una ventana para que el correo se envíe de salida. Utilice el comando **exclude** en su lugar. Pero, a título ilustrativo, se agregan estos comandos.

```
aaa authentication include tcp/25 inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthOutbound
!--- OR the new 5.2 feature allows these three statements !--- to replace the previous
statements. !--- Note: Do not mix the old and new verbiage.

access-list 101 permit tcp any any eq smtp
access-list 101 permit tcp any any eq telnet
aaa authentication match 101 inside AuthOutbound
!
!--- plus ! virtual telnet 99.99.99.30
!--- The IP address on the outside of PIX is not used for anything else.
```

Para enviar correo desde adentro hacia afuera, active un indicador de comandos en el host de correo y Telnet a 99.99.99.30. Esto abre el agujero para que el correo pase. El correo se envía de 172.18.124.114 a 99.99.99.2:

```
   305002: Translation built for gaddr 99.99.99.99
```

```
      to laddr 172.18.124.114
   109001: Auth start for user '???' from
      172.18.124.114/32860 to 99.99.99.30/23
   109011: Authen Session Start: user 'cse', Sid 14
   109005: Authentication succeeded for user 'cse'
      from 172.18.124.114/32860 to    99.99.99.30/23
      on interface inside
   302001: Built outbound TCP connection 22 for faddr
      99.99.99.2/25 gaddr 99.99.99.99/32861
      laddr 172.18.124.114/32861 (cse)

pixfirewall#show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
user 'cse' at 172.18.124.114, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

Desconexión de Virtual Telnet

Cuando los usuarios hacen Telnet a la dirección IP Telnet virtual, el comando show uauth muestra la hora en que se abre el orificio. Si los usuarios quieren evitar que el tráfico pase luego de finalizar sus sesiones (cuando el tiempo permanece en uauth) tienen que hacer una conexión Telnet a la dirección IP de Telnet virtual otra vez. Esto finaliza la sesión. Esto se ilustra en este ejemplo.

La primera autenticación

```
 109001: Auth start for user '???'
    from 172.18.124.114/32862 to 99.99.99.30/23
 109011: Authen Session Start: user 'cse', Sid 15
 109005: Authentication succeeded for user
    'cse' from 172.18.124.114/32862 to
    99.99.99.30/23 on interface inside
```

Después de la primera autenticación

```
pixfirewall#show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
user 'cse' at 172.18.124.114, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

La segunda autenticación

```
   pixfirewall# 109001: Auth start for user 'cse'
      from 172.18.124.114/32863 to    99.99.99.30/23
   109005: Authentication succeeded for user 'cse'
      from 172.18.124.114/32863 to    99.99.99.30/23
      on interface inside
```

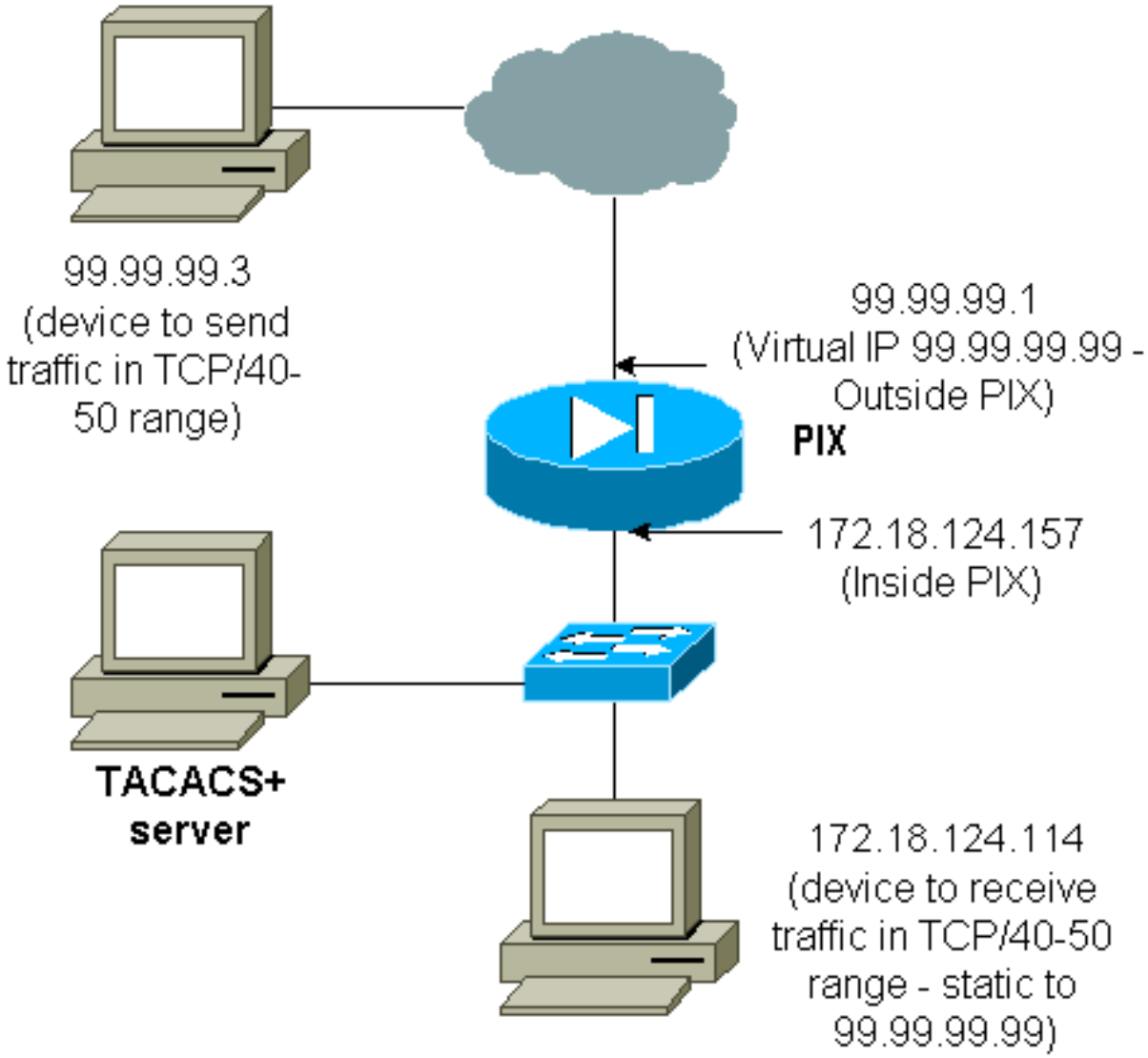
Después de la segunda autenticación

```
pixfirewall#show uauth
```

```
                        Current     Most Seen
Authenticated Users       0           2
Authen In Progress        0           1
```

‘Autorización del puerto

Diagrama de la red



La autorización se permite para rangos de puertos. Si Telnet virtual se configura en el PIX y la autorización se configura para un rango de puertos, el usuario abre el agujero con Telnet virtual. Luego, si la autorización para un rango de puertos está activada y el tráfico de ese rango llega al PIX, el PIX envía el comando al servidor TACACS+ para solicitar autorización. Este ejemplo muestra la autorización entrante en un rango de puertos.

```
aaa authentication include any outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authorization include tcp/40-50 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
!--- OR the new 5.2 feature allows these three statements !--- to perform the same function as
the previous two statements. !--- Note: The old and new verbiage should not be mixed.

access-list 116 permit tcp any any range 40 50
aaa authentication match 116 outside AuthInbound
```

```
aaa authorization match 116 outside AuthInbound
!
!--- plus ! static (inside,outside) 99.99.99.99 172.18.124.114
netmask 255.255.255.255 0 0
conduit permit tcp any any
virtual telnet 99.99.99.99
```

Ejemplo de configuración del servidor TACACS+ (freeware):

```
  user = cse {
  login = cleartext "numeric"
  cmd = tcp/40-50 {
  permit 172.18.124.114
  }
  }
```

El usuario primero debe establecer una conexión Telnet a la dirección IP virtual 99.99.99.99. Después de la autenticación, cuando un usuario intenta enviar el tráfico TCP en el rango 40-50 del puerto a través del PIX a 99.99.99.99 (172.18.124.114), cmd=tcp/40-50 se envía al servidor TACACS+ con cmd-arg=1722.2 18.124.114 como se ilustra aquí:

```
109001: Auth start for user '???' from 99.99.99.3/11075
    to 172.18.124.114/23
109011: Authen Session Start: user 'cse', Sid 13
109005: Authentication succeeded for user 'cse'
    from 172.18.124.114/23 to 99.99.99.3/11075
    on interface outside
109001: Auth start for user 'cse' from 99.99.99.3/11077
    to 172.18.124.114/49
109011: Authen Session Start: user 'cse', Sid 13
109007: Authorization permitted for user 'cse'
    from 99.99.99.3/11077 to 172.18.124.114/49
    on interface outside
```

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

Después de asegurarse de que Telnet virtual funciona para permitir el tráfico TCP/40-50 al host dentro de la red, agregue contabilidad para este tráfico con estos comandos.

```
aaa accounting include any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
!--- OR the new 5.2 feature allows these !--- two statements to replace the previous statement.
!--- Note: Do not mix the old and new verbiage.

aaa accounting match 116 outside AuthInbound
access-list 116 permit ip any any
```

Ejemplo de registros contables TACACS+

```
   Thu Aug 24 08:06:09 2000 172.18.124.157 cse PIX 99.99.99.3
   start task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
   cmd=tcp/40-50
   Thu Aug 24 08:06:17 2000 172.18.124.157 cse PIX 99.99.99.3
```

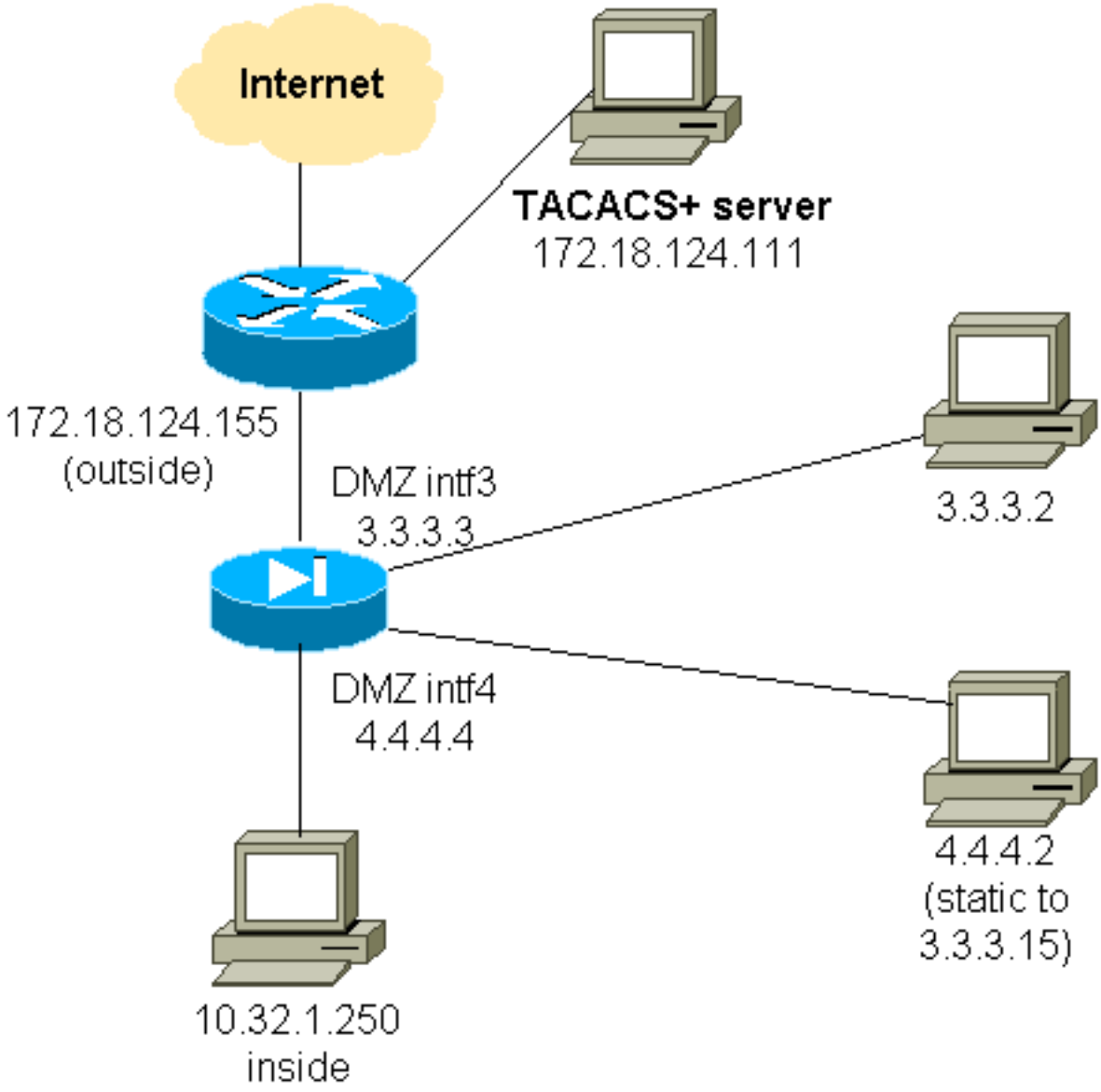
```
stop task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
cmd=tcp/40-50 elapsed_time=8 bytes_in=80 bytes_out=101
```

Autenticación en DMZ

Para autenticar a los usuarios que van de una interfaz DMZ a otra, dile al PIX que autentique el tráfico para las interfaces nombradas. En el PIX, el arreglo es el siguiente:

```
least secure
PIX outside (security0) = 172.18.124.155
pix/intf3 (DMZ - security15) = 3.3.3.3 & device 3.3.3.2
pix/intf4 (DMZ - security20) = 4.4.4.4 & device 4.4.4.2 (static to 3.3.3.15)
PIX inside (security100) = 10.32.1.250
most secure
```

Diagrama de la red



Configuración parcial de PIX

Autentique el tráfico Telnet entre pix/intf3 y pix/intf4, como se muestra aquí.

Configuración parcial de PIX

```
  nameif ethernet0 outside security0
  nameif ethernet1 inside security100
  (nameif ethernet2 pix/intf2 security10)
  nameif ethernet3 pix/intf3 security15
  nameif ethernet4 pix/intf4 security20
  (nameif ethernet5 pix/intf5 security25)
  interface ethernet0 auto
  interface ethernet1 auto
  (interface ethernet2 auto shutdown)
  interface ethernet3 auto
  interface ethernet4 auto
  (interface ethernet5 auto shutdown)
  ip address outside 172.18.124.155 255.255.255.0
  ip address inside 10.32.1.250 255.255.255.0
  ip address pix/intf3 3.3.3.3 255.255.255.0
  ip address pix/intf4 4.4.4.4 255.255.255.0
  static (pix/intf4,pix/intf3) 3.3.3.15 4.4.4.2 netmask
255.255.255.255 0 0
  conduit permit tcp host 3.3.3.15 host 3.3.3.2
  aaa-server xway protocol tacacs+
  aaa-server xway (outside) host 172.18.124.111 timeout
5
  aaa authentication include telnet pix/intf4 4.4.4.0
255.255.255.0 3.3.3.0
  255.255.255.0 3.3.3.0 255.255.255.0 xway
  aaa authentication include telnet pix/intf3 4.4.4.0
255.255.255.0 3.3.3.0
  255.255.255.0 3.3.3.0 255.255.255.0 xway
!--- OR the new 5.2 feature allows these four statements
!--- to replace the previous two statements. !--- Note:
Do not mix the old and new verbiage.

  access-list 103 permit tcp 3.3.3.0 255.255.255.0
4.4.4.0 255.255.255.0 eq telnet
  access-list 104 permit tcp 4.4.4.0 255.255.255.0
3.3.3.0 255.255.255.0 eq telnet
  aaa authentication match 103 pix/intf3 xway
  aaa authentication match 104 pix/intf4 xway
```

Información para recopilar si abre un caso del TAC

Si todavía necesita ayuda después de seguir los pasos de solución de problemas anteriores y desea abrir un caso con el TAC de Cisco, asegúrese de incluir esta información para solucionar el problema de su firewall PIX.
• Descripción del problema y detalles relevantes de la topología • Solucione problemas antes de abrir el caso • Resultado del comando show tech-support • Salida del comando **show log** después de ejecutar con el comando **logging buffered debugging**, o capturas de consola que muestran el problema (si están disponibles) Adjunte los datos recopilados para su caso en un texto sin formato (.txt), sin compactar. Adjunte la información a

su caso subiéndola con la ayuda de la Herramienta de Consulta de Casos (sólo clientes registrados). Si no puede acceder a la herramienta Case Query Tool, envíe la información en un archivo adjunto de correo electrónico a attach@cisco.com con su número de caso en el asunto del mensaje.

Información Relacionada

- Cisco PIX Firewall Software
- Referencias de Comandos de Cisco Secure PIX Firewall
- Avisos de campos de productos de seguridad (incluido PIX)
- Solicitudes de Comentarios (RFC)
- Cisco Secure Access Control Server para Windows
- Cisco Secure Access Control Server para Unix
- Sistema de control de acceso del controlador de acceso a terminales (TACACS+)
- Servicio de usuario de acceso telefónico de autenticación remota (RADIUS)
- Soporte Técnico y Documentación - Cisco Systems