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

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Convenciones
Autenticación, autorización y contabilidad
Qué ve el usuario con la autenticación/autorización activada
Pasos de depuración
Sólo autenticación
Diagrama de la red
Configuración del servidor – Sólo autenticación
Puertos RADIUS configurables (5.3 y posteriores)
Ejemplos de errores de depuración de autenticación PIX
Autenticación más autorización
Configuración del servidor – Autenticación más autorización
Configuración de PIX - Adición de autorización
Ejemplos de depuración de autorización y autenticación PIX
Nueva función Access List (Lista de accesos)
Configuración de PIX
Perfiles del servidor
Nueva lista de acceso por usuario descargable con versión 6.2
Agregar contabilidad
Configuración PIX - Agregue las estadísticas
Ejemplos de contabilidad
Utilización del comando exclude
Sesiones máximas y usuarios conectados al sistema de la visión
Interfaz del usuario
Cambie a los usuarios del prompt ven
Personalice a los usuarios del mensaje ven
Tiempos de Espera Absolutos e Inactivos por Usuario
Salida de HTTP virtual
Virtual telnet
Entrada de Telnet virtual
Virtual Telnet de salida

Desconexión de Virtual Telnet
'Autorización del puerto
Diagrama de la red
Contabilización AAA para cualquier otro tráfico que no sea HTTP, FTP y Telnet
Ejemplo de registros contables TACACS+
Autenticación en DMZ
Diagrama de la red
Configuración parcial de PIX
Información para recopilar si abre un caso del TAC
Información Relacionada

Introducción

El RADIUS y autenticación de TACACS+ se puede hacer para el FTP, Telnet, y las conexiones HTTP con el Cisco Secure PIX Firewall. La autenticación para otros menos protocolos comunes se hace generalmente para trabajar. Autorización TACACS+ se soporta. La autorización de RADIUS no se soporta. Los cambios en el Authentication, Authorization, and Accounting (AAA) PIX 5.2 sobre la versión anterior incluyen el soporte de la lista de acceso a AAA para controlar se autentica quién y qué recursos los accesos del usuario. En PIX 5.3 y posterior, el cambio del Authentication, Authorization, and Accounting (AAA) sobre las versiones anteriores del código es que los puertos RADIUS son configurables.

Nota: El PIX 6.x puede hacer explicar el paso con el tráfico pero no para el tráfico destinated al PIX.

prerrequisitos

Requisitos

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Nota: Si usted funciona con la versión de software 7.x del PIX/ASA y posterior, refiera a configurar los servidores de 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

Aquí está una explicación de autenticación, una autorización y las estadísticas:

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

Qué ve el usuario con la autenticación/autorización activada

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

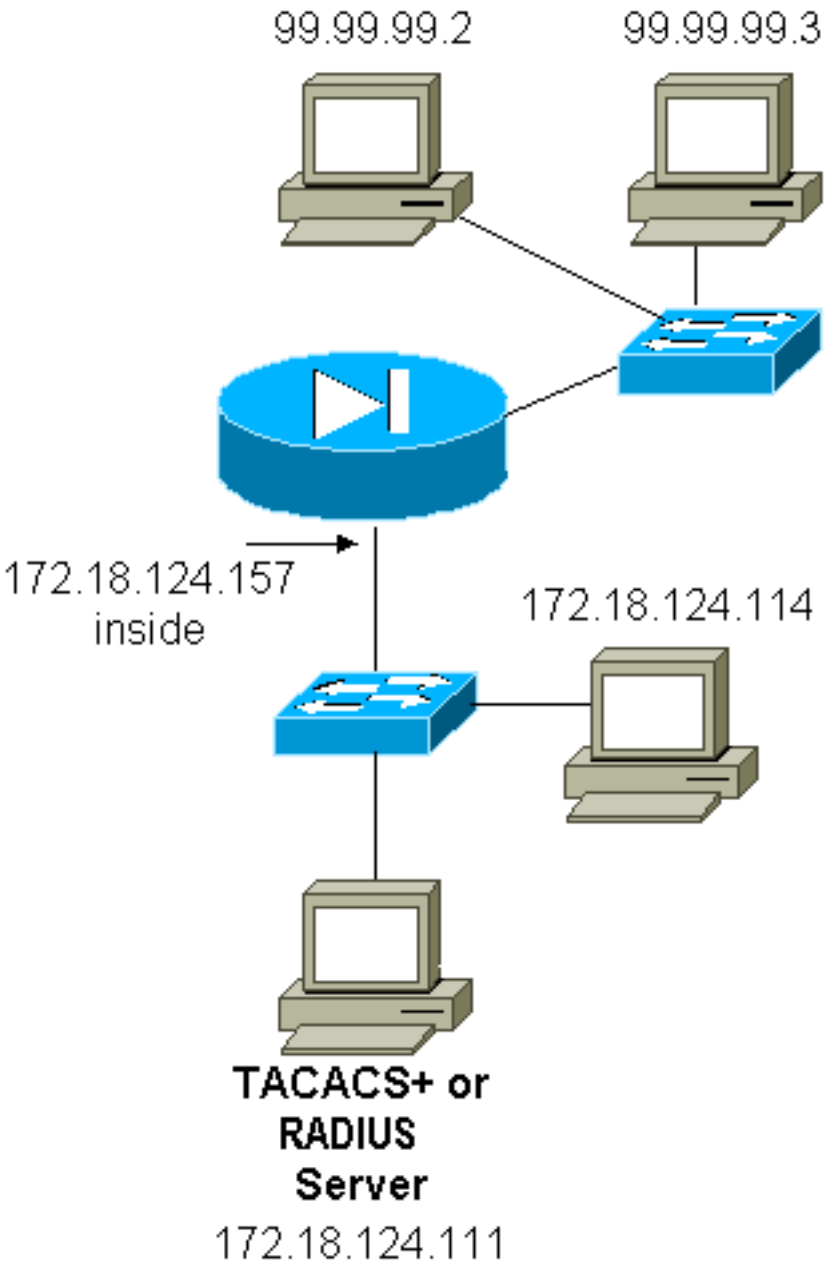
- Telnet - El usuario ve una solicitud de nombre de usuario y luego una solicitud de la contraseña. Si la autenticación (y autorización) resulta exitosa en el PIX/servidor, el siguiente host de destino le pide al usuario el nombre de usuario y contraseña.
- **FTP** — El usuario ve un prompt de nombre de usuario subir. El usuario debe ingresar "nombredeusuario_local@nombredeusuario_remoto" para el nombre de usuario y "contraseña_local@contraseña_remota" para la contraseña. El PIX envía el “local_username” y el “local_password” al servidor de seguridad local. Si la autenticación (y la autorización) es acertadas en el PIX/server, el “remote_username” y el “remote_password” se pasan al servidor FTP de destino más allá.
- **HTTP** — Una ventana se visualiza en el nombre de usuario del buscador requerido y la contraseña. Si la autenticación (y la autorización) se realiza con éxito, el usuario accederá al sitio Web siguiente. Tenga presente que los *navegadores ocultan los nombres de usuario y contraseña.* Si aparece que el PIX debe medir el tiempo hacia fuera una conexión HTTP pero no hace así pues, es probable que la reautentificación ocurra realmente con el navegador “tiroteo” el nombre de usuario guardado en memoria caché y la contraseña al PIX. El PIX adelante esto al servidor de autenticación. El debug del syslog PIX y/o del servidor muestra este fenómeno. Si Telnet y el FTP parecen trabajar “normalmente”, pero no lo hacen las conexiones HTTP, ésta es la razón.

Pasos de depuración

- Aseegurese los trabajos de la configuración PIX antes de que usted agregue la autenticación AAA y la autorización. Si usted no puede pasar el tráfico antes de que usted instituya la autenticación y autorización, usted no puede hacer tan luego.
- Habilite algún tipo de registro en el PIX.Publique el **comando logging console debug** de girar el debugging de la consola de registro.**Nota:** No utilice el debugging de la consola de registro en pesadamente un sistema cargado.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 de servidor TACACS segura de Cisco UNIX

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

Cisco asegura la Configuración del servidor del UNIX RADIUS

Nota: Agregue la dirección IP y la clave PIX a la lista del servidor de acceso a la red (NAS) con la ayuda del GUI avanzado.

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

Cisco asegura el Windows RADIUS

Utilice estos pasos para configurar Cisco aseguran el Windows RADIUS separan.

1. Obtenga una contraseña en la **sección de configuración de 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 Windows seguro TACACS+

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

'Configuración del servidor Livingston RADIUS'

Nota: Agregue la dirección IP PIX y la clave a los *clientes* clasifía.

- cargue en cuenta el User-service-type = al Usuario de Shell del " foo" de Password=

Configuración del servidor Merit RADIUS

Nota: Agregue la dirección IP PIX y la clave a los *clientes* clasifía.

- 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 posterior, la autenticación de RADIUS y los puertos de contabilidad se pueden cambiar algo con excepción del 1645/1646 predeterminado con estos comandos:

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

Ejemplos de errores de depuración de autenticación PIX

Vea los pasos de debugging para la información sobre cómo dar vuelta encendido a hacer el debug de. Éstos son ejemplos de un usuario en 99.99.99.2 que inicie el tráfico a 172.18.124.114 interior (99.99.99.99) y vice versa. El tráfico entrante es TACACS-autenticado y saliente RADIUS-se autentica.

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 el “error: Número máximo de intentos excedidos.”

```
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 el “error: Número máximo de intentos excedidos.”

```
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 petición para el nombre de usuario, después la contraseña, tiene tres oportunidades de ingresar éstos, y si es fracasada, considera el “error: Número máximo de intentos excedidos.”

```
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 el nombre de usuario, después la contraseña, después al "servidor de RADIUS fallado," y entonces finalmente "error: Número máximo de intentos excedidos."

```
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 usted quiere permitir que todos los usuarios autenticados realicen todas las operaciones (HTTP, FTP, y Telnet) con el PIX, después la autenticación es suficiente y la autorización no es necesaria. Sin embargo, si usted quiere permitir un cierto subconjunto de servicios a los ciertos usuarios o limitar a los usuarios de ir a los determinados sitios, la autorización es necesaria. La autorización de RADIUS es inválida para el tráfico con el PIX. Autorización TACACS+ es válido en este caso.

Si la autenticación pasa y la autorización está prendido, el PIX envía el comando que el usuario está haciendo al servidor. Por ejemplo, el "HTTP el 1.2.3.4." en la versión 5.2 del PIX, autorización TACACS+ se utiliza conjuntamente con las Listas de acceso para controlar donde van los usuarios.

Si usted quiere implementar la autorización para HTTP (Web site visitados), utilice el software tal como Websense puesto que un solo Web site puede tener un gran número de IP Addresses asociados a él.

Configuración del servidor – Autenticación más autorización

Configuración de servidor TACACS segura de Cisco 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 Windows seguro TACACS+

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

1. Haga clic los **comandos deny unmatched ios** en la parte inferior de la configuración de grupo.
2. Haga clic el **comando add/edit new (FTP, HTTP, Telnet)**.Por ejemplo, si usted quiere permitir Telnet a un sitio específico (“telnet el 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). Entonces **comando editing del** clic en Finalizar.
3. Realice el paso 2 para cada uno de los comandos permitidos (por ejemplo, Telnet, HTTP, y FTP).
4. Agregue la dirección IP PIX en la sección de Configuración de NAS con la ayuda del 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

Comandos Add de requerir la 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 característica 5.2 permite que esta declaración conjuntamente con la lista de acceso previamente definida 101 substituya las tres declaraciones anteriores. No deberían mezclarse la verbiage anterior y la nueva.

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

Ejemplos de depuración de autorización y autenticación PIX

La buena autenticación y la autorización tiene éxito - 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 error del mensaje “: Autorización negada.”

```
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 el software PIX versión 5.2 y posterior, defina las Listas de acceso en el PIX. Apliqúelas sobre por usuario una base basada en el perfil del usuario en el servidor. TACACS+ requiere autenticación y autorización. RADIUS sólo requiere autenticación. En este ejemplo, la autenticación de salida y la autorización al TACACS+ se cambian. Una lista de acceso en el PIX se configura.

Nota: En la versión de PIX 6.0.1 y posterior, si usted utiliza el RADIO, las Listas de acceso son implementadas ingresando la lista en el atributo 11 IETF RADIUS estándar 11 (id del filtro) [CSCdt50422]. En este ejemplo, el atributo 11 se fija a 115 en lugar de hacer el verbiage específico del vendedor del "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 TACACS+ freeware no reconoce el verbiage “acl”.

Configuración del servidor segura de Cisco UNIX TACACS+

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

Cisco Windows seguro TACACS+

Para agregar la autorización al PIX de controlar donde el usuario va con las Listas de acceso, marque el **shell/el ejecutivo**, marque el **cuadro de lista de control de acceso**, y complete el número (hace juego 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 asegura el Windows RADIUS

El tipo de dispositivo es RADIUS/Cisco Las necesidades de usuario del “pixa” un nombre de usuario, una contraseña, y un control y un "acl=115" en cuadro rectangular de Cisco/RADIUS donde dice el Par AV 009\001 (específico del vendedor).

Resultado

El usuario de salida “pixa” con el "acl=115" en el perfil autentica y autoriza. El servidor pasa abajo del acl=115 al PIX, y el PIX muestra esto:

```
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 a cualquier dirección IP excepto 99.99.99.2, porque hay un implícito niega), el usuario ve esto:

```
Error: acl authorization denied
```

Nueva lista de acceso por usuario descargable con versión 6.2

En el Software Release 6.2 y Posterior del firewall PIX, las Listas de acceso se definen en un Access Control Server (ACS) para descargar al PIX después de la autenticación. Esto trabaja

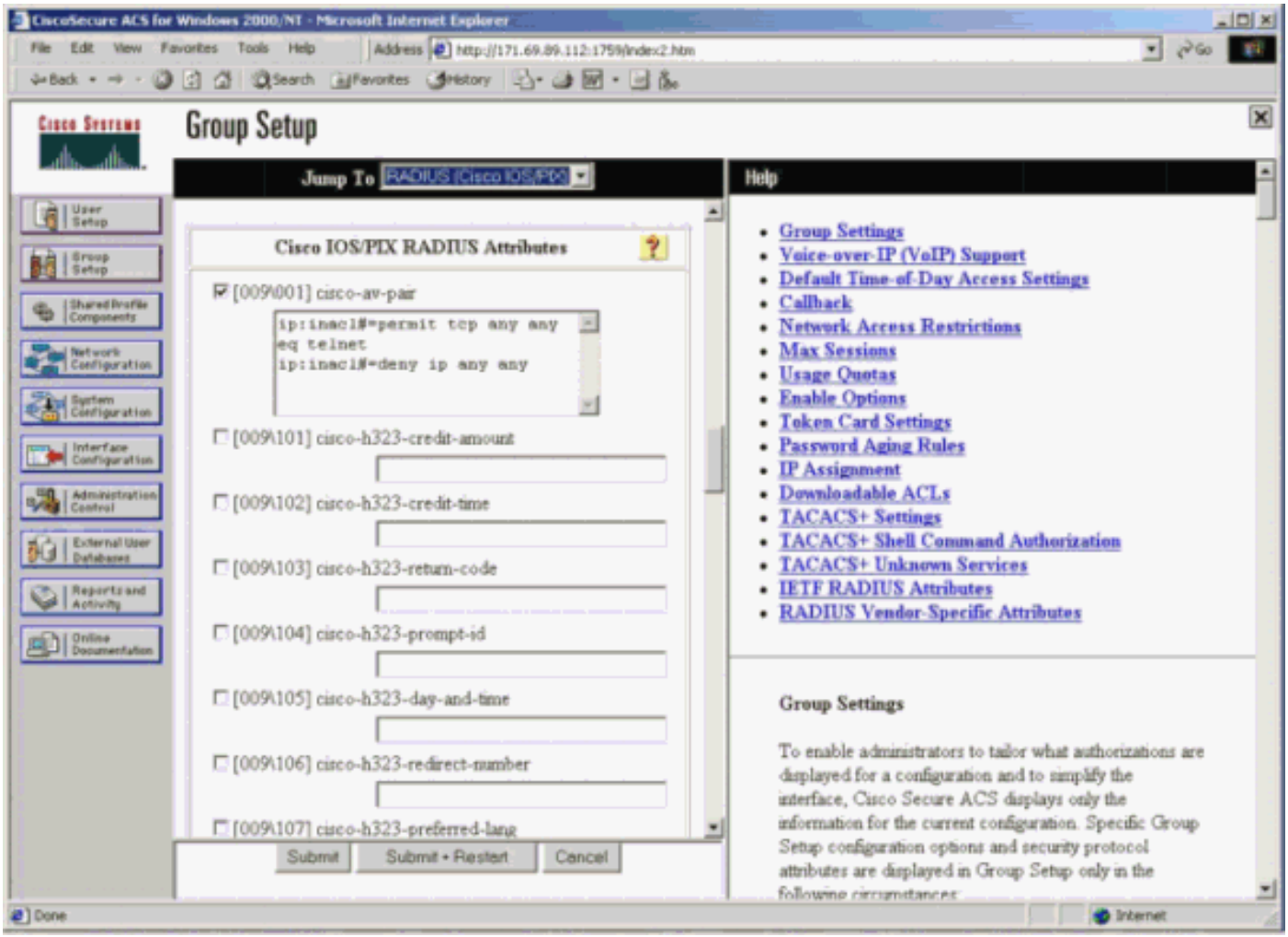
solamente con el protocolo RADIUS. No es necesario configurar la lista de acceso en el PIX. Una plantilla del grupo se aplica a los usuarios múltiples.

En las versiones anteriores, la lista de acceso se define en el PIX. Sobre la autenticación, el ACS avanzó el nombre de la lista de acceso al PIX. La nueva versión permite que el ACS avance la lista de acceso directamente al PIX.

Nota: Si ocurre la Conmutación por falla, la tabla del uauth no es usuarios copiados reauthenticated. La lista de acceso se descarga otra vez.

Configuración de ACS

Haga clic la **configuración de grupo** y seleccione el tipo de dispositivo **RADIUS (Cisco IOS/PIX)** configurar una cuenta de usuario. Asigne un nombre de usuario (“cse”, en este ejemplo) y la contraseña para el usuario. De la lista de atributos, seleccione la opción para configurar los vendedor-AV-**pares [009\001]**. Defina la lista de acceso como se ilustra en este ejemplo:



Depuración de PIX: Autenticación válida y lista de acceso descargada

- Permite solamente Telnet y niega el 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 solamente Telnet y permite el 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

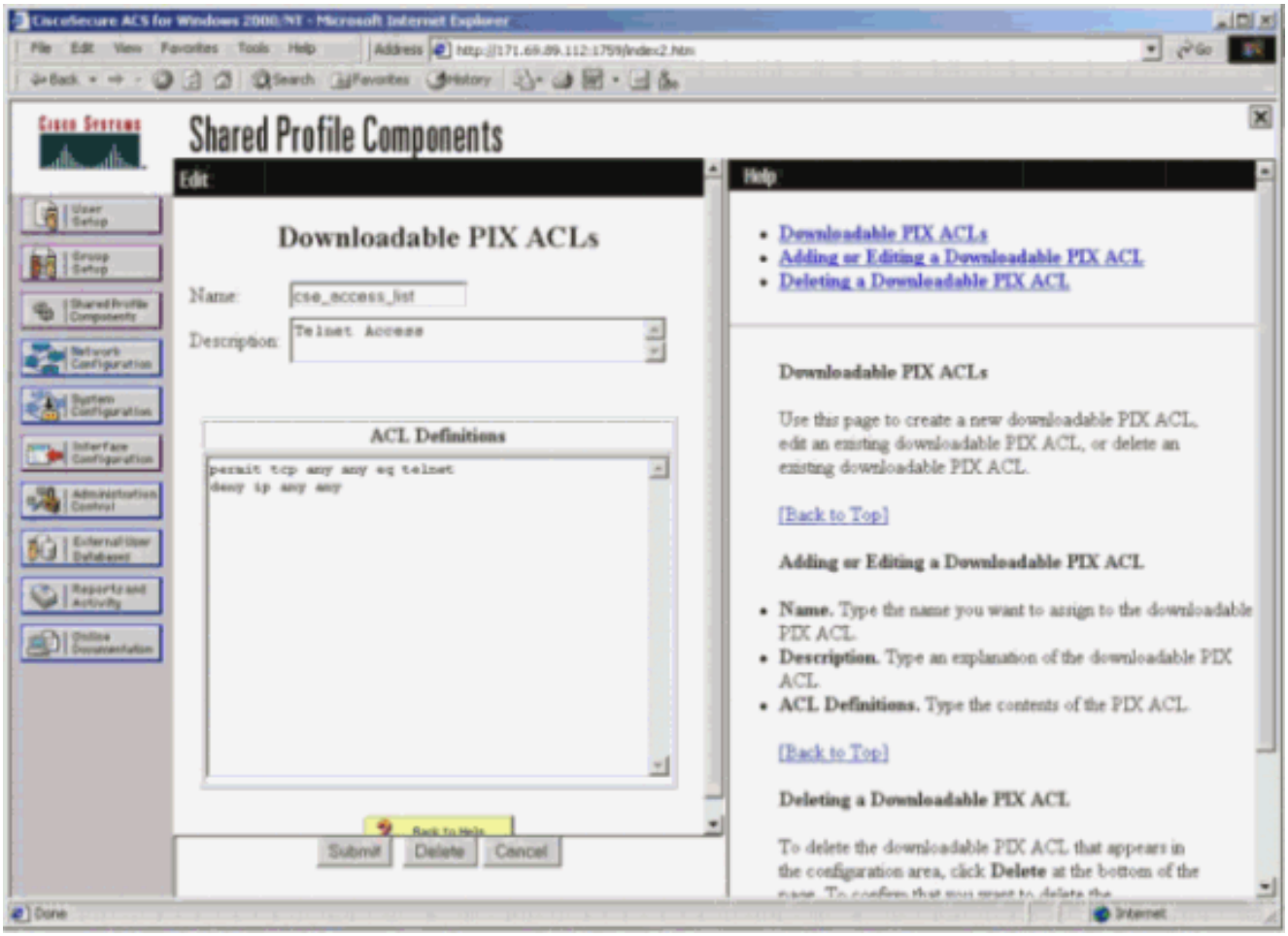
En la versión 3.0, el componente del perfil compartido le permite al usuario crear una plantilla de lista de accesos y definir el nombre de la plantilla para usuarios o grupos específicos. El nombre de la plantilla se puede utilizar con tantos usuarios o grupos según las necesidades. Esto elimina la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

Nota: Si ocurre la Conmutación por falla, el uauth no se copia al PIX secundario. En la falla de estado, se sostiene la sesión. Sin embargo, la nueva conexión debe reauthenticated y la lista de acceso se debe descargar otra vez.

Uso de perfiles compartidos

Complete estos pasos cuando usted utiliza los perfiles compartidos.

1. Haga clic en Interface Configuration (Configuración de interfaz).
2. Marque el **nivel de usuario ACL transferibles** y/o el Grupo-**nivel ACL transferibles**.
3. Haga clic a los **componentes del perfil compartidos**. Haga clic el **nivel de usuario ACL transferibles**.
4. Defina las ACL descargables.
5. Haga clic la **configuración de grupo**. Bajo los ACL transferibles, asigne la lista de acceso PIX a la lista de acceso creada
   anterior.



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

- Permite solamente Telnet y niega el 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 solamente Telnet y permite el 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 PIX - Agregue las estadísticas

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 utilice la nueva función en 5.2 para definir cuál debe ser considerado por 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 utilice la nueva función en 5.2 para definir cuál debe ser considerado por las Listas de acceso.

aaa accounting match 101 outside AuthOutbound

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

Nota: Los registros de contabilidad 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 de 99.99.99.2 afuera 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 de 172.18.124.114 dentro a 99.99.99.2 fuera de (Telnet) y a 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 usted decide que una fuente particular o un destino no necesita la autenticación, la autorización, o considerar, publique 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: Usted tiene ya los **comandos include**.

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

O, con la nueva función en 5.2, defina lo que usted quiere 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 usted excluye un cuadro de la autenticación y usted tiene autorización encendido, usted debe también excluir el cuadro de la autorización.

Sesiones máximas y usuarios conectados al sistema de la visión

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 trabaja bien para el HTTP. En este ejemplo, se utiliza una diversa configuración de red, pero los conceptos son lo mismo.

Telnets del usuario con el PIX, autenticando en la manera.

```
(pix) 109001: Auth start for user '???' from
         171.68.118.100/1200 to 9.9.9.25 /23
     (pix) 109011: Authen Session Start: user 'cse', Sid 3
     (pix) 109005: Authentication succeeded for user
         'cse' from 171.68.118.100/1200 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
```

Porque el servidor ha visto un expediente del “comienzo” pero ningún expediente de la “parada”, en este momento, el servidor muestra que abren una sesión al usuario de “Telnet”. Si el usuario intenta otra conexión que requiera la autenticación (quizás de otro PC), y si fijan a las sesiones máximas hasta el "1" en el servidor para este usuario (si se asume que las sesiones máximas de los soportes de servidor), la conexión es rechazada por el servidor. El usuario va alrededor su Telnet o negocio FTP en el host de destino, después las salidas (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. Aquí está un ejemplo de HTTP donde el usuario hojea de 171.68.118.100 a 9.9.9.25 con el PIX.

```
(pix) 109001: Auth start for user '???' from
    171.68.118.100/1281 to 9.9.9.25 /80
(pix) 109011: Authen Session Start: user 'cse', Sid 5
(pix) 109005: Authentication succeeded for user
    'cse' from 171.68.118.100/12 81 to 9.9.9.25/80
(pix) 302001: Built TCP connection 5 for faddr
    9.9.9.25/80 gaddr 9.9.9.10/12 81 laddr
    171.68.118.100/1281 (cse)
(server start account) Sun Nov 8 16:35:34 1998
    rtp-pinecone.rtp.cisco.com
cse PIX 171.68.118.100 start task_id=0x9
    foreign_ip=9.9.9.25 local_ip=171.68.118.100 cmd=http
(pix) 302002: Teardown TCP connection 5 faddr
    9.9.9.25/80 gaddr 9.9.9.10/128 1
laddr 171.68.118.100/1281 duration 0:00:00 bytes 1907 (cse)
(server stop account) Sun Nov 8 16:35.35 1998
    rtp-pinecone.rtp.cisco .com
cse PIX 171.68.118.100 stop task_id=0x9
    foreign_ip =9.9.9.25 local_ip=171.68.118.100
    cmd=http elapsed_time=0 bytes_ in=1907 bytes_out=223
```

El usuario lee la página web descargada. El registro de 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). No abren una sesión al usuario al sitio web. La conexión no está abierta cuando el usuario está leyendo la página web. Las sesiones máximas o los usuarios conectados al sistema de la visión no trabajan aquí. Esto es porque el tiempo de conexión (el tiempo entre “construido” y el “desmontaje”) en el HTTP es demasiado corto. El registro "iniciar" y "detener" es subsegundo. No hay expediente del “comienzo” sin un expediente de la “parada” puesto que los expedientes ocurren en virtualmente el mismo instante. Todavía hay un expediente del “comienzo” y de la “parada” enviado al servidor para cada transacción si el uauth está fijado para 0 o algo más grande. Sin embargo, las sesiones máximas y los usuarios conectados al sistema de la visión no trabajan debido a las naturalezas de la conexión HTTP.

Interfaz del usuario

Cambie a los usuarios del prompt ven

Si usted tiene el comando:

`auth-prompt prompt PIX515B`

entonces los usuarios que pasan con el PIX ven este prompt.

```
PIX515B
```

Personalice a los usuarios del mensaje ven

Si usted tiene los comandos:

auth-prompt accept "GOOD_AUTHENTICATION" auth-prompt reject "BAD_AUTHENTICATION"
entonces los usuarios ven un mensaje sobre el estado de autenticación en un registro 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 autenticación de TACACS+/autorización está prendido, esto se controla sobre por usuario una base. Este perfil del usuario se configura para controlar el descanso (éste está en el servidor Freeware TACACS+ y los descansos son en los 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

En el final de dos minutos:

Tiempo de espera absoluto - la sesión consigue derribada:

```
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

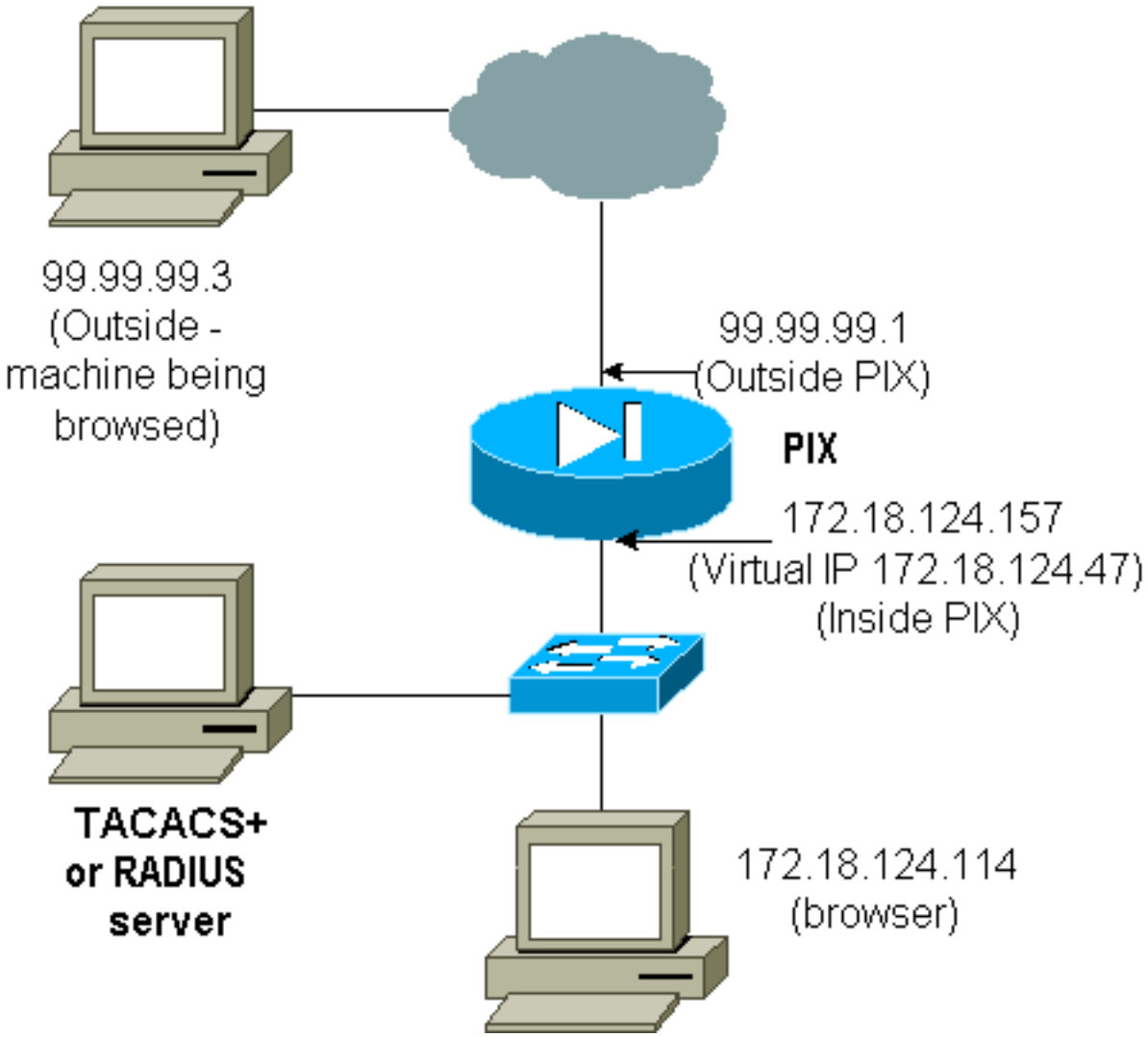
Si la autenticación se requiere en los sitios fuera del PIX así como en el PIX sí mismo, la conducta inusual del buscador se observa a veces, puesto que los navegadores ocultan el nombre de usuario y contraseña.

Para evitar esto, implemente el HTTP virtual agregando un direccionamiento del RFC 1918 (dirección no enrutable en el Internet, pero válido y único para la red interna PIX) a la configuración PIX en el formato.

virtual http #.#.#.# <warn>
Cuando el usuario intente salir de PIX, se le pedirá autenticación. Si está el parámetro de

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

Nota: El HTTP y los Telnet IP Address virtuales virtuales se deben incluir en las **sentencias de autenticación aaa**. En este ejemplo, especificar 0.0.0.0 incluye estos direccionamientos.



En la configuración PIX agregue este comando.

```
virtual http 172.18.124.47
```

El usuario señala al navegador en 99.99.99.3. Se visualiza este mensaje.

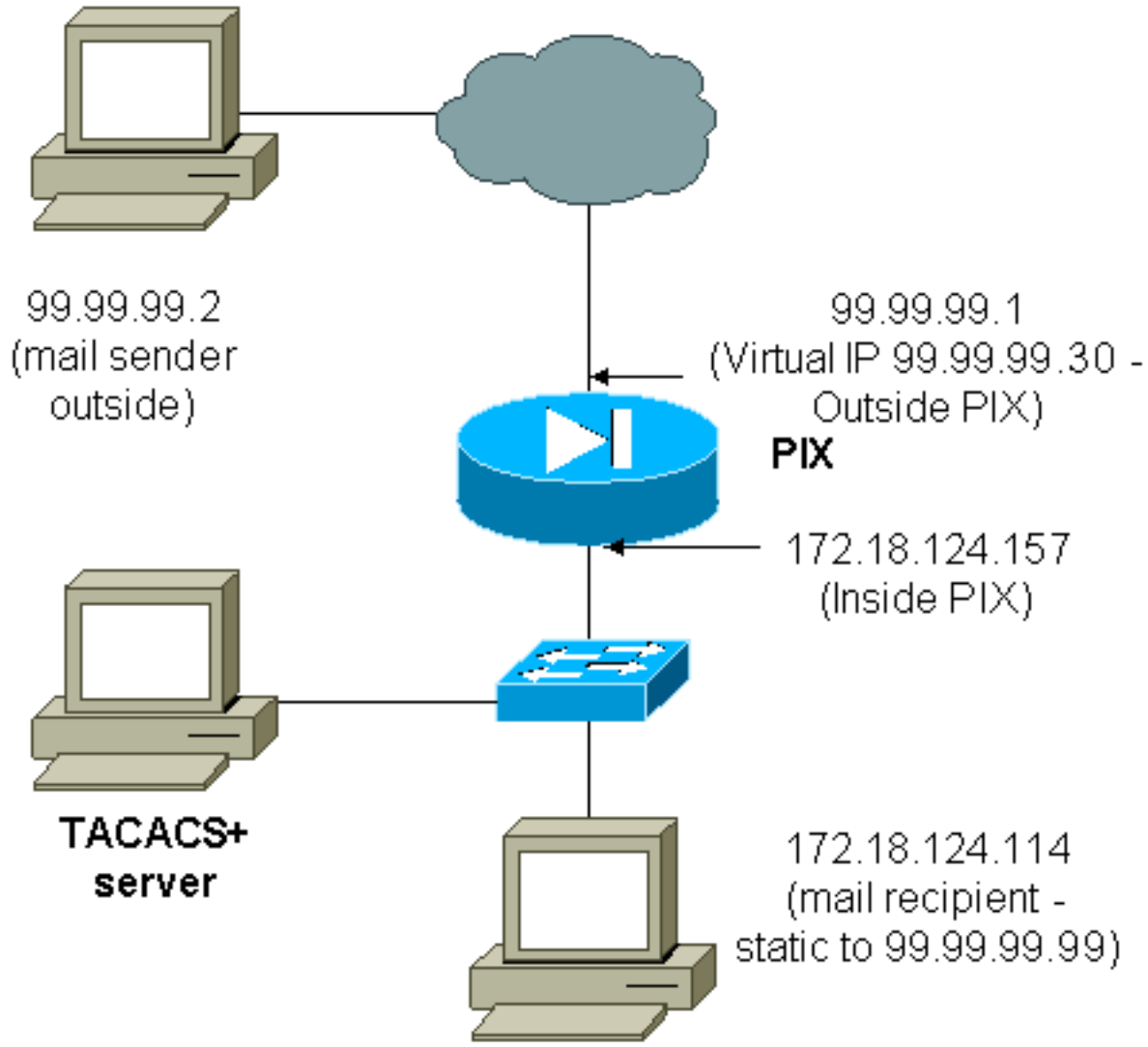
```
Enter username for PIX515B (IDXXX) at 172.18.124.47
```

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

Virtual telnet

Nota: El HTTP y los Telnet IP Address virtuales virtuales se deben incluir en las **sentencias de autenticación aaa**. En este ejemplo, especificar 0.0.0.0 incluye estos direccionamientos.

Entrada de Telnet virtual



No es una idea fabulosa autenticar el correo entrante puesto que una ventana no se visualiza para que el correo sea enviado entrante. Utilice el **comando exclude** en lugar de otro. Pero para el objetivo de la 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 (éste es freeware TACACS+):

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


user = pixuser {
login = cleartext "pixuser"
service = exec {
```

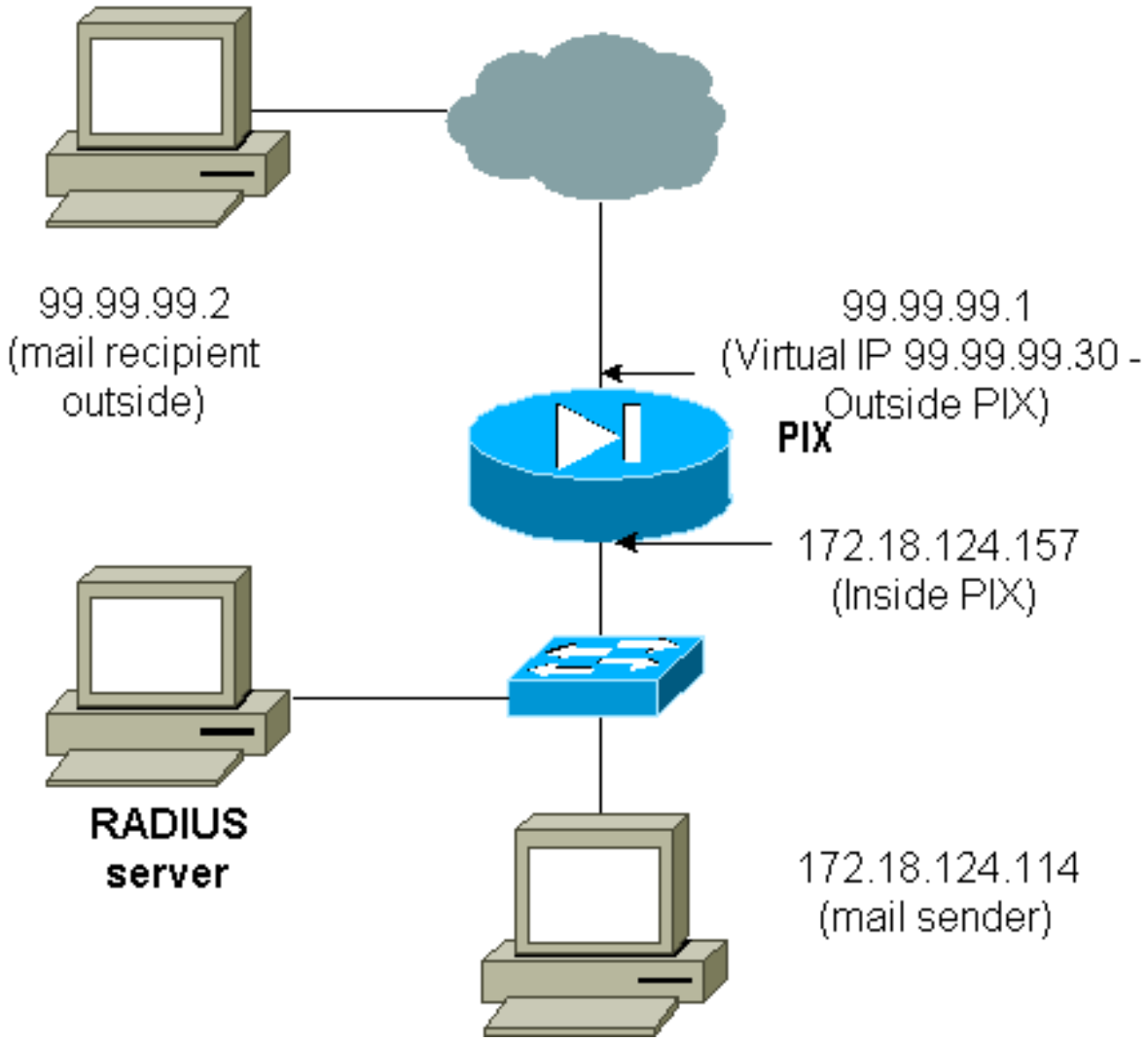
```
  }
  cmd = telnet {
  permit .*
  }
  }
```

Si solamente la autenticación está prendido, ambos usuarios envían el correo entrante después de autenticar en Telnet a la dirección IP 99.99.99.30. Si se habilita la autorización, el Telnets del “cse” del usuario a 99.99.99.30, y ingresa el nombre de usuario TACACS+/la contraseña. Los descensos de la conexión Telnet. El usuario “cse” entonces envía el correo a 99.99.99.99 (172.18.124.114). La autenticación tiene éxito para el usuario “pixuser”. Sin embargo, cuando el PIX envía el pedido de autorización para cmd=tcp/25 y cmd-arg=172.18.124.114, la petición falla, tal y como se muestra en de esta salida.

```
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 idea fabulosa autenticar el correo entrante puesto que una ventana no se visualiza para que el correo sea enviado entrante. Utilice el **comando exclude** en lugar de otro. Pero para el objetivo de la ilustración, se agregan estos comandos.

No es una idea fabulosa autenticar el correo saliente puesto que una ventana no se visualiza para que el correo sea enviado saliente. Utilice el **comando exclude** en lugar de otro. Pero con objeto del ejemplo, 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 el correo desde adentro a afuera, traiga para arriba un comando prompt en el host de correo y Telnet a 99.99.99.30. Esto abre el agujero para que el correo vaya a través. 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 es ilustrada por 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

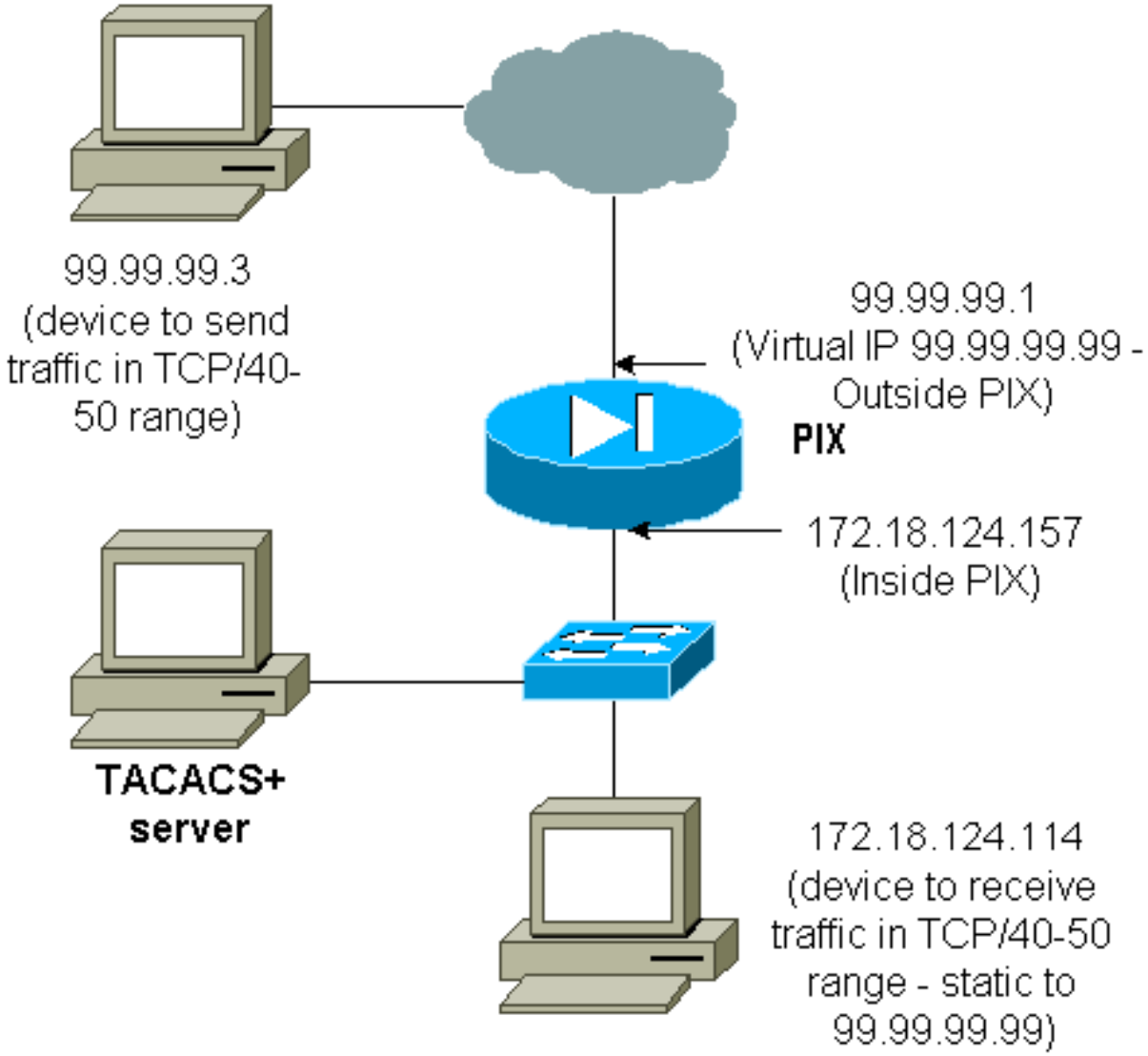
```
   pixfirewall#109001: Auth start for user 'cse' from 172.18.124.114/32863 to 99.99.99.30/23
109005: Authentication succeeded for user 'cse' from 172.18.124.114/32863 to 99.99.99.30/23 on
interface inside
```

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 la Telnet virtual se configura en el PIX, y la autorización se configura para un rango de puertos, el usuario abre el agujero con la 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 empujar tráfico TCP hacia adentro el rango del puerto 40-50 con el PIX a 99.99.99.99 (172.18.124.114), cmd=tcp/40-50 se envía al

servidor TACACS+ con cmd-arg=172.18.124.114 según lo ilustrado 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 que usted se aseegure los trabajos de la Telnet virtual para permitir el tráfico TCP/40-50 al host dentro de la red, agregue explicar 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+

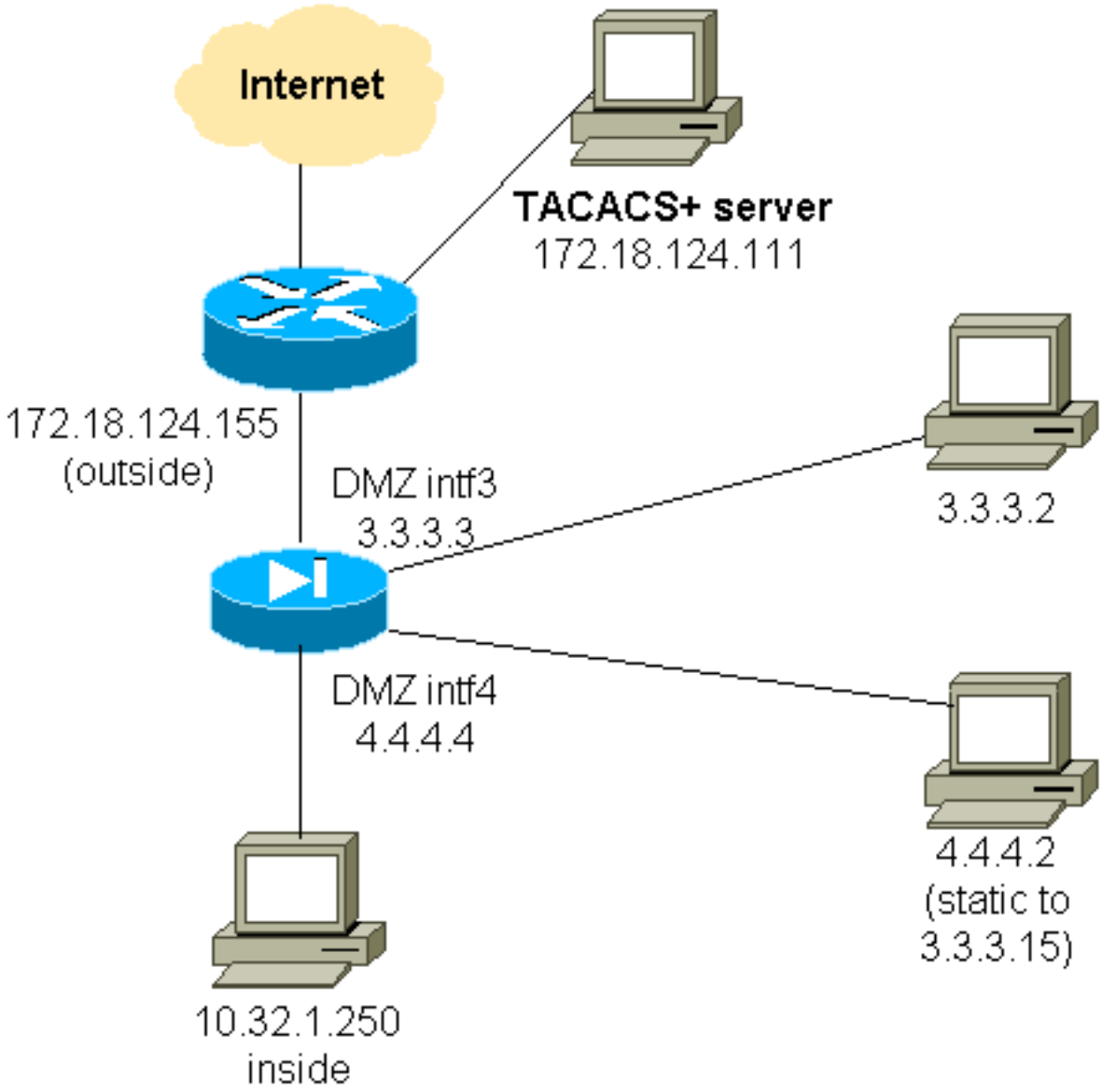
```
   Thu Aug 24 08:06:09 2000 172.18.124.157 cse PIX 99.99.99.3
   start task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
   cmd=tcp/40-50
   Thu Aug 24 08:06:17 2000 172.18.124.157 cse PIX 99.99.99.3
   stop task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
   cmd=tcp/40-50 elapsed_time=8 bytes_in=80 bytes_out=101
```

Autenticación en DMZ

Para autenticar a los usuarios que van a partir de una interfaz DMZ a otra, diga el PIX autenticar el tráfico para las interfaces mencionadas. En el PIX, el arreglo es como esto:

```
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 de Telnet entre pix/intf3 y pix/intf4, según lo demostrado 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 usted todavía necesita la ayuda después de seguir los pasos de Troubleshooting arriba y quiere abrir un caso con el TAC de Cisco, esté seguro de incluir esta información para resolver problemas su firewall PIX.

- Descripción del problema y detalles relevantes de la topología
- Troubleshooting antes de que usted abra el caso
- Resultado del comando show tech-support
- Salida del **comando show log** después de que usted se ejecute con el **comando logging buffered debugging**, o capturas de consola que demuestran el problema (si está disponible)

Adjunte los datos recopilados para su caso en un texto sin formato (.txt), sin compactar. Adjunte la información a su caso cargandolo con la ayuda de la herramienta del Case Query (clientes registrados solamente). Si usted no puede acceder la herramienta del Case Query, envíe la información en un elemento adjunto de correo electrónico a attach@cisco.com con su número de caso en el asunto de su 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
- Terminal Access Controller Access Control System (TACACS+)
- Remote Authentication Dial-In User Service (RADIUS)
- Soporte Técnico y Documentación - Cisco Systems