Configurar PIX 5.1.x: TACACS+ y RADIUS

Contenido

Introducción

El RADIUS y autenticación de TACACS+ se puede hacer para el FTP, Telnet, y las conexiones HTTP. Generalmente, se pueden hacer funcionar autenticaciones para otros protocolos menos comunes. Autorización TACACS+ se soporta; La autorización de RADIUS no. Los cambios en el Authentication, Authorization, and Accounting (AAA) PIX 5.1 sobre la versión anterior incluyen el Autenticación ampliada (Xauth)-- autenticación de los túneles IPsec del Cliente Cisco Secure VPN 1.1.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Antecedentes

Autenticación vs. Autorización

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

Suponga usted tiene cientos usuarios interiores y usted querer quisiera solamente que seis de estos usuarios pudieran hacer el FTP, Telnet, o el HTTP fuera de la red. Usted diría el PIX autenticar el tráfico saliente y dar los seis ID de los usuarios en el servidor de seguridad TACACS+/RADIUS. Con la autenticación simple, estos seis usuarios podrían ser autenticados con el nombre de usuario y contraseña, después salen. Los otros noventa y cuatro usuarios no podrían salir. El PIX indica a los usuarios para el nombre de usuario/la contraseña, después pasa su nombre de usuario y contraseña al servidor de seguridad TACACS+/RADIUS, y dependiendo de la respuesta, abre o niega la conexión. Estos seis usuarios podrían hacer el FTP, Telnet, o el HTTP.

Pero suponga a *uno de* estos seis usuarios, “Festus,” no es ser confiado en. Usted quisiera permitir que Festus hagan el FTP, pero no el HTTP o Telnet al exterior. Esto significa tener que agregar la *autorización*, es decir, autorizando *lo que* pueden hacer los usuarios además de autenticar quién son. Esto es solamente válido con el TACACS+. Cuando agregamos la *autorización al* PIX, el PIX primero envía el nombre de usuario y contraseña de Festus al servidor de seguridad, después envía un pedido de autorización que dice al servidor de seguridad lo que está intentando el “*comando*” Festus hacer. Con la configuración de servidor correctamente, Festus se podía permitir a “ftp 1.2.3.4” pero sería negado la capacidad al HTTP o a Telnet dondequiera.

Qué ve el usuario con la autenticación/autorización activada

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

- Telnet - El usuario ve una 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 necesita ingresar **local_username@remote_username** para el nombre de usuario y **local_password@remote_password** para la contraseña. El PIX envía el local_username y el local_password al servidor de seguridad local, y si la autenticación (y la autorización) es acertadas en el PIX/server, el remote_username y el remote_password se pasa al servidor FTP de destino más allá.
- **HTTP** - Una ventana se visualiza en el navegador que pide un nombre de usuario y contraseña. Si la autenticación (y la autorización) se realiza con éxito, el usuario accederá al sitio Web siguiente. Tenga presente que los *navegadores ocultan los nombres de usuario y contraseña*. Si aparece que el PIX debe medir el tiempo hacia fuera una conexión HTTP pero no está haciendo así pues, es probable que la reautentificación ocurra realmente con el navegador que tira el nombre de usuario guardado en memoria caché y la contraseña al PIX, que entonces 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, esta es la razón por la cual.
- **Túnel** - Al intentar hacer un túnel el tráfico IPSec en la red con el cliente VPN y el Xauth encendido, un cuadro gris para la “autenticación de usuario para la nueva conexión” se visualiza para el nombre de usuario/la contraseña.**Nota:** Esta autenticación se soporta empezando por el Cliente Cisco Secure VPN 1.1. Si el menú del **Help (Ayuda) > About (Acerca de)** no muestra la versión 2.1.x o posterior, éste no trabaja.

Configuración del servidor de seguridad utilizado para todos los escenarios

Configuración de servidor TACACS segura de Cisco UNIX

En esta sección, le presentan con la información para configurar a su servidor de seguridad.

Aseegurese que usted tiene la dirección IP o nombre y clave de dominio completamente calificar PIX en el archivo CSU.cfg.

```
user = ddunlap {
password = clear "rtp"
default service = permit
}

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

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

user = httponly {
password = clear "httponly"
service = shell {
cmd = http {
permit .*
}
}
}
```

Cisco asegura la Configuración del servidor del UNIX RADIUS

Utilice el GUI para agregar la dirección IP y la clave PIX a la lista del servidor de acceso a la red (NAS).

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

Cisco Secure ACS for Windows 2.x RADIUS

Utilice estos pasos para configurar el Cisco Secure ACS for Windows 2.x RADIUS.

1. Obtenga una contraseña en la sección de la GUI de configuración de usuario.
2. De la sección GUI de la configuración de grupo, fije el atributo 6 (tipo de servicio) **para iniciar sesión** o **administrativo**.
3. Agregue la dirección IP PIX en la sección de Configuración de NAS GUI.

EasyACS TACACS+

La documentación de EasyACS describe la configuración.

1. En la sección de grupo, **ejecutivo del shell del** tecleo para dar los privilegios exec.
2. Para agregar la autorización al PIX, haga clic en los **comandos deny unmatched ios** en la parte inferior de la configuración de grupo.
3. Seleccione el **comando add/edit new** para cada comando que usted desea permitir, por ejemplo, **Telnet**.
4. Si el Telnetting a los sitios específicos se permite, complete la dirección IP en la sección de argumento en el formulario “permiso #.#.#.#”. Si no, permitan el Telnetting, el tecleo **permite que todos los argumentos no enumerados**.
5. **Comando editing del** clic en Finalizar.
6. Realice los pasos 1 a 5 para cada uno de los comandos permitidos (por ejemplo, Telnet, HTTP o FTP).
7. Agregue el IP PIX en la sección GUI de la Configuración de NAS.

Cisco 2.x seguro TACACS+

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

1. En la sección de grupo, haga clic en el **ejecutivo del shell** para dar los privilegios exec.
2. Para agregar la autorización al PIX, en la parte inferior de la configuración de grupo, hace clic los **comandos deny unmatched ios**.
3. **Comando add/edit new** selecto para cada comando que usted desea permitir (por ejemplo, **Telnet**).
4. Para permitir el Telnetting a los sitios específicos, ingrese el IP Address en la sección de argumento en la forma “permiso #.#.#.#”. Para permitir el Telnetting a cualquier sitio, el tecleo **permite todos los argumentos no enumerados**.
5. **Comando editing del** clic en Finalizar.
6. Realice los pasos 1 a 5 para cada uno de los comandos permitidos (por ejemplo, Telnet, HTTP, o FTP).
7. Asegúrese que la dirección IP PIX esté agregada en la sección GUI de la Configuración de NAS.

‘Configuración del servidor Livingston RADIUS’

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

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

Configuración del servidor Merit RADIUS

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

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

Configuración del servidor freeware TACACS+

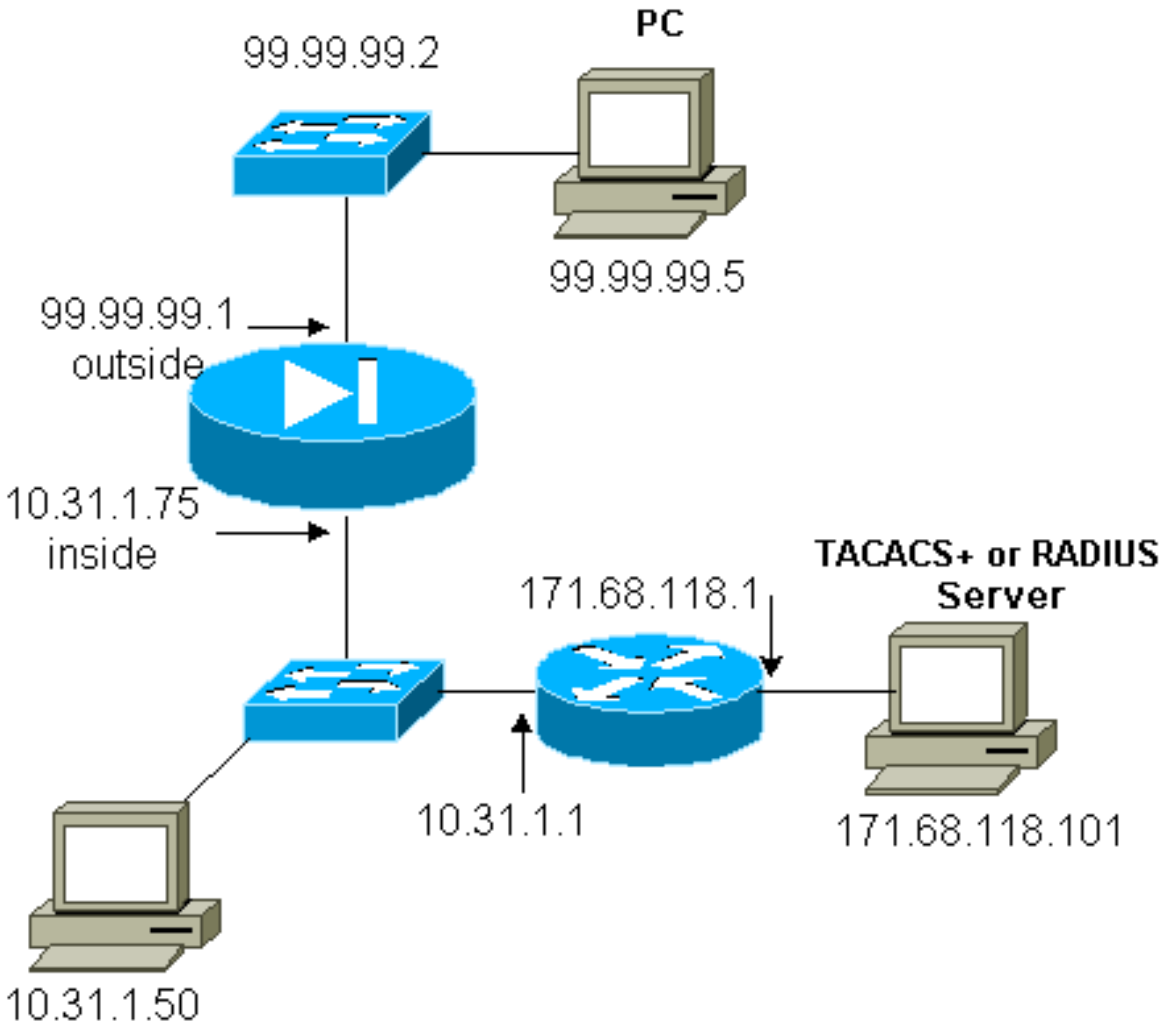
```
key = "cisco"
user = adminuser {
login = cleartext "all"
default service = permit
}

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

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

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

Pasos de depuración

Nota: La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- Aseegurese la configuración PIX está trabajando antes de agregar el AAA. Si usted no puede pasar el tráfico antes de instituir la autenticación y autorización, usted no podrá hacer tan luego.
- Permiso que abre una sesión el PIX.El debugging de la consola de registro no se debe utilizar en pesadamente un sistema cargado.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.
- Dé vuelta encendido a hacer el debug de en el TACACS+ o los servidores de RADIUS (todos los servidores tienen esta opción).

Diagrama de la red



Configuración de PIX

```
PIX Version 5.1(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 pix/intf2 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix3
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
names
pager lines 24
no logging timestamp
no logging standby
logging console debugging
no logging monitor
no logging buffered
no logging trap
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
```

```
mtu outside 1500
mtu inside 1500
mtu pix/intf2 1500
ip address outside 99.99.99.1 255.255.255.0
ip address inside 10.31.1.75 255.255.255.0
ip address pix/intf2 127.0.0.1 255.255.255.255
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address pix/intf2 0.0.0.0
arp timeout 14400
global (outside) 1 99.99.99.7-99.99.99.10 netmask
255.255.255.0
nat (inside) 1 10.31.1.0 255.255.255.0 0 0
static (inside,outside) 99.99.99.99 10.31.1.50 netmask
255.255.255.255 0 0
conduit permit icmp any any
conduit permit tcp any any
conduit permit udp any any
route outside 0.0.0.0 0.0.0.0 99.99.99.2 1
route inside 171.68.118.0 255.255.255.0 10.31.1.1 1
route inside 171.68.120.0 255.255.255.0 10.31.1.1 1
timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00
udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server AuthInbound protocol tacacs+
aaa-server AuthInbound (inside) host 171.68.118.101
cisco timeout 5
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 171.68.118.101
cisco timeout 5
aaa authentication include telnet outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication include telnet inbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authentication include http outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication include http inbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthInbound
aaa authentication include ftp outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication include ftp inbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthInbound
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
telnet timeout 5
terminal width 80
Cryptochecksum:b26b560b20e625c9e23743082484caca
: end
[OK]
```

Ejemplos de PIX del comando authentication debug

Esta sección muestra las muestras de debugs de la autenticación para los diversos escenarios.

Entrante

El usuario externo en 99.99.99.2 inicia el tráfico a 10.31.1.50 interior (99.99.99.99) y se autentica con el TACACS (es decir, el tráfico entrante utiliza la lista de servidores “AuthInbound” que incluye al servidor TACACS 171.68.118.101).

PIX debug - Buena autenticación - TACACS+

El ejemplo abajo muestra un PIX debug con la buena autenticación:

```
109001: Auth start for user '???' from
    99.99.99.2/11008 to 10.31.1.50/23
109011: Authen Session Start: user 'cse', sid 4
109005: Authentication succeeded for user 'cse'
    from 10.31.1.50/23 to 99.99.99.e
302001: Built inbound TCP connection 10 for
    faddr 99.99.99.2/11008 gaddr 99.99.)
```

PIX debug - Autentificación que resultó mal (nombre de usuario o contraseña) - TACACS+

El ejemplo abajo muestra un PIX debug con la autentificación que resultó mal (nombre de usuario o contraseña). El usuario ve tres nombres de usuario/contraseñas definidas, seguidos por este mensaje: `Error: Número máximo de intentos excedidos.`

```
109001: Auth start for user '???' from
     99.99.99.2/11010 to 10.31.1.50/23
  109006: Authentication failed for user '' from
     10.31.1.50/23 to 99.99.99.2/11010 on
     interface outside
```

PIX debug - Puede hacer ping el servidor, ninguna respuesta - TACACS+

El ejemplo abajo muestra un PIX debug donde está pingable el servidor, pero el discurso al PIX. El usuario ve el nombre de usuario una vez, pero el PIX nunca pide una contraseña (éste está en Telnet). El usuario ve el `error: Número máximo de intentos excedidos.`

```
109001: Auth start for user '???' from 99.99.99.2/11011
     to 10.31.1.50/23
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
  109006: Authentication failed for user '' from 10.31.1.50/23
     to 99.99.99.2/11011 on interface outside
```

PIX debug - Incapaz de hacer ping el servidor - TACACS+

El ejemplo abajo muestra a PIX debug donde no está pingable el servidor. El usuario ve el nombre de usuario una vez, pero el PIX nunca pide una contraseña (éste está en Telnet). Se

visualizan los siguientes mensajes: `Descanso al servidor` y al `error TACACS+: Número máximo de intentos excedidos` (intercambiaron a un servidor ficticio adentro la configuración).

```
111005: console end configuration: OK
  109001: Auth start for user '???' from
     99.99.99.2/11012 to 10.31.1.50/23
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109006: Authentication failed for user '' from
     10.31.1.50/23 to 99.99.99.2/11012 on interface
     outside
```

PIX debug - Buena autenticación - RADIUS

El ejemplo abajo muestra un PIX debug con la buena autenticación:

```
109001: Auth start for user '???' from
     10.31.1.50/11008 to 99.99.99.2/23
  109011: Authen Session Start: user 'pixuser', sid 8
  109005: Authentication succeeded for user
     'pixuser' from 10.31.1.50/11008 to
     99.99.99.2/23 on interface inside
  302001: Built outbound TCP connection 16 for faddr
     99.99.99.2/23 gaddr 99.99.99.99/11008
     laddr 10.31.1.50/11008 (pixuser)
```

PIX debug - Autentificación que resultó mal (nombre de usuario o contraseña) - RADIUS

El ejemplo abajo muestra un PIX debug con la autentificación que resultó mal (nombre de usuario o contraseña). El usuario ve la petición para un nombre de usuario y contraseña, y tiene tres oportunidades de ingresar éstos. Cuando la entrada es fracasada, se visualiza el siguiente mensaje: `Error: Número máximo de intentos excedidos`.

```
109001: Auth start for user '???' from 10.31.1.50/11010
     to 99.99.99.2/23
  109006: Authentication failed for user ''
     from 10.31.1.50/11010 to 99.99.99.2/23
     on interface inside
```

PIX debug - Puede hacer ping el servidor, la daemon abajo - RADIUS

El ejemplo abajo muestra a PIX debug donde está pingable el servidor, pero la daemon está abajo y no comunicará con el PIX. El usuario ve el nombre de usuario, entonces contraseña, el `mensaje fallido del servidor de RADIUS`, y el `error: Número máximo de intentos excedidos.`.

```
109001: Auth start for user '???' from 10.31.1.50/11011
     to 99.99.99.2/23
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  1ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
```

```
  09002: Auth from 10.31.1.50/11011 to 99.99.99.2/23
     failed (server 171.68.118.101 failed) on interface inside
  109002: Auth from 10.31.1.50/11011 to 99.99.99.2/23 failed
     (server 171.68.118.101 failed) on interface inside
  109002: Auth from 10.31.1.50/11011 to 99.99.99.2/23 failed
     (server 171.68.118.101 failed) on interface inside
  109006: Authentication failed for user '' from 10.31.1.50/11011
     to 99.99.99.2/23 on interface inside
```

PIX debug - Incapaz de hacer ping el servidor o la discrepancia de clave/cliente - RADIUS

El ejemplo abajo muestra a PIX debug donde no está pingable el servidor o hay un cliente/una discrepancia de clave. El usuario ve un nombre de usuario, la contraseña, el `descanso al` mensaje del `servidor de RADIUS`, y el `error: El Número máximo de` mensaje `excedido los intentos un` servidor ficticio fue intercambiado adentro la configuración).

```
109001: Auth start for user '???' from 10.31.1.50/11012
     to 99.99.99.2/23
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109006: Authentication failed for user '' from 10.31.1.50/11012
     to 99.99.99.2/23 on interface inside
```

Agregado de autorización

Si usted decide agregar la autorización, puesto que la autorización es inválida sin la autenticación, usted necesita requerir la autorización para el mismo rango de origen y de destino.

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

Observe que usted no agrega la autorización para saliente porque el tráfico saliente se autentica con el RADIUS, y la autorización de RADIUS es inválida.

Ejemplos de Depuración de Autenticación y Autorización de PIX

PIX debug - Buena autenticación y autorización exitosa - TACACS+

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

```
109001: Auth start for user '???' from 99.99.99.2/11016
   to 10.31.1.50/23
109011: Authen Session Start: user 'cse', Sid 11
109005: Authentication succeeded for user 'cse'
   from 10.31.1.50/23 to 99.99.99.2/11016 on interface outside
109011: Authen Session Start: user 'cse', Sid 11
109007: Authorization permitted for user 'cse' from
   99.99.99.2/11016 to 10.31.1.50/23 on interface outside
```

```
302001: Built inbound TCP connection 19 for faddr 99.99.99.2/11016
   gaddr 99.99.99.99/23 laddr 10.31.1.50/23 (cse)
```

PIX debug - Buena autenticación, autorización fallida - TACACS+

El ejemplo abajo muestra el PIX debug con la buena autenticación pero la autorización fallida. Aquí el usuario también ve el mensaje de error: `Autorización negada`.

```
109001: Auth start for user '???' from
    99.99.99.2/11017 to 10.31.1.50/23
109011: Authen Session Start: user 'httponly',
   Sid 12
109005: Authentication succeeded for user 'httponly'
   from 10.31.1.50/23 to 99.99.99.2/11017 on
   interface outside
109008: Authorization denied for user 'httponly' from
   10.31.1.50/23 to 99.99.99.2/11017 on interface outside
```

Incorporación de contabilidad

TACACS+

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

Freeware TACACS+ hecho salir:

```
Tue Feb 22 08:52:20 2000  10.31.1.75 cse PIX
   99.99.99.2 start task_id=0x14
   foreign_ip=99.99.99.2 local_ip=10.31.1.50
   cmd=telnet
Tue Feb 22 08:52:25 2000  10.31.1.75 cse PIX
   99.99.99.2 stop task_id=0x14
   foreign_ip=99.99.99.2 local_ip=10.31.1.50
   cmd=telnet elapsed_time=5
   bytes_in=39 bytes_out=126
```

RADIUS

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

Merit RADIUS hecho salir:

```
Tue Feb 22 08:56:17 2000
        Acct-Status-Type = Start
        NAS-IP-Address = 10.31.1.75
        Login-IP-Host = 10.31.1.50
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000015
        User-Name = pixuser
```

```
        Tue Feb 22 08:56:24 2000
        Acct-Status-Type = Stop
        NAS-IP-Address = 10.31.1.75
        Login-IP-Host = 10.31.1.50
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000015
        Username = pixuser
        Acct-Session-Time = 6
        Acct-Input-Octets = 139
        Acct-Output-Octets = 36
```

Uso del comando Exclude

Si agregamos otro exterior del host (en 99.99.99.100) a nuestra red, y se confía en este host, usted puede excluirlos de la autenticación y autorización con los siguientes comandos:

```
aaa authentication exclude telnet inbound 0.0.0.0 0.0.0.0 99.99.99.100
 255.255.255.255 AuthInbound

aaa authorization exclude telnet inbound 0.0.0.0 0.0.0.0 99.99.99.100 255.255.255.255
AuthInbound
```

Establecer el número máximo de sesiones y ver a los usuarios conectados

Algunos servidores TACACS+ y RADIUS tienen funciones que permiten establecer un número máximo de sesiones o ver a los usuarios conectados. La posibilidad de establecer un número máximo de sesiones o verificar los usuarios conectados depende de los registros de contabilidad. Cuando se genera un 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. Esto no funciona bien para HTTP debido a la naturaleza de la conexión. En el siguiente ejemplo, se utiliza una diversa configuración de red, pero los conceptos son lo mismo.

El usuario establece una conexión Telnet por medio de PIX, autenticación en camino.

```
   171.68.118.100/1200 to 9.9.9.25 /23
  (pix) 109011: Authen Session Start: user
     'cse', Sid 3
  (pix) 109005: Authentication succeeded for user
     'cse' from 171.68.118.100/12 00 to 9.9.9.25/23
  (pix) 302001: Built TCP connection 5 for faddr
     9.9.9.25/23 gaddr 9.9.9.10/12 00
     laddr 171.68.118.100/1200 (cse)
  (server start account) Sun Nov 8 16:31:10 1998
     rtp-pinecone.rtp.cisco.com cse
  PIX 171.68.118.100 start task_id=0x3 foreign_ip=9.9.9.25
     local_ip=171.68.118.100 cmd=telnet
```

Porque el servidor ha visto un registro de 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 a 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. Abajo está un ejemplo de HTTP:

El usuario hojea de 171.68.118.100 a 9.9.9.25 con el PIX:

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

El usuario lee la página web descargada.

El registro de 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). ¿Está el usuario conectado aún con el sitio web y la conexión está abierta aún cuando el usuario está leyendo la página web? No. ¿Se utilizarán aquí las funciones que permiten establecer un número máximo de sesiones y ver a los usuarios conectados? No, porque el tiempo de conexión (el tiempo entre la 'conexión' y la 'desconexión') en HTTP es demasiado corto. El registro de inicio y de detención es sub-segundo. No hay un registro de comienzo sin un expediente de la parada puesto que los expedientes ocurren en virtualmente el mismo instante. Todavía habrá registro de inicio y de detención enviado al servidor para cada transacción si el uauth está fijado para 0 o algo más grande. Sin embargo, las funciones número máximo de

sesiones y ver usuarios conectados no funcionarán debido a la índole de las conexiones HTTP.

Autenticación y activación en el PIX mismo

La explicación anterior se refiere al tráfico de autenticidad de Telnet (y HTTP, FTP) con el PIX. Asegure Telnet a los trabajos PIX sin la autenticación encendido:

```
telnet 10.31.1.5 255.255.255.255
passwd ww
```

Entonces agregue el comando de autenticar el Telnetting de los usuarios al PIX:

```
aaa authentication telnet console AuthInbound
```

Cuando indican al usuario de telnet al PIX, él para la contraseña de Telnet (**WW**). El PIX también pide el TACACS+ o el nombre de usuario de RADIUS y la contraseña. En este caso puesto que se utiliza la lista de servidores del AuthInbound, el PIX pide el nombre de usuario y contraseña TACACS+.

Si el servidor está abajo, usted puede acceder el PIX ingresando el **pix** para el nombre de usuario, y entonces la contraseña habilitada (**contraseña habilitada *sea cual sea***). Con el comando:

```
aaa authentication enable console AuthInbound
```

Indican al usuario para un nombre de usuario y contraseña que se envíe al TACACS o al servidor de RADIUS. En este caso puesto que se utiliza la lista de servidores del AuthInbound, el PIX pide el nombre de usuario y contraseña TACACS+.

Puesto que el paquete de autenticación para el permiso es lo mismo que el paquete de autenticación para el login, si el usuario puede iniciar sesión al PIX con el TACACS o el RADIUS, pueden habilitar con el TACACS o el RADIUS con el mismo nombre de usuario/la contraseña. Este problema se ha asignado el Id. de bug Cisco CSCdm47044 (clientes registrados solamente).

Si el servidor está abajo, usted puede acceder el enable mode PIX entrando el **pix** para el nombre de usuario y la contraseña habilitada normal del PIX (**contraseña habilitada *sea cual sea***). Si enable password lo que sea no se encuentra en la configuración PIX, ingrese pix para el nombre de usuario y presione Enter (Aceptar). Si se fija pero no se sabe la contraseña habilitada, un disco de recuperación de contraseña necesita ser construido para reajustar la contraseña.

Modificación de la línea de comando que ven los usuarios

Si usted tiene el comando:

```
auth-prompt PIX_PIX_PIX
```

los usuarios que pasan con el PIX ven la secuencia siguiente:

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

En la llegada en el destino final, los usuarios verían el nombre de usuario: y contraseña: prompt visualizado por el cuadro de destino. Este prompt afecta solamente a los usuarios que van *con el* PIX, no al PIX.

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

Personalizar el mensaje que ven los usuarios en Éxito/Fracaso

Si el youh tiene los comandos:

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

entonces los usuarios ven la secuencia siguiente en un registro fallido/exitoso con el PIX:

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

Tiempos de Espera Absolutos e Inactivos por Usuario

Esta función no está trabajando actualmente y el problema se ha asignado el Id. de bug Cisco CSCdp93492 (clientes registrados solamente).

HTTP virtual

Si se requiere autenticación en los sitios fuera del PIX como así también en el mismo PIX, a veces se puede observar un comportamiento inusual del explorador, ya que los exploradores colocan el nombre de usuario y la contraseña en la memoria caché.

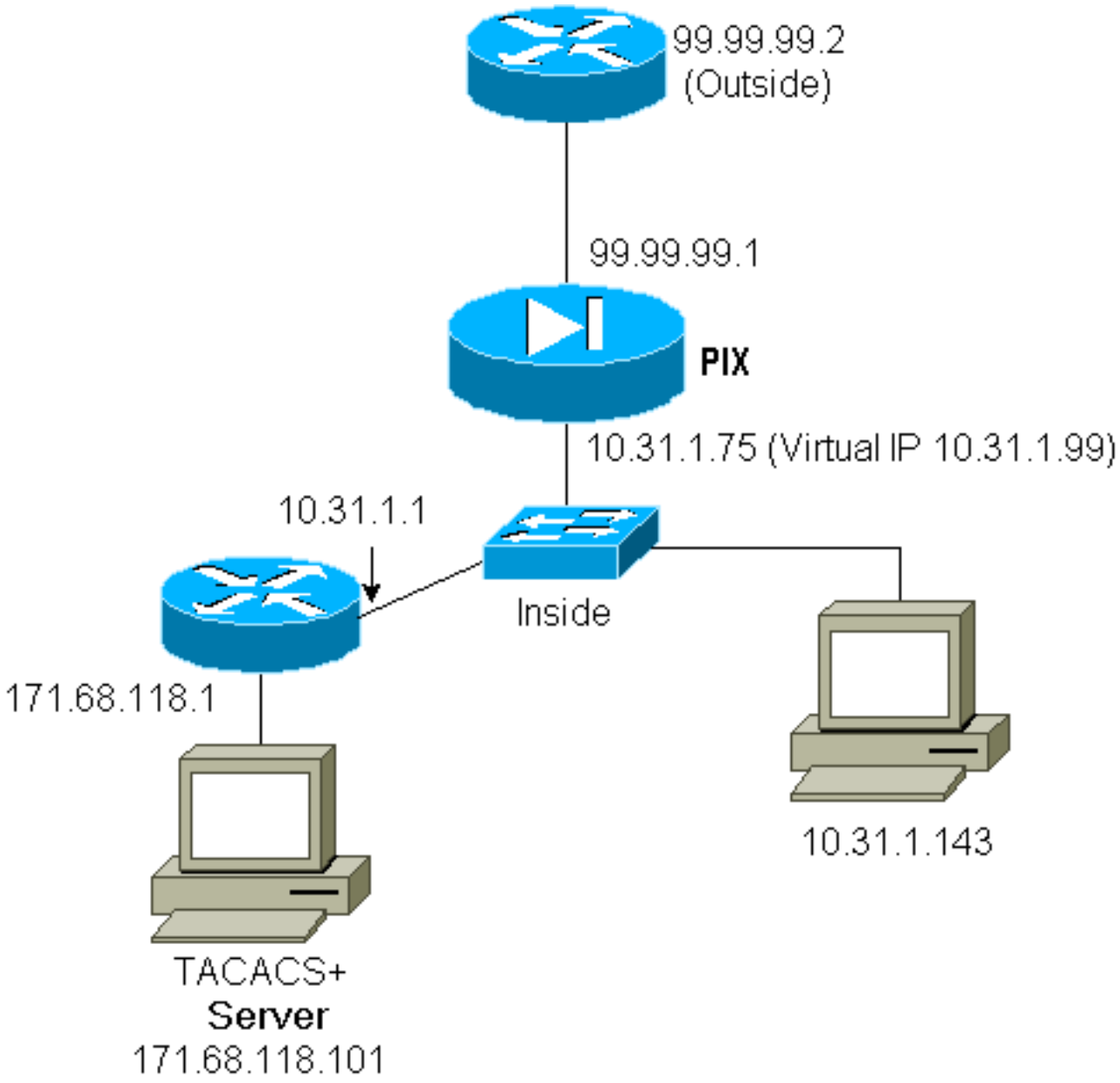
Para evitar esto, usted puede implementar el HTTP virtual agregando un direccionamiento del RFC 1918 (es decir, un direccionamiento que es unroutable en el Internet, pero válido y único para la red interna PIX) a la configuración PIX usando el siguiente comando:

```
virtual http #.#.#.# [warn]
```

Cuando el usuario intente salir de PIX, se le pedirá autenticación. Si está el parámetro de advertencia, el usuario recibe un mensaje de redirección. La autenticación sirve durante el

período de tiempo en uauth. Como se indica en la documentación, no 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.

Ejemplo de salida de HTTP virtual



Configuración PIX HTTP de salida virtual:

```
ip address outside 99.99.99.1 255.255.255.0
ip address inside 10.31.1.75 255.255.255.0
global (outside) 1 99.99.99.7-99.99.99.10 netmask 255.255.255.0
timeout uauth 01:00:00
aaa authentication include http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa-server RADIUS protocol radius
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 5
virtual http 10.31.1.99
```

Virtual telnet

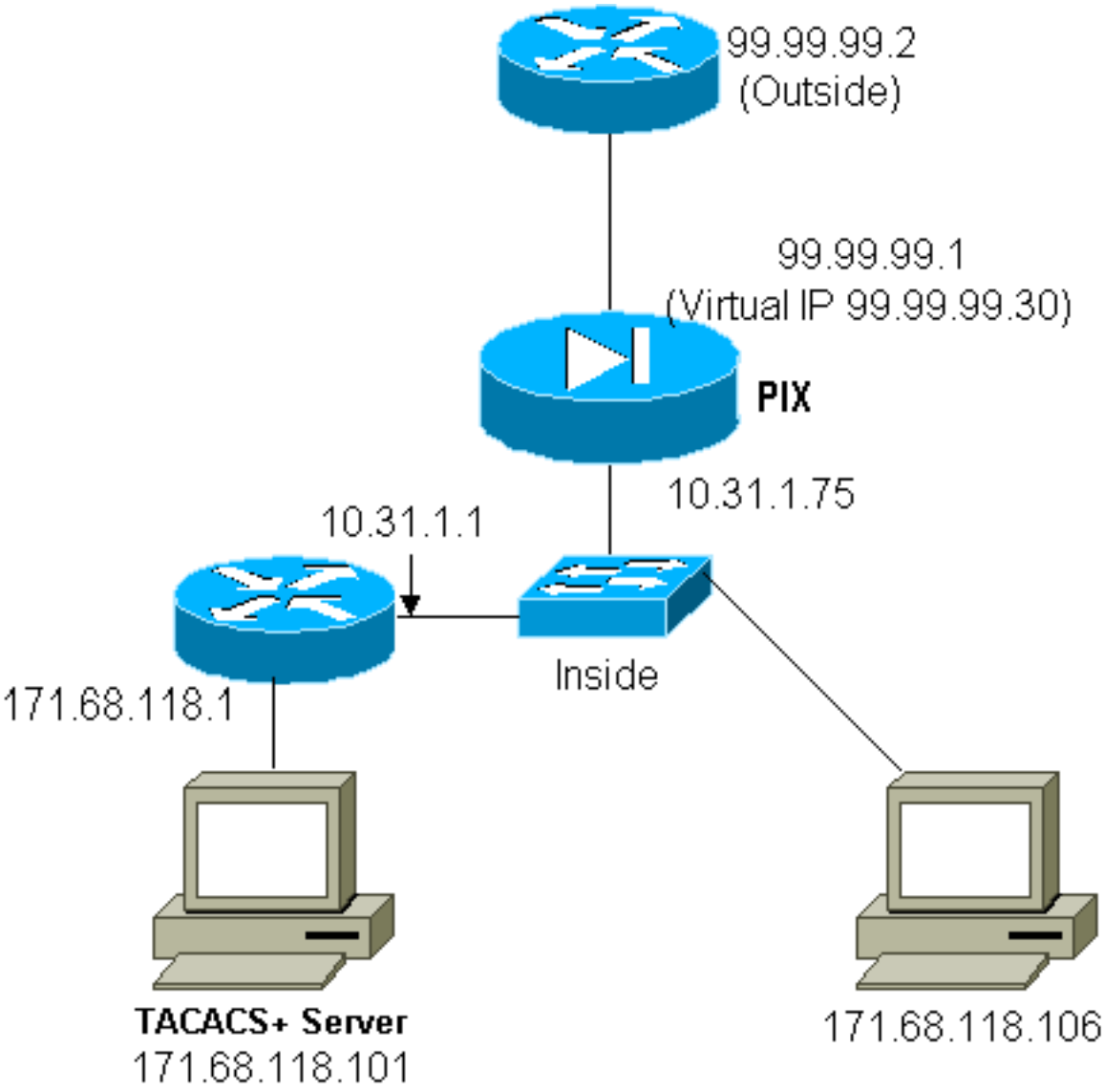
Es posible configurar el PIX para autenticar todo entrante y saliente, pero no es una buena idea porque algunos protocolos, tales como correo, no se autentican fácilmente. Cuando un mail server y un cliente intentan comunicar con el PIX cuando todo el tráfico con el PIX se está autenticando, el syslog PIX para los protocolos no autenticables muestra los mensajes por ejemplo:

```
109013: User must authenticate before using
    this service
109009: Authorization denied from 171.68.118.106/49
    to 9.9.9.10/11094    (not authenticated)
```

Sin embargo, si hay realmente una necesidad de autenticar una cierta clase de servicio inusual, esto se puede hacer por medio del **comando virtual telnet**. Este comando permite que la autenticación ocurra al Telnet IP Address virtual. Después de esta autenticación, el tráfico para el servicio inusual puede ir al servidor real.

En este ejemplo, usted quisiera que el tráfico del puerto TCP 49 fluyera del host exterior 99.99.99.2 al host interior 171.68.118.106. Puesto que este tráfico no es realmente authenticatable, configure una Telnet virtual. Para la Telnet virtual, debe haber parásitos atmosféricos asociados. Aquí, 99.99.99.20 y 171.68.118.20 son direcciones virtuales.

Entrada de Telnet virtual



Entrada Telnet virtual de la configuración PIX

```
ip address outside 99.99.99.1 255.255.255.0
ip address inside 10.31.1.75 255.255.255.0
static (inside,outside) 99.99.99.20 171.68.118.20 netmask 255.255.255.255 0 0
static (inside,outside) 99.99.99.30 171.68.118.106 netmask 255.255.255.255 0 0
conduit permit tcp host 99.99.99.20 eq telnet any
conduit permit tcp host 99.99.99.30 eq tacacs any
aaa-server TACACS+ protocol tacacs+
aaa-server Incoming protocol tacacs+
aaa-server Incoming (inside) host 171.68.118.101 cisco timeout 5
aaa authentication include telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Incoming
aaa authentication include tcp/49 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Incoming
virtual telnet 99.99.99.20
```

Entrada Telnet virtual del PIX debug

El usuario en 99.99.99.2 debe primero autenticar por el Telnetting al direccionamiento de 99.99.99.20 en el PIX:

```
109001: Auth start for user '???' from
    99.99.99.2/22530 to 171.68.118.20/23
 109011: Authen Session Start: user 'cse', Sid 13
 109005: Authentication succeeded for user
    'cse' from 171.68.118.20/23 to
    99.99.99.2/22530 on interface outside
```

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

```
pixfirewall# show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
user 'cse' at 99.99.99.2, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

Y cuando el dispositivo en 99.99.99.2 quiere enviar el tráfico TCP/49 al dispositivo en 171.68.118.106:

```
302001: Built inbound TCP connection 16
    for faddr 99.99.99.2/11054 gaddr
    99.99.99.30/49 laddr 171.68.118.106/49 (cse)
```

La autorización puede ser agregada:

```
aaa authorization include tcp/49 inbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

de modo que cuando el tráfico TCP/49 se intenta con el PIX, el PIX también envíe la interrogación de la autorización al servidor:

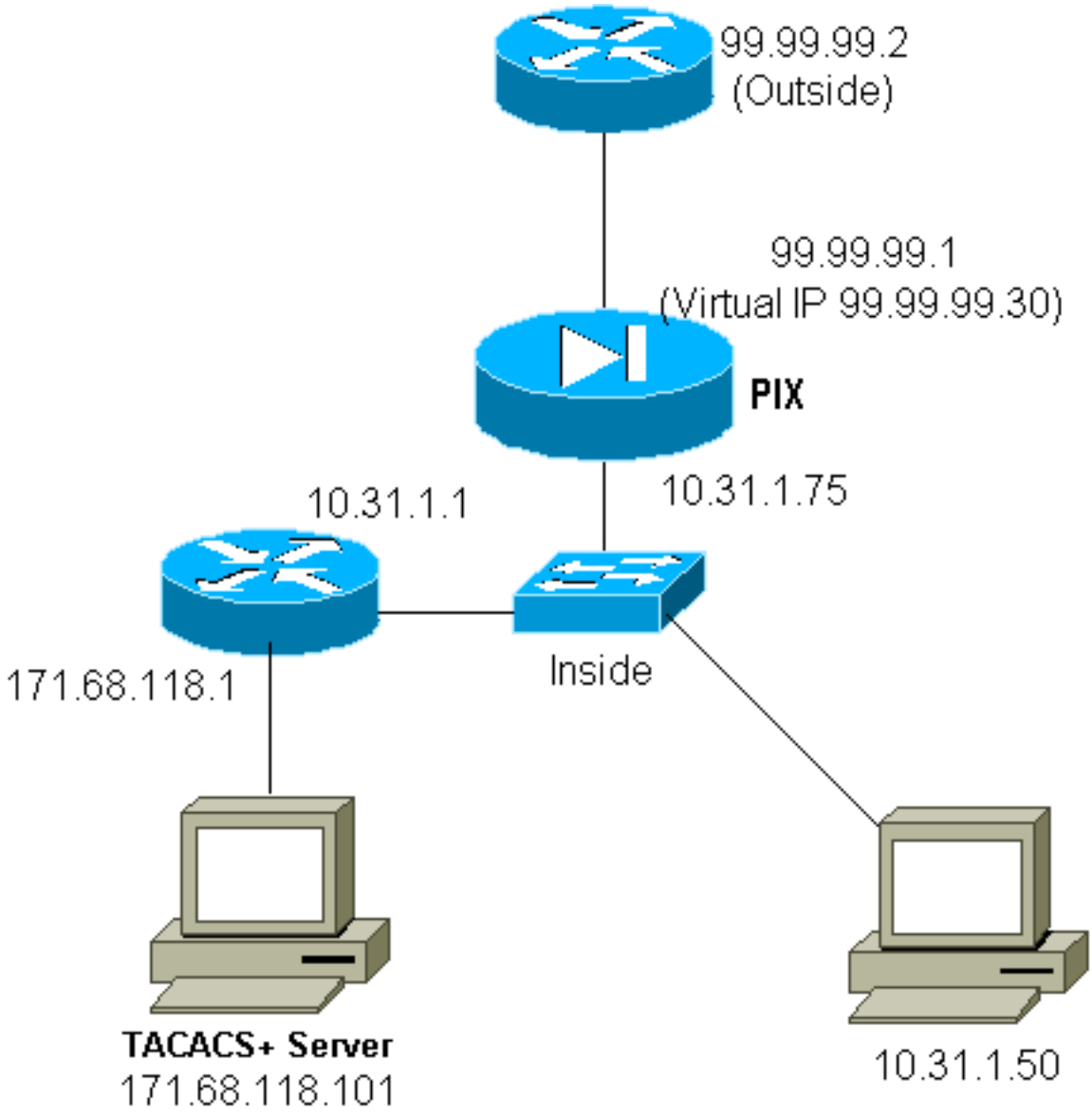
```
109007: Authorization permitted for user 'cse'
    from 99.99.99.2/11057 to 171.68.118.106/49
    on interface outside
```

En el servidor TACACS+, esto se ve como:

```
service=shell,
  cmd=tcp/49,
  cmd-arg=171.68.118.106
```

Virtual Telnet de salida

Puesto que el tráfico saliente se permite por abandono, no estático se requiere para el uso de la Telnet virtual saliente. En el siguiente ejemplo, el usuario interior en el Telnets de 10.31.1.50 a 99.99.99.30 virtual y autentica; la conexión Telnet se cae inmediatamente. Una vez que está autenticado, tráfico TCP se permite de 10.31.1.50 al servidor en 99.99.99.2:



Telnet virtual saliente de la configuración PIX:

```
ip address outside 99.99.99.1 255.255.255.0
ip address inside 10.31.1.75 255.255.255.0
global (outside) 1 99.99.99.7-99.99.99.10 netmask 255.255.255.0
timeout uauth 0:05:00 absolute
aaa-server RADIUS protocol radius
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 5
aaa authentication include telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication include tcp/49 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
virtual telnet 99.99.99.30
```

Nota: No hay autorización puesto que éste es RADIUS.

Telnet virtual saliente del PIX debug:

```
109001: Auth start for user '???' from 10.31.1.50/11034
    to 99.99.99.30/23
```

```
109011: Authen Session Start: user 'pixuser', Sid 16
109005: Authentication succeeded for user 'pixuser'
   from 10.31.1.50/11034 to 99.99.99.30/23 on interface
   inside
302001: Built outbound TCP connection 18 for faddr
   99.99.99.2/49 gaddr 99.99.99.8/11036 laddr
   10.31.1.50/11036 (pixuser)
302002: Teardown TCP connection 18 faddr 99.99.99.2/49
   gaddr 99.99.99.8/11036 laddr 10.31.1.50/11036
   duration 0:00:02 bytes 0 (pixuser)
```

Desconexión de Virtual Telnet

Cuando el usuario de telnet al Telnet IP Address virtual, el **comando show uauth** muestra su uauth. Si los usuarios quieren evitar que vaya el tráfico a través después de que se acaben sus sesiones cuando hay tiempo dejado en el uauth, necesitan Telnet al Telnet IP Address virtual otra vez. Esto finaliza la sesión.

Después de la primera autenticación:

```
pix3# show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
user 'pixuser' at 10.31.1.50, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
pix3# 109001: Auth start for user 'pixuser' from
   10.31.1.50/11038 to 99.99.99.30/23
109005: Authentication succeeded for user 'pixuser'
   from 10.31.1.50/11038 to 99.99.99.30/23 on
   interface inside
```

Después de la segunda autenticación (es decir, el agujero se conecta cerrado):

```
pix3# show uauth
                        Current    Most Seen
Authenticated Users       0          2
Authen In Progress        0          1
```

'Autorización del puerto

La autorización se permite para los rangos de puertos (como el TCP/30-100). Si la Telnet virtual se configura en el PIX y la autorización para un rango de puertos, una vez que el agujero se abre con la Telnet virtual, el PIX publica un **comando tcp/30-100 al** servidor para autorización TACACS+:

```
static (inside,outside) 99.99.99.75 10.31.1.50 netmask 255.255.255.255 0 0
conduit permit tcp host 99.99.99.75 host 99.99.99.2
static (inside,outside) 99.99.99.75 10.31.1.50 netmask 255.255.255.255 0 0
virtual telnet 99.99.99.75
aaa authentication include any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authorization include tcp/30-100 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
virtual telnet 99.99.99.30
```

Configuración de servidor Freeware TACACS+:

```
user = anyone {
         login = cleartext "anyone"
         cmd = tcp/30-100 {
         permit 10.31.1.50
         }
         }
```

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

Después de aseegurarse la Telnet virtual trabajada para permitir el tráfico TCP/49 al host dentro de la red, decidíamos que quisiéramos explicar esto, así que agregamos:

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

Esto da lugar al hacer un registro de contabilidad cortar cuando va el tráfico tcp/49 a través (este ejemplo es del freeware TACACS+):

```
Sun Feb 27 05:24:44 2000 10.31.1.75 cse PIX
    99.99.99.2 start task_id=0x14 foreign_ip=99.99.99.2 local_ip=171.68.118.106
    cmd=tcp/49
```

Autenticación ampliada (Xauth)

Configuraciones de Ejemplo

- Finalización de túneles IPSec en interfaces Cisco Secure PIX Firewall múltiples con Xauth.
- IPSec entre el Cisco Secure PIX Firewall y un cliente VPN con la autenticación ampliada

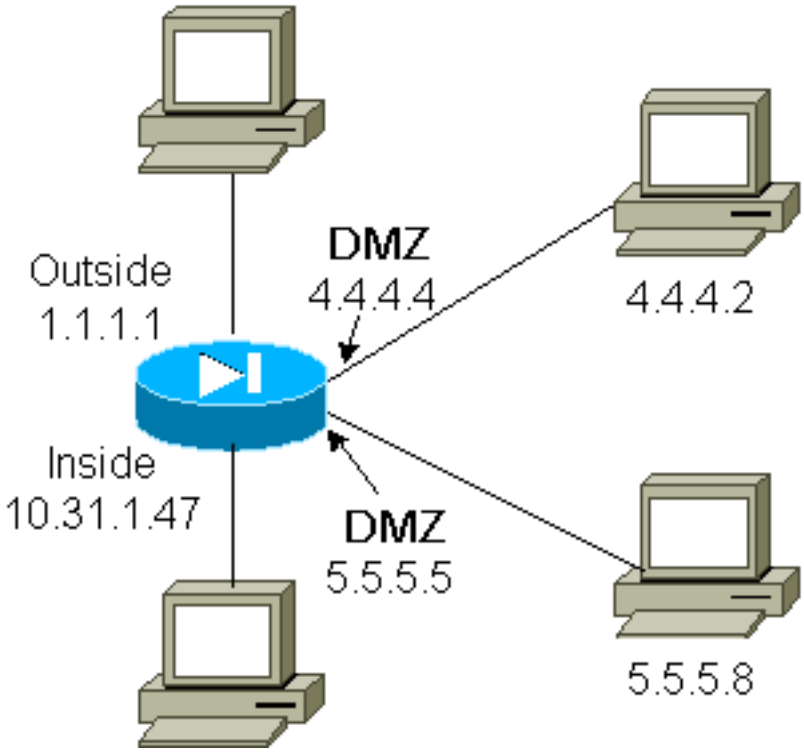
Autenticación en DMZ

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 nuestro PIX el arreglo es:

```
least secure

PIX outside (security0) = 1.1.1.1

pix/intf4 (DMZ - security20) = 4.4.4.4 & device 4.4.4.2

pix/intf5 (DMZ - security25) = 5.5.5.5 & device 5.5.5.8

(static to 4.4.4.15)

PIX inside (security100) = 10.31.1.47
```

most secure

Diagrama de la red



Configuración de PIX

Queremos autenticar el tráfico de Telnet entre pix/intf4 y pix/intf5:

```
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
ip address outside 1.1.1.1 255.255.255.0
ip address inside 10.31.1.47 255.255.255.0
(ip address pix/intf2 127.0.0.1 255.255.255.255
ip address pix/intf3 127.0.0.1 255.255.255.255)
ip address pix/intf4 4.4.4.4 255.255.255.0
ip address pix/intf5 5.5.5.5 255.255.255.0
static (pix/intf5,pix/intf4) 4.4.4.15 5.5.5.8 netmask 255.255.255.255 0 0
aaa authentication telnet pix/intf4 5.5.5.0 255.255.255.0
4.4.4.0 255.255.255.0 AuthInbound
aaa authentication telnet pix/intf5 5.5.5.0 255.255.255.0
4.4.4.0 255.255.255.0 AuthInbound
aaa-server TACACS+ protocol tacacs+
aaa-server AuthInbound protocol tacacs+
aaa-server AuthInbound (inside) host 171.68.118.101 cisco timeout 5
```

Contabilidad Xauth

Si configuran al **comando sysopt connection permit-ipsec**, no el **comando sysopt ipsec pl-compatible**, en el PIX con el Xauth, el considerar es válido para las conexiones TCP, pero no el

ICMP o el UDP.

Información Relacionada

- Página de soporte de producto PIX
- Referencia de Comandos PIX
- Página de soporte de RADIUS
- Solicitudes de Comentarios (RFC)
- Página de soporte de Secure para UNIX de Cisco
- Página de soporte de Cisco Secure ACS para Windows
- Soporte Técnico - Cisco Systems