PIX, TACACS+, y configuraciones de ejemplo de RADIUS: 4.2.x

Contenido

Introducción

El RADIUS y autenticación de TACACS+ se puede hacer para el FTP, Telnet, y las conexiones HTTP. Autorización TACACS+ se soporta; La autorización de RADIUS no.

La sintaxis de autenticación cambiada levemente en software PIX 4.2.2. Este documento utiliza el

sintaxis para las versiones de software 4.2.2.

prerrequisitos

Requisitos

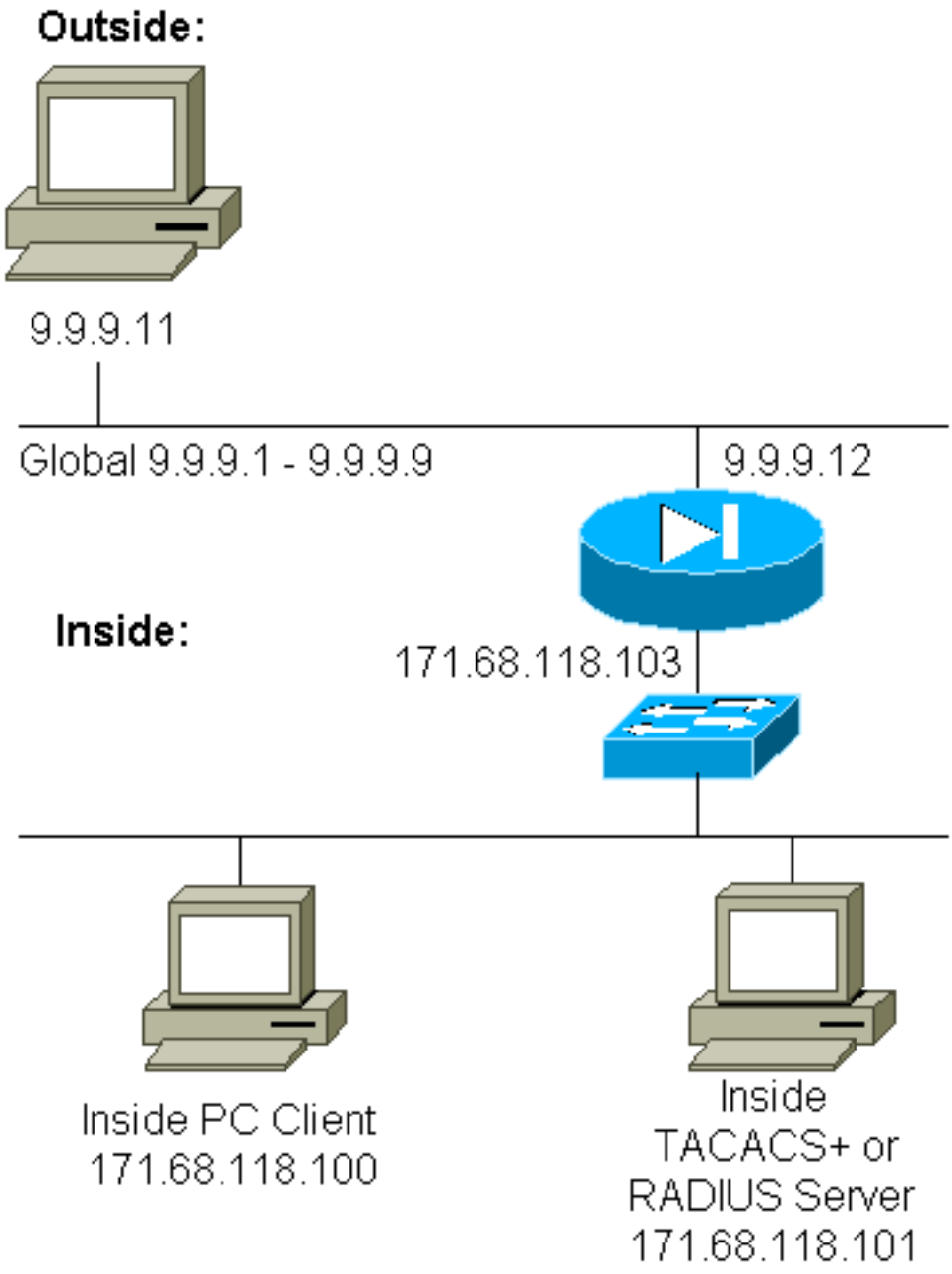
No hay requisitos específicos para este documento.

Componentes Utilizados

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

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuración de PIX

```
pix2# write terminal Building configuration : Saved :
PIX Version 4.2(2) nameif ethernet0 outside security0
nameif ethernet1 inside security100 enable password
8Ry2YjIyt7RRXU24 encrypted passwd OnTrBUG1Tp0edmkr
encrypted hostname pix2 fixup protocol http 80 fixup
protocol smtp 25 no fixup protocol ftp 21 no fixup
protocol h323 1720 no fixup protocol rsh 514 no fixup
protocol sqlnet 1521 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 0.0.0.0 names
pager lines 24 logging console debugging no logging
monitor logging buffered debugging logging trap
debugging logging facility 20 interface ethernet0 auto
interface ethernet1 auto interface ethernet2 auto ip
address outside 9.9.9.12 255.255.255.0 ip address inside
171.68.118.103 255.255.255.0 ip address 0.0.0.0 0.0.0.0
arp timeout 14400 global (outside) 1 9.9.9.1-9.9.9.9
netmask 255.0.0.0 static (inside,outside) 9.9.9.10
171.68.118.100 netmask 255.255.255.255 0 0 conduit
permit icmp any any conduit permit tcp host 9.9.9.10 eq
telnet any no rip outside passive no rip outside default
no rip inside passive no rip inside default timeout
xlate 3:00:00 conn 1:00:00 udp 0:02:00 timeout rpc
0:10:00 h323 0:05:00 timeout uauth 0:00:00 absolute ! !-
-- The next entry depends on whether TACACS+ or RADIUS
is used. ! tacacs-server (inside) host 171.68.118.101
cisco timeout 5 radius-server (inside) host
171.68.118.101 cisco timeout 10 ! !--- The focus of
concern is with hosts on the inside network !---
accessing a particular outside host. ! aaa
authentication any outbound 171.68.118.0 255.255.255.0
9.9.9.11 255.255.255.255 tacacs+|radius ! !--- It is
possible to be less granular and authenticate !--- all
outbound FTP, HTTP, Telnet traffic with: aaa
authentication ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 tacacs+|radius aaa authentication http outbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius aaa
authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 tacacs+|radius ! !--- Accounting records are
sent for !--- successful authentications to the TACACS+
or RADIUS server. ! aaa accounting any outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius ! no snmp-server
location no snmp-server contact snmp-server community
public no snmp-server enable traps telnet 171.68.118.100
255.255.255.255 mtu outside 1500 mtu inside 1500 mtu
1500 Smallest mtu: 1500 floodguard 0 tcpchecksum silent
Cryptochecksum:be28c9827e13baf89a937c617cfe6da0 : end
[OK]
```

Convenciones

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

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.

Como como ejemplo, asuma usted tiene cientos usuarios interiores y le solamente quisiera que seis de estos usuarios pudieran hacer el FTP, Telnet, o el HTTP fuera de la red. Diga 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 pueden ser autenticados con el nombre de usuario y contraseña, después salen. Los otros noventa y cuatro usuarios no pueden 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. También, dependiendo de la respuesta, abre o niega la conexión. Estos seis usuarios podrían hacer el FTP, Telnet, o el HTTP.

Sin embargo, asuma a uno de estos tres usuarios, “Terry”, no es ser confiado en. Usted quisiera permitir que Terry hagan el FTP, pero no el HTTP o Telnet al exterior. Esto le significa necesidad de agregar la autorización. Es decir, autorizando lo que pueden hacer los usuarios además de autenticar quién son. Cuando usted agrega la autorización al PIX, el PIX primero envía el nombre de usuario y contraseña de Terry al servidor de seguridad, después envía un pedido de autorización que diga a servidor de seguridad lo que está intentando el “comando” Terry hacer. Con la configuración de servidor correctamente, Terry se puede permitir a “FTP 1.2.3.4” pero se niega la capacidad al “HTTP” o a “Telnet” dondequiera.

Qué ve el usuario con la autenticación/autorización activada

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

- **Telnet** - El usuario ve una pantalla de prompt de nombre de usuario, seguida por una petición para 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 “nombredeusuario_local” y “contraseña_local” al servidor de seguridad local y si la autenticación (y autorización) resulta exitosa en el PIX/servidor, el “nombredeusuario_remoto” y “contraseña_remota” se envían al servidor FTP de destino posterior.
- **HTTP** - 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 “tiroteo” el nombre de usuario guardado en memoria caché y la contraseña al PIX. Él entonces adelante esto al servidor de autenticación. Los debugs del syslog PIX y/o del servidor muestran este fenómeno. Si Telnet y el FTP parecen trabajar normalmente, pero no lo hacen las conexiones HTTP, ésta es la razón.

Configuraciones del servidor utilizada para todos los escenarios

En los ejemplos de configuración del servidor TACACS+, si solamente la autenticación está prendido, los usuarios “todos”, “telnetonly”, “httponly”, y “ftponly” todos trabajan. En los ejemplos

de la configuración de servidor de RADIUS, el usuario “todo” trabaja.

Cuando la autorización se agrega al PIX, además de enviar el nombre de usuario y contraseña al autenticación de TACACS+ el servidor, el PIX envía los comandos (Telnet, HTTP, o FTP) al servidor TACACS+. El servidor TACACS+ entonces marca para ver si autorizan a ese usuario para ese comando.

En un ejemplo posterior, el usuario en 171.68.118.100 publica el comando telnet **9.9.9.11**. Cuando esto se recibe en el PIX, el PIX pasa el nombre de usuario, contraseña, y ordena al servidor TACACS+ para procesar.

Tan con la autorización encendido además de la autenticación, el usuario “telnetonly” puede realizar los funcionamientos de Telnet con el PIX. Sin embargo, los usuarios “httponly” y “ftponly” no pueden realizar los funcionamientos de Telnet con el PIX.

(Una vez más la autorización no se soporta con RADIUS a causa de a la naturaleza de la especificación del protocolo).

Configuración del servidor segura de Cisco UNIX TACACS+

Cisco 2.x seguro

- Las secciones del usuario se visualizan aquí.
- Agregue la dirección IP o el nombre y clave de dominio completamente calificar PIX al CSU.cfg.

```
user = all {
password = clear "all"
default service = permit
}

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

user = ftponly {
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 la interfaz del usuario gráfica avanzada (GUI) para agregar el IP PIX y la clave a la lista del servidor de acceso a la red (NAS). La sección del usuario aparece según lo considerado aquí:

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

Cisco Secure NT 2.x RADIUS

La sección de configuraciones de muestra del 2.1 del CiscoSecure en línea y de la documentación Web describe la configuración; el atributo 6 (tipo de servicio) sería login o administrativo.

Agregue el IP del PIX en la sección de Configuración de NAS usando el GUI.

EasyACS TACACS+

La documentación de EasyACS proporciona la información de configuración.

1. En la sección de grupo, **ejecutivo del shell del** tecleo (dar los privilegios exec).
2. Para agregar la autorización al PIX, **comandos deny unmatched ios del** tecleo en la parte inferior de la configuración de grupo.
3. Selecto **agregue/edite** para cada comando que usted quiere permitir (Telnet, por ejemplo).
4. Si usted quiere permitir el telnet a los sitios específicos, ingrese el IP en la sección de argumento. Para permitir Telnet a todos los sitios, el tecleo **permite todos los argumentos no enumerados**.
5. **Comando editing del final del** tecleo.
6. Realice los pasos 1through 5 para cada uno de los comandos permitidos (Telnet, HTTP y/o FTP, por ejemplo).
7. Agregue el IP del PIX en la sección de Configuración de NAS usando el GUI.

Cisco Secure NT 2.x TACACS+

La documentación segura 2.x de Cisco proporciona la información de configuración.

1. En la sección de grupo, **ejecutivo del shell del** tecleo (dar los privilegios exec).
2. Para agregar la autorización al PIX, **comandos deny unmatched ios del** tecleo en la parte inferior de la configuración de grupo.
3. Seleccione el checkbox del **comando** en la parte inferior y ingrese el comando que usted quiere permitir (telnet, por ejemplo).
4. Si usted quiere permitir el telnet a los sitios específicos, ingrese el IP en la sección de argumento (por ejemplo, el “permiso el 1.2.3.4"). Para permitir Telnet a todos los sitios, haga clic los **argumentos no enumerados del permiso**.
5. Haga clic en Submit (Enviar).
6. Realice los pasos 1through 5 para cada uno de los comandos permitidos (Telnet, FTP, y/o HTTP, por ejemplo).
7. Agregue el IP del PIX en la sección de Configuración de NAS usando el GUI.

‘Configuración del servidor Livingston RADIUS’

Agregue el IP PIX y la clave a los clientes clasifían.

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

Configuración del servidor Merit RADIUS

Agregue el IP PIX y la clave a los clientes clasifían.

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

Configuración del servidor freeware TACACS+

```
# Handshake with router--PIX needs 'tacacs-server host #.#.#.# cisco':
key = "cisco"

user = all {
default service = permit
login = cleartext "all"
}

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

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

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

Pasos de depuración

- Aseegurese que las configuraciones PIX están trabajando antes de agregar el Authentication, Authorization, and Accounting (AAA).Si usted no puede pasar el tráfico antes de instituir el AAA, usted no podrá hacer tan luego.
- Permiso que abre una sesión el PIX:**El comando logging console debugging** no debe ser utilizado en pesadamente un sistema cargado.Puede usarse el comando logging buffered debugging (depuración guardada en la memoria intermedia del registro). La salida de los **comandos show logging o logging** puede después ser enviada a un servidor de Syslog y ser examinada.
- Aseegurese que el hacer el debug de está prendido para el TACACS+ o los servidores de RADIUS. Todos los servidores tienen esta opción.

Ejemplos de PIX del comando authentication debug

PIX debug - Buena autenticación - RADIUS

Éste es un ejemplo de un PIX debug con la buena autenticación:

```
109001: Auth start for user '???' from 171.68.118.100/1116 to 9.9.9.11/23
 109011: Authen Session Start: user 'bill', sid 1
 109005: Authentication succeeded for user 'bill'
   from 171.68.118.100/1116 to 9.9.9.11/23
 109012: Authen Session End: user 'bill', sid 1, elapsed 1 seconds
 302001: Built TCP connection 1 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1116
   laddr 171.68.118.100/1116 (bill)
```

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

Éste es un ejemplo de un PIX debug con la autentificación que resultó mal (nombre de usuario o contraseña). El usuario ve cuatro nombres de usuario/contraseñas definidas. El “error: el Número máximo de” mensaje excedido las recomprobaciones se visualiza.

Nota: Si esto es una tentativa FTP, se permite un intento. Para el HTTP, se permiten los intentos infinitos.

```
109001: Auth start for user '???' from 171.68.118.100/1132 to 9.9.9.11/23
 109006: Authentication failed for user '' from
   171.68.118.100/1132 to 9.9.9.11/23
```

PIX debug - Servidor abajo - RADIUS

Éste es un ejemplo de un PIX debug con el servidor abajo. El usuario ve el nombre de usuario una vez. El servidor después “cuelga” y pide una contraseña (tres veces).

```
109001: Auth start for user '???' from 171.68.118.100/1151 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1151 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1151 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
```

PIX debug - Buena autenticación - TACACS+

Éste es un ejemplo de un PIX debug con la buena autenticación:

```
109001: Auth start for user '???' from 171.68.118.100/1200 to 9.9.9.11/23
 109011: Authen Session Start: user 'cse', sid 3
 109005: Authentication succeeded for user 'cse'
   from 171.68.118.100/1200 to 9.9.9.11/23
 109012: Authen Session End: user 'cse', sid 3, elapsed 1 seconds
 302001: Built TCP connection 3 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1200
  laddr 171.68.118.100/1200 (cse)
```

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

Éste es un ejemplo de un PIX debug con la autentificación que resultó mal (nombre de usuario o contraseña). El usuario ve cuatro nombres de usuario/contraseñas definidas. El “error: el Número máximo de” mensaje excedido las recomprobaciones se visualiza.

Nota: Si esto es una tentativa FTP, se permite un intento. Para el HTTP, se permiten los intentos infinitos.

```
109001: Auth start for user '???' from 171.68.118.100/1203 to 9.9.9.11/23
```

```
 109006: Authentication failed for user ''
   from 171.68.118.100/1203 to 9.9.9.11/23
```

PIX debug - Servidor abajo - TACACS+

Éste es un ejemplo de un PIX debug con el servidor abajo. El usuario ve el nombre de usuario una vez. Inmediatamente, el “error: El Número máximo de” mensaje excedido los intentos se visualiza.

```
109001: Auth start for user '???' from 171.68.118.100/1212 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109006: Authentication failed for user '' from 171.68.118.100/1212 to 9.9.9.11/23
```

Agregado de autorización

Porque la autorización es inválida sin la autenticación, la autorización se requiere para la misma fuente y destino:

```
aaa authorization any outbound 171.68.118.0 255.255.255.0 9.9.9.11 255.255.255.255
tacacs+|radius
```

O, si autenticaron a los tres servicios salientes originalmente:

```
aaa authorization http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius aaa authorization
ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius aaa authorization telnet outbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius
```

Ejemplos de Depuración de Autenticación y Autorización de PIX

PIX debug - Buena autenticación y autorización - TACACS+

Éste es un ejemplo de un PIX debug con la buena autenticación y la autorización:

```
109001: Auth start for user '???' from 171.68.118.100/1218 to 9.9.9.11/23
 109011: Authen Session Start: user 'telnetonly', sid 5
 109005: Authentication succeeded for user 'telnetonly' from
   171.68.118.100/1218 to 9.9.9.11/23
 109011: Authen Session Start: user 'telnetonly', sid 5
 109007: Authorization permitted for user 'telnetonly' from
   171.68.118.100/1218 to 9.9.9.11/23
 109012: Authen Session End: user 'telnetonly', sid 5, elapsed 1 seconds
 302001: Built TCP connection 4 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1218
   laddr 171.68.118.100/1218 (telnetonly)
```

PIX debug - Buena autenticación, pero error en la autorización - TACACS+

Éste es un ejemplo de un PIX debug con la buena autenticación pero el error en la autorización:

```
109001: Auth start for user '???' from 171.68.118.100/1223 to 9.9.9.11/23
 109011: Authen Session Start: user 'httponly', sid 6
 109005: Authentication succeeded for user 'httponly'
   from 171.68.118.100/1223 to 9.9.9.11/23
 109008: Authorization denied for user 'httponly'
   from 171.68.118.100/1223 to 9.9.9.11/23
```

PIX debug - Autentificación que resultó mal, autorización no frustrada - TACACS+

Esto es un ejemplo de un PIX debug con la autenticación y autorización, pero no frustrado de la autorización debido a la autentificación que resultó mal (nombre de usuario o contraseña). El usuario ve cuatro nombres de usuario/contraseñas definidas. El “error: Número máximo de recomprobaciones excedidas.” se visualiza el mensaje

Nota: Si esto es una tentativa FTP, se permite un intento. Para el HTTP, se permiten los intentos infinitos.

```
109001: Auth start for user '???' from 171.68.118.100/1228 to 9.9.9.11/23
 109006: Authentication failed for user '' from 171.68.118.100/1228
   to 9.9.9.11/23
```

PIX debug - Autenticación/autorización, servidor abajo - TACACS+

Éste es un ejemplo de un PIX debug con la autenticación y autorización. El servidor está abajo. El usuario ve el nombre de usuario una vez. Inmediatamente, el “error: Número máximo de intentos excedidos.” se visualiza.

```
109001: Auth start for user '???' from 171.68.118.100/1237 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109006: Authentication failed for user '' from 171.68.118.100/1237
   to 9.9.9.11/23
```

Agregar contabilidad

TACACS+

aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0: tacacs+

El debug mira lo mismo si el considerar es con./desc. Sin embargo, a la hora del “construyó,” registro de contabilidad del “comienzo” a se envía. También, a la hora del “desmontaje,” se envía el registro de contabilidad de la “parada” a:

```
109011: Authen Session Start: user 'telnetonly', sid 13
 109005: Authentication succeeded for user 'telnetonly'
   from 171.68.118.100/1299 to 9.9.9.11/23
 109011: Authen Session Start: user 'telnetonly', sid 13
 109007: Authorization permitted for user 'telnetonly'
   from 171.68.118.100/1299 to 9.9.9.11/23
 109012: Authen Session End: user 'telnetonly', sid 13, elapsed 1 seconds
 302001: Built TCP connection 11 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1299
  laddr 171.68.118.100/1299 (telnetonly)
 302002: Teardown TCP connection 11 faddr 9.9.9.11/23 gaddr 9.9.9.10/1299
  laddr 171.68.118.100/1299 duration 0:00:02 bytes 112
```

Los registros de contabilidad TACACS+ parecen esta salida (éstos son de CiscoSecure UNIX; los expedientes en Cisco Windows seguro pueden ser coma delimitada en lugar de otro):

```
Tue Sep 29 11:00:18 1998 redclay cse PIX 171.68.118.103
   start task_id=0x8 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet
 Tue Sep 29 11:00:36 1998 redclay cse PIX 171.68.118.103
```

```
   stop task_id=0x8 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet elapsed_time=17
   bytes_in=1198 bytes_out=62
 Tue Sep 29 11:02:08 1998 redclay telnetonly PIX 171.68.118.103
   start task_id=0x9 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet
 Tue Sep 29 11:02:27 1998 redclay telnetonly PIX 171.68.118.103
   stop task_id=0x9 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet elapsed_time=19
   bytes_in=2223 bytes_out=64
```

Los campos analizan según lo considerado aquí:

```
DAY MO DATE TIME YEAR NAME_OF_PIX USER SENDER PIX_IP START/STOP
   UNIQUE_TASK_ID DESTINATION SOURCE
   SERVICE <TIME> <BYTES_IN> <BYTES_OUT>
```

RADIUS

aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 radius

El debug mira lo mismo si el considerar es con./desc. Sin embargo, a la hora del “construyó,” registro de contabilidad del “comienzo” a se envía. También, a la hora del “desmontaje,” se envía el registro de contabilidad de la “parada” a:

```
109001: Auth start for user '???' from 171.68.118.100/1316 to 9.9.9.11/23
 109011: Authen Session Start: user 'bill', sid 16
 109005: Authentication succeeded for user 'bill'
   from 171.68.118.100/1316 to 9.9.9.11/23
 109012: Authen Session End: user 'bill', sid 16, elapsed 1 seconds
 302001: Built TCP connection 14 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1316
  laddr 171.68.118.100/1316 (bill)
 302002: Teardown TCP connection 14 faddr 9.9.9.11/23 gaddr 9.9.9.10/1316
  laddr 171.68.118.100/1316 duration 0:00:03 bytes 112
```

Los registros de contabilidad RADIUS parecen esta salida (éstos son de Cisco UNIX seguro; los que está en Cisco Windows seguro son coma delimitada):

```
Mon Sep 28 10:47:01 1998
Acct-Status-Type = Start
Client-Id = 171.68.118.103
Login-Host = 171.68.118.100
Login-TCP-Port = 23
Acct-Session-Id = "0x00000004"
User-Name = "bill"

Mon Sep 28 10:47:07 1998
Acct-Status-Type = Stop
Client-Id = 171.68.118.103
Login-Host = 171.68.118.100
Login-TCP-Port = 23
Acct-Session-Id = "0x00000004"
User-Name = "bill"
Acct-Session-Time = 5
```

Los campos analizan según lo considerado aquí:

```
Acct-Status-Type = START or STOP
Client-ID = IP_OF_PIX
Login_Host = SOURCE_OF_TRAFFIC
Login-TCP-Port = #
Acct-Session-ID = UNIQUE_ID_PER_RADIUS_RFC
User-name = <whatever>
<Acct-Session-Time = #>
```

Sesiones MAX y vista de usuarios conectados al sistema

Algún TACACS y servidores de RADIUS tienen “sesión máxima” o “vea las características a los usuarios conectados al sistema”. La posibilidad de establecer un número máximo de sesiones o verificar los usuarios conectados depende de los registros de contabilidad. Cuando hay un expediente del “comienzo” de las estadísticas generado pero ningún expediente de la “parada”, el TACACS o el servidor de RADIUS asume que todavía abren una sesión a la persona (que es; tiene una sesión con el PIX). Esto funciona bien en conexiones Telnet y FTP debido a la naturaleza de las conexiones. Por ejemplo:

Las telnets del usuario de 171.68.118.100 a 9.9.9.25 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 171.68.118.100/12
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 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, la conexión es rechazada por el servidor.

El usuario va alrededor negocio en el host de destino, después las salidas (pasa 10 minutos allí).

```
(pix) 302002: Teardown TCP connection 5 faddr 9.9.9.25/80 gaddr 9.9.9.10/128 1
  laddr 171.68.118.100/1281 duration 0:00:00 bytes 1907 (cse)

 (server stop account) Sun Nov  8 16:41:17 1998
   rtp-pinecone.rtp.cisco.com cse PIX
   171.68.118.100  stop task_id=0x3 foreign_ip=9.9.9.25
   local_ip=171.68.118.100
   cmd=telnet elapsed_time=5  bytes_in=98 bytes_out=36
```

Si el uauth es 0 (que es; autentique cada vez) o más (autentique una vez y no otra vez durante el período uauth), habrá un corte del registro de contabilidad para cada sitio accedido.

Pero el HTTP trabaja diverso debido a la naturaleza del protocolo. Aquí tiene un ejemplo:

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 una página web descargada.

Observe el tiempo. Esta descarga tardó al segundo (había menos que el segundo entre el comienzo y el expediente de la parada). ¿Todavía todavía abren una sesión al usuario al sitio web y a la conexión abiertos? 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 en el HTTP es demasiado corto. El tiempo entre “construido” y el “desmontaje” (el expediente del “comienzo” y de la “parada”) es sub-segundo. No habrá un expediente del “comienzo” sin un expediente de la “parada”, puesto que los expedientes ocurren en virtualmente el mismo instante. Seguirá habiendo un registro de "iniciar" y "detener" enviado al servidor para cada transacción sin importar si el valor de uauth es 0 ó un valor mayor. Sin embargo, las sesiones máximas y los usuarios conectados al sistema de la visión no trabajarán debido a las naturalezas de la conexión HTTP.

Utilización del comando Except (excepción)

En nuestra red, si decidimos que un usuario saliente (171.68.118.100) no necesita ser autenticado, podemos hacer esto:

```
aaa authentication any outbound 171.68.118.0 255.255.255.0 9.9.9.11 255.255.255.255 tacacs+ aaa
authentication except outbound 171.68.118.100 255.255.255.255 9.9.9.11 255.255.255.255 tacacs+
```

Autenticación al PIX mismo

La explicación anterior está de autenticar el tráfico de Telnet (y HTTP, FTP) con el PIX. Con 4.2.2, las conexiones Telnet al PIX pueden también ser autenticadas. Aquí, definimos los IP de los cuadros que pueden Telnet al PIX:

```
telnet 171.68.118.100 255.255.255.255
```

Entonces suministre la contraseña de Telnet: **passwd ww**.

Agregue el comando new de autenticar el Telnetting de los usuarios al PIX:

```
aaa authentication telnet console tacacs+|radius
```

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.

Cambio del mensaje de solicitud que ve el usuario

Si usted agrega el comando: **el auténtico-prompt YOU_ARE_AT_THE_PIX**, los usuarios que pasan con el PIX considerará la secuencia:

`YOU_ARE_AT_THE_PIX [`*`at which point you enter the username`*`] Password:[`*`at which point you enter the password`*`]`

Sobre la llegada en el destino final, el “nombre de usuario: ” y “contraseña: los” prompts serán visualizados. 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.

Información Relacionada

- Soporte de productos del Software Cisco PIX Firewall
- Referencias de Comandos de Cisco Secure PIX Firewall
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems