Configurando PIX 5.0.x: TACACS+ e RADIUS

Índice

Introdução

O RAIO e a autenticação TACACS+ podem ser feitos para o FTP, o telnet, e as conexões de HTTP. A autenticação para outros menos protocolos TCP comuns pode geralmente ser feita para trabalhar.

A autorização TACACS+ é apoiada. A autorização de RADIUS não é. As mudanças no Authentication, Authorization, and Accounting (AAA) PIX 5.0 sobre a versão anterior incluem o tráfego esclarecendo AAA a não ser o HTTP, o FTP, e o telnet.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Convenções

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Autenticação vs. Autorização

- A autenticação é quem o usuário é.
- A autorização é o que o usuário pode fazer.
- A autenticação é válida sem autorização.
- A autorização não é válida sem autenticação.

Como um exemplo, supõe que você tem cem usuários internos e você para querer quer somente seis destes usuários poder fazer o FTP, o telnet, ou o HTTP fora da rede. Diga o PIX para autenticar o tráfego de saída e dar a todos os seis usuários ID no servidor de segurança TACACS+/RADIUS. Com autenticação simples, estes seis usuários podem ser autenticados com nome de usuário e senha, a seguir saem. Os outros usuários da noventa-quatro são incapazes de sair. O PIX alerta usuários para o username/senha, a seguir passa seu nome de usuário e senha ao servidor de segurança TACACS+/RADIUS. Segundo a resposta, abre ou nega a conexão. Estes seis usuários podem fazer o FTP, o telnet, ou o HTTP.

Por outro lado, supõe *um d*estes três usuários, “Terry,” não é ser confiado. Você gostaria de permitir que Terry façam o FTP, mas não o HTTP ou o telnet à parte externa. Isto significa-o necessidade de adicionar a *autorização*. Isto é, autorizando *o que os* usuários podem fazer além do que a autenticação de *quem* são. Quando você adiciona a *autorização ao* PIX, o PIX primeiramente envia o nome de usuário e senha de Terry ao servidor de segurança, a seguir envia a um pedido de autorização que diz ao servidor de segurança o que o “*comando*” Terry está tentando fazer. Com a instalação do server corretamente, Terry pode ser permitido a “FTP 1.2.3.4” mas é negado a capacidade ao “HTTP” ou ao “telnet” em qualquer lugar.

O que o usuário visualiza com o modo de autenticação/autorização Ligado

Quando você tentar ir do interior à parte externa (ou vice versa) com autenticação/autorização sobre:

- **Telnet** - O usuário vê uma exibição de alerta de nome de usuário, seguida por um pedido para a senha. Se a autenticação (e autorização) for bem-sucedida no PIX/servidor, o usuário está pronto para obter nome de usuário e senha pelo host de destino.
- **FTP** - O usuário vê uma alerta de nome de usuário vir acima. O usuário precisa inserir local_username@remote_username para nome de usuário e local_password@remote_password para senha. O PIX envia "local_username" e "local_password" para o servidor de segurança local e, se a autenticação (e autorização) for bem-sucedida no PIX/servidor, "remote_username" e "remote_password” vão mais além do servidor FTP de destino.
- **HTTP** - Um indicador indicado no navegador que pede o nome de usuário e senha. Se a autenticação (e autorização) for concluída com sucesso, o usuário chega ao web site de destino. Mantenha na mente que os **navegadores põem em esconderijo nomes de usuário e senha**. Se parecer que o PIX está esgotando uma conexão http mas não estiver, é provável que a re-autenticação esteja de fato ocorrendo com o navegador "disparando" o nome de usuário e a senha em cache para o PIX, que, em seguida, o encaminha ao servidor de autenticação. Syslog de PIX e/ou depuração de servidor mostrarão esse fenômeno. Se o

telnet e o FTP parecem trabalhar normalmente, mas as conexões de HTTP não fazem, eis porque.

Configurações de servidor de segurança utilizadas para todos os cenários

Configuração de servidor de TACACS segura de Cisco UNIX

Certifique-se de que você tem o endereço IP de Um ou Mais Servidores Cisco ICM NT ou o nome e chave de domínio totalmente qualificados PIX no arquivo 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 .*
}
}
}
```

Configuração do servidor segura dos RADIUS UNIX de Cisco

Use a interface gráfica de usuário (GUI) para adicionar o IP PIX e a chave à lista do servidor do acesso de rede (NAS).

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

}

RAIO seguro de Cisco Windows 2.x

Siga estes passos:

1. Obtenha uma senha na seção GUI de instalação de usuário.
2. Da seção gui da instalação de grupo, ajuste o atributo 6 (tipo de serviço) para entrar ou administrativo.
3. Adicionar o IP PIX na configuração de NAS GUI.

EasyACS TACACS+

A documentação easyacs descreve a instalação.

1. Na seção de grupo, **executivo do shell do** clique (para dar privilégios de exec).
2. Para adicionar a autorização ao PIX, **comandos deny unmatched ios do** clique na parte inferior da instalação de grupo.
3. **Comando add/edit new** seleto para cada comando que você deseja permitir (por exemplo, telnet).
4. Se você quer permitir o telnet aos locais específicos, incorpore o IP à seção de argumento no formulário “licença #.#.#.#”. Para permitir o telnet a todos os locais, o clique **permite todos os argumentos não listados**.
5. **Comando editing do revestimento do** clique.
6. Execute etapas 1 com 5 para cada um dos comandos permitidos (por exemplo, telnet, HTTP, ou FTP).
7. Adicionar o IP PIX na seção gui da configuração de NAS.

Cisco 2.x seguro TACACS+

O usuário obtém uma senha na seção GUI de instalação de usuário.

1. Na seção de grupo, **executivo do shell do** clique (para dar privilégios de exec).
2. Para adicionar a autorização ao PIX, **comandos deny unmatched ios do** clique na parte inferior da instalação de grupo.
3. **Comando add/edit new** seleto para cada comando que você quer permitir (por exemplo, telnet).
4. Se você quer permitir o telnet aos locais específicos, incorpore o IP da licença ao retângulo de argumentação (por exemplo, “licença 1.2.3.4"). Para permitir o telnet a todos os locais, o clique **permite todos os argumentos não listados**.
5. **Comando editing do revestimento do** clique.
6. Execute as etapas precedentes para cada um dos comandos permitidos (por exemplo, telnet, HTTP e/ou FTP).
7. Adicionar o IP PIX na seção gui da configuração de NAS.

Configuração de servidor Livingston RADIUS

Adicionar o IP PIX e a chave aos clientes arquivam.

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

Configuração de servidor Merit RADIUS

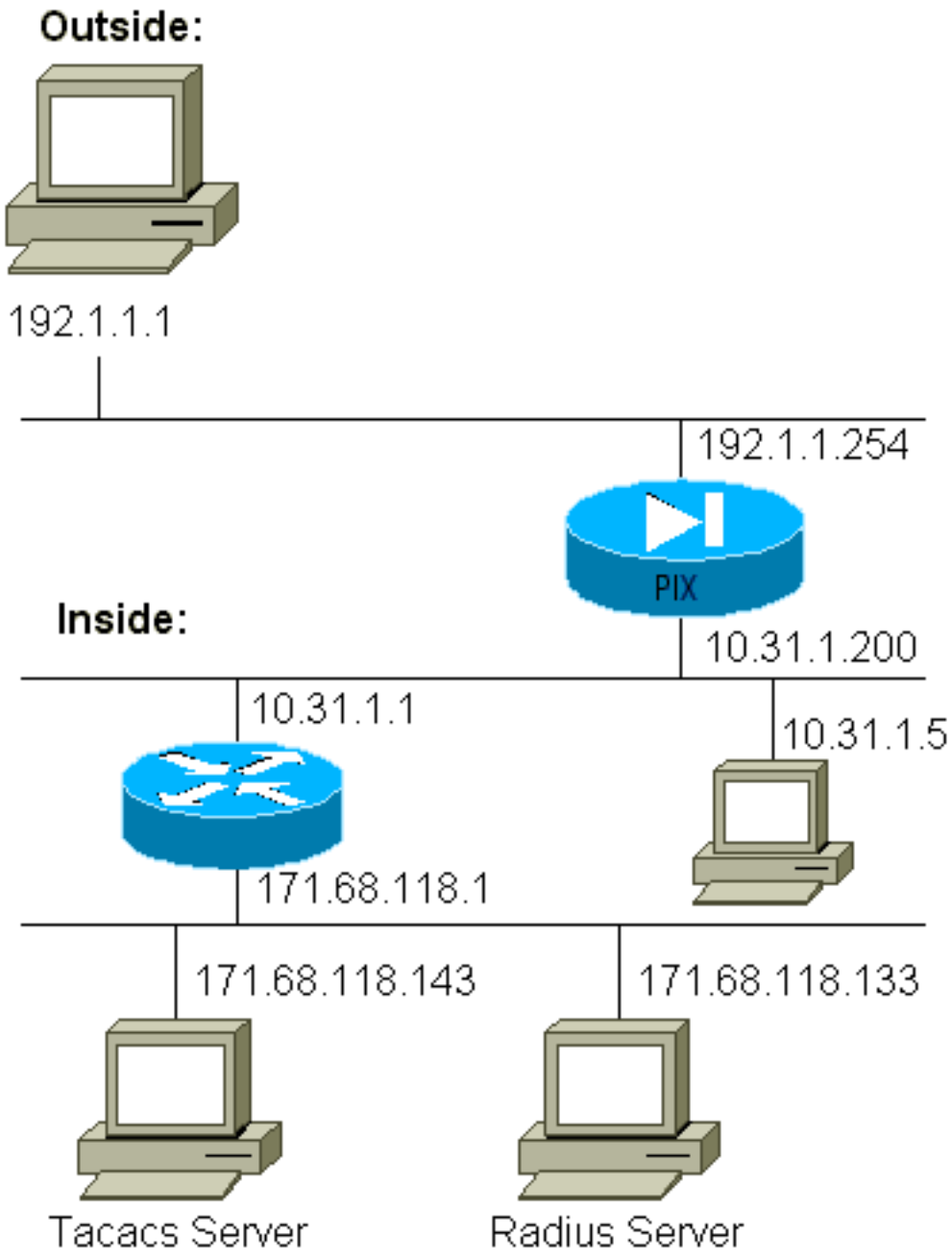
Adicionar o IP PIX e a chave aos clientes arquivam.

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

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 .*
}
}
```

Etapas de depuração

- Certifique-se de que as configurações de PIX trabalham antes que você adicione o AAA.Se você não passar o tráfego antes de instituir autenticação e autorização, não conseguirá fazê-lo depois disso.
- Enable que entra o PIXO comando de depuração do console de registro não deve ser usado em um sistema com carga pesada.O comando logging buffered debugging poder ser utilizado. A saída dos **comandos show logging ou logging** pode ser enviada a um servidor de SYSLOG e ser examinada.
- Certifique-se de que debugar está ligada para o TACACS+ ou os servidores Radius. Todos os servidores possuem esta opção.

Diagrama de Rede



Configuração de PIX

```
pix-5# write terminal
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pixfirewall
 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
 name 1.1.1.1 abcd
 name 1.1.1.2 a123456789
 name 1.1.1.3 a123456789123456
 pager lines 24
 logging timestamp
 no logging standby
```

```
 logging console debugging
 no logging monitor
 logging buffered debugging
 no logging trap
 logging facility 20
 logging queue 512
 interface ethernet0 auto
 interface ethernet1 auto
 mtu outside 1500
 mtu inside 1500
 ip address outside 192.1.1.254 255.255.255.0
 ip address inside 10.31.1.200 255.255.255.0
 no failover
 failover timeout 0:00:00
 failover ip address outside 0.0.0.0
 failover ip address inside 0.0.0.0
 arp timeout 14400
 global (outside) 1 192.1.1.10-192.1.1.20 netmask
255.255.255.0
 static (inside,outside) 192.1.1.25 171.68.118.143
netmask 255.255.255.255 0 0
 static (inside,outside) 192.1.1.30 10.31.1.5 netmask
255.255.255.255 0 0
 conduit permit tcp any any
 conduit permit icmp any any
 conduit permit udp any any
 no rip outside passive
 no rip outside default
 no rip inside passive
 no rip inside default
 route inside 171.68.118.0 255.255.255.0 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 0:00:00 absolute
 aaa-server TACACS+ protocol tacacs+
 aaa-server RADIUS protocol radius
 aaa-server AuthInbound protocol tacacs+
 aaa-server AuthInbound (inside) host 171.68.118.143
cisco timeout 5
 aaa-server AuthOutbound protocol radius
 aaa-server AuthOutbound (inside) host 171.68.118.133
cisco timeout 5
 aaa authentication telnet outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound
 aaa authentication telnet inbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthInbound
 aaa authentication http outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound
 aaa authentication http inbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 AuthInbound
 aaa authentication ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 AuthOutbound
 aaa authentication 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
 telnet timeout 5
 terminal width 80
 Cryptochecksum:fef4bfc9801d7692dce0cf227fe7859b
 : end
```

A autenticação debuga exemplos de PIXAuthentication debuga exemplos do PIX

Nestes debugar exemplos:

Saída

O usuário interno em 10.31.1.5 inicia o tráfego a 192.1.1.1 exterior e é autenticado com o TACACS+. O tráfego de saída usa a lista de servidor “AuthOutbound” que inclui o servidor Radius 171.68.118.133.

Entrada

O usuário externo em 192.1.1.1 inicia o tráfego a 10.31.1.5 interno (192.1.1.30) e é autenticado com o TACACS. O tráfego de entrada usa a lista de servidor “AuthInbound” que inclui o servidor de TACACS 171.68.118.143).

PIX debug - Boa autenticação - TACACS+

Este exemplo mostra um PIX debug com boa autenticação:

```
pix-5# write terminal
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pixfirewall
 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
 name 1.1.1.1 abcd
 name 1.1.1.2 a123456789
 name 1.1.1.3 a123456789123456
 pager lines 24
 logging timestamp
 no logging standby
 logging console debugging
 no logging monitor
 logging buffered debugging
 no logging trap
 logging facility 20
 logging queue 512
 interface ethernet0 auto
 interface ethernet1 auto
 mtu outside 1500
 mtu inside 1500
 ip address outside 192.1.1.254 255.255.255.0
 ip address inside 10.31.1.200 255.255.255.0
 no failover
 failover timeout 0:00:00
 failover ip address outside 0.0.0.0
```

```
failover ip address inside 0.0.0.0
arp timeout 14400
global (outside) 1 192.1.1.10-192.1.1.20 netmask 255.255.255.0
static (inside,outside) 192.1.1.25 171.68.118.143 netmask 255.255.255.255 0 0
static (inside,outside) 192.1.1.30 10.31.1.5 netmask 255.255.255.255 0 0
conduit permit tcp any any
conduit permit icmp any any
conduit permit udp any any
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
route inside 171.68.118.0 255.255.255.0 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 0:00:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server AuthInbound protocol tacacs+
aaa-server AuthInbound (inside) host 171.68.118.143 cisco timeout 5
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 171.68.118.133 cisco timeout 5
aaa authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authentication http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authentication ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication 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
telnet timeout 5
terminal width 80
Cryptochecksum:fef4bfc9801d7692dce0cf227fe7859b
: end
```

PIX debug - Autenticação inválida (username ou senha) - TACACS+

Este exemplo mostra o PIX debug com autenticação inválida (username ou senha). O usuário vê quatro conjuntos de nome de usuário/senha e `erro da` mensagem "`: número máximo de tentativas excedidas.`"

```
pix-5# write terminal
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pixfirewall
 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
 name 1.1.1.1 abcd
 name 1.1.1.2 a123456789
 name 1.1.1.3 a123456789123456
 pager lines 24
 logging timestamp
 no logging standby
```

```
 logging console debugging
 no logging monitor
 logging buffered debugging
 no logging trap
 logging facility 20
 logging queue 512
 interface ethernet0 auto
 interface ethernet1 auto
 mtu outside 1500
 mtu inside 1500
 ip address outside 192.1.1.254 255.255.255.0
 ip address inside 10.31.1.200 255.255.255.0
 no failover
 failover timeout 0:00:00
 failover ip address outside 0.0.0.0
 failover ip address inside 0.0.0.0
 arp timeout 14400
 global (outside) 1 192.1.1.10-192.1.1.20 netmask 255.255.255.0
 static (inside,outside) 192.1.1.25 171.68.118.143 netmask 255.255.255.255 0 0
 static (inside,outside) 192.1.1.30 10.31.1.5 netmask 255.255.255.255 0 0
 conduit permit tcp any any
 conduit permit icmp any any
 conduit permit udp any any
 no rip outside passive
 no rip outside default
 no rip inside passive
 no rip inside default
 route inside 171.68.118.0 255.255.255.0 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 0:00:00 absolute
 aaa-server TACACS+ protocol tacacs+
 aaa-server RADIUS protocol radius
 aaa-server AuthInbound protocol tacacs+
 aaa-server AuthInbound (inside) host 171.68.118.143 cisco timeout 5
 aaa-server AuthOutbound protocol radius
 aaa-server AuthOutbound (inside) host 171.68.118.133 cisco timeout 5
 aaa authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
 aaa authentication telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
 aaa authentication http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
 aaa authentication http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
 aaa authentication ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
 aaa authentication 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
 telnet timeout 5
 terminal width 80
 Cryptochecksum:fef4bfc9801d7692dce0cf227fe7859b
 : end
```

PIX debug - Pode sibilar o server, nenhuma resposta - TACACS+

Este exemplo mostra o PIX debug onde o server pode ser sibilado mas não está falando ao PIX. O usuário vê o username uma vez, mas o PIX nunca pede uma senha (este está no telnet). O usuário vê o "`erro: Número máximo de tentativas excedidas.`"

```
pix-5# write terminal
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 enable password 8Ry2YjIyt7RRXU24 encrypted
```

```
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
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
name 1.1.1.1 abcd
name 1.1.1.2 a123456789
name 1.1.1.3 a123456789123456
pager lines 24
logging timestamp
no logging standby
logging console debugging
no logging monitor
logging buffered debugging
no logging trap
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 192.1.1.254 255.255.255.0
ip address inside 10.31.1.200 255.255.255.0
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
global (outside) 1 192.1.1.10-192.1.1.20 netmask 255.255.255.0
static (inside,outside) 192.1.1.25 171.68.118.143 netmask 255.255.255.255 0 0
static (inside,outside) 192.1.1.30 10.31.1.5 netmask 255.255.255.255 0 0
conduit permit tcp any any
conduit permit icmp any any
conduit permit udp any any
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
route inside 171.68.118.0 255.255.255.0 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 0:00:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server AuthInbound protocol tacacs+
aaa-server AuthInbound (inside) host 171.68.118.143 cisco timeout 5
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 171.68.118.133 cisco timeout 5
aaa authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authentication http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authentication ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication 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
telnet timeout 5
terminal width 80
```

```
 Cryptochecksum:fef4bfc9801d7692dce0cf227fe7859b
 : end
```

PIX debug - Incapaz de sibilar o server - TACACS+

Este exemplo mostra a um PIX debug onde o server não é processo de ping. O usuário vê o username uma vez, mas o PIX nunca pede uma senha (este está no telnet). Estas mensagens são indicadas: "`Intervalo ao server TACACS+`" e ao "`erro: Número máximo de tentativas excedidas`" (nós trocamos dentro um servidor falso na configuração).

```
pix-5# write terminal
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pixfirewall
 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
 name 1.1.1.1 abcd
 name 1.1.1.2 a123456789
 name 1.1.1.3 a123456789123456
 pager lines 24
 logging timestamp
 no logging standby
 logging console debugging
 no logging monitor
 logging buffered debugging
 no logging trap
 logging facility 20
 logging queue 512
 interface ethernet0 auto
 interface ethernet1 auto
 mtu outside 1500
 mtu inside 1500
 ip address outside 192.1.1.254 255.255.255.0
 ip address inside 10.31.1.200 255.255.255.0
 no failover
 failover timeout 0:00:00
 failover ip address outside 0.0.0.0
 failover ip address inside 0.0.0.0
 arp timeout 14400
 global (outside) 1 192.1.1.10-192.1.1.20 netmask 255.255.255.0
 static (inside,outside) 192.1.1.25 171.68.118.143 netmask 255.255.255.255 0 0
 static (inside,outside) 192.1.1.30 10.31.1.5 netmask 255.255.255.255 0 0
 conduit permit tcp any any
 conduit permit icmp any any
 conduit permit udp any any
 no rip outside passive
 no rip outside default
 no rip inside passive
 no rip inside default
 route inside 171.68.118.0 255.255.255.0 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 0:00:00 absolute
 aaa-server TACACS+ protocol tacacs+
```

```
 aaa-server RADIUS protocol radius
 aaa-server AuthInbound protocol tacacs+
 aaa-server AuthInbound (inside) host 171.68.118.143 cisco timeout 5
 aaa-server AuthOutbound protocol radius
 aaa-server AuthOutbound (inside) host 171.68.118.133 cisco timeout 5
 aaa authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
 aaa authentication telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
 aaa authentication http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
 aaa authentication http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
 aaa authentication ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
 aaa authentication 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
 telnet timeout 5
 terminal width 80
 Cryptochecksum:fef4bfc9801d7692dce0cf227fe7859b
 : end
```

PIX debug - Boa autenticação - RAIO

Este exemplo mostra um PIX debug com boa autenticação:

```
pix-5# write terminal
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pixfirewall
 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
 name 1.1.1.1 abcd
 name 1.1.1.2 a123456789
 name 1.1.1.3 a123456789123456
 pager lines 24
 logging timestamp
 no logging standby
 logging console debugging
 no logging monitor
 logging buffered debugging
 no logging trap
 logging facility 20
 logging queue 512
 interface ethernet0 auto
 interface ethernet1 auto
 mtu outside 1500
 mtu inside 1500
 ip address outside 192.1.1.254 255.255.255.0
 ip address inside 10.31.1.200 255.255.255.0
 no failover
 failover timeout 0:00:00
 failover ip address outside 0.0.0.0
 failover ip address inside 0.0.0.0
 arp timeout 14400
 global (outside) 1 192.1.1.10-192.1.1.20 netmask 255.255.255.0
 static (inside,outside) 192.1.1.25 171.68.118.143 netmask 255.255.255.255 0 0
```

```
 static (inside,outside) 192.1.1.30 10.31.1.5 netmask 255.255.255.255 0 0
 conduit permit tcp any any
 conduit permit icmp any any
 conduit permit udp any any
 no rip outside passive
 no rip outside default
 no rip inside passive
 no rip inside default
 route inside 171.68.118.0 255.255.255.0 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 0:00:00 absolute
 aaa-server TACACS+ protocol tacacs+
 aaa-server RADIUS protocol radius
 aaa-server AuthInbound protocol tacacs+
 aaa-server AuthInbound (inside) host 171.68.118.143 cisco timeout 5
 aaa-server AuthOutbound protocol radius
 aaa-server AuthOutbound (inside) host 171.68.118.133 cisco timeout 5
 aaa authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
 aaa authentication telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
 aaa authentication http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
 aaa authentication http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
 aaa authentication ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
 aaa authentication 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
 telnet timeout 5
 terminal width 80
 Cryptochecksum:fef4bfc9801d7692dce0cf227fe7859b
 : end
```

PIX debug - Autenticação inválida (username ou senha) - RAIO

Este exemplo mostra um PIX debug com autenticação inválida (username ou senha). O usuário vê um pedido para o nome de usuário e senha. O usuário tem três oportunidades para o username/entrada de senha bem sucedidos.

```
pix-5# write terminal
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pixfirewall
 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
 name 1.1.1.1 abcd
 name 1.1.1.2 a123456789
 name 1.1.1.3 a123456789123456
 pager lines 24
 logging timestamp
 no logging standby
 logging console debugging
 no logging monitor
 logging buffered debugging
 no logging trap
```

```
 logging facility 20
 logging queue 512
 interface ethernet0 auto
 interface ethernet1 auto
 mtu outside 1500
 mtu inside 1500
 ip address outside 192.1.1.254 255.255.255.0
 ip address inside 10.31.1.200 255.255.255.0
 no failover
 failover timeout 0:00:00
 failover ip address outside 0.0.0.0
 failover ip address inside 0.0.0.0
 arp timeout 14400
 global (outside) 1 192.1.1.10-192.1.1.20 netmask 255.255.255.0
 static (inside,outside) 192.1.1.25 171.68.118.143 netmask 255.255.255.255 0 0
 static (inside,outside) 192.1.1.30 10.31.1.5 netmask 255.255.255.255 0 0
 conduit permit tcp any any
 conduit permit icmp any any
 conduit permit udp any any
 no rip outside passive
 no rip outside default
 no rip inside passive
 no rip inside default
 route inside 171.68.118.0 255.255.255.0 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 0:00:00 absolute
 aaa-server TACACS+ protocol tacacs+
 aaa-server RADIUS protocol radius
 aaa-server AuthInbound protocol tacacs+
 aaa-server AuthInbound (inside) host 171.68.118.143 cisco timeout 5
 aaa-server AuthOutbound protocol radius
 aaa-server AuthOutbound (inside) host 171.68.118.133 cisco timeout 5
 aaa authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
 aaa authentication telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
 aaa authentication http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
 aaa authentication http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
 aaa authentication ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
 aaa authentication 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
 telnet timeout 5
 terminal width 80
 Cryptochecksum:fef4bfc9801d7692dce0cf227fe7859b
 : end
```

O sibilo debuga - Pode sibilar o server, o demônio para baixo - RAIO

Este exemplo mostra a um PIX debug onde o server é processo de ping, mas o demônio está para baixo e não se comunicará com o PIX. O usuário vê o username, a senha, e `servidor Radius das` mensagens o "`falhado`" e o "`erro: Número máximo de tentativas excedidas.`"

```
pix-5# write terminal
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pixfirewall
 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
name 1.1.1.1 abcd
name 1.1.1.2 a123456789
name 1.1.1.3 a123456789123456
pager lines 24
logging timestamp
no logging standby
logging console debugging
no logging monitor
logging buffered debugging
no logging trap
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 192.1.1.254 255.255.255.0
ip address inside 10.31.1.200 255.255.255.0
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
global (outside) 1 192.1.1.10-192.1.1.20 netmask 255.255.255.0
static (inside,outside) 192.1.1.25 171.68.118.143 netmask 255.255.255.255 0 0
static (inside,outside) 192.1.1.30 10.31.1.5 netmask 255.255.255.255 0 0
conduit permit tcp any any
conduit permit icmp any any
conduit permit udp any any
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
route inside 171.68.118.0 255.255.255.0 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 0:00:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server AuthInbound protocol tacacs+
aaa-server AuthInbound (inside) host 171.68.118.143 cisco timeout 5
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 171.68.118.133 cisco timeout 5
aaa authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authentication http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authentication ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication 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
telnet timeout 5
terminal width 80
Cryptochecksum:fef4bfc9801d7692dce0cf227fe7859b
: end
```

[PIX debug - Incapaz de sibilar o server ou a incompatibilidade de chave/cliente -]

RAIO

Este exemplo calça um PIX debug onde o server não seja processo de ping ou haja uma incompatibilidade de chave/cliente. O usuário vê o username, a senha, e `intervalo das` mensagens o “ao `servidor Radius`” e ao “`erro: Número máximo de tentativas excedidas`” (um servidor falso foi trocado dentro a configuração).

```
pix-5# write terminal
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pixfirewall
 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
 name 1.1.1.1 abcd
 name 1.1.1.2 a123456789
 name 1.1.1.3 a123456789123456
 pager lines 24
 logging timestamp
 no logging standby
 logging console debugging
 no logging monitor
 logging buffered debugging
 no logging trap
 logging facility 20
 logging queue 512
 interface ethernet0 auto
 interface ethernet1 auto
 mtu outside 1500
 mtu inside 1500
 ip address outside 192.1.1.254 255.255.255.0
 ip address inside 10.31.1.200 255.255.255.0
 no failover
 failover timeout 0:00:00
 failover ip address outside 0.0.0.0
 failover ip address inside 0.0.0.0
 arp timeout 14400
 global (outside) 1 192.1.1.10-192.1.1.20 netmask 255.255.255.0
 static (inside,outside) 192.1.1.25 171.68.118.143 netmask 255.255.255.255 0 0
 static (inside,outside) 192.1.1.30 10.31.1.5 netmask 255.255.255.255 0 0
 conduit permit tcp any any
 conduit permit icmp any any
 conduit permit udp any any
 no rip outside passive
 no rip outside default
 no rip inside passive
 no rip inside default
 route inside 171.68.118.0 255.255.255.0 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 0:00:00 absolute
 aaa-server TACACS+ protocol tacacs+
 aaa-server RADIUS protocol radius
 aaa-server AuthInbound protocol tacacs+
 aaa-server AuthInbound (inside) host 171.68.118.143 cisco timeout 5
```

```
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 171.68.118.133 cisco timeout 5
aaa authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authentication http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authentication ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication 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
telnet timeout 5
terminal width 80
Cryptochecksum:fef4bfc9801d7692dce0cf227fe7859b
: end
```

Adicionar a autorização

Se você decide adicionar a autorização, você exigirá a autorização para o mesmo intervalo de origem e de destino (desde que a autorização é inválida sem autenticação):

```
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
```

Note que a autorização não está adicionada para “que parte” porque o tráfego de saída é autenticado com RAIO, e a autorização RADIUS é inválida.

A authentication e autorização debuga exemplos do PIX

PIX debug - Boa autenticação e autorização bem sucedida - TACACS+

Este exemplo mostra um PIX debug com boa autenticação e autorização bem sucedida:

```
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
```

PIX debug - Boa autenticação, autorização falha - TACACS+

Este exemplo mostra um PIX debug com boa autenticação mas com autorização falha. Aqui o usuário igualmente vê `erro da` mensagem “`: Autorização negada.`”

```
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
```

Adicionar relatório

TACACS+

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

Debugar o olhar o mesmos se explicar é de ligar/desligar. Contudo, na altura do “construiu, registro de contabilidade do “começo”” a é enviado. Na altura do “Teardown, o registro de contabilidade da “parada”” a é enviado.

Os registros de contabilidade TACACS+ olham como esta saída (estes são do Cisco Secure NT, daqui do formato delimitado por vírgula):

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

RADIUS

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

Debugar olhares o mesmos se explicar é de ligar/desligar. Contudo, na altura do “construiu, registro de contabilidade do “começo”” a é enviado. Na altura do “Teardown, o registro de contabilidade da “parada”” a é enviado.

Os registros de contabilidade do RAIO olham como esta saída (estes são de Cisco UNIX seguro; no Cisco Secure NT podem ser delimitados por vírgula pelo contrário):

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

Uso do comando Except

Em nossa rede, se nós decidimos que um origem específica e/ou um destino não precisam a autenticação, a autorização, ou explicar, nós podemos fazer qualquer outra coisa semelhante output:

```
aaa authentication except inbound 192.1.1.1 255.255.255.255
   0.0.0.0 0.0.0.0 AuthInbound
```

Se você é “com exceção” de uma caixa da autenticação e tem a autorização sobre, você deve igualmente exceptuar a caixa da autorização.

Max-sessions e visualização de usuários que fizeram login

Alguns servidores de TACACS+ e RADIUS possuem recursos “max-session” ou “visualizar usuários que fizeram login”. A habilidade de realizar max-sessions ou verificar usuários que fizeram login depende dos registros de contabilidade. Quando há um registro do “começo” da

contabilidade gerado mas nenhum registro da “parada”, o TACACS+ ou o servidor Radius supõem que a pessoa está entrada ainda (tem uma sessão com o PIX).

Isto funciona bem para conexões Telnet e FTP devido à natureza das conexões. Isso não funciona bem para HTTP devido à natureza da conexão. Nestas saídas de exemplo, uma configuração de rede diferente é usada, mas os conceitos são os mesmos.

O usuário Telnets com o PIX, autenticando na maneira:

```
aaa authentication except inbound 192.1.1.1 255.255.255.255
   0.0.0.0 0.0.0.0 AuthInbound
```

Desde que o server não viu um registro do “começo” mas nenhum registro da “parada” (neste momento), o server mostra que o usuário do “telnet” está entrado. Se o usuário tenta uma outra conexão que exija a autenticação (talvez de um outro PC) e se as sessões máx. são ajustadas a "1" no server para este usuário (que supõe as sessões máx. dos suportes de servidor), a conexão é recusada pelo server.

O usuário vai sobre com o telnet ou o negócio FTP no host de destino, a seguir nas saídas (passa os minutos 10 lá):

```
aaa authentication except inbound 192.1.1.1 255.255.255.255
   0.0.0.0 0.0.0.0 AuthInbound
```

Se o uauth é 0 (autentique todas as vezes) ou mais (autentique uma vez e não outra vez durante o período de uauth), um registro de contabilidade é cortado para cada local alcançado.

O HTTP trabalha de forma diferente devido à natureza do protocolo. Esta saída mostra um exemplo de HTTP:

O usuário consulta de 171.68.118.100 a 9.9.9.25 com o PIX:

```
aaa authentication except inbound 192.1.1.1 255.255.255.255
   0.0.0.0 0.0.0.0 AuthInbound
```

O usuário lê a página da Web baixada.

O registro inicial afixado em 16:35:34, e o registro da parada afixado em 16:35:35. Esse download levou um segundo (ou seja, houve menos de um segundo entre o início e o término da gravação). O usuário é entrado ainda ao site e à conexão ainda abertos quando estão lendo o página da web? No. Max-sessions ou visualizar usuários que fizeram login funcionará aqui? Não, porque o tempo de conexão (o tempo entre “Built” (Construção) e Teardown (Destruição)) em HTTP é muito curto. O registro “start” (iniciar) e “stop” (parar) é sub-segundo. Não haverá um registro do “começo” sem um registro da “parada”, desde que os registros ocorrem virtualmente no mesmo instante. Ainda haverá um “começo” e “pare” o registro enviado ao server para cada transação, se o uauth está ajustado para 0 ou algo maior. Contudo, as sessões máx. e os usuários que fez login da vista não trabalham devido às naturezas da conexão de HTTP.

Autenticação e habilitação no próprio PIX

A discussão anterior descreveu autenticar o tráfego do telnet (e o HTTP, o FTP) *com o* PIX. Nós certificamo-nos do telnet aos trabalhos PIX *sem* autenticação sobre:

```
telnet 10.31.1.5 255.255.255.255 passwd ww
```

```
aaa authentication telnet console AuthInbound
```

Quando os usuários Telnet ao PIX, eles forem alertados para a senha telnet (**ww**). Então o PIX igualmente pede o TACACS+ (neste caso, desde que a lista de servidor do “AuthInbound” é usada) ou nome de usuário RADIUS e senha. Se o server está para baixo, você pode obter no PIX incorporando o **pix** para o username, e na senha da possibilidade (**permita a senha *o que quer que***) para aceder então.

Com este comando:

```
aaa authentication enable console AuthInbound
```

o usuário é alertado para um nome de usuário e senha, que seja enviado ao TACACS (neste caso, desde que a lista de servidor do “AuthInbound” é usada, o pedido vai ao servidor de TACACS) ou ao servidor Radius. Desde que o pacote de autenticação para permite é o mesmo que o pacote de autenticação para o início de uma sessão, se o usuário pode entrar ao PIX com TACACS ou RAIO, eles pode permitir através do TACACS ou do RAIO com o mesmo nome de usuário/senha. Este problema foi atribuído a identificação de bug Cisco CSCdm47044 (clientes registrados somente).

Autenticação no console serial

O comando aaa authentication serial console AuthInbound exige a verificação de autenticação a fim alcançar o console serial do PIX.

Quando os comandos user performs configuration do console, mensagens do syslog são cortados (supondo o PIX é configurado para enviar o Syslog a nível de debug a um syslog host). Este é um exemplo do que é indicado no servidor de SYSLOG:

```
aaa authentication enable console AuthInbound
```

Mude a alerta que os usuários veem

Se você tem o **comando auth-prompt PIX_PIX_PIX**, os usuários que atravessam o PIX veem esta sequência:

```
aaa authentication enable console AuthInbound
```

Em cima da chegada na máquina de destino final, o “username: ” e “senha: a” alerta é indicada. Esta alerta afeta somente os usuários que vão *com o* PIX, não ao PIX.

Nota: Não há nenhum registro de contabilidade cortado para o acesso ao PIX.

Personalize os usuários da mensagem veem no sucesso/falha

Se você tem os comandos:

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

os usuários veem esta sequência em um login bem-sucedido/falha no login com o PIX:

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

Tempo ocioso e intervalos absolutos por usuário

A quietude e os uauth timeout absolutos podem ser enviados para baixo do server TACACS+ em uma base do usuário per. Se todos os usuários em sua rede devem ter o mesmo “timeout uauth,” não execute isto! Mas se você precisa uauths diferentes por usuário, continue a ler.

Neste exemplo, o **comando timeout uauth 3:00:00** é usado. Uma vez que uma pessoa autentica, não têm que autenticar novamente por três horas. Contudo, se você estabelece um usuário com este perfil e tem a autorização de AAA TACACS sobre no PIX, a quietude e os timeouts absolutos no perfil de usuário cancelam o timeout uauth no PIX para esse usuário. Isto não significa que a sessão de Telnet com o PIX está desligada após a quietude/timeout absoluto. Apenas controla se a reautenticação ocorre.

Este perfil vem do freeware TACACS+:

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

Após a autenticação, execute um **comando show uauth no** PIX:

```
pix-5# show uauth
                        Current    Most Seen
 Authenticated Users       1          1
 Authen In Progress        0          1
 user 'timeout' at 10.31.1.5, authorized to:
```

```
    port 11.11.11.15/telnet
    absolute   timeout: 0:02:00
    inactivity timeout: 0:01:00
```

Depois que o usuário senta a quietude para um minuto, debugar no PIX mostra:

```
pix-5# show uauth
                        Current    Most Seen
 Authenticated Users       1          1
 Authen In Progress        0          1
 user 'timeout' at 10.31.1.5, authorized to:
    port 11.11.11.15/telnet
    absolute   timeout: 0:02:00
    inactivity timeout: 0:01:00
```

O usuário tem que autenticar novamente quando retorna ao mesmo host de destino ou a um host diferente.

HTTP Virtual

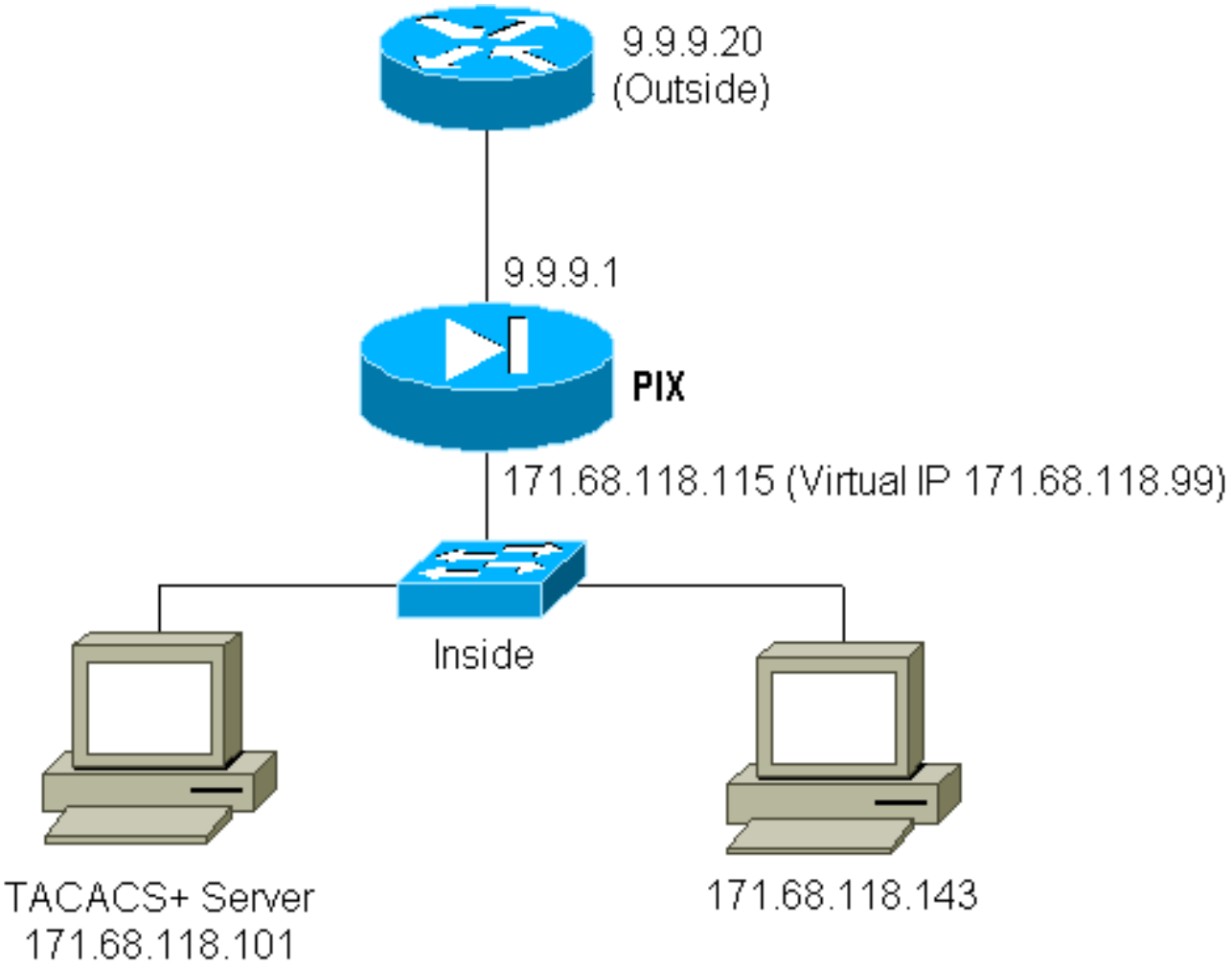
Se a autenticação é exigida em locais fora do PIX, assim como no PIX próprio, o comportamento incomum do navegador pode às vezes ser observado desde que os navegadores põem em esconderijo o nome de usuário e senha.

Para evitar isto, você pode executar o HTTP virtual adicionando um endereço do RFC 1918 (um endereço que seja não-roteável no Internet, mas válido e original para a rede interna PIX) à configuração de PIX usando este comando:

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

Quando o usuário tenta sair do PIX, a autenticação é necessária. Se o parâmetro de advertência estiver presente, o usuário recebe uma mensagem redirecionada. A autenticação é boa para a durante o tempo do uauth. Como indicado na documentação, não ajuste a duração do **comando timeout uauth aos** segundos 0 com HTTP virtual. isso evita conexões de HTTP ao servidor da Web real.

Diagrama das Saídas HTTP Virtual



Saídas HTTP Virtual da configuração de PIX

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

Telnet Virtual

Épossível configurar o PIX para autenticar todo o tráfego de entrada e de saída, mas não é uma boa ideia fazer assim. Isto é porque alguns protocolos, tais como o “correio,” não são autenticados facilmente. Quando um mail server e um cliente tentarem se comunicar com o PIX quando todo o tráfego com o PIX estiver autenticado, Syslog PIX para protocolos não autenticáveis exibem mensagem como:

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

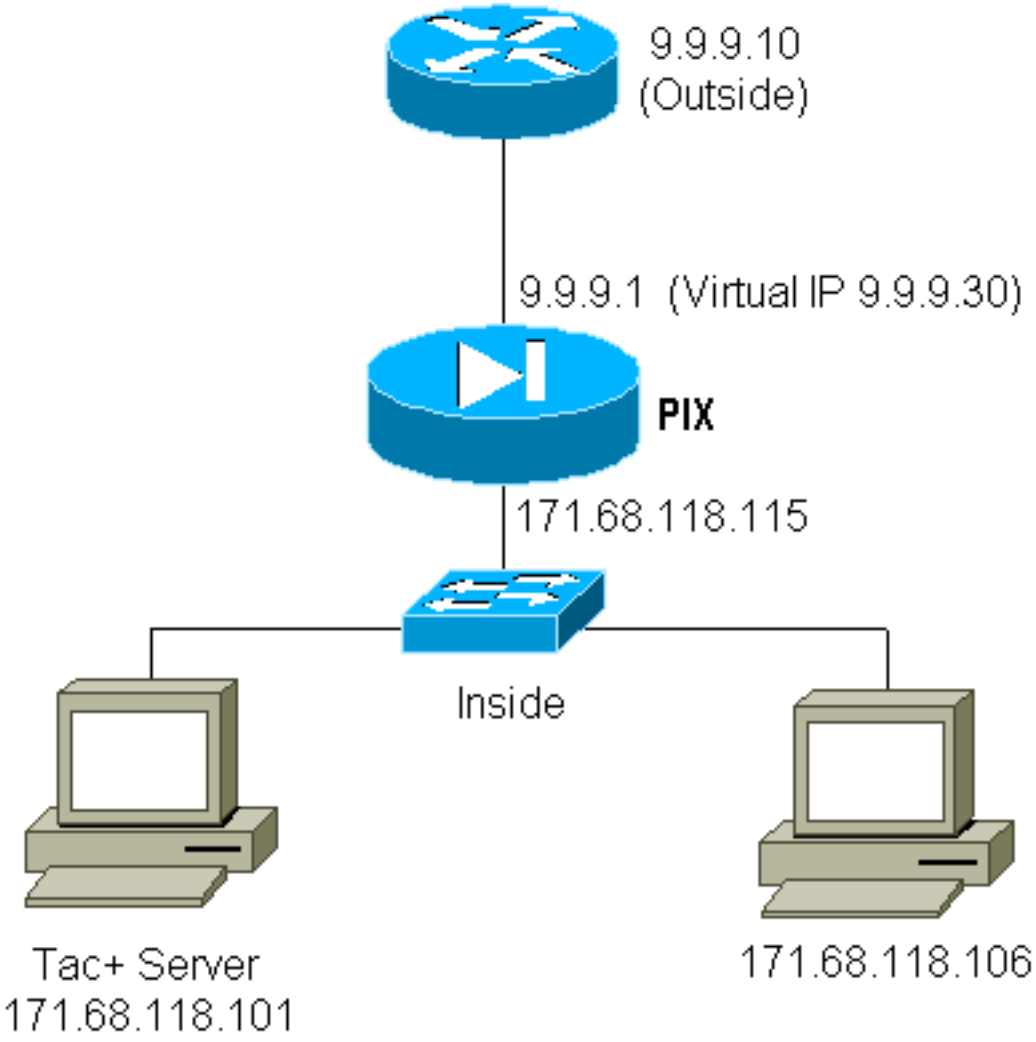
Desde que o correio e alguns outros serviços não são interativos bastante autenticar, uma solução é usar o **comando except** para a autenticação/autorização (autentique tudo à exceção da fonte/destino do mail server/cliente).

Se há uma necessidade real de autenticar algum tipo do serviço incomun, este pode ser feito por meio do **comando virtual telnet**. Este comando permite que a autenticação ocorra ao IP de Telnet

virtual. Após esta autenticação, o tráfego para o serviço incomun pode ir ao servidor real.

Neste exemplo, nós queremos o tráfego da porta TCP 49 fluir do host exterior 9.9.9.10 ao host interno 171.68.118.106. Desde que este tráfego não é realmente authenticatable, nós estabelecemos um telnet virtual. Para o telnet virtual de entrada, deve haver uma estática associada. Aqui, 9.9.9.20 e 171.68.118.20 são endereços virtuais.

Diagrama da entrada de telnet virtual



Entrada de telnet virtual da configuração de PIX

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

Telnet virtual de configuração de usuário do servidor TACACS+ de entrada

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

Entrada de telnet virtual do PIX debug

O usuário em 9.9.9.10 deve primeiramente autenticar por Telnetting ao endereço de 9.9.9.20 no PIX:

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

Após a autenticação bem sucedida, o **comando show uauth** mostra que o usuário tem o “tempo no medidor”:

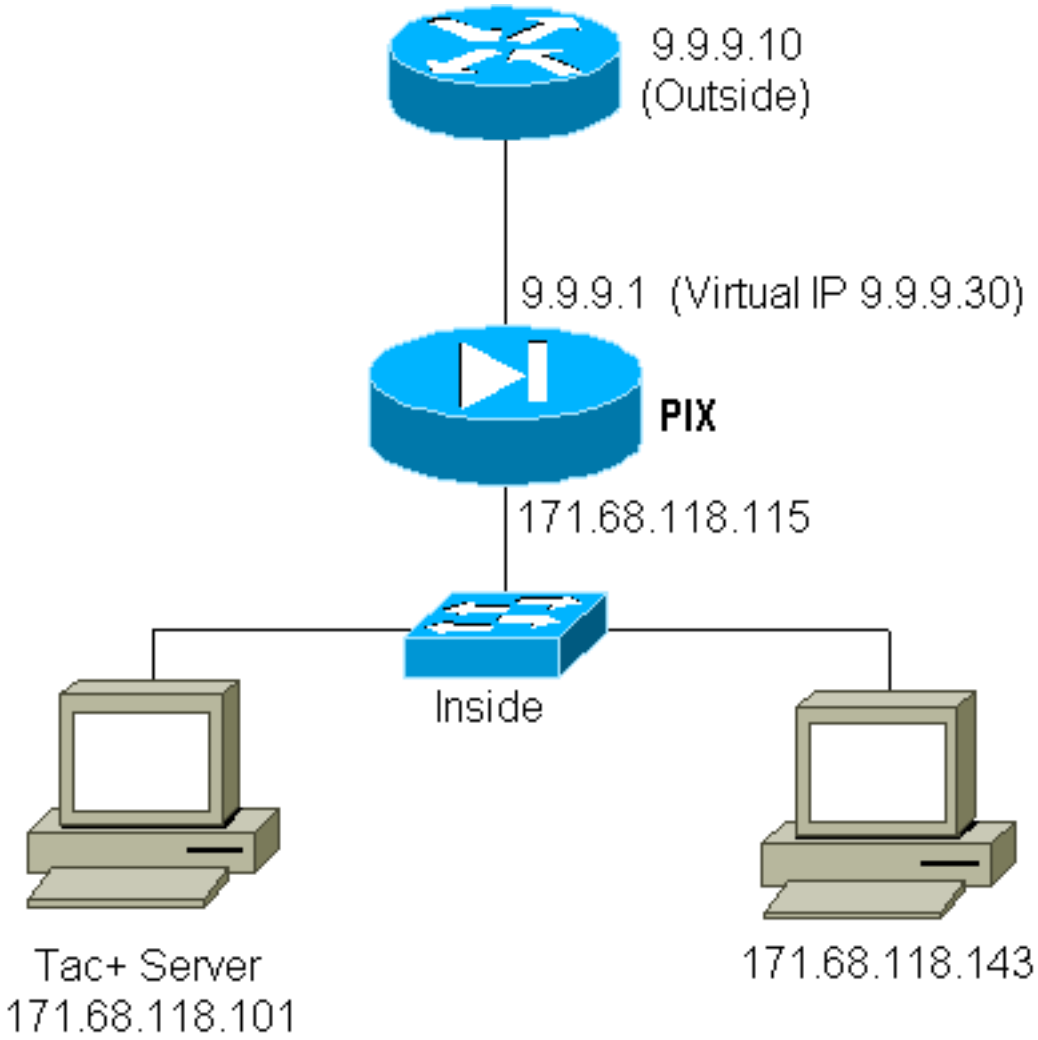
```
pixfirewall# show uauth
                        Current    Most Seen
 Authenticated Users       1          1
 Authen In Progress        0          1
 user 'pinecone' at 9.9.9.10, authenticated
    absolute   timeout: 0:10:00
    inactivity timeout: 0:10:00
```

Aqui, o dispositivo em 9.9.9.10 quer enviar o tráfego TCP/49 ao dispositivo em 171.68.118.106:

```
pixfirewall# show uauth
                        Current    Most Seen
 Authenticated Users       1          1
 Authen In Progress        0          1
 user 'pinecone' at 9.9.9.10, authenticated
    absolute   timeout: 0:10:00
    inactivity timeout: 0:10:00
```

Saída Telnet Virtual

Desde que o tráfego de saída é permitido à revelia, não estático é exigido para o uso das saídas telnet virtuais. Neste exemplo, o usuário interno em 171.68.118.143 Telnets a 9.9.9.30 virtual e autentica. A conexão Telnet é deixada cair imediatamente. Uma vez que autenticado, o tráfego TCP é permitido de 171.68.118.143 ao server em 9.9.9.10:



Saídas telnet virtuais da configuração de PIX

```
pixfirewall# show uauth
                        Current    Most Seen
 Authenticated Users       1          1
 Authen In Progress        0          1
 user 'pinecone' at 9.9.9.10, authenticated
    absolute   timeout: 0:10:00
    inactivity timeout: 0:10:00
```

Saídas telnet virtuais do PIX debug

```
pixfirewall# show uauth
                        Current    Most Seen
 Authenticated Users       1          1
 Authen In Progress        0          1
 user 'pinecone' at 9.9.9.10, authenticated
    absolute   timeout: 0:10:00
    inactivity timeout: 0:10:00
```

Desconexão de Telnet Virtual

Quando o usuário Telnets ao IP de Telnet virtual, o **comando show uauth** mostrar o uauth.

Se o usuário quer impedir que o tráfego vá completamente depois que a sessão está terminada

(quando houver um tempo deixado no uauth), o usuário precisa o telnet ao IP de Telnet virtual outra vez. Esta ação desliga a sessão.

Autorização da porta

Você pode exigir a autorização em uma faixa de porta. Neste exemplo, a autenticação foi exigida ainda para toda de partida, mas somente a autorização foi exigida para portas TCP 23-49.

Configuração de PIX

```
AAA authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
AAA authorization tcp/23-49 outbound 0.0.0.0 0.0.0.0
   0.0.0.0 0.0.0.0 AuthOutbound
```

Quando o telnet foi feito de 171.68.118.143 a 9.9.9.10, a authentication e autorização ocorreu porque a porta 23 do telnet está na escala 23-49.

Quando uma sessão de HTTP é feita de 171.68.118.143 a 9.9.9.10, você ainda tem que autenticar, mas o PIX não pede o server TACACS+ para autorizar o HTTP porque 80 não estão na escala 23-49.

TACACS+ Configuração do programa gratuito de servidor

```
AAA authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
AAA authorization tcp/23-49 outbound 0.0.0.0 0.0.0.0
   0.0.0.0 0.0.0.0 AuthOutbound
```

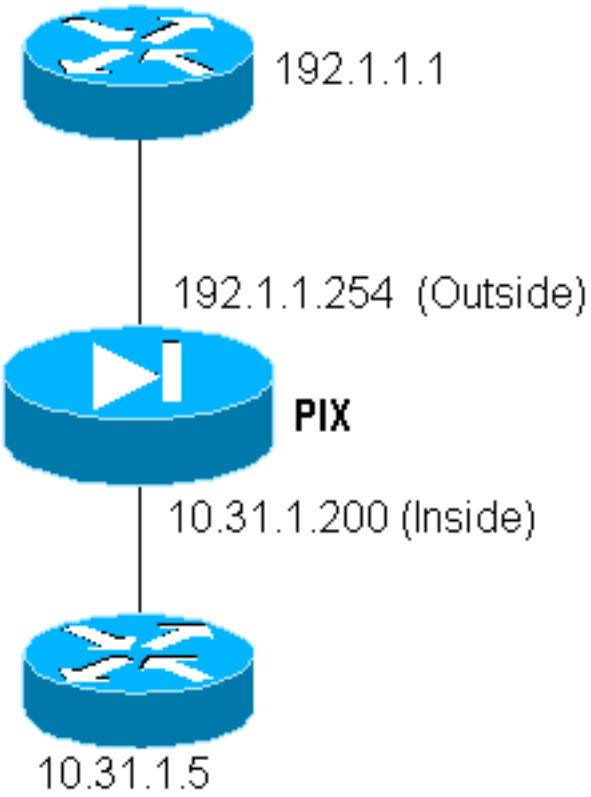
Note que o PIX envia “`cmd=tcp/23-49"` e “`cmd-arg=9.9.9.10" ao` server TACACS+.

Debugar no PIX

```
AAA authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
AAA authorization tcp/23-49 outbound 0.0.0.0 0.0.0.0
   0.0.0.0 0.0.0.0 AuthOutbound
```

Relatório de AAA para tráfego diferente de HTTP, FTP e Telnet

A versão de software de PIX 5.0 muda a funcionalidade da contabilidade do tráfego. Os registros de contabilidade podem agora ser cortados para o tráfego a não ser o HTTP, o FTP, e o telnet, uma vez que a autenticação é terminada.



A TFTP-cópia um arquivo do roteador exterior (192.1.1.1) ao roteador interno (10.31.1.5), adiciona o telnet virtual para abrir um furo para o processo TFTP:

```
virtual telnet 192.1.1.30
static (inside,outside) 192.1.1.30 10.31.1.5 netmask 255.255.255.255 0 0
conduit permit udp any any
AAA authentication udp/69 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
AAA authorization udp/69 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
AAA accounting udp/0 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

Em seguida, o telnet do roteador exterior em 192.1.1.1 ao IP virtual 192.1.1.30 e autentica ao endereço virtual que permite que o UDP atravesse o PIX. Neste exemplo, o processo do **flash de tftp da cópia** foi começado da parte externa ao interior:

```
virtual telnet 192.1.1.30
static (inside,outside) 192.1.1.30 10.31.1.5 netmask 255.255.255.255 0 0
conduit permit udp any any
AAA authentication udp/69 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
AAA authorization udp/69 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
AAA accounting udp/0 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

Para cada **flash de tftp da cópia no** PIX (havia três durante esta cópia IO), um registro de contabilidade é cortado e enviado ao Authentication Server. Seguir é um exemplo de um registro TACACS em Cisco fixa Windows):

```
virtual telnet 192.1.1.30
static (inside,outside) 192.1.1.30 10.31.1.5 netmask 255.255.255.255 0 0
```

```
conduit permit udp any any
AAA authentication udp/69 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
AAA authorization udp/69 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
AAA accounting udp/0 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

Informações Relacionadas

- Referências de comando PIX
- Página de Suporte do Produto PIX