Configurando o PIX 5.0.x: TACACS+ e RADIUS

Contents

Introduction

A autenticação RADIUS e TACACS+ pode ser feita para conexões FTP, Telnet e HTTP. A autenticação para outros protocolos TCP menos comuns geralmente pode ser feita para funcionar.

A autorização TACACS+ é suportada. A autorização de RADIUS não é. As alterações na autenticação, autorização e contabilização (AAA) do PIX 5.0 sobre a versão anterior incluem a contabilização AAA para tráfego diferente de HTTP, FTP e Telnet.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

Conventions

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

Autenticação vs. Autorização

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

Por exemplo, suponha que você tenha cem usuários dentro e que você queira que apenas seis desses usuários sejam capazes de executar FTP, Telnet ou HTTP fora da rede. Diga ao PIX para autenticar o tráfego de saída e fornecer todos os seis IDs de usuários no servidor de segurança TACACS+/RADIUS. Com *autenticação* simples, esses seis usuários podem ser autenticados com nome de usuário e senha e depois saem. Os outros 94 usuários não podem sair. O PIX solicita aos usuários o nome de usuário/senha e, em seguida, passa o nome de usuário e a senha para o servidor de segurança TACACS+/RADIUS. Dependendo da resposta, ela abre ou nega a conexão. Esses seis usuários podem fazer FTP, Telnet ou HTTP.

Por outro lado, suponha que *um* desses três usuários, "Terry", não seja confiável. Você gostaria de permitir que Terry faça FTP, mas não HTTP ou Telnet para fora. Isso significa que você precisa adicionar *autorização*. Ou seja, autorizar *o que* os usuários podem fazer além de autenticar *quem* são. Quando você adiciona *autorização* ao PIX, o PIX primeiro envia o nome de usuário e a senha de Terry para o servidor de segurança e, em seguida, envia uma solicitação de autorização informando ao servidor de segurança o que o "*comando*" Terry está tentando fazer. Com o servidor configurado corretamente, Terry pode ter permissão para "FTP 1.2.3.4", mas tem a capacidade de "HTTP" ou "Telnet" negada em qualquer lugar.

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

Quando você tenta ir de dentro para fora (ou vice-versa) com autenticação/autorização ativada:

- **Telnet** - O usuário vê um prompt de nome de usuário, seguido de uma solicitação de 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 a exibição de um prompt de nome de usuário.** 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** - Uma janela exibida no navegador que solicita nome de usuário e senha. Se a autenticação (e autorização) for concluída com sucesso, o usuário chega ao web site de destino. Lembre-se de que **os navegadores armazenam em cache nomes de usuário e senhas.**. 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 funcionar normalmente, mas as conexões HTTP não funcionam, é

por isso que.

Configurações de servidor de segurança utilizadas para todos os cenários

Configuração do servidor Cisco Secure UNIX TACACS

Verifique se você tem o endereço IP do PIX ou o nome de domínio e a chave totalmente qualificados 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 Cisco Secure UNIX RADIUS

Use a GUI (Graphical User Interface, interface gráfica do usuário) para adicionar o PIX IP e a chave à lista do NAS (Network Access Server, servidor de acesso à rede).

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

Cisco Secure Windows 2.x RADIUS

Siga estes passos:

1. Obtenha uma senha na seção User Setup GUI (GUI de configuração do usuário).
2. Na seção GUI da configuração do grupo, defina o atributo 6 (Tipo de serviço) como Login ou Administrativo.
3. Adicione o PIX IP na GUI de configuração do NAS.

EasyACS TACACS+

A documentação do EasyACS descreve a configuração.

1. Na seção de grupo, clique em **Shell exec** (para conceder privilégios exec).
2. Para adicionar autorização ao PIX, clique em **Negar comandos IOS não correspondentes** na parte inferior da configuração do grupo.
3. Selecione **Add/Edit new command** para cada comando que deseja permitir (por exemplo, Telnet).
4. Se quiser permitir Telnet para sites específicos, digite o(s) IP(s) na seção de argumento no formato "permit #.#.#.#". Para permitir Telnet para todos os sites, clique em **Permitir todos os argumentos não listados**.
5. Clique em **Concluir comando de edição**.
6. Execute as etapas de 1 a 5 para cada um dos comandos permitidos (por exemplo, Telnet, HTTP ou FTP).
7. Adicione o PIX IP na seção NAS Configuration GUI (GUI de configuração de NAS).

Cisco Secure 2.x TACACS+

O usuário obtém uma senha na seção GUI de configuração do usuário.

1. Na seção de grupo, clique em **Shell exec** (para conceder privilégios exec).
2. Para adicionar autorização ao PIX, clique em **Negar comandos IOS não correspondentes** na parte inferior da configuração do grupo.
3. Selecione **Add/Edit new command** para cada comando que deseja permitir (por exemplo, Telnet).
4. Se quiser permitir Telnet para sites específicos, insira permit IP(s) no retângulo do argumento (por exemplo, "permit 1.2.3.4"). Para permitir Telnet para todos os sites, clique em **Permitir todos os argumentos não listados**.
5. Clique em **concluir comando de edição**.
6. Execute as etapas anteriores para cada um dos comandos permitidos (por exemplo, Telnet, HTTP e/ou FTP).
7. Adicione o PIX IP na seção NAS Configuration GUI (GUI de configuração de NAS).

Configuração de servidor Livingston RADIUS

Adicione o PIX IP e a chave ao arquivo de clientes.

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

Configuração de servidor Merit RADIUS

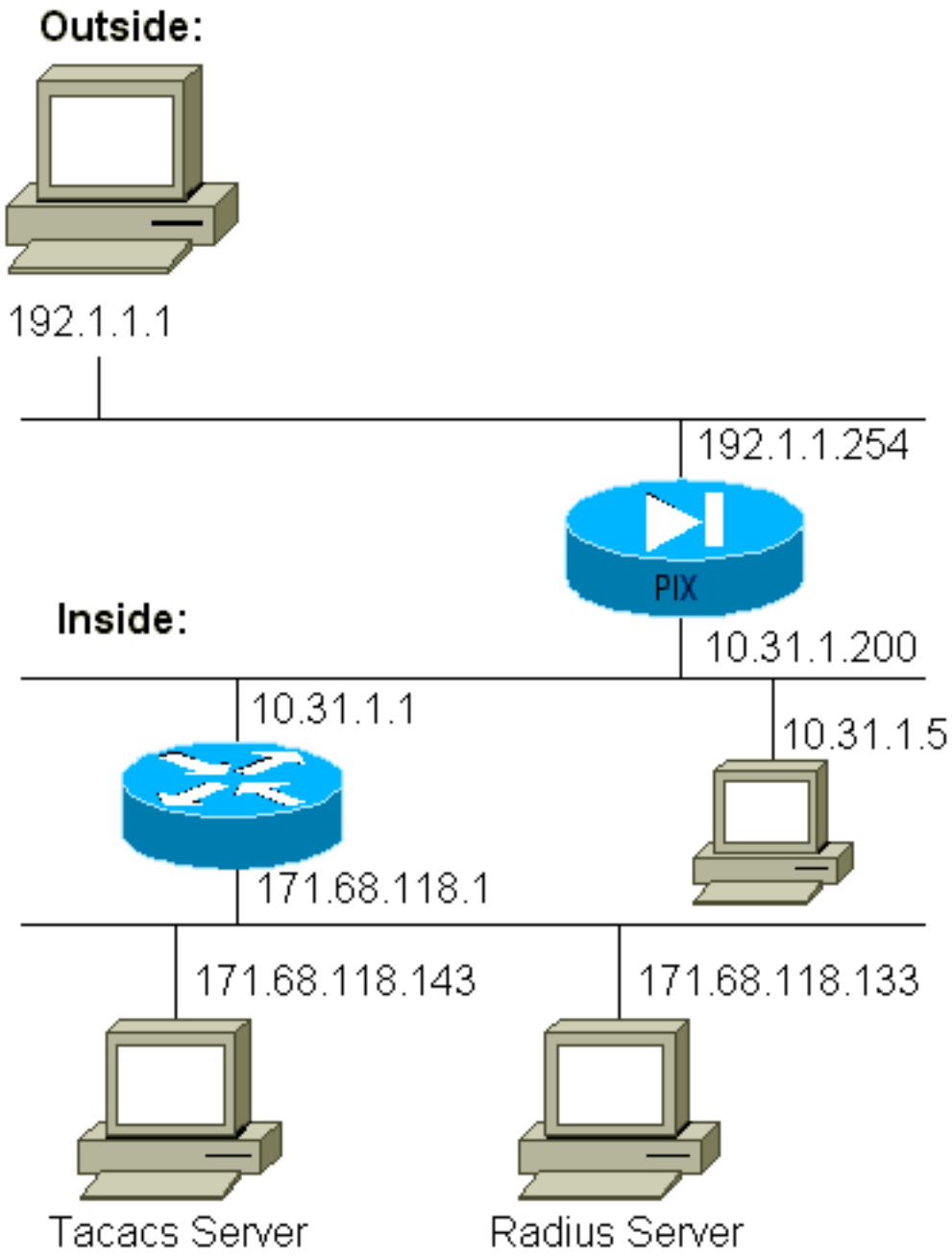
Adicione o PIX IP e a chave ao arquivo de clientes.

```
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 do PIX funcionem antes de adicionar AAA.Se você não passar o tráfego antes de instituir autenticação e autorização, não conseguirá fazê-lo depois disso.
- Habilitar registro no 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 para um servidor syslog e examinada.
- Verifique se a depuração está ativada para os servidores TACACS+ ou 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
```

Exemplos de depuração de autenticação do PIXAuthentication Debug Exemplos do PIX

Nesses exemplos de depuração:

Saída

O usuário interno em 10.31.1.5 inicia o tráfego para fora de 192.1.1.1 e é autenticado através do TACACS+. O tráfego de saída usa a lista de servidores "AuthOutbound" que inclui o servidor RADIUS 171.68.118.133.

Entrada

O usuário externo em 192.1.1.1 inicia o tráfego para o interior 10.31.1.5 (192.1.1.30) e é autenticado por TACACS. O tráfego de entrada usa a lista de servidores "AuthInbound" que inclui o servidor TACACS 171.68.118.143).

Depuração de PIX - Boa autenticação - TACACS+

Este exemplo mostra uma depuração de PIX com boa autenticação:

```
pixfirewall# 109001: Auth start for user "???" from 192.1.1.1/13155
    to 10.31.1.5/23
 109011: Authen Session Start: user 'pixuser', sid 6
 109005: Authentication succeeded for user 'pixuser' from 10.31.1.5/23
    to 192.1.1.1/13155
 109012: Authen Session End: user 'pixuser', Sid 6, elapsed 1 seconds
 302001: Built inbound TCP connection 6 for faddr 192.1.1.1/13155
    gaddr 192.1.1.30/23 laddr 10.31.1.5/23 (pixuser)
```

Depuração de PIX - Autenticação incorreta (nome de usuário ou senha) - TACACS+

Este exemplo mostra a depuração de PIX com autenticação incorreta (nome de usuário ou senha). O usuário vê quatro conjuntos de nome de usuário/senha e a mensagem "`Erro: número máximo de tentativas excedido.`"

```
pixfirewall# 109001: Auth start for user '???' from 192.1.1.1/13157
    to 10.31.1.5/23
 109006: Authentication failed for user '' from 10.31.1.5/23
    to 192.1.1.1/13157
```

Depuração de PIX - Pode efetuar ping no servidor, sem resposta - TACACS+

Este exemplo mostra a depuração de PIX em que o servidor pode receber ping, mas não está falando com o PIX. O usuário vê o nome de usuário uma vez, mas o PIX nunca pede uma senha (isso está no Telnet). O usuário vê "`Erro: Número máximo de tentativas excedido.`"

```
Auth start for user '???' from 192.1.1.1/13159 to
    10.31.1.5/23
```

```
pixfirewall# 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13159
   failed (server 171.68.118.143 failed)
109002: Auth from 10.31.1.5/23 to 192.1.1.1/13159 failed
   (server 171.68.118.143 failed)
109002: Auth from 10.31.1.5/23 to 192.1.1.1/13159 failed
   (server 171.68.118.143 failed)
109006: Authentication failed for user '' from 10.31.1.5/23
   to 192.1.1.1/13159
```

Depuração de PIX - Não é possível fazer ping no servidor - TACACS+

Este exemplo mostra uma depuração de PIX em que o servidor não pode executar ping. O usuário vê o nome de usuário uma vez, mas o PIX nunca pede uma senha (isso está no Telnet). Essas mensagens são exibidas: "`Timeout to TACACS+ server`" and "`Error: Número máximo de tentativas excedido`" (trocamos em um servidor falso na configuração).

```
109001: Auth start for user '???' from 192.1.1.1/13158
   to 10.31.1.5/23
109002: Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed
   (server 171.68.118.143 failed)
109002: Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed
   (server 171.68.118.143 failed)
109002: Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed
   (server 171.68.118.143 failed)
109006: Authentication failed for user '' from 10.31.1.5/23
   to 192.1.1.1/13158
```

Depuração de PIX - Boa autenticação - RADIUS

Este exemplo mostra uma depuração de PIX com boa autenticação:

```
109001: Auth start for user '???' from 10.31.1.5/11074
   to 192.1.1.1/23
109011: Authen Session Start: user 'pixuser', Sid 7
109005: Authentication succeeded for user 'pixuser'
   from 10.31.1.5/11074 to 192.1.1.1/23
109012: Authen Session End: user 'pixuser', Sid 7,
   elapsed 1 seconds
302001: Built outbound TCP connection 7 for faddr 192.1.1.1/23
   gaddr 192.1.1.30/11074 laddr 10.31.1.5/11074 (pixuser)
```

Depuração de PIX - Autenticação incorreta (nome de usuário ou senha) - RADIUS

Este exemplo mostra uma depuração de PIX com autenticação incorreta (nome de usuário ou senha). O usuário vê uma solicitação de Nome de usuário e Senha. O usuário tem três oportunidades para a entrada de nome de usuário/senha bem-sucedida.

```
- 'Error: max number of tries exceeded'
pixfirewall# 109001: Auth start for user '???' from
   192.1.1.1/13157 to 10.31.1.5/23
109001: Auth start for user '???' from 10.31.1.5/11075
   to 192.1.1.1/23
109002: Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed
   (server 171.68.118.133 failed)
109002: Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed
   (server 171.68.118.133 failed)
109002: Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed
   (server 171.68.118.133 failed)
```

```
 109006: Authentication failed for user '' from 10.31.1.5/11075
    to 192.1.1.1/23
```

Depuração de ping - Pode Fazer ping no servidor, Daemon desativado - RADIUS

Este exemplo mostra uma depuração de PIX em que o servidor pode fazer ping, mas o daemon está inoperante e não se comunicará com o PIX. O usuário vê o nome de usuário, a senha e as mensagens "`Falha no servidor RADIUS`" e "`Erro: Número máximo de tentativas excedido.`"

```
pixfirewall# 109001: Auth start for user '???'
    from 10.31.1.5/11076 to 192.1.1.1/23
 109002: Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109002: Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109002: Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11076
    to 192.1.1.1/23
```

Depuração de PIX - Não é possível executar ping para o servidor ou para a incompatibilidade de chave/cliente - RADIUS

Este exemplo mostra uma depuração de PIX em que o servidor não pode executar ping ou há uma incompatibilidade chave/cliente. O usuário vê o nome de usuário, a senha e as mensagens "`Timeout to RADIUS server`" e "`Error: Número máximo de tentativas excedido`" (um servidor falso foi trocado na configuração).

```
109001: Auth start for user '???' from 10.31.1.5/11077
    to 192.1.1.1/23
 109002: Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed
    (server 100.100.100.100 failed)
 109002: Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed
    (server 100.100.100.100 failed)
 109002: Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed
    (server 100.100.100.100 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11077
    to 192.1.1.1/23
```

Adicionar autorização

Se decidir adicionar autorização, você precisará de autorização para o mesmo intervalo de origem e destino (uma vez que a autorização não é válida 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
```

Observe que a autorização não é adicionada para "saída" porque o tráfego de saída é autenticado com RADIUS e a autorização RADIUS não é válida.

Exemplos de depuração de autenticação e de autorização do PIX

Depuração de PIX - Boa autenticação e autorização bem-sucedida - TACACS+

Este exemplo mostra uma depuração de PIX com boa autenticação e autorização bem-sucedida:

```
109011: Authen Session Start: user 'pixuser', Sid 8
 109007: Authorization permitted for user 'pixuser'
    from 192.1.1.1/13160 to 10.31.1.5/23
 109012: Authen Session End: user 'pixuser', Sid 8,
    elapsed 1 seconds
 302001: Built inbound TCP connection 8 for faddr 192.1.1.1/13160
    gaddr 192.1.1.30/23 laddr 10.31.1.5/23 (pixuser)
```

Depuração de PIX - Boa autenticação, falha na autorização - TACACS+

Este exemplo mostra uma depuração de PIX com boa autenticação, mas com falha de autorização. Aqui o usuário também vê a mensagem "`Erro: Autorização negada.`"

```
109001: Auth start for user '???' from 192.1.1.1/13162
    to 10.31.1.5/23
 109011: Authen Session Start: user 'userhttp', Sid 10
 109005: Authentication succeeded for user 'userhttp'
    from 10.31.1.5/23 to 192.1.1.1/13162
 109008: Authorization denied for user 'userhttp'
    from 10.31.1.5/23 to 192.1.1.1/13162
 109012: Authen Session End: user 'userhttp', Sid 10,
    elapsed 1 seconds
 302010: 0 in use, 2 most used
```

Adicionar relatório

TACACS+

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

A depuração é igual, esteja a contabilidade ativada ou desativada. No entanto, no momento do "Built", um registro de contabilidade "start" é enviado. No momento do "Teardown", um registro de contabilidade "stop" é enviado.

Os registros de contabilidade TACACS+ se parecem com esta saída (são do Cisco Secure NT, portanto, o formato delimitado por vírgulas):

```
04/26/2000,01:31:22,pixuser,Default Group,192.1.1.1,
  start,,,,,,,0x2a,,PIX,10.31.1.200,telnet,6,
  Login,1,,,1,,,,,,,,,,,local_ip=10.31.1.5 foreign_ip=192.1.1.1,
  ,, ,,,,,,,,,zekie,,,,,,,,^
04/26/2000,01:31:26,pixuser,Default Group,192.1.1.1,stop,4,
  ,36,82,,,0x2a,,PIX,10.31.1.200,telnet,6,
  Login,1,,,1,,,,,,,,,,,local_ip=10.31.1.5 foreign_ip=192.1.1. 1,
  ,,,,,,,,,,,zekie,,,,,,,,
```

RADIUS

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

A depuração é igual, esteja a contabilidade ativada ou desativada. No entanto, no momento do "Built", um registro de contabilidade "start" é enviado. No momento do "Teardown", um registro de contabilidade "stop" é enviado.

Os registros de contabilidade RADIUS se parecem com esta saída (eles são do Cisco Secure UNIX; alguns no Cisco Secure NT podem ser delimitados por vírgula):

```
radrecv: Request from host a1f01c8 code=4, id=18, length=65
Acct-Status-Type = Start
Client-Id = 10.31.1.200
Login-Host = 10.31.1.5
Login-TCP-Port = 23
Acct-Session-Id = "0x0000002f"
User-Name = "pixuser"
Sending Accounting Ack of id 18 to a1f01c8 (10.31.1.200)
radrecv: Request from host a1f01c8 code=4, id=19, length=83
Acct-Status-Type = Stop
Client-Id = 10.31.1.200
Login-Host = 10.31.1.5
Login-TCP-Port = 23
Acct-Session-Id = "0x0000002f"
Username = "pixuser"
Acct-Session-Time = 7
```

Uso do comando Except

Em nossa rede, se decidirmos que uma origem e/ou destino específicos não precisa de autenticação, autorização ou contabilidade, podemos fazer algo como esta saída:

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

Se estiver "excluindo" uma caixa da autenticação e tiver autorização ativada, você também deverá exceto a caixa de 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 "start" de contabilidade gerado, mas nenhum registro "stop", o servidor TACACS+ ou RADIUS supõe que a pessoa ainda está conectada (tem uma sessão através do 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. Neste exemplo de saída, uma configuração de rede diferente é usada, mas os conceitos são os mesmos.

O usuário faz Telnet através do PIX, autenticando no caminho:

```
(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
```

Como o servidor viu um registro de "início", mas nenhum registro de "parada" (neste momento), o servidor mostra que o usuário "Telnet" está conectado. Se o usuário tentar outra conexão que exija autenticação (talvez de outro PC) e se o número máximo de sessões estiver definido como "1" no servidor para esse usuário (supondo que o servidor suporte o número máximo de sessões), a conexão será recusada pelo servidor.

O usuário continua com o negócio Telnet ou FTP no host de destino e sai (passa 10 minutos lá):

```
(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
```

Se uauth é 0 (autenticar sempre) ou mais (autenticar uma vez e não novamente durante o período de uauth), um registro contábil é cortado para cada site acessado.

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

O usuário navega de 171.68.118.100 a 9.9.9.25 através do 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
```

O usuário lê a página da Web baixada.

O registro inicial foi publicado às 16:35:34, e o registro de parada foi publicado às 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 ainda está conectado ao site e a conexão ainda está aberta quando está lendo a página da Web? Não. O número máximo de sessões ou a visualização de usuários conectados funcionarão 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 "start" sem um registro "stop", uma vez que os registros ocorrem praticamente no mesmo momento. Ainda haverá um registro "start" e "stop" enviado ao servidor para cada transação, independentemente de uauth estar definido como 0 ou algo maior. No entanto, o número máximo de sessões e a visualização de usuários conectados não funcionam devido à natureza das conexões HTTP.

Autenticação e habilitação no próprio PIX

A discussão anterior descreveu a autenticação do tráfego Telnet (e HTTP, FTP) *através* do PIX. Asseguramos que o Telnet *para* o PIX funcione *sem* autenticação em:

```
telnet 10.31.1.5 255.255.255.255 passwd ww
```

```
aaa authentication telnet console AuthInbound
```

Quando os usuários fazem Telnet para o PIX, eles são solicitados a fornecer a senha do Telnet (**ww**). Em seguida, o PIX também solicita o TACACS+ (nesse caso, já que a lista de servidores "AuthInbound" é usada) ou o nome de usuário e a senha RADIUS. Se o servidor estiver inoperante, você pode entrar no PIX inserindo **pix** para o nome de usuário e, em seguida, a senha de ativação (**enable password *o que***) para obter acesso.

Com este comando:

```
aaa authentication enable console AuthInbound
```

o usuário é solicitado a fornecer um nome de usuário e uma senha, que são enviados ao TACACS (nesse caso, uma vez que a lista de servidores "AuthInbound" é usada, a solicitação vai para o servidor TACACS) ou para o servidor RADIUS. Como o pacote de autenticação para habilitação é o mesmo que o pacote de autenticação para login, se o usuário puder fazer login no PIX com TACACS ou RADIUS, ele poderá habilitar por meio de TACACS ou RADIUS com o mesmo nome de usuário/senha. Esse problema foi atribuído à ID de bug da Cisco CSCdm47044 (somente para clientes registrados) .

Autenticação no console serial

O comando **aaa authentication serial console AuthInbound** requer verificação de autenticação para acessar o console serial do PIX.

Quando o usuário executa comandos de configuração a partir do console, as mensagens de syslog são cortadas (supondo que o PIX esteja configurado para enviar syslog no nível de

depuração para um host syslog). Este é um exemplo do que é exibido no Servidor syslog:

```
logmsg: pri 245, flags 0, from [10.31.1.200.2.2], msg Nov 01 1999
 03:21:14: %PIX-5-111008: User 'pixuser' executed the 'logging' command.
```

Alterar o prompt que os usuários veem

Se você tiver o comando **auth-prompt PIX_PIX_PIX**, os usuários que passam pelo PIX verão esta sequência:

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

Na chegada à caixa de destino final, os avisos "Nome de usuário:" e "Senha:" são exibidos. Este prompt afeta somente os usuários que *passam pelo* PIX, não *pelo* PIX.

Observação: não há registros contábeis cortados para acesso ao PIX.

Personalize a mensagem que os usuários veem sobre sucesso/falha

Se você tiver os comandos:

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

os usuários veem esta sequência em um login com falha/êxito através do PIX:

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

Tempo ocioso e intervalos absolutos por usuário

Os tempos limite de uauth ocioso e absoluto podem ser enviados do servidor TACACS+ por usuário. Se todos os usuários da rede tiverem o mesmo "timeout uauth", não implemente isso! Mas, se você precisar de uauths diferentes por usuário, continue lendo.

Neste exemplo, o comando **timeout uauth 3:00:00** é usado. Quando uma pessoa se autentica, ela não precisa se autenticar novamente por três horas. No entanto, se você configurar um usuário com esse perfil e tiver *autorização* TACACS AAA no PIX, os tempos limite ociosos e absolutos no perfil do usuário substituirão o tempo limite no PIX desse usuário. Isso não significa que a sessão Telnet através do PIX é desconectada após o timeout de ociosidade/absoluto. Ele apenas controla se a reautenticação ocorre.

Este perfil vem do freeware TACACS+:

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

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
```

Após o usuário ficar ocioso por um minuto, a depuração no PIX mostra:

```
109012: Authen Session End: user 'timeout', Sid 19, elapsed 91 seconds
```

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

HTTP Virtual

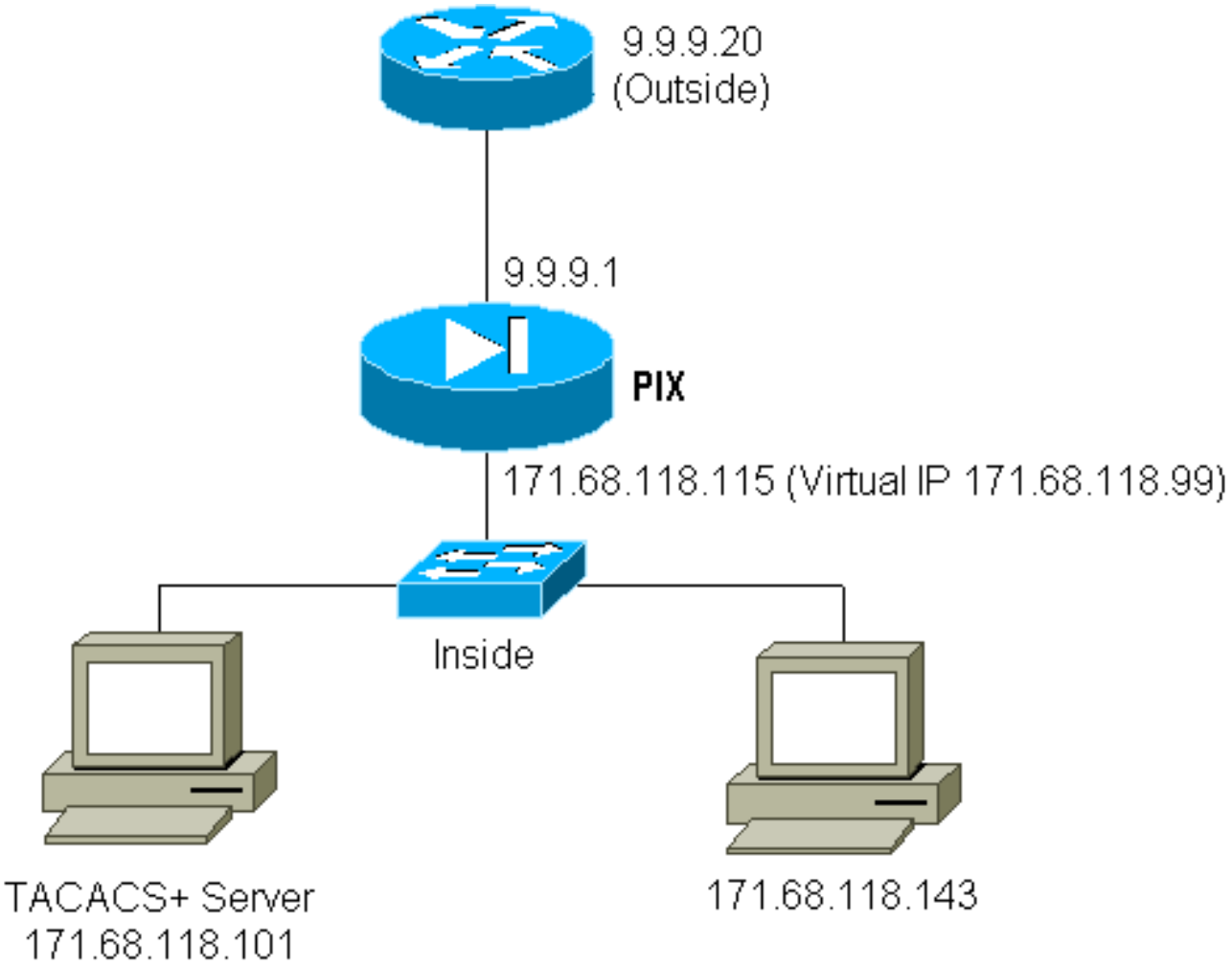
Se a autenticação for necessária em sites fora do PIX, assim como no próprio PIX, um comportamento incomum do navegador pode, às vezes, ser observado, já que os navegadores armazenam em cache o nome de usuário e a senha.

Para evitar isso, você pode implementar o HTTP virtual adicionando um endereço RFC 1918 (um endereço não roteável na Internet, mas válido e exclusivo para o PIX dentro da rede) à configuração do 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 defina a duração do comando **timeout uauth** como 0 segundo com HTTP virtual. isso evita conexões de HTTP ao servidor da Web real.

Diagrama de Saída HTTP Virtual



Saída HTTP Virtual de Configuração de PIX

```
ip address outside 9.9.9.1 255.255.255.0
 ip address inside 171.68.118.115 255.255.255.0
 global (outside) 1 9.9.9.5-9.9.9.9 netmask 255.0.0.0
 timeout uauth 01:00:00
 aaa-server TACACS+ protocol tacacs+
 aaa-server AuthOutbound protocol tacacs+
 aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 10
 aaa authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
 virtual http 171.68.118.99
 auth-prompt THIS_IS_PIX_5
```

Telnet Virtual

Épossível configurar o PIX para autenticar todo o tráfego de entrada e saída, mas não é uma boa ideia fazer isso. Isso ocorre porque alguns protocolos, como "correio", não são facilmente autenticados. Quando um servidor de e-mail e um cliente tentam se comunicar através do PIX quando todo o tráfego através do PIX está sendo autenticado, o syslog PIX para protocolos não autenticáveis mostra mensagens como:

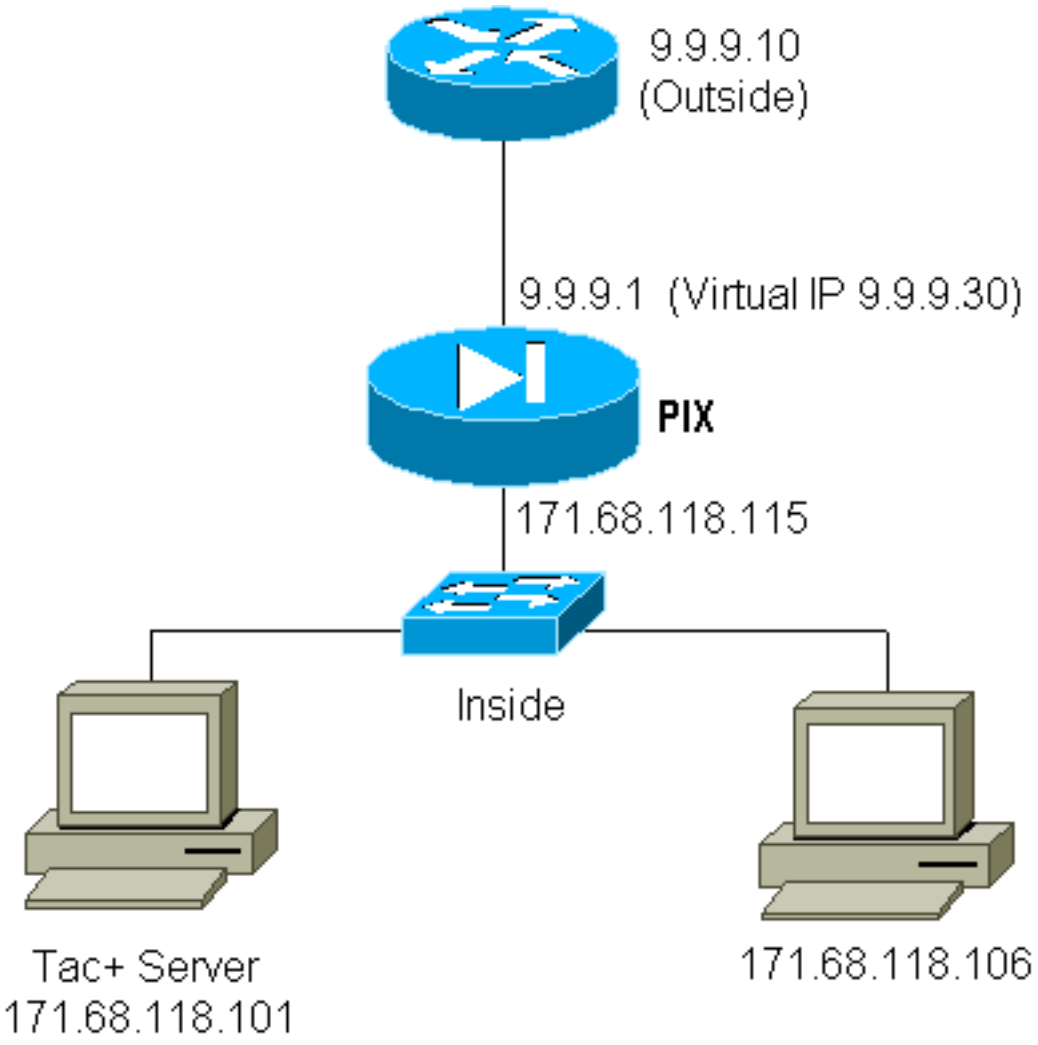
```
109001: Auth start for user '???' from 9.9.9.10/11094
    to 171.68.118.106/25
 109009: Authorization denied from 171.68.118.106/49 to
    9.9.9.10/11094 (not authenticated
```

Como o correio e alguns outros serviços não são interativos o suficiente para autenticação, uma solução é usar o **exceto** o comando para autenticação/autorização (autenticar tudo, exceto a origem/destino do servidor de correio/cliente).

Se houver uma necessidade real de autenticar algum tipo de serviço incomum, isso pode ser feito por meio do comando **virtual telnet**. Esse comando permite que ocorra autenticação no IP Telnet virtual. Depois dessa autenticação, o tráfego do serviço incomum pode ir para o servidor real.

Neste exemplo, queremos que o tráfego da porta TCP 49 flua do host externo 9.9.9.10 para o host interno 171.68.118.106. Como esse tráfego não é realmente autenticável, configuramos um Telnet virtual. Para Telnet virtual de entrada, deve haver um estático associado. Aqui, 9.9.9.20 e 171.68.118.20 são endereços virtuais.

Diagrama de Entrada Telnet Virtual



Entrada Telnet virtual de configuração de PIX

```
ip address outside 9.9.9.1 255.255.255.0
 ip address inside 171.68.118.115 255.255.255.0
 static (inside,outside) 9.9.9.20 171.68.118.20 netmask 255.255.255.255 0 0
 static (inside,outside) 9.9.9.30 171.68.118.106 netmask 255.255.255.255 0 0
 conduit permit tcp host 9.9.9.20 eq telnet any
 conduit permit tcp host 9.9.9.30 eq tacacs any
 aaa-server TACACS+ protocol tacacs+
```

```
aaa-server AuthInbound protocol tacacs+
aaa-server AuthInbound (inside) host 171.68.118.101 cisco timeout 5
AAA authentication any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
virtual telnet 9.9.9.20
```

Entrada Telnet virtual de configuração de usuário de servidor TACACS+

```
user = pinecone {
default service = permit
        login = cleartext "pinecone"
service = exec {
        timeout = 10
        idletime = 10
        }
}
```

Entrada Telnet virtual de depuração de PIX

O usuário em 9.9.9.10 deve primeiro autenticar por Telnet para o endereço 9.9.9.20 no PIX:

```
pixfirewall# 109001: Auth start for user '???' from 9.9.9.10/11099
    to 171.68.118.20/23
 109011: Authen Session Start: user 'pinecone', Sid 13
 109005: Authentication succeeded for user 'pinecone'
    from 171.68.118.20/23 to 9.9.9.10/1470
```

Após a autenticação bem-sucedida, o comando **show uauth** mostra que o usuário tem "time on the meter":

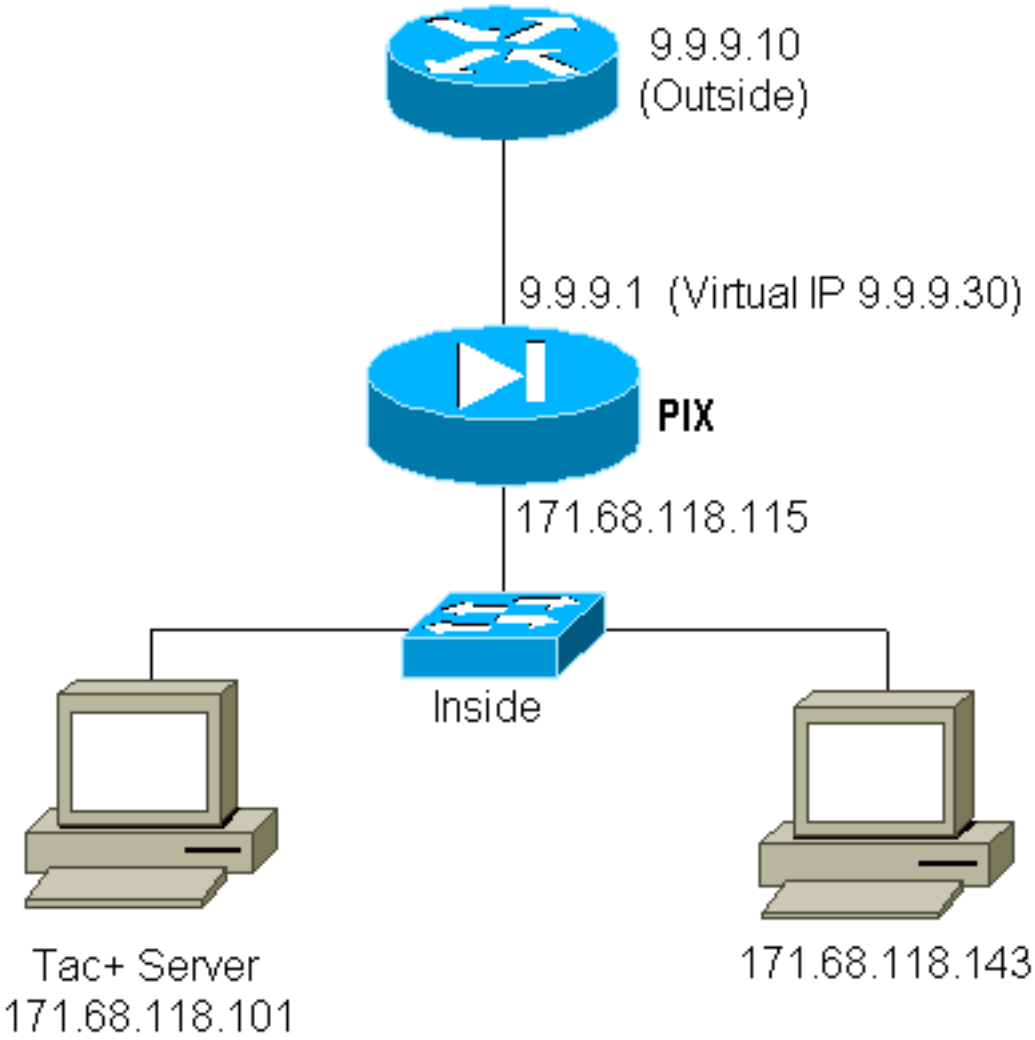
```
pixfirewall# show uauth
                         Current    Most Seen
 Authenticated Users       1          1
 Authen In Progress        0          1
 user 'pinecone' at 9.9.9.10, authenticated
    absolute   timeout: 0:10:00
    inactivity timeout: 0:10:00
```

Aqui, o dispositivo em 9.9.9.10 deseja enviar tráfego TCP/49 para o dispositivo em 171.68.118.106:

```
pixfirewall# 109001: Auth start for user 'pinecone' from 9.9.9.10/11104
     to 171.68.118.20/23
 109011: Authen Session Start: user 'pinecone', Sid 14
 109005: Authentication succeeded for user 'pinecone' from 171.68.118.20/23
     to 9.9.9.10/1470
 302001: Built TCP connection 23 for faddr 9.9.9.10/11104 gaddr 9.9.9.30/49
  laddr 171.68.118.106/49 (pinecone)
 302002: Teardown TCP connection 23 faddr 9.9.9.10/11104 gaddr 9.9.9.30/49
  laddr 171.68.118.106/49 duration 0:00:10 bytes 179 (pinecone)
```

Saída Telnet Virtual

Como o tráfego de saída é permitido por padrão, não é necessário estático para o uso de saída Telnet virtual. Neste exemplo, o usuário interno em 171.68.118.143 faz Telnet para virtual 9.9.9.30 e autentica. A conexão Telnet é imediatamente descartada. Depois de autenticado, o tráfego TCP é permitido de 171.68.118.143 para o servidor em 9.9.9.10:



Saída Telnet virtual de configuração de PIX

```
ip address outside 9.9.9.1 255.255.255.0
 ip address inside 171.68.118.115 255.255.255.0
 global (outside) 1 9.9.9.5-9.9.9.9 netmask 255.0.0.0
 timeout uauth 00:05:00
 aaa-server TACACS+ protocol tacacs+
 aaa-server AuthOutbound protocol tacacs+
 aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 10
 AAA authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
 virtual telnet 9.9.9.30
```

Saída Telnet virtual de depuração de PIX

```
109001: Auth start for user '???' from 171.68.118.143/1536
     to 9.9.9.30/23
 109011: Authen Session Start: user 'timeout_143', Sid 25
 109005: Authentication succeeded for user 'timeout_143' from
    171.68.118.143/1536 to 9. 9.9.30/23
 302001: Built TCP connection 46 for faddr 9.9.9.10/80 gaddr
    9.9.9.30/1537 laddr 171.68 .118.143/1537 (timeout_143)
 304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
 302001: Built TCP connection 47 for faddr 9.9.9.10/80 gaddr
    9.9.9.30/1538 laddr 171.68 .118.143/1538 (timeout_143)
 302002: Teardown TCP connection 46 faddr 9.9.9.10/80 gaddr
    9.9.9.30/1537 laddr 171.68. 118.143/1537 duration 0:00:03
```

```
    bytes 625 (timeout_143)
 304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
 302002: Teardown TCP connection 47 faddr 9.9.9.10/80 gaddr
    9.9.9.30/1538 laddr 171.68. 118.143/1538 duration 0:00:01
    bytes 2281 (timeout_143)
 302009: 0 in use, 1 most used
```

Desconexão de Telnet Virtual

Quando o usuário faz Telnet para o IP Telnet virtual, o comando **show uauth** mostra o uauth.

Se o usuário quiser impedir que o tráfego passe após a sessão ser concluída (quando houver tempo restante na uauth), o usuário precisará executar telnet para o IP Telnet virtual novamente. Esta ação desliga a sessão.

Autorização da porta

Você pode exigir autorização em um intervalo de portas. Neste exemplo, a autenticação ainda era necessária para toda a saída, mas somente a autorização era necessária para as 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 autenticação e a autorização ocorreram porque a porta 23 do Telnet está no intervalo de 23 a 49.

Quando uma sessão HTTP é realizada de 171.68.118.143 a 9.9.9.10, você ainda precisa se autenticar, mas o PIX não pede ao servidor TACACS+ para autorizar HTTP porque 80 não está no intervalo 23-49.

TACACS+ Configuração do programa gratuito de servidor

```
user = telnetrange {
        login = cleartext "telnetrange"
        cmd = tcp/23-49 {
        permit 9.9.9.10
        }
        }
```

Observe que o PIX envia "`cmd=tcp/23-49`" e "`cmd-arg=9.9.9.10`" para o servidor TACACS+.

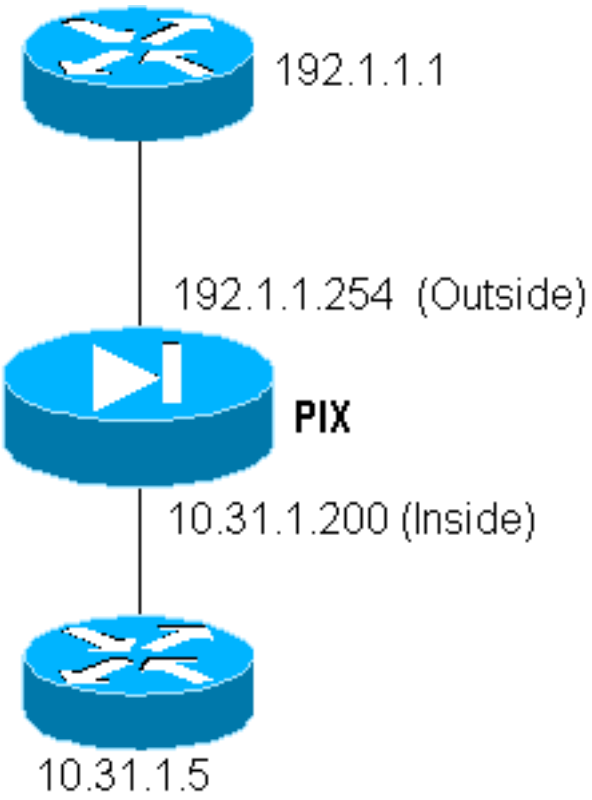
Depurar no PIX

```
109001: Auth start for user '???' from 171.68.118.143/1051
    to 9.9.9.10/23
 109011: Authen Session Start: user 'telnetrange', Sid 0
 109005: Authentication succeeded for user 'telnetrange'
```

```
   from 171.68.118.143/1051 to 9. 9.9.10/23
109011: Authen Session Start: user 'telnetrange', Sid 0
109007: Authorization permitted for user 'telnetrange'
   from 171.68.118.143/1051 to 9.9 .9.10/23
302001: Built TCP connection 0 for faddr 9.9.9.10/23
   gaddr 9.9.9.5/1051 laddr 171.68.1 18.143/1051 (telnetrange)
109001: Auth start for user '???' from 171.68.118.143/1105
   to 9.9.9.10/80
109001: Auth start for user '???' from 171.68.118.143/1110
   to 9.9.9.10/80
109011: Authen Session Start: user 'telnetrange', Sid 1
109005: Authentication succeeded for user 'telnetrange'
   from 171.68.118.143/1110 to 9. 9.9.10/80
302001: Built TCP connection 1 for faddr 9.9.9.10/80 gaddr 9.9.9.5/1110
 laddr 171.68.1 18.143/1110 (telnetrange)
302001: Built TCP connection 2 for faddr 9.9.9.10/80 gaddr 9.9.9.5/1111
 laddr 171.68.1 18.143/1111 (telnetrange)
302002: Teardown TCP connection 1 faddr 9.9.9.10/80 gaddr 9.9.9.5/1110
 laddr 171.68.11 8.143/1110 duration 0:00:08 bytes 338 (telnetrange)
304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
302002: Teardown TCP connection 2 faddr 9.9.9.10/80 gaddr 9.9.9.5/1111
 laddr 171.68.11 8.143/1111 duration 0:00:01 bytes 2329 (telnetrange)
```

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

A versão 5.0 do software PIX altera a funcionalidade de contabilização de tráfego. Os registros de contabilidade agora podem ser cortados para tráfego diferente de HTTP, FTP e Telnet, quando a autenticação for concluída.



Para copiar TFTP um arquivo do roteador externo (192.1.1.1) para o roteador interno (10.31.1.5), adicione Telnet virtual para abrir um buraco 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, faça Telnet do roteador externo em 192.1.1.1 para o IP virtual 192.1.1.30 e autentique para o endereço virtual que permite que o UDP passe pelo PIX. Neste exemplo, o processo **copy tftp flash** foi iniciado de fora para dentro:

```
302006: Teardown UDP connection for faddr 192.1.1.1/7680
    gaddr 192.1.1.30/69 laddr 10.31.1.5/69
```

Para cada **cópia tftp flash** no PIX (houve três durante esta cópia do IOS), um registro contábil é cortado e enviado ao servidor de autenticação. Veja a seguir um exemplo de um registro TACACS no Cisco Secure Windows):

```
Date,Time,Username,Group-Name,Caller-Id,Acct-Flags,elapsed_time,
    service,bytes_in,bytes_out,paks_in,paks_out,
    task_id,addr,NAS-Portname,NAS-IP-Address,cmd
 04/28/2000,03:08:26,pixuser,Default Group,192.1.1.1,start,,,,,,,
    0x3c,,PIX,10.31.1.200,udp/69
```

Informações Relacionadas

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