Exemplo de configurações de PIX, TACACS+ e RADIUS: 4.4.x

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 4.4.1 em relação à versão anterior incluem: Grupos de servidores AAA e failover, autenticação para acesso de console serial e de ativação e aceitação e rejeição de mensagens de prompt.

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.

Suponha que você tenha 100 usuários dentro e que você deseje que apenas 6 desses usuários possam fazer FTP, Telnet ou HTTP fora da rede. Você diria ao PIX para autenticar o tráfego de saída e fornecer todos os seis IDs de usuários no servidor de segurança TACACS+/RADIUS. Com uma autenticação simples, esses 6 usuários podem ser autenticados com nome de usuário e senha e depois saem. Os outros 94 usuários não puderam sair. O PIX solicita aos usuários nome de usuário/senha, depois passa seu nome de usuário e senha para o servidor de segurança TACACS+/RADIUS e, dependendo da resposta, abre ou nega a conexão. Esses 6 usuários podem fazer FTP, Telnet ou HTTP.

Mas suponha que um desses três usuários, "Terry", não seja de confiança. Você gostaria de permitir que Terry faça FTP, mas não HTTP ou Telnet para fora. Isso significa ter que adicionar autorização, ou seja, autorizar o que os usuários podem fazer além de autenticar quem eles são. Quando adicionamos autorização ao PIX, o PIX envia primeiro 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 "comando" que Terry está tentando fazer. Com o servidor configurado corretamente, Terry poderia ter permissão para "FTP 1.2.3.4", mas teria negado a capacidade para HTTP ou Telnet em qualquer lugar.

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

Quando tentar ir de dentro para fora (ou vice-versa) com a autenticação/autorização ligada:

- **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 é exibida no navegador solicitando o nome de usuário e a 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 nomes de usuário e senhas no cache. 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 parecerem funcionar “normalmente”, mas as conexões http não, esse será o motivo.

Configurações de servidor de segurança utilizadas para todos os cenários

Configuração do servidor CiscoSecure 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 CiscoSecure UNIX RADIUS

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

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

CiscoSecure NT 2.x RADIUS

Siga estas etapas.

1. Obtenha uma senha na seção 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 o comando **Add/Edit** new 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 e/ou FTP).
7. Adicione o PIX IP na seção NAS Configuration GUI (GUI de configuração de NAS).

CiscoSecure 2.x TACACS+

O usuário obtém uma senha na seção User setup da GUI.

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** para cada comando que deseja permitir (por exemplo, Telnet).
4. Se quiser permitir Telnet para sites específicos, insira o(s) IP(s) de permissão 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 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).

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
```

TACACS+ Configuração do programa gratuito de servidor

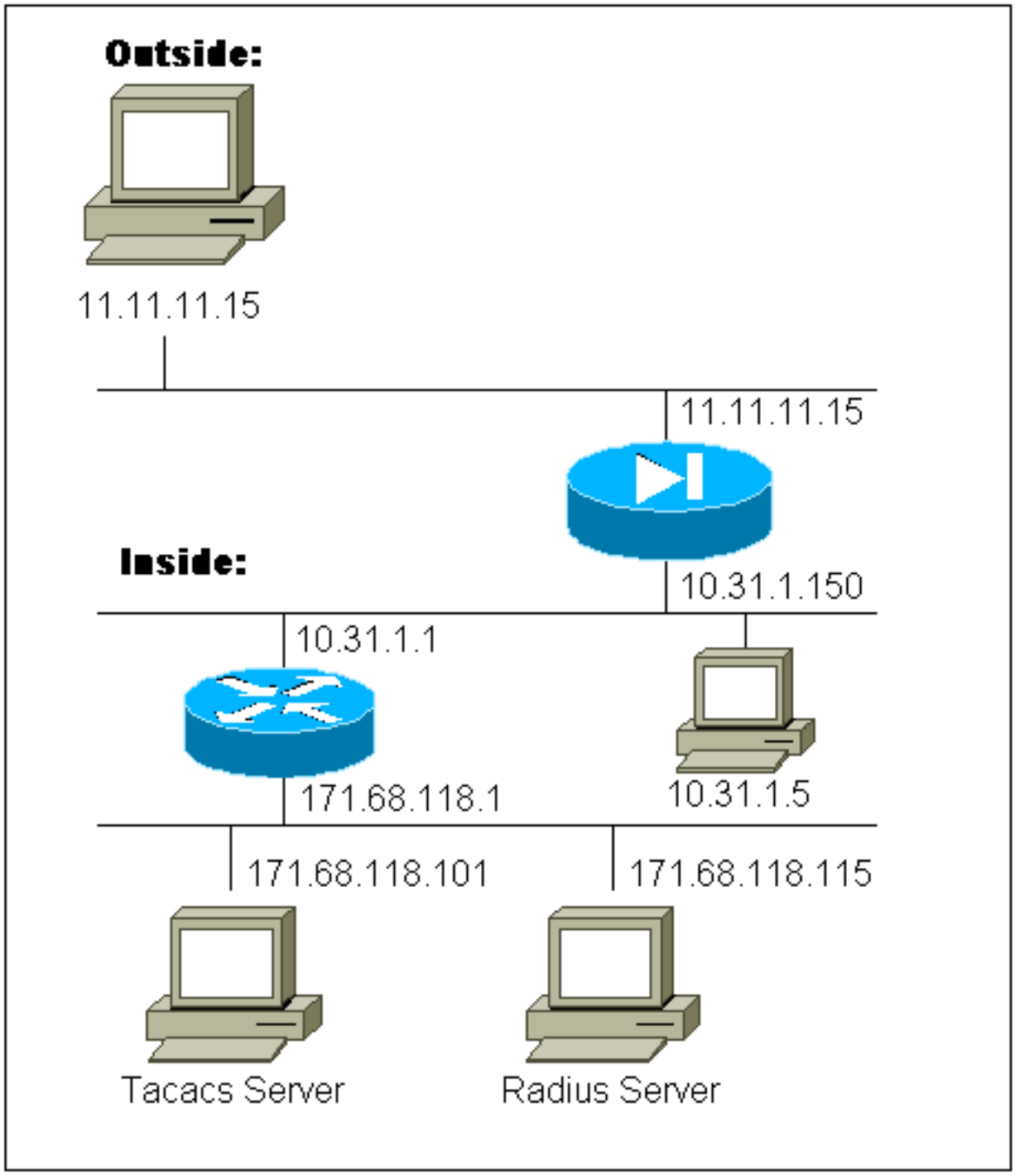
```
key = "cisco"

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 PIX estejam funcionando antes de adicionar autenticação, autorização e contabilização (AAA).Se você não passar o tráfego antes de instituir autenticação e autorização, não conseguirá fazê-lo depois disso.
- Habilite o login no PIX:O comando **logging console debugging** não deve ser usado em um sistema altamente carregado.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
 Building configuration...
 : Saved
 :
 PIX Version 4.4(1)
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 nameif ethernet2 pix/intf2 security10
 nameif ethernet3 pix/intf3 security15
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pix-5
 fixup protocol ftp 21
 fixup protocol http 80
 fixup protocol smtp 25
 fixup protocol h323 1720
```

```
 fixup protocol rsh 514
 fixup protocol sqlnet 1521
 names
 pager lines 24
 no logging timestamp
 logging console debugging
 no logging monitor
 no logging buffered
 logging trap debugging
 logging facility 20
 interface ethernet0 auto
 interface ethernet1 auto
 interface ethernet2 auto
 interface ethernet3 auto
 mtu outside 1500
 mtu inside 1500
 mtu pix/intf2 1500
 mtu pix/intf3 1500
 ip address outside 11.11.11.1 255.255.255.0
 ip address inside 10.31.1.150 255.255.255.0
 ip address pix/intf2 127.0.0.1 255.255.255.255
 ip address pix/intf3 127.0.0.1 255.255.255.255
 no failover
 failover timeout 0:00:00
 failover ip address outside 0.0.0.0
 failover ip address inside 0.0.0.0
 failover ip address pix/intf2 0.0.0.0
 failover ip address pix/intf3 0.0.0.0
 arp timeout 14400
 global (outside) 1 11.11.11.10-11.11.11.14 netmask
255.255.255.0
 static (inside,outside) 11.11.11.20 171.68.118.115
netmask 255.255.255.255 0 0
 static (inside,outside) 11.11.11.21 171.68.118.101
netmask 255.255.255.255 0 0
 static (inside,outside) 11.11.11.22 10.31.1.5 netmask
255.255.255.255 0 0
 conduit permit icmp any any
 conduit permit tcp any any
 no rip outside passive
 no rip outside default
 no rip inside passive
 no rip inside default
 no rip pix/intf2 passive
 no rip pix/intf2 default
 no rip pix/intf3 passive
 no rip pix/intf3 default
 route inside 0.0.0.0 0.0.0.0 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
!
!--- For any given list, multiple AAA servers can !---
be configured. They will be !--- tried sequentially if
any one of them is down. ! aaa-server Outgoing protocol
tacacs+ aaa-server Outgoing (inside) host 171.68.118.101
cisco timeout 10 aaa-server Incoming protocol radius
aaa-server Incoming (inside) host 171.68.118.115 cisco
timeout 10 aaa authentication ftp outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa authentication http
outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa
```

```
authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 Outgoing aaa authentication ftp inbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa authentication http
inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa
authentication telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 Incoming no snmp-server location no snmp-server
contact snmp-server community public no snmp-server
enable traps telnet timeout 5 terminal width 80
Cryptochecksum:b287a37a676262275a4201cac52399ca : end
```

Exemplos de debug de autenticação a partir de PIX

Nesses exemplos de depuração:

Saída

O usuário interno em 10.31.1.5 inicia o tráfego para fora de 11.11.11.15 e é autenticado por TACACS+ (o tráfego de saída usa a lista de servidores "Saída", que inclui o servidor TACACS 171.68.118.101).

Entrada

O usuário externo em 11.11.11.15 inicia o tráfego para o interior 10.31.1.5 (11.11.11.22) e é autenticado por RADIUS (o tráfego de entrada usa a lista de servidores "Entrada", que inclui o servidor RADIUS 171.68.115).

Depuração de PIX - Boa autenticação - TACACS+

O exemplo abaixo mostra a depuração de PIX com boa autenticação:

```
109001: Auth start for user '???' from 10.31.1.5/11004 to 11.11.11.15/23
 109011: Authen Session Start: user 'ddunlap', sid 3
 109005: Authentication succeeded for user 'ddunlap'
 from 10.31.1.5/11004 to 11.11.11.15/23
 109012: Authen Session End: user 'ddunlap', sid 3, elapsed 1 seconds
 302001: Built outbound TCP connection 4 for faddr 11.11.11.15/23 gaddr
11.11.11.22/11004 laddr 10.31.1.5/11004
```

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

O exemplo abaixo mostra a depuração de PIX com autenticação incorreta (nome de usuário ou senha). O usuário vê quatro conjuntos de nome de usuário/senha. A seguinte mensagem é exibida: “Erro: número máximo de tentativas excedido".

```
109001: Auth start for user '???' from 10.31.1.5/11005 to 11.11.11.15/23
 109006: Authentication failed for user '' from 10.31.1.5/11005 to 11.11.11.15/23
```

Depuração de PIX - Pode fazer ping, mas sem resposta - TACACS+

O exemplo abaixo mostra a depuração de PIX para um servidor que pode ser executado por ping que não está falando para o PIX. O usuário vê o nome de usuário uma vez, e o PIX nunca pede uma senha (isso está no Telnet).

```
'Error: Max number of tries exceeded'
 109001: Auth start for user '???' from 10.31.1.5/11006 to 11.11.11.15/23
 109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
 (server 171.68.118.101 failed)
 109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
 (server 171.68.118.101 failed)
 304006: URL Server 171.68.118.101 not responding, trying 171.68.118.101
 109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
 (server 171.68.118.101 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11006 to 11.11.11.15/23
```

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

O exemplo abaixo mostra a depuração de PIX para um servidor que não pode ser executado ping. O usuário vê o nome de usuário uma vez. O PIX nunca pede uma senha (isso é no Telnet). A seguinte mensagem é exibida: "Timeout to TACACS+ server" e "Error: Número máximo de tentativas excedido" (a configuração neste exemplo reflete um servidor falso).

```
109001: Auth start for user '???' from 10.31.1.5/11007 to 11.11.11.15/23
 109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
 (server 171.68.118.199 failed)
 109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
 (server 171.68.118.199 failed)
 304006: URL Server 171.68.118.199 not responding, trying 171.68.118.199
 109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
 (server 171.68.118.199 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11007 to 11.11.11.15/23
```

Depuração de PIX - Boa autenticação - RADIUS

O exemplo abaixo mostra a depuração de PIX com boa autenticação:

```
109001: Auth start for user '???' from 11.11.11.15/11003 to 10.31.1.5/23
 109011: Authen Session Start: user 'adminuser', sid 4
 109005: Authentication succeeded for user 'adminuser'
 from 10.31.1.5/23 to 11.11.11.15/11003
 109012: Authen Session End: user 'adminuser', sid 4, elapsed 1 seconds
 302001: Built inbound TCP connection 5 for faddr
 11.11.11.15/11003 gaddr 11.11.11.22/23 laddr 10.31.1.5/23
```

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

O exemplo abaixo mostra a depuração de PIX com autenticação incorreta (nome de usuário ou senha). O usuário vê uma solicitação de Nome de usuário e Senha. Se uma das opções estiver errada, a mensagem "Senha incorreta" será exibida quatro vezes. Em seguida, o usuário é desconectado. Esse problema foi atribuído à ID de bug #CSCdm46934.

```
'Error: Max number of tries exceeded'
 109001: Auth start for user '???' from 11.11.11.15/11007 to 10.31.1.5/23
 109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11007
```

Depuração de PIX - Deamon Down, não se comunicará com PIX - RADIUS

O exemplo abaixo mostra a depuração de PIX com um servidor que pode ser executado por ping, mas o daemon está inoperante. O servidor não se comunicará com o PIX. O usuário vê o nome

de usuário, seguido por senha. As seguintes mensagens são exibidas: "RADIUS server failed" e "Error: Número máximo de tentativas excedido".

```
109001: Auth start for user '???' from 11.11.11.15/11008 to 10.31.1.5/23
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
 (server 171.68.118.115 failed)
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
 (server 171.68.118.115 failed)
 304006: URL Server 171.68.118.115 not responding, trying 171.68.118.115
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
 (server 171.68.118.115 failed)
 109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11008
```

Depuração de PIX - Não é possível efetuar ping no servidor ou na incompatibilidade de chave/cliente - RADIUS

O exemplo abaixo mostra a depuração de PIX para um servidor que não pode ser executado ping ou onde há uma incompatibilidade de chave/cliente. O usuário vê Nome de usuário e Senha. As seguintes mensagens são exibidas: "Timeout to RADIUS server" (Tempo limite para servidor RADIUS) e "Error: Número máximo de tentativas excedido" (o servidor na configuração é apenas para fins de exemplo).

```
109001: Auth start for user '???' from 11.11.11.15/11009 to 10.31.1.5/23
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
 (server 171.68.118.199 failed)
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
 (server 171.68.118.199 failed)
 304006: URL Server 171.68.118.199 not responding, trying 171.68.118.199
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
 (server 171.68.118.199 failed)
 109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11009
```

Autorização de adição

Como a autorização não é válida sem autenticação, exigiremos autorização para o mesmo intervalo de origem e destino:

```
aaa authorization ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
aaa authorization http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
aaa authorization telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

Saída

Observe que não adicionamos autorização para "entrada" porque o tráfego de entrada é autenticado com RADIUS e a autorização RADIUS não é válida

Exemplos de depuração de autenticação e de autorização do PIX

Depuração de PIX com boa autenticação e autorização bem-sucedida - TACACS+

O exemplo abaixo mostra a depuração de PIX com boa autenticação e autorização bem-sucedida:

```
109001: Auth start for user '???' from 10.31.1.5/11002 to 11.11.11.15/23
 109011: Authen Session Start: user 'can_only_do_telnet', sid 7
 109005: Authentication succeeded for user 'can_only_do_telnet'
 from 10.31.1.5/11002 to 11.11.11.15/23
 109011: Authen Session Start: user 'can_only_do_telnet', sid 7
 109007: Authorization permitted for user 'can_only_do_telnet'
 from 10.31.1.5/11002 to 11.11.11.15/23
 109012: Authen Session End: user 'can_only_do_telnet', sid 7,
 elapsed 1 seconds
 302001: Built outbound TCP connection 6 for faddr 11.11.11.15/23
 gaddr 11.11.11.22/11002 laddr 10.31.1.5/11002 (can_only_do_telnet)
```

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

O exemplo abaixo mostra a depuração de PIX com boa autenticação, mas falha na autorização:

Aqui o usuário também vê a mensagem "Erro: Autorização negada"

```
109001: Auth start for user '???' from 10.31.1.5/11000 to 11.11.11.15/23
 109011: Authen Session Start: user 'can_only_do_ftp', sid 5
 109005: Authentication succeeded for user 'can_only_do_ftp'
 from 10.31.1.5/11000 to 11.11.11.15/23
 109008: Authorization denied for user 'can_only_do_ftp' from
 10.31.1.5/11000 to 11.11.11.15/23
 109012: Authen Session End: user 'can_only_do_ftp', sid 5, elapsed 33 seconds
```

Relatório de adição

TACACS+

aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing

A depuração será igual se a contabilidade estiver ativada ou desativada. No entanto, no momento do "Built", será enviado um registro contábil de "início". No momento do "Teardown", será enviado um registro de contabilidade "stop".

Os registros de contabilidade TACACS+ são parecidos com os seguintes (são do CiscoSecure UNIX; os do CiscoSecure NT podem ser delimitados por vírgula):

```
Thu Jun  3 10:41:50 1999 10.31.1.150 can_only_do_telnet
 PIX 10.31.1.5 start task_id=0x7 foreign_ip=11.11.11.15
local_ip=10.31.1.5  cmd=telnet
Thu Jun  3 10:41:55 1999 10.31.1.150 can_only_do_telnet PIX 10.31.1.5
 stop task_id=0x7 foreign_ip=11.11.11.15
local_ip=10.31.1.5 cmd=telnet elapsed_time=4 bytes_in=74 bytes_out=27
```

RADIUS

```
aaa accounting any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming
```

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

Os registros de contabilidade RADIUS têm a seguinte aparência: (são do CiscoSecure UNIX; os do CiscoSecure NT podem ser delimitados por vírgula):

```
10.31.1.150adminuser -- start server=rtp-evergreen.rtp.cisco.com
time=14:53:11 date=06/3/1999 task_id=0x00000008
 Thu Jun  3 15:53:11 1999
         Acct-Status-Type = Start
         Client-Id = 10.31.1.150
         Login-Host = 10.31.1.5
         Login-TCP-Port = 23
         Acct-Session-Id = "0x00000008"
         User-Name = "adminuser"
 10.31.1.150 adminuser -- stop server=rtp-evergreen.rtp.cisco.com
time=14:54:24 date=06/ 3/1999 task_id=0x00000008
 Thu Jun  3 15:54:24 1999
         Acct-Status-Type = Stop
         Client-Id = 10.31.1.150
         Login-Host = 10.31.1.5
         Login-TCP-Port = 23
         Acct-Session-Id = "0x00000008"
         User-Name = "adminuser"
         Acct-Session-Time = 73
         Acct-Input-Octets = 27
         Acct-Output-Octets = 73
```

Uso do comando Except

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

```
aaa authentication except outbound 10.31.1.60 255.255.255.255
11.11.11.15 255.255.255.255 Outgoing
aaa authorization except outbound 10.31.1.60 255.255.255.255
11.11.11.15 255.255.255.255 Outgoing
```

Se você estiver "excluindo" endereços ip da autenticação e tiver autorização ativada, você também deverá excluí-los 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 "start" de contabilidade gerado, mas nenhum registro "stop", o servidor TACACS+ ou RADIUS supõe que a pessoa ainda está conectada (ou seja, 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. No exemplo a seguir, 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 sem um registro de "parada" (neste momento), o servidor mostrará 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 seu negócio de 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.

Entretanto, o HTTP funciona de forma diferente devido à natureza do protocolo. Abaixo está 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. Este download levou um segundo (ou seja, houve menos de um segundo entre o registro de início e de parada). 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. Entretanto, os usuários que efetuaram logon em visualização e máximo de sessões não funcionarão devido à natureza das conexões de HTTP.

Autenticação e habilitação no próprio PIX

A discussão anterior era de autenticar tráfego Telnet (e HTTP, FTP) através do PIX. No exemplo abaixo, garantimos que o Telnet para o pix funcione sem autenticação em:

```
telnet 10.31.1.5 255.255.255.255
passwd ww
```

Em seguida, adicionamos o comando para autenticar usuários de Telnet ao PIX:

```
aaa authentication telnet console Outgoing
```

Quando os usuários fazem Telnet para o PIX, é-lhes solicitada a senha do Telnet ("ww"). O PIX também solicita o TACACS+ nesse caso (já que a lista de servidores "Saída" é usada) ou nome de usuário e senha RADIUS.

```
aaa authentication enable console Outgoing
```

Com esse comando, o usuário é solicitado a fornecer um nome de usuário e uma senha que são enviados ao servidor TACACS ou RADIUS. Nesse caso, como a lista de servidores "Saída" é usada, a solicitação vai para o servidor TACACS. Como o pacote de autenticação para habilitação é o mesmo que o pacote de autenticação para login, o usuário pode habilitar através de TACACS ou RADIUS com o mesmo nome de usuário/senha, supondo que o usuário possa fazer login no PIX com TACACS ou RADIUS. Esse problema foi atribuído à ID de bug #CSCdm47044.

Caso o servidor esteja inoperante, o usuário pode obter acesso ao modo de habilitação de PIX inserindo "PIX" para o nome de usuário e a senha de habilitação normal do PIX ("enable password any"). Se "enable password what" não estiver na configuração do PIX, o usuário deve digitar "PIX" como nome de usuário e pressionar a tecla Enter. Se a senha de ativação estiver definida, mas não for conhecida, será necessário um disco de recuperação de senha para redefini-la.

Autenticação no console serial

O comando **aaa authentication serial console** 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 serão cortadas (se o PIX estiver configurado para enviar syslog no nível de depuração para um host syslog). Abaixo está um exemplo do Servidor syslog:

```
Jun  5 07:24:09 [10.31.1.150.2.2] %PIX-5-111008: User 'cse' executed
the 'hostname' command.
```

Alterando o prompt que os usuários visualizam

Se tivermos o comando:

```
auth-prompt THIS_IS_PIX_5
```

os usuários que estão passando pelo PIX veem a sequência:

```
THIS_IS_PIX_5 [at which point one would enter the username]
 Password:[at which point one would enter the password]
```

e então, na chegada à caixa de destino final, o prompt "Nome de usuário:" e "Senha:" exibirá a caixa de destino.

Esse prompt afeta somente os usuários que passam pelo PIX, não pelo PIX.

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

Personalizando a mensagem que os usuários visualizam no êxito/na falha

Se tivermos os comandos:

```
auth-prompt accept "You're allowed through the pix"
auth-prompt reject "You blew it"
```

Os usuários verão o seguinte em um login com falha/êxito através do PIX:

```
THIS_IS_PIX_5
 Username: asjdkl
 Password:
 "You blew it"
 "THIS_IS_PIX_5"
 Username: cse
 Password:
 "You're allowed through the pix"
```

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 sua rede tiverem o mesmo "timeout uauth", não implemente isso! Mas, se precisar de diferentes uaus por usuário, leia.

Em nosso exemplo no PIX, usamos o comando **timeout uauth 3:00:00**. Isso significa que, uma vez que uma pessoa se autentica, ela não precisará se reautenticar por 3 horas. Mas se configurarmos um usuário com o seguinte perfil e tivermos autorização AAA TACACS ativada no PIX, os tempos limite ociosos e absolutos no perfil do usuário substituem o tempo limite no PIX desse usuário. Isso não significa que a sessão Telnet através do PIX seja desconectada após o timeout de ociosidade/absoluto. Ele apenas controla se a reautenticação ocorre ou não.

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

Após a autenticação, emita 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 terá que autenticar novamente ao retornar 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.

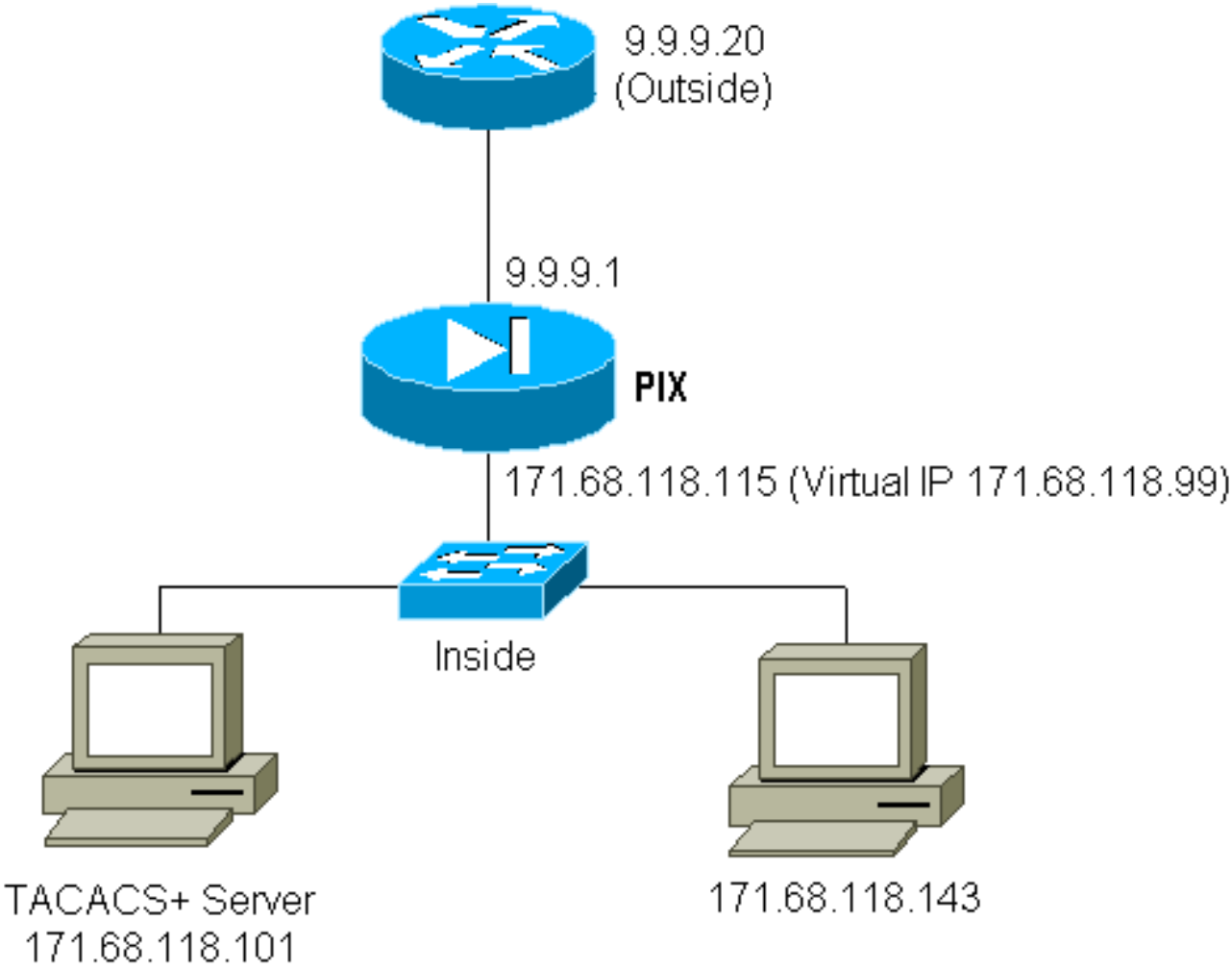
Para evitar isso, você pode implementar o HTTP virtual adicionando um endereço RFC 1918 (ou seja, um endereço que não pode ser roteado na Internet, mas é válido e exclusivo para o PIX dentro da rede) à configuração do PIX usando o seguinte comando:

```
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 segundos com HTTP virtual; isso evita conexões de HTTP ao servidor da

Web real.

Exemplo 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 Outgoing protocol tacacs+
 aaa-server Outgoing (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 Outgoing
 virtual http 171.68.118.99
 auth-prompt THIS_IS_PIX_5
```

Telnet Virtual

Configurar o PIX para autenticar todo o tráfego de entrada e saída não é uma boa ideia 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 do PIX para protocolos não autenticáveis mostrará mensagens como:

```
109001: Auth start for user '???' from 9.9.9.10/11094 to 171.68.118.106/25
```

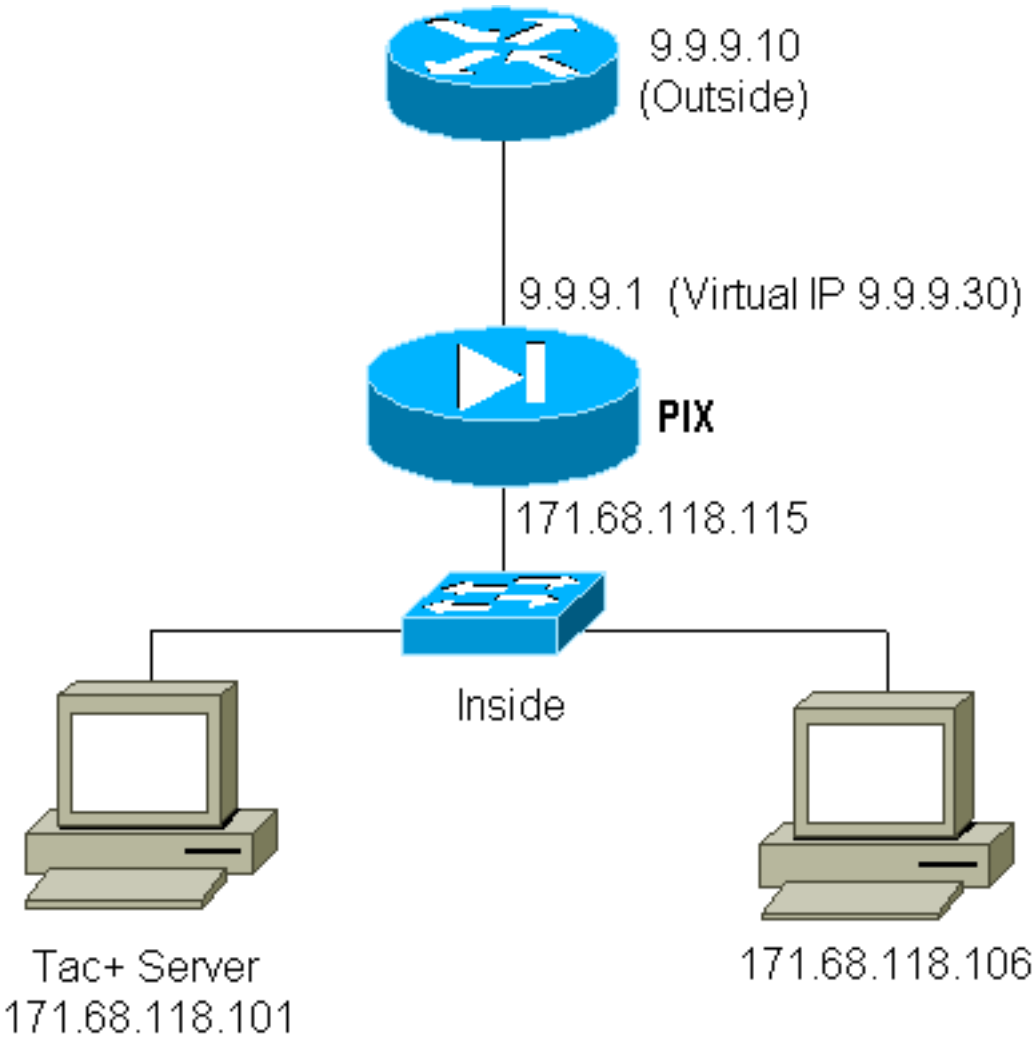
```
109009: Authorization denied from 171.68.118.106/49 to 9.9.9.10/11094
(not authenticated
```

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).

Mas se realmente há necessidade 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 que está vinculado ao IP virtual.

Em nosso exemplo, queremos permitir 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 o Telnet virtual.

Entrada de Telnet Virtual:



Entrada Telnet virtual de configuração 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) 9.9.9.30 171.68.118.106 netmask 255.255.255.255 0 0
 conduit permit tcp host 9.9.9.30 host 9.9.9.10
 aaa-server TACACS+ protocol tacacs+
 aaa-server Incoming protocol tacacs+
```

```
 aaa-server Incoming (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 Incoming
 virtual telnet 9.9.9.30
```

Entrada Telnet virtual de configuração de usuário do 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, fazendo telnet para o endereço 9.9.9.30 no PIX:

```
pixfirewall# 109001: Auth start for user '???' from 9.9.9.10/11099
 to 171.68.118.106/23
 109011: Authen Session Start: user 'pinecone', sid 13
 109005: Authentication succeeded for user 'pinecone' from
 171.68.118.106/23 to 9.9.9.10/11099
```

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
```

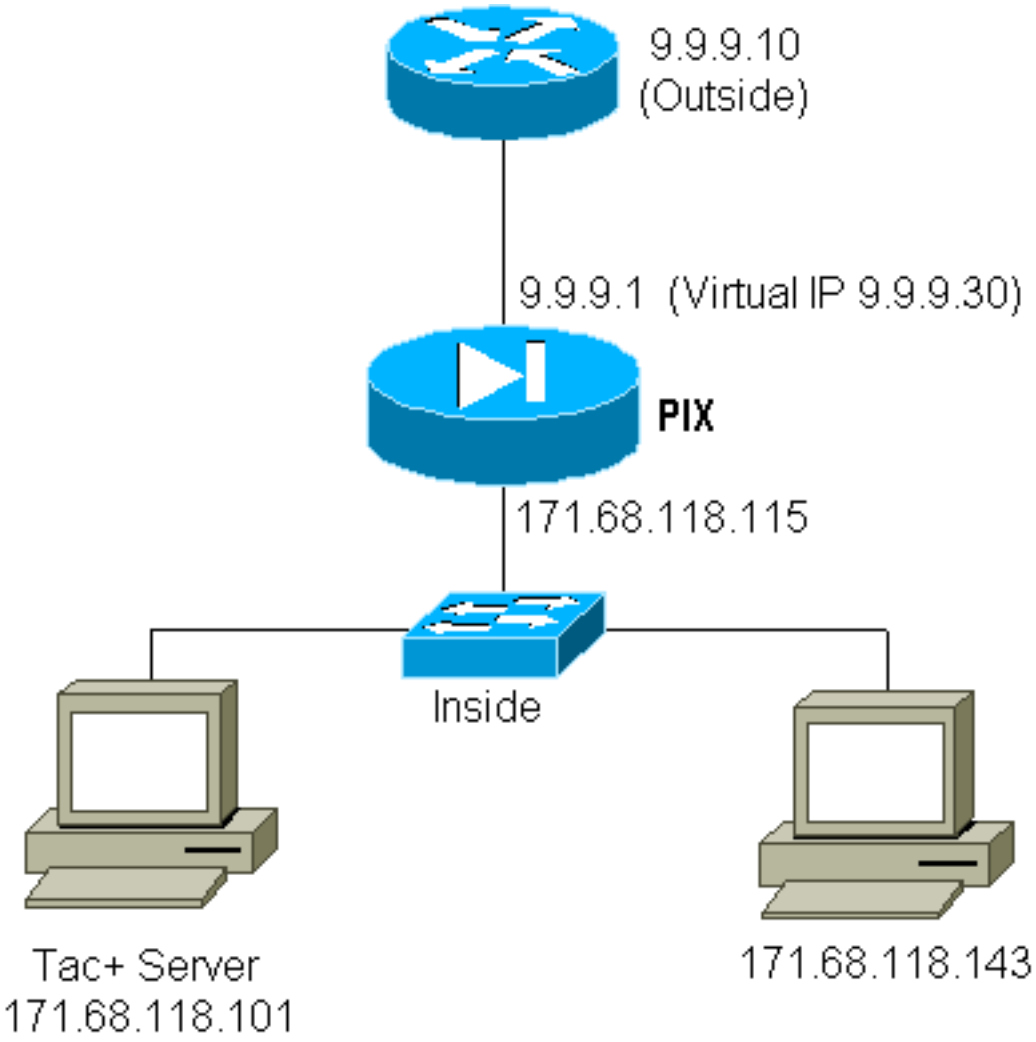
E quando o dispositivo em 9.9.9.10 deseja enviar tráfego TCP/49 para o dispositivo em 171.68.118.106:

```
pixfirewall# 109001: Auth start for user 'pinecone'
 from 9.9.9.10/11104 to 171.68.118.106/49
 109011: Authen Session Start: user 'pinecone', sid 14
 109007: Authorization permitted for user 'pinecone' from 9.9.9.10/11104
 to 171.68.118.106/49
 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. No exemplo a seguir, o usuário interno em 171.68.118.143 fará Telnet para virtual 9.9.9.30 e autenticará. 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 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 Outgoing protocol tacacs+
 aaa-server Outgoing (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 Outgoing
 virtual telnet 9.9.9.30
```

Saída de 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 seu uauth. Se o usuário quiser impedir que o tráfego passe após a conclusão da sessão (quando sobrar tempo no uauth), ele 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. No exemplo a seguir, a autenticação ainda era necessária para toda a saída, mas a autorização é necessária somente 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 Outgoing
aaa authorization tcp/23-49 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
```

Então, quando usamos o Telnet de 171.68.118.143 para 9.9.9.10, a autenticação e a autorização ocorreram porque a porta 23 do Telnet está no intervalo de 23 a 49. Quando fazemos uma sessão HTTP de 171.68.118.143 a 9.9.9.10, ainda temos que 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 está enviando "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)
```

Informações Relacionadas

- Suporte ao produto do software Cisco PIX Firewall
- Referências do comando Cisco Secure PIX Firewall