Realizando autenticação, autorização e relatório de usuários por meio do PIX versões 5.2 e posteriores

Contents

Introduction

A autenticação RADIUS e TACACS+ pode ser feita para conexões FTP, Telnet e HTTP através do Cisco Secure PIX Firewall. A autenticação para outros protocolos menos comuns geralmente é feita para funcionar. A autorização TACACS+ é suportada. A autorização RADIUS não é suportada. As alterações na autenticação, autorização e contabilização (AAA) do PIX 5.2 sobre a versão anterior incluem o suporte à lista de acesso AAA para controlar quem é autenticado e quais recursos o usuário acessa. No PIX 5.3 e posterior, a alteração de autenticação, autorização e contabilização (AAA) em relação às versões anteriores do código é que as portas RADIUS são configuráveis.

Observação: o PIX 6.x pode contabilizar o tráfego de passagem, mas não o tráfego destinado ao PIX.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Software de firewall Cisco Secure PIX versões 5.2.0.205 e 5.2.0.207

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Observação: se você executar o software PIX/ASA versão 7.x ou posterior, consulte Configuração de Servidores AAA e Banco de Dados Local.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Autenticação, autorização e contabilidade

Aqui está uma explicação de Autenticação, Autorização e Contabilidade:

- A autenticação é quem é o usuário.
- Autorização é o que o usuário faz.
- A autenticação é válida sem autorização.
- A autorização não é válida sem autenticação.
- Contabilidade é o que o usuário fez.

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

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

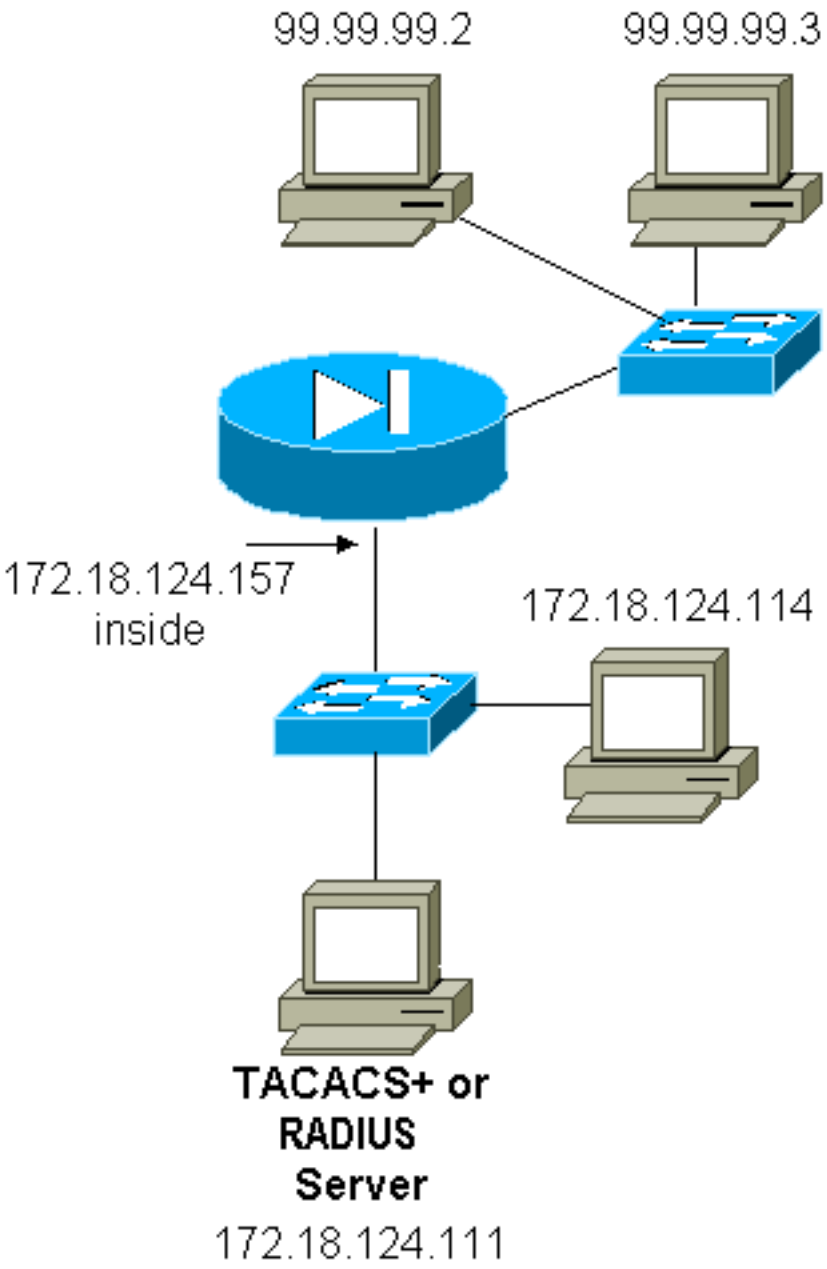
- **Telnet** —O usuário vê um prompt de nome de usuário surgindo e, em seguida, uma solicitação de senha. Se a autenticação (e autorização) for bem-sucedida no PIX/servidor, o usuário está pronto para obter nome de usuário e senha pelo host de destino.
- **FTP** — O usuário vê um prompt de nome de usuário sendo exibido. 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. Se a autenticação (e autorização) for bem-sucedida no PIX/servidor, "remote_username" e "remote_password" serão passados para o servidor FTP de destino além.
- **HTTP** — Uma janela é exibida no navegador solicitando 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 nomes de usuário e senhas no cache. Se parecer que o PIX deve expirar uma conexão HTTP, mas não o faz, é provável que a reautenticação ocorra com o navegador "fotografando" o nome de usuário e a senha em cache para o PIX. O PIX encaminha isso ao servidor de autenticação. O syslog PIX e/ou a depuração do servidor mostra esse fenômeno. Se o Telnet e o FTP parecem funcionar "normalmente", mas as conexões HTTP não, esse é o motivo.

Etapas de depuração

- Certifique-se de que a configuração do PIX funcione antes de adicionar autenticação e autorização de AAA. Se você não puder passar o tráfego antes de instituir a autenticação e a autorização, não poderá fazê-lo posteriormente.
- Habilite algum tipo de registro no PIX.Emita o comando **logging console debug** para ativar a depuração do console de registro.**Observação:** não use o logging console debugging em um sistema altamente carregado.Utilize o comando logging monitor debug para registrar uma sessão de Telnet.A depuração de registro colocado em buffer pode ser usada; em seguida, execute o comando show logging.O registro também pode ser enviado a um servidor syslog e examinado lá.
- Ativar depuração no TACACS+ ou nos servidores RADIUS.

Somente autenticação

Diagrama de Rede



Configuração do servidor – apenas autenticação

Configuração do servidor Cisco Secure UNIX TACACS

```
User = cse {
password = clear "cse"
default service = permit
}
```

Configuração do servidor Cisco Secure UNIX RADIUS

Observação: adicione o endereço IP PIX e a chave à lista Network Access Server (NAS) com a ajuda da GUI avançada.

```
user=bill {
radius=Cisco {
check_items= {
2="foo"
}
reply_attributes= {
6=6
}
}
}
```

Cisco Secure Windows RADIUS

Siga estas etapas para configurar um servidor Cisco Secure Windows RADIUS.

1. Obtenha uma senha na seção **User Setup**.
2. Na seção Configuração de Grupo, defina o atributo 6 (Tipo de Serviço) como Login ou Administrador.
3. Adicione o endereço IP de PIX na seção Configuração de NAS da GUI.

Cisco Secure Windows TACACS+

O usuário obtém uma senha na seção Configuração de Usuário.

Configuração de servidor Livingston RADIUS

Observação: adicione o endereço IP e a chave do PIX ao arquivo *dos clientes*.

- bill Password="foo" User-Service-Type = Shell-User

Configuração de servidor Merit RADIUS

Observação: adicione o endereço IP e a chave do PIX ao arquivo *dos clientes*.

- bill Password="foo" Service-Type = Shell-User

TACACS+ Configuração do programa gratuito de servidor

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

Configuração inicial do PIX – Somente autenticação

Configuração inicial do PIX – Somente autenticação
PIX Version 5.2(0)205 nameif ethernet0 outside security0 nameif ethernet1 inside security100 enable password 8Ry2YjIyt7RRXU24 encrypted passwd OnTrBUG1Tp0edmkr encrypted

```
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
!
!--- These lines are necessary !--- if the new feature
in 5.2 is used to define which !--- target/source IP
addresses are to be authenticated. access-list 101
permit tcp any any eq telnet
access-list 101 permit tcp any any eq ftp
access-list 101 permit tcp any any eq www
!
pager lines 24
logging on
no logging timestamp
no logging standby
logging console debugging
no logging monitor
no logging buffered
logging trap debugging
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 10baset
mtu outside 1500
mtu inside 1500
ip address outside 99.99.99.1 255.255.255.0
ip address inside 172.18.124.157 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
global (outside) 1 99.99.99.10-99.99.99.20 netmask
255.255.255.0
nat (inside) 1 172.18.124.0 255.255.255.0 0 0
static (inside,outside) 99.99.99.99 172.18.124.114
netmask 255.255.255.255 0 0
conduit permit tcp any any
conduit permit udp any any
conduit permit icmp any any
route inside 172.18.0.0 255.255.0.0 172.18.124.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h323 0:05:00
si p 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
!
!--- For the purposes of illustration, the TACACS+
process is used !--- to authenticate inbound users and
RADIUS is used to authenticate outbound users. aaa-
server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server AuthInbound protocol tacacs+
aaa-server AuthInbound (inside) host 172.18.124.111
```

```
cisco timeout 5
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 172.18.124.111
cisco timeout 5
!
!--- The next six statements are used to authenticate
all inbound !--- and outbound FTP, Telnet, and HTTP
traffic. aaa authentication include ftp outside 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authentication include telnet outside 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authentication include http outside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0
   AuthInbound
aaa authentication include http inside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0
   AuthOutbound
aaa authentication include telnet inside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0
   AuthOutbound
aaa authentication include ftp inside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0
   AuthOutbound
!
!--- OR the new 5.2 feature allows these two statements
in !--- conjunction with access-list 101 to replace the
previous six statements. !--- Note: Do not mix the old
and new verbiage.

aaa authentication match 101 outside AuthInbound
aaa authentication match 101 inside AuthOutbound
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
no sysopt route dnat
isakmp identity hostname
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:5882f514247589d784a0d74c800907b8
: end
```

Portas RADIUS configuráveis (5.3 e posterior)

Alguns servidores RADIUS utilizam portas RADIUS diferentes de 1645/1646 (geralmente 1812/1813). No PIX 5.3 e posterior, as portas de autenticação e tarifação RADIUS podem ser alteradas para algo diferente do padrão 1645/1646 com estes comandos:

```
aaa-server radius-authport #
aaa-server radius-acctport #
```

Exemplos de depuração de autenticação de PIX

Consulte Etapas de depuração para obter informações sobre como ativar a depuração. Estes são

exemplos de um usuário em 99.99.99.2 que inicia o tráfego para o interior 172.18.124.114 (99.99.99.99) e vice-versa. O tráfego de entrada é autenticado por TACACS e a saída é autenticada por RADIUS.

Autenticação bem-sucedida - TACACS+ (entrada)

```
109001: Auth start for user '???' from 99.99.99.2/11003 to 172.18.124.114/23
109011: Authen Session Start: user 'cse', sid 2
109005: Authentication succeeded for user 'cse' from 172.18.124.114/23
  to 99.99. 99.2/11003 on interface outside
302001: Built inbound TCP connection 4 for faddr 99.99.99.2/11003
  gaddr 99.99.99 .99/23 laddr 172.18.124.114/23 (cse)
```

Autenticação malsucedida devido a nome de usuário/senha incorretos - TACACS+ (entrada). O usuário vê "Erro: Número máximo de tentativas excedido."

```
109001: Auth start for user '???' from 99.99.99.2/11004 to 172.18.1 24.114/23
109006: Authentication failed for user '' from 172.18.124.114/23
  to 99.99.99.2/1 1004 on interface outside
```

O servidor não fala com PIX - TACACS+ (entrada). O usuário visualiza o nome de usuário uma vez e o PIX nunca solicita uma senha (isto ocorre no Telnet). O usuário vê "Erro: Número máximo de tentativas excedido."

```
109001: Auth start for user '???' from 99.99.99.2/11005 to 172.18.124.114/23
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
  (server 172.18.12 4.111 failed) on interface outside
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
  (server 172.18.12 4.111 failed) on interface outside
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
  (server 172.18.12 4.111 failed) on interface outside
109006: Authentication failed for user '' from 172.18.124.114/23
  to 99.99.99.2/1 1005 on interface outside
```

Good authentication - RADIUS (outbound)

```
109001: Auth start for user '???' from 172.18.124.114/35931 to 99.99.99.2/23
109011: Authen Session Start: user 'bill', Sid 0
109005: Authentication succeeded for user 'bill' from 172.18.124.114/35931
  to 99 .99.99.2/23 on interface inside
```

Autenticação inválida (nome de usuário ou senha) - RADIUS (externo). O usuário vê uma solicitação de Nome de usuário, depois Senha, tem três oportunidades para inseri-las e, se não for bem-sucedido, consulte "Erro: Número máximo de tentativas excedido."

```
109001: Auth start for user '???' from 172.18.124.114/35932 to 99.99.99.2/23
109002: Auth from 172.18.124.114/35932 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109006: Authentication failed for user '' from 172.18.124.114/35932
  to 99.99.99. 2/23 on interface inside
```

O servidor pode ser alcançado através de ping mas o daemon está inativo, o servidor não responde ao ping ou há incompatibilidade chave/cliente – não se comunica com o PIX – RADIUS (externo). O usuário vê o nome de usuário, a senha e, em seguida, "falha no servidor RADIUS" e, finalmente, "Erro: Número máximo de tentativas excedido."

```
109001: Auth start for user '???' from 172.18.124.114/35933 to 99.99.99.2/23
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109006: Authentication failed for user '' from 172.18.124.114/35933
  to 99.99.99. 2/23 on interface inside
```

Autenticação e autorização

Se você quiser permitir que todos os usuários autenticados executem todas as operações (HTTP, FTP e Telnet) através do PIX, a autenticação é suficiente e a autorização não é necessária. No entanto, se você quiser permitir algum subconjunto de serviços a determinados usuários ou limitar os usuários de ir a determinados sites, a autorização será necessária. A autorização RADIUS não é válida para o tráfego através do PIX. A autorização TACACS+ é válida neste caso.

Se a autenticação passar e a autorização estiver ativada, o PIX envia o comando que o usuário está fazendo ao servidor. Por exemplo, "http 1.2.3.4". Na versão 5.2 do PIX, a autorização TACACS+ é usada em conjunto com listas de acesso para controlar onde os usuários vão.

Se você quiser implementar a autorização para HTTP (sites visitados), use software como Websense, pois um único site pode ter um grande número de endereços IP associados a ele.

Configuração do servidor – Autenticação mais autorização

Configuração do servidor Cisco Secure UNIX TACACS

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

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

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

Cisco Secure Windows TACACS+

Conclua estes passos para configurar um servidor Cisco Secure Windows TACACS+.

1. Clique em **Negar comandos IOS não correspondentes** na parte inferior da Configuração do grupo.
2. Clique em **Add/Edit New Command (FTP, HTTP, Telnet)**.Por exemplo, se você quiser permitir Telnet para um site específico ("telnet 1.2.3.4"), o comando é **telnet**. O argumento é *1.2.3.4* . Depois de preencher "command=telnet", preencha os endereços IP "permit" no retângulo Argument (Argumento) (por exemplo, "permit 1.2.3.4"). Se todos os Telnets forem ser permitidos, o comando ainda será telnet, mas clique em Allow all unlisted arguments (Permitir todos os argumentos não listados). Em seguida, clique em **Concluir comando de edição**.
3. Execute a etapa 2 para cada um dos comandos permitidos (por exemplo, Telnet, HTTP e FTP).
4. Adicione o endereço IP PIX na seção Configuração NAS com a ajuda da GUI.

TACACS+ Configuração do programa gratuito de servidor

```
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 .*
   }
   }
```

Configuração de PIX – Adicionando autorização

Adicione comandos para exigir autorização:

```
aaa authorization include telnet outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authorization include http outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authorization include ftp outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
```

O novo recurso 5.2 permite que essa instrução em conjunto com a lista de acesso 101 previamente definida substitua as três instruções anteriores. As expressões novas e antigas não devem ser misturadas.

```
aaa authorization match 101 outside AuthInbound
```

Exemplos de depuração de autenticação e autorização de PIX

Boa autenticação e autorização bem-sucedidas - TACACS+

```
109001: Auth start for user '???' from
   99.99.99.2/11010 to 172.18.124.114/23
109011: Authen Session Start: user 'cse', Sid 3
109005: Authentication succeeded for user
   'cse' from 172.18.124.114/23 to 99.99.99.2/11010
   on interface outside
109011: Authen Session Start: user 'cse', Sid 3
109007: Authorization permitted for user 'cse'
   from 99.99.99.2/11010 to 172.18.1  24.114/23
   on interface outside
302001: Built inbound TCP connection 2 for faddr
   99.99.99.2/11010 gaddr 99.99.99.99/23 laddr
   172.18.124.114/23 (cse)
```

Autenticação válida mas a autorização é falha TACACS+. O usuário também vê a mensagem "Erro: Autorização negada."

```
109001: Auth start for user '???' from
   99.99.99.2/11011 to 172.18.124.114/23
109011: Authen Session Start: user 'httponly', Sid 4
109005: Authentication succeeded for user 'httponly'
   from 172.18.124.114/23 to  9 9.99.99.2/11011
   on interface outside
109008: Authorization denied for user 'httponly'
   from 172.18.124.114/23 to 99.99.99.2/11011
   on interface outside
```

Novo recurso de lista de acesso

No PIX Software Release 5.2 e Mais Recente, defina as listas de acesso no PIX. Aplique-os por usuário com base no perfil do usuário no servidor. O TACACS+ exige autenticação e autorização. O RADIUS exige apenas a autenticação. Neste exemplo, a autenticação de saída e a autorização para TACACS+ são alteradas . Uma lista de acesso no PIX está configurada.

Observação: no PIX versão 6.0.1 e posterior, se você usar o RADIUS, as listas de acesso serão implementadas inserindo a lista no atributo 11 (Filter-Id) IETF padrão (IETF RADIUS) [CSCdt50422]. Neste exemplo, o atributo 11 é definido como 115 em vez de fazer a argumentação "acl=115" específica do fornecedor.

Configuração de PIX

```
access-list 115 permit tcp any host 99.99.99.2 eq telnet
access-list 115 permit tcp any host 99.99.99.2 eq www
access-list 115 permit tcp any host 99.99.99.2 eq ftp
access-list 115 deny tcp any host 99.99.99.3 eq www
access-list 115 deny tcp any host 99.99.99.3 eq ftp
```

```
access-list 115 deny tcp any host 99.99.99.3 eq telnet
```

Perfis do servidor

Observação: a versão 2.1 do freeware TACACS+ não reconhece a versão "acl".

Configuração do servidor Cisco Secure UNIX TACACS+

```
user = pixa{
  password = clear "********"
  service=shell {
  set acl=115
  }
  }
```

Cisco Secure Windows TACACS+

Para adicionar autorização ao PIX para controlar onde o usuário vai com as listas de acesso, marque **shell/exec**, marque a caixa **Access Control List** e preencha o número (corresponde ao número da lista de acesso no PIX).

Cisco Secure UNIX RADIUS

```
user = pixa{
  password = clear "********"
  radius=Cisco {
  reply_attributes= {
  9,1="acl=115"
  }
  }
  }
```

Cisco Secure Windows RADIUS

RADIUS/Cisco é o tipo de dispositivo. O usuário "pixa" precisa de um nome de usuário, uma senha e uma marca e "acl=115" na caixa retangular Cisco/RADIUS, onde diz 009\001 AV-Pair (específico do fornecedor).

Saída

O usuário de saída "pixa" com "acl=115" no perfil autentica e autoriza. O servidor passa a acl=115 para o PIX, e o PIX mostra o seguinte:

```
pixfirewall#show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          2
user 'pixa' at 172.18.124.114, authenticated
   access-list 115
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

Quando o usuário "pixa" tenta ir para 99.99.99.3 (ou qualquer endereço IP, exceto 99.99.99.2,

porque há uma negação implícita), o usuário vê isto:

```
Error: acl authorization denied
```

Nova lista de acesso disponível com a versão 6.2 para download por usuário

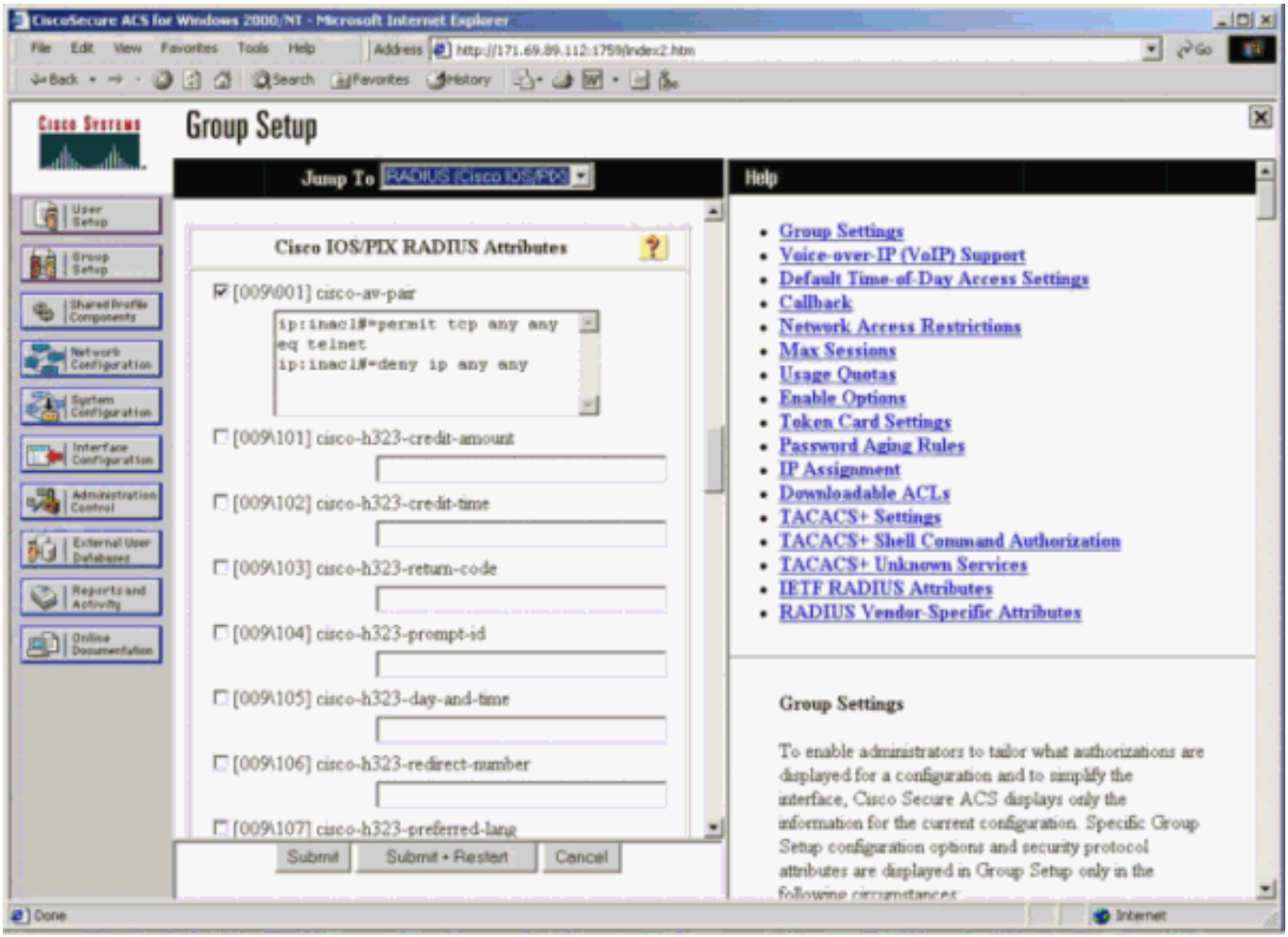
No software versão 6.2 e posterior do PIX Firewall, as listas de acesso são definidas em um servidor de controle de acesso (ACS) para download no PIX após a autenticação. Isso funciona somente com o protocolo RADIUS. Não é necessário configurar a lista de acesso no próprio PIX. Um modelo de grupo é aplicado a vários usuários.

Em versões anteriores, a lista de acesso é definida no PIX. Na autenticação, o ACS imprimiu o nome da lista de acesso ao PIX. A nova versão permite que o ACS envie a lista de acesso diretamente para o PIX.

Observação: se ocorrer failover, a tabela uauth não será copiada. Os usuários serão reautenticados. A lista de acesso é baixada novamente.

Instalação do ACS

Clique em **Group Setup** e selecione o tipo de dispositivo **RADIUS (Cisco IOS/PIX)** para configurar uma conta de usuário. Atribua um nome de usuário ("cse", neste exemplo) e uma senha para o usuário. Na lista Atributos, selecione a opção para configurar **[009\001]** ***fornecedor-av*-par**. Defina a lista de acesso conforme ilustrado neste exemplo:



Depurações de PIX: Autenticação Válida e Lista de Acesso Transferida por Download

- Permite somente Telnet e nega outro tráfego.

```
pix# 305011: Built dynamic TCP translation from inside:
  172.16.171.33/11063 to outside:172.16.171.201/1049
109001: Auth start for user '???' from 172.16.171.33/11063
   to 172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 10
109005: Authentication succeeded for user 'cse'
   from 172.16.171.33/11063
   to 172.16.171.202/23 on interface inside

302013: Built outbound TCP connection 123 for outside:
   172.16.171.202/23 (172.16.171.202/23) to inside:
   172.16.171.33/11063 (172.16.171.201/1049) (cse)
```

Saída do comando **show uauth**.

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list AAA-user-cse
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
```

Saída do comando **show access-list**.

```
pix#show access-list
access-list AAA-user-cse; 2 elements
access-list AAA-user-cse permit tcp any any eq telnet (hitcnt=1)
access-list AAA-user-cse deny ip any any (hitcnt=0)
```

- Nega somente Telnet e permite outro tráfego.

```
pix# 305011: Built dynamic TCP translation from inside:
   172.16.171.33/11064 to outside:172.16.171.201/1050
109001: Auth start for user '???' from 172.16.171.33/11064 to
   172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 11
109005: Authentication succeeded for user 'cse'
   from 172.16.171.33/11064
   to 172.16.171.202/23 on interface inside
109015: Authorization denied (acl= AAA-user-cse) for user 'cse'
  from 172.16.171.33/11064 to 172.16.171.202/23 on interface inside
```

Saída do comando **show uauth**.

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list AAA-user-cse
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
```

Saída do comando **show access-list**.

```
pix#show access-list
access-list AAA-user-cse; 2 elements
access-list AAA-user-cse deny tcp any any eq telnet (hitcnt=1)
access-list AAA-user-cse permit ip any any (hitcnt=0)
```

Nova lista de acesso para download por usuário usando o ACS 3.0

No ACS versão 3.0, o componente de perfil compartilhado permite que o usuário crie um modelo

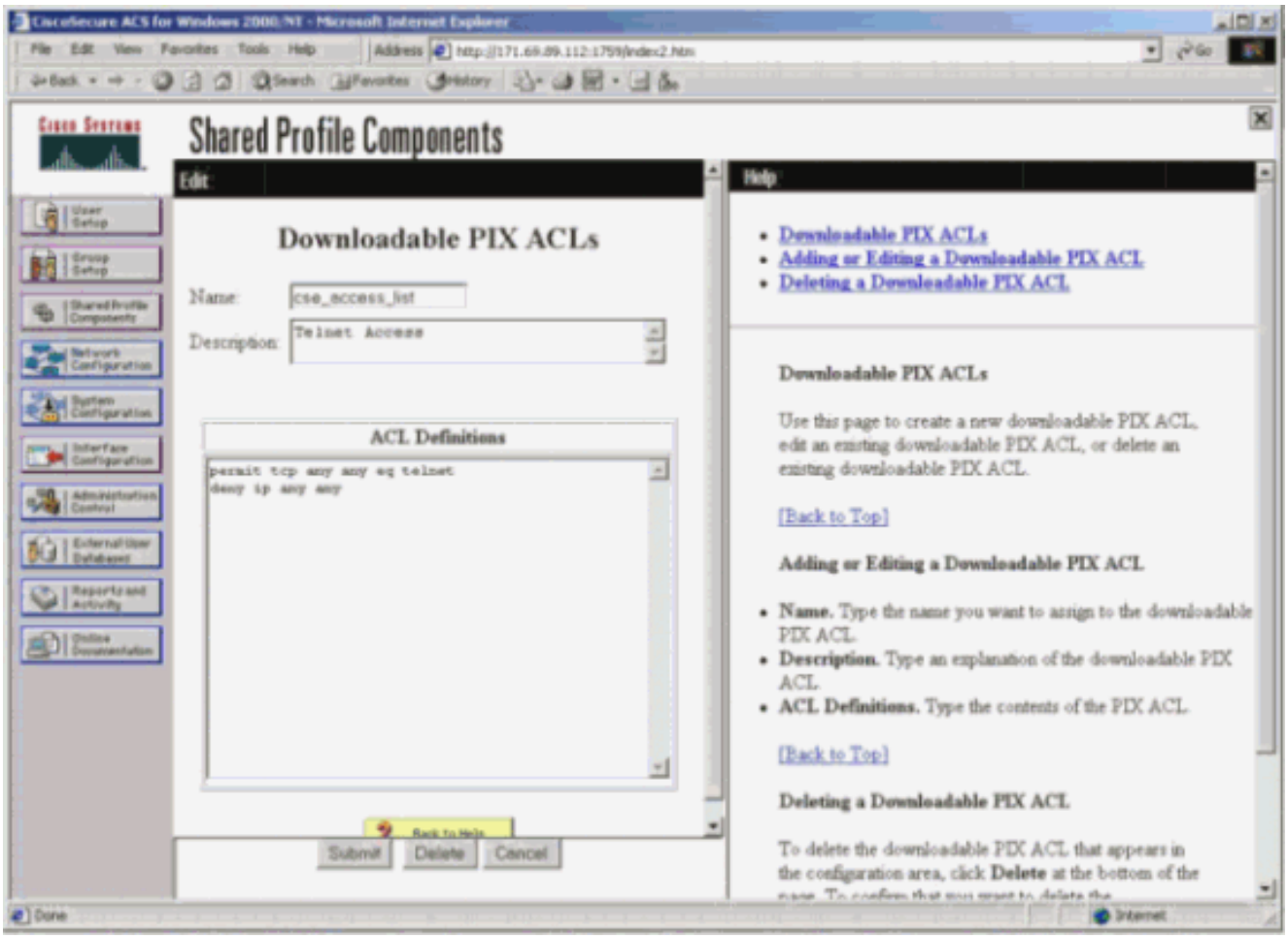
de lista de acesso e defina o nome do modelo para especificar usuários ou grupos. O nome do modelo pode ser usado com tantos usuários ou grupos quanto necessário. Isso elimina a necessidade de configurar listas de acesso idênticas para cada usuário.

Observação: se ocorrer failover, o uauth não será copiado para o PIX secundário. No failover stateful, a sessão é mantida. No entanto, a nova conexão deve ser reautenticada e a lista de acesso deve ser baixada novamente.

Usando perfis compartilhados

Conclua estes passos quando utilizar perfis partilhados.

1. Clique em Interface Configuration.
2. Verifique **ACLs que podem ser baixadas no nível do usuário** e/ou **ACLs que podem ser baixadas no nível do grupo**.
3. Clique em **Shared Profile Components (Componentes de perfil compartilhados)**. Clique em **ACLs para download no nível do usuário**.
4. Defina os ACLs que podem ser descarregados via download.
5. Clique em **Group Setup (Configuração do grupo)**. Em ACLs para download, atribua a lista de acesso PIX à lista de acesso criada anteriormente.



Depurações de PIX: Autenticação válida e lista de acesso baixada usando perfis compartilhados

- Permite somente Telnet e nega outro tráfego.

```
pix# 305011: Built dynamic TCP translation from inside:
```

```
   172.16.171.33/11065 to outside:172.16.171.201/1051
109001: Auth start for user '???' from 172.16.171.33/11065 to
   172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 12
109005: Authentication succeeded for user 'cse' from
   172.16.171.33/11065 to 172.16.171.202/23 on interface inside
302013: Built outbound TCP connection 124 for outside:
   172.16.171.202/23 (172.16.171.202/23) to inside:
   172.16.171.33/11065 (172.16.171.201/1051) (cse)
```

Saída do comando **show uauth**.

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
pix# 111009: User 'enable_15' executed cmd: show uauth
pix#
```

Saída do comando **show access-list**.

```
pix#show access-list
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3; 2 elements
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3
   permit tcp any any eq telnet (hitcnt=1)
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3
   deny ip any any (hitcnt=0)
pix# 111009: User 'enable_15' executed cmd: show access-list
```

- Nega somente Telnet e permite outro tráfego.

```
pix# 305011: Built dynamic TCP translation from inside:
   172.16.171.33/11066 to outside:172.16.171.201/1052
109001: Auth start for user '???' from 172.16.171.33/11066 to
   172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 13
109005: Authentication succeeded for user 'cse'
   from 172.16.171.33/11066
   to 172.16.171.202/23 on interface inside
109015: Authorization denied (acl=#ACSACL#-PIX-cse_access_list-3cff1dd6)
   for user 'cse' from 172.16.171.33/11066
   to 172.16.171.202/23 on interface inside
```

Saída do comando **show uauth**.

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
pix# 111009: User 'enable_15' executed cmd: show uauth
```

Saída do comando **show access-list**.

```
pix#show access-list
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6; 2 elements
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6
   deny tcp any any eq telnet (hitcnt=1)
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6
   permit ip any any (hitcnt=0)
pix# 111009: User 'enable_15' executed cmd: show access-listpix#
```

Adicionar relatório

Configuração de PIX - Adicionar relatório

TACACS (AuthInbound=tacacs)

Adicione esse comando.

```
aaa accounting include any inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthInbound
```

Ou use o novo recurso na seção 5.2 para definir o que deve ser contabilizado pelas listas de acesso.

```
aaa accounting match 101 outside AuthInbound
```

Observação: a lista de acesso 101 é definida separadamente.

RADIUS (AuthOutbound=radius)

Adicione esse comando.

```
aaa accounting include any inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthOutbound
```

Ou use o novo recurso na seção 5.2 para definir o que deve ser contabilizado pelas listas de acesso.

```
aaa accounting match 101 outside AuthOutbound
```

Observação: a lista de acesso 101 é definida separadamente.

Observação: os registros contábeis podem ser gerados para sessões administrativas no PIX a partir do código PIX 7.0.

Exemplos de relatórios

- Exemplo de contabilização TACACS para Telnet de 99.99.99.2 fora para 172.18.124.114 dentro (99.99.99.99).

```
172.18.124.157 pixuser PIX 99.99.99.2 start server=rtp-cherry
   time=10:36:16 date=08/23/2000 task_id=0x0 foreign_ip=99.99.99.2
   local_ip=172.18.124.114 cmd=telnet
172.18.124.157 pixuser PIX 99.99.99.2 stop server=rtp-cherry
   time=10:37:50 date=08/23/2000 task_id=0x0 foreign_ip=99.99.99.2
   local_ip=172.18.124.114
   cmd=telnet elapsed_time=94 bytes_in=61 bytes_out=254
```

- Exemplo de relatório RADIUS para conexão de 172.18.124.114 dentro para 99.99.99.2

externa (Telnet) e 99.99.99.3 externa (HTTP).

```
Sun Aug  6 03:59:28 2000
        Acct-Status-Type = Start
        NAS-IP-Address = 172.18.124.157
        Login-IP-Host = 172.18.124.114
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000004
        User-Name = cse
        Vendor-Specific = Source-IP=172.18.124.114
        Vendor-Specific = Source-Port=35937
        Vendor-Specific = Destination-IP=99.99.99.2
        Vendor-Specific = Destination-Port=23

Sun Aug  6 03:59:32 2000
        Acct-Status-Type = Stop
        NAS-IP-Address = 172.18.124.157
        Login-IP-Host = 172.18.124.114
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000004
         Username = cse
        Acct-Session-Time = 4
        Acct-Input-Octets = 101
        Acct-Output-Octets = 143
        Vendor-Specific = Source-IP=172.18.124.114
        Vendor-Specific = Source-Port=35937
        Vendor-Specific = Destination-IP=99.99.99.2
        Vendor-Specific = Destination-Port=23

Sun Aug  6 04:05:02 2000
        Acct-Status-Type = Start
        NAS-IP-Address = 172.18.124.157
        Login-IP-Host = 172.18.124.114
        Login-TCP-Port = 80
        Username = cse
        Vendor-Specific = Source-IP=172.18.124.114
        Vendor-Specific = Source-Port=35949
        Vendor-Specific = Destination-IP=99.99.99.3
        Vendor-Specific = Destination-Port=80

Sun Aug  6 04:05:02 2000
        Acct-Status-Type = Stop
        NAS-IP-Address = 172.18.124.157
        Login-IP-Host = 172.18.124.114
        Login-TCP-Port = 80
        Acct-Session-Id = 0x0000000a
        Username = cse
        Acct-Session-Time = 0
        Acct-Input-Octets = 1277
        Acct-Output-Octets = 310
        Vendor-Specific = Source-IP=172.18.124.114
        Vendor-Specific = Source-Port=35949
        Vendor-Specific = Destination-IP=99.99.99.3
        Vendor-Specific = Destination-Port=80
```

Uso do comando exclude

Nesta rede, se você decidir que uma origem ou um destino específico não precisa de autenticação, autorização ou contabilização, emita esses comandos.

```
aaa authentication exclude telnet outside 172.18.124.114 255.255.255.255
  99.99.99.3 255.255.255.255 AuthInbound
aaa authorization exclude telnet outside 172.18.124.114 255.255.255.255
  99.99.99.3 255.255.255.255 AuthInbound
aaa accounting exclude telnet outside 172.18.124.114 255.255.255.255
  99.99.99.3 255.255.255.255 AuthInbound
```

Observação: você já tem os comandos **include**.

```
aaa authentication|authorization|accounting include http|ftp|telnet
```

Ou, com o novo recurso na seção 5.2, defina o que deseja excluir.

```
access-list 101 deny tcp host 99.99.99.3 host 172.18.124.114 eq telnet
access-list 101 deny tcp host 99.99.99.3 host 172.18.124.114 eq ftp
access-list 101 deny tcp host 99.99.99.3 host 172.18.124.114 eq www
access-list 101 permit tcp any any eq telnet
access-list 101 permit tcp any any eq www
access-list 101 permit tcp any any eq ftp
aaa authentication match 101 outside AuthInbound
aaa authorization match 101 outside AuthInbound
aaa accounting match 101 outside AuthInbound
```

Nota: Se você excluir uma caixa da autenticação e tiver autorização ativada, também deverá excluir a caixa da autorização.

Máx. de sessões e Exibir usuários conectados

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 relatório gerado, mas não há um registro "stop", o servidor TACACS+ ou RADIUS admite que a pessoa ainda está conectada (ou seja, o usuário tem uma sessão no PIX). Isto funciona bem para conexões Telnet e FTP devido à natureza das conexões. No entanto, isso não funciona bem para HTTP. Neste exemplo, uma configuração de rede diferente é usada, mas os conceitos são os mesmos.

Usuário estabelece um Telnet por meio 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 171.68.118.100/1200 to 9.9.9.25/23
    (pix) 302001: Built TCP connection 5 for
        faddr 9.9.9.25/23 gaddr 9.9.9.10/1200 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 "start" mas sem registro "stop", 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 trata de seus negócios de Telnet ou FTP no host de destino e sai (passa dez 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
```

Seja o uauth 0 (isto é, autenticar sempre) ou mais (autenticar uma vez e não mais durante o período de uauth), um registro de contabilidade será cortado para cada local acessado.

O HTTP trabalha de forma diferente devido à natureza do protocolo. Aqui está um exemplo de HTTP em que o usuário navega de 171.68.118.100 para 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 de início foi lançado às 16:35:34, e o registro de interrupção, 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 não está conectado ao site. A conexão não é aberta quando o usuário está lendo a página da Web. Máximo de sessões ou visualização de usuários conectados não funcionam aqui. Isso ocorre porque o tempo de conexão (o tempo entre o "Built" e o "Teardown") no HTTP é muito curto. O registro “start” (iniciar) e “stop” (parar) é sub-segundo. Não há registro "start" sem um registro "stop", pois os registros ocorrem praticamente no mesmo momento. Ainda há um registro "start" e "stop" enviado ao servidor para cada transação, independentemente de uauth estar definido para 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.

Interface de usuário

Altere o prompt que os usuários veem

Se você tiver o comando:

```
auth-prompt prompt PIX515B
```

em seguida, os usuários que estão passando pelo PIX veem esse prompt.

```
PIX515B
```

Personalizar a mensagem que os usuários veem

Se você tiver os comandos:

```
auth-prompt accept "GOOD_AUTHENTICATION"
auth-prompt reject "BAD_AUTHENTICATION"
```

em seguida, os usuários veem uma mensagem sobre o status da autenticação em um login com falha/êxito.

```
  PIX515B
  Username: junk
  Password:
  "BAD_AUTHENTICATION"

  PIX515B
  Username: cse
  Password:
  "GOOD_AUTHENTICATION"
```

Tempo ocioso e intervalos absolutos por usuário

O comando PIX timeout uauth controla com que freqüência é necessário realizar novas autenticações. Se a autenticação/autorização TACACS+ estiver ativada, isso é controlado por usuário. Este perfil de usuário está configurado para controlar o tempo limite (isto é, no servidor freeware TACACS+ e os tempos limite estão em minutos).

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

Após a autenticação/autorização:

```
show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
user 'cse' at 99.99.99.3, authorized to:
   port 172.18.124.114/telnet
   absolute   timeout: 0:02:00
   inactivity timeout: 0:01:00
```

No final de dois minutos:

Tempo limite absoluto - a sessão é interrompida:

```
109012: Authen Session End: user 'cse', Sid 20, elapsed 122 seconds
302002: Teardown TCP connection 32 faddr 99.99.99.3/11025
   gaddr 99.99.99.99/23 l addr 172.18.124.114/23 duration 0:02:26
   bytes 7547 (TCP FINs)
```

Saída de HTTP virtual

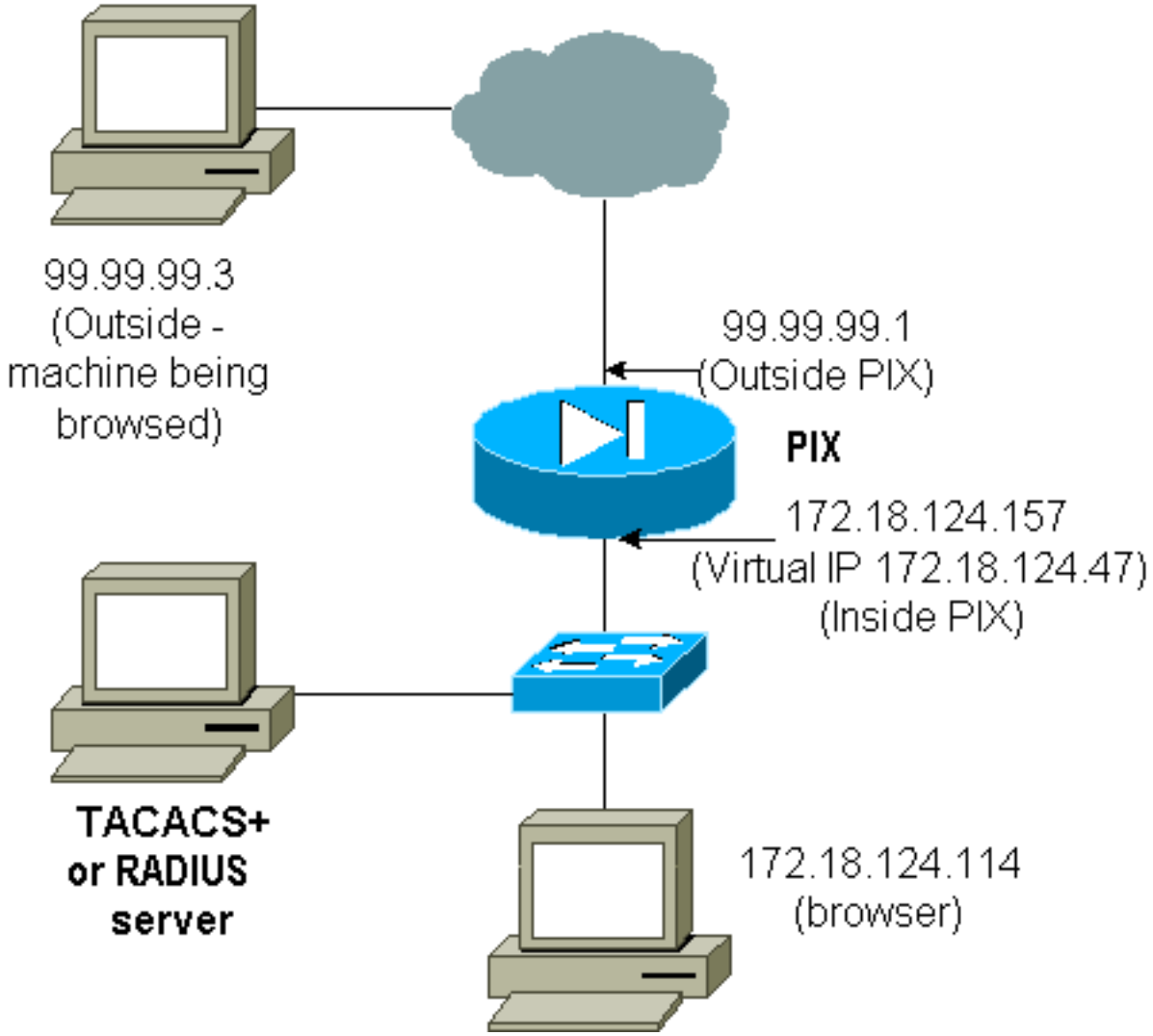
Se a autenticação for necessária em sites fora do PIX, bem como no próprio PIX, às vezes, um comportamento incomum do navegador é observado, já que os navegadores armazenam em cache o nome de usuário e a senha.

Para evitar isso, implemente 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 no formato.

```
virtual http #.#.#.#
```

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.

Observação: os endereços IP virtuais HTTP e Telnet devem ser incluídos nas instruções **de autenticação** de **aaa**. Neste exemplo, especificar 0.0.0.0 inclui esses endereços.



Na configuração do PIX, adicione este comando.

```
virtual http 172.18.124.47
```

O usuário aponta o navegador para 99.99.99.3. Esta mensagem é exibida.

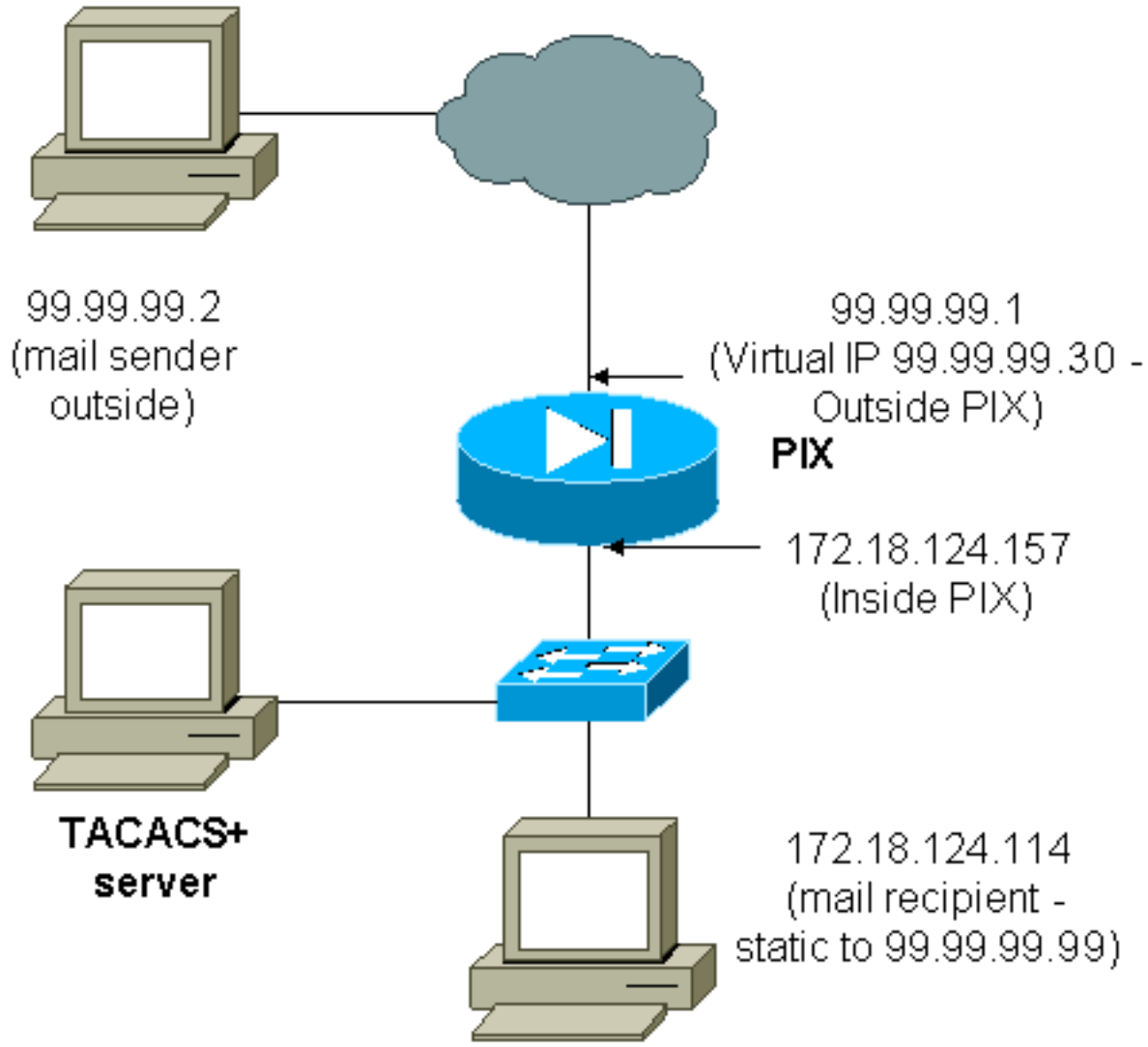
```
Enter username for PIX515B (IDXXX) at 172.18.124.47
```

Após a autenticação, o tráfego é redirecionado para 99.99.99.3.

Telnet Virtual

Observação: os endereços IP virtuais HTTP e Telnet devem ser incluídos nas instruções **de autenticação** de **aaa**. Neste exemplo, especificar 0.0.0.0 inclui esses endereços.

Entrada de Telnet Virtual



Não é uma boa ideia autenticar a entrada de correio, uma vez que não é apresentada uma janela para o correio ser enviado para entrada. Use o comando **exclude** em vez disso. Mas, para fins de ilustração, esses comandos são adicionados.

```
aaa authentication include tcp/25 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authorization include tcp/25 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
!--- OR the new 5.2 feature allows these !--- four statements to perform the same function. !---
Note: The old and new verbiage should not be mixed.

access-list 101 permit tcp any any eq smtp
!--- The "mail" was a Telnet to port 25. access-list 101 permit tcp any any eq telnet
aaa authentication match 101 outside AuthInbound
aaa authorization match 101 outside AuthInbound
!
!--- plus ! virtual telnet 99.99.99.30
static (inside,outside) 99.99.99.30 172.18.124.30
   netmask 255.255.255.255 0 0
static (inside,outside) 99.99.99.99 172.18.124.114
   netmask 255.255.255.255 0 0
conduit permit tcp host 99.99.99.30 eq telnet any
conduit permit tcp host 99.99.99.99 eq telnet any
conduit permit tcp host 99.99.99.99 eq smtp any
```

Os usuários (este é o freeware TACACS+):

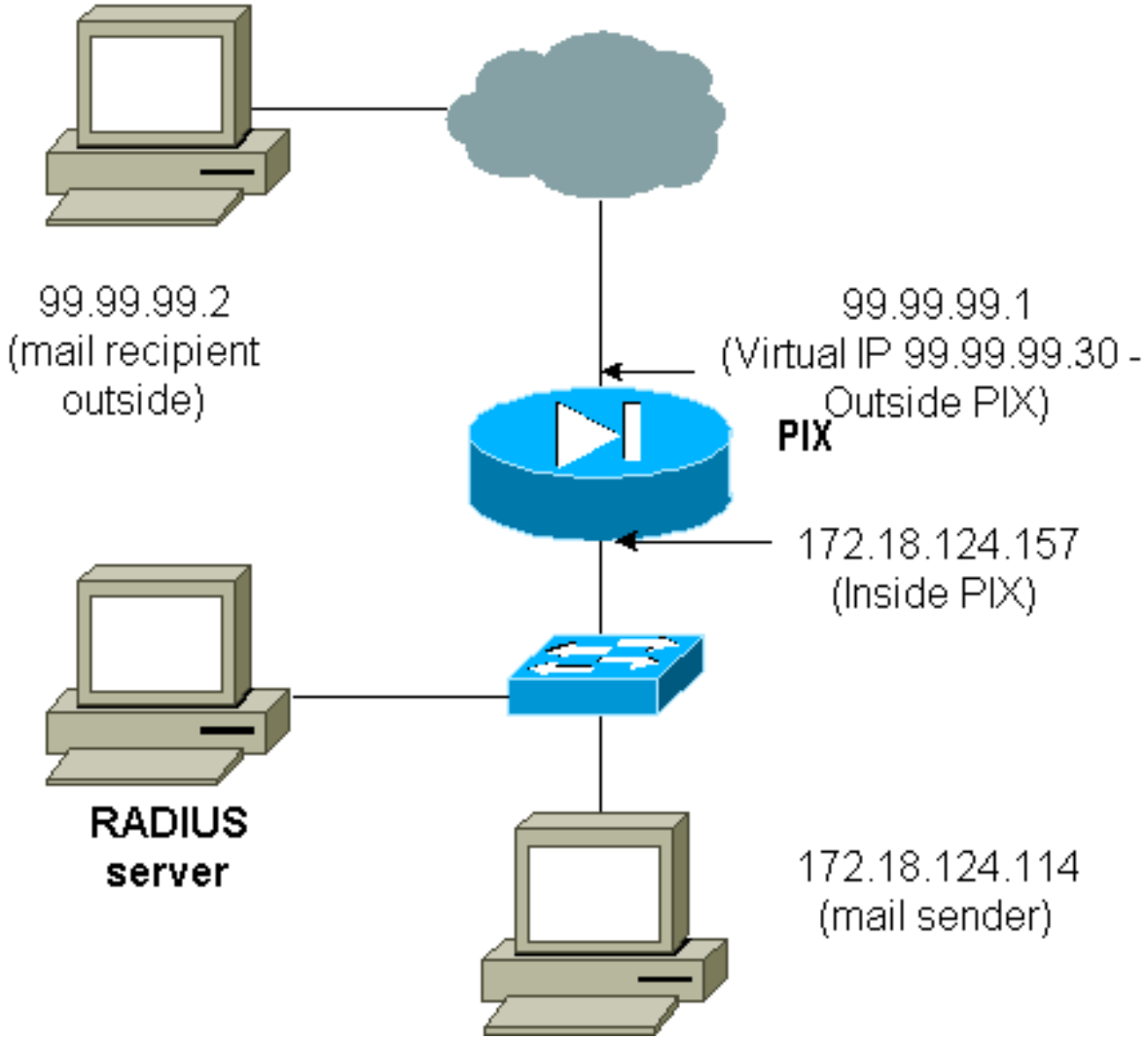
```
  user = cse {
  default service = permit
  login = cleartext "csecse"
  }


  user = pixuser {
  login = cleartext "pixuser"
  service = exec {
  }
  cmd = telnet {
  permit .*
  }
  }
```

Se apenas a autenticação estiver ativada, ambos os usuários enviarão e-mails de entrada após a autenticação em um Telnet para o endereço IP 99.99.99.30. Se a autorização estiver habilitada, o usuário "cse" Telnets para 99.99.99.30 e insere o nome de usuário/senha TACACS+. A conexão Telnet cai. O usuário "cse" envia e-mail para 99.99.99.99 (172.18.124.114). A autenticação foi bem-sucedida para o usuário "pixuser". No entanto, quando o PIX envia a solicitação de autorização para cmd=tcp/25 e cmd-arg=172.18.124.114, a solicitação falha, como mostrado nesta saída.

```
109001: Auth start for user '???' from
   99.99.99.2/11036 to 172.18.124.114/23
109005: Authentication succeeded for user
   'cse' from 172.18.124.114/23 to
   99.99.99.2/11036 on interface outside

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

pixfirewall# 109001: Auth start for user '???' from
    99.99.99.2/11173 to 172.18.124.30/23
109011: Authen Session Start: user 'cse', sid 10
109005: Authentication succeeded for user 'cse' from 99.99.99.2/23
    to 172.18.124.30/11173 on interface outside
109011: Authen Session Start: user 'cse', sid 10
109007: Authorization permitted for user 'cse' from 99.99.99.2/11173
    to 172.18.124.30/23 on interface outside
109001: Auth start for user 'cse' from 99.99.99.2/11174 to
    172.18.124.114/25
109011: Authen Session Start: user 'cse', sid 10
109007: Authorization permitted for user 'cse' from 99.99.99.2/11174
    to 172.18.124.114/25 on interface outside
302001: Built inbound TCP connection 5 for faddr 99.99.99.2/11174
    gaddr 99.99.99.99/25 laddr 172.18.124.114/25 (cse)

pixfirewall# 109001: Auth start for user '???' from 99.99.99.2/11175
    to 172.18.124.30/23
109011: Authen Session Start: user 'pixuser', sid 11
109005: Authentication succeeded for user 'pixuser' from 99.99.99.2/23
```

```
    to 172.18.124.30/11175 on interface outside
109011: Authen Session Start: user 'pixuser', sid 11
109007: Authorization permitted for user 'pixuser' from 99.99.99.2/11175
    to 172.18.124.30/23 on interface outside
109001: Auth start for user 'pixuser' from 99.99.99.2/11176
    to 172.18.124.114/25
109008: Authorization denied for user 'pixuser' from 99.99.99.2/25
    to 172.18.124.114/11176 on interface outside
```

Saída Telnet Virtual



Não é uma boa ideia autenticar a entrada de correio, uma vez que não é apresentada uma janela para o correio ser enviado para entrada. Use o comando **exclude** em vez disso. Mas, para fins de ilustração, esses comandos são adicionados.

Não é uma boa ideia autenticar a saída de e-mails, pois não é exibida uma janela para que o e-mail seja enviado. Use o comando **exclude** em vez disso. Mas, para fins de ilustração, esses comandos são adicionados.

```
aaa authentication include tcp/25 inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthOutbound
!--- OR the new 5.2 feature allows these three statements !--- to replace the previous
statements. !--- Note: Do not mix the old and new verbiage.

access-list 101 permit tcp any any eq smtp
access-list 101 permit tcp any any eq telnet
```

```
aaa authentication match 101 inside AuthOutbound
!
!--- plus ! virtual telnet 99.99.99.30
!--- The IP address on the outside of PIX is not used for anything else.
```

Para enviar e-mails de dentro para fora, ative um prompt de comando no host de e-mail e Telnet para 99.99.99.30. Isso abre o caminho para o correio passar. O e-mail é enviado de 172.18.124.114 para 99.99.99.2:

```
   305002: Translation built for gaddr 99.99.99.99
      to laddr 172.18.124.114
   109001: Auth start for user '???' from
      172.18.124.114/32860 to 99.99.99.30/23
   109011: Authen Session Start: user 'cse', Sid 14
   109005: Authentication succeeded for user 'cse'
      from 172.18.124.114/32860 to    99.99.99.30/23
      on interface inside
   302001: Built outbound TCP connection 22 for faddr
      99.99.99.2/25 gaddr 99.99.99.99/32861
      laddr 172.18.124.114/32861 (cse)

pixfirewall#show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
user 'cse' at 172.18.124.114, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

Desconexão de Telnet Virtual

Quando os usuários usarem Telnet para o endereço IP virtual de Telnet, o comando show uauth mostra o tempo em que o furo fica aberto. Se os usuários quiserem impedir que o tráfego passe após a finalização de suas sessões (quando o tempo permanecer em uauth), eles precisarão criar uma sessão Telnet novamente com o endereço IP Telnet virtual. Esta ação desliga a sessão. Isso é ilustrado por este exemplo.

A primeira autenticação

```
 109001: Auth start for user '???'
    from 172.18.124.114/32862 to 99.99.99.30/23
 109011: Authen Session Start: user 'cse', Sid 15
 109005: Authentication succeeded for user
    'cse' from 172.18.124.114/32862 to
    99.99.99.30/23 on interface inside
```

Após a primeira autenticação

```
pixfirewall#show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
user 'cse' at 172.18.124.114, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

A segunda autenticação

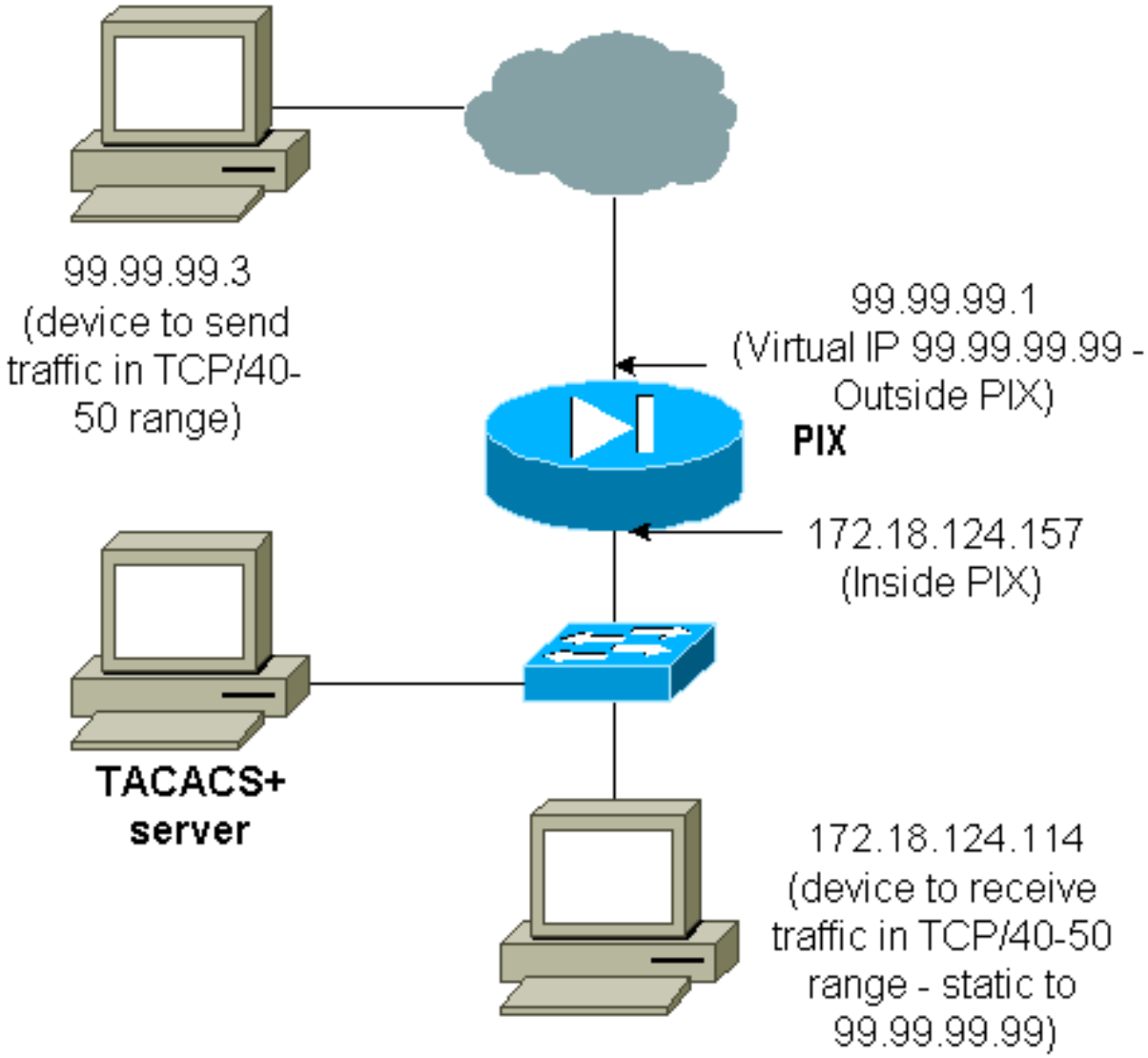
```
pixfirewall# 109001: Auth start for user 'cse'
   from 172.18.124.114/32863 to    99.99.99.30/23
109005: Authentication succeeded for user 'cse'
   from 172.18.124.114/32863 to    99.99.99.30/23
   on interface inside
```

Após a segunda autenticação

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

Autorização da porta

Diagrama de Rede



A autorização é permitida para intervalos de porta. Se o Telnet virtual estiver configurado no PIX e a autorização for configurada para um intervalo de portas, o usuário abrirá o buraco com o Telnet virtual. Em seguida, se a autorização para um intervalo de porta estiver ativa e o tráfego nesse intervalo atingir o PIX, o PIX enviará o comando para o servidor TACACS+ para obter autorização. Este exemplo mostra a autorização de entrada em um intervalo de portas.

```
aaa authentication include any outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authorization include tcp/40-50 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
!--- OR the new 5.2 feature allows these three statements !--- to perform the same function as
the previous two statements. !--- Note: The old and new verbiage should not be mixed.

access-list 116 permit tcp any any range 40 50
aaa authentication match 116 outside AuthInbound
aaa authorization match 116 outside AuthInbound
!
!--- plus ! static (inside,outside) 99.99.99.99 172.18.124.114
netmask 255.255.255.255 0 0
conduit permit tcp any any
virtual telnet 99.99.99.99
```

Exemplo de configuração do servidor TACACS+ (freeware):

```
  user = cse {
  login = cleartext "numeric"
  cmd = tcp/40-50 {
  permit 172.18.124.114
  }
  }
```

O usuário deve primeiramente fazer Telnet para o endereço IP virtual 99.99.99.99. Após a autenticação, quando um usuário tenta empurrar o tráfego TCP no intervalo de porta 40-50 através do PIX para 99.99.99.99 (172.18.124.114), cmd=tcp/40-50 é enviado para o servidor TACACS+ com cmd-arg=17 2.18.124.114 como ilustrado aqui:

```
109001: Auth start for user '???' from 99.99.99.3/11075
    to 172.18.124.114/23
109011: Authen Session Start: user 'cse', Sid 13
109005: Authentication succeeded for user 'cse'
    from 172.18.124.114/23 to 99.99.99.3/11075
    on interface outside
109001: Auth start for user 'cse' from 99.99.99.3/11077
    to 172.18.124.114/49
109011: Authen Session Start: user 'cse', Sid 13
109007: Authorization permitted for user 'cse'
    from 99.99.99.3/11077 to 172.18.124.114/49
    on interface outside
```

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

Depois de verificar se o Telnet virtual funciona para permitir o tráfego TCP/40-50 para o host dentro da rede, adicione a contabilização desse tráfego com esses comandos.

```
aaa accounting include any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
!--- OR the new 5.2 feature allows these !--- two statements to replace the previous statement.
!--- Note: Do not mix the old and new verbiage.

aaa accounting match 116 outside AuthInbound
access-list 116 permit ip any any
```

Exemplo de registros de relatórios TACACS+

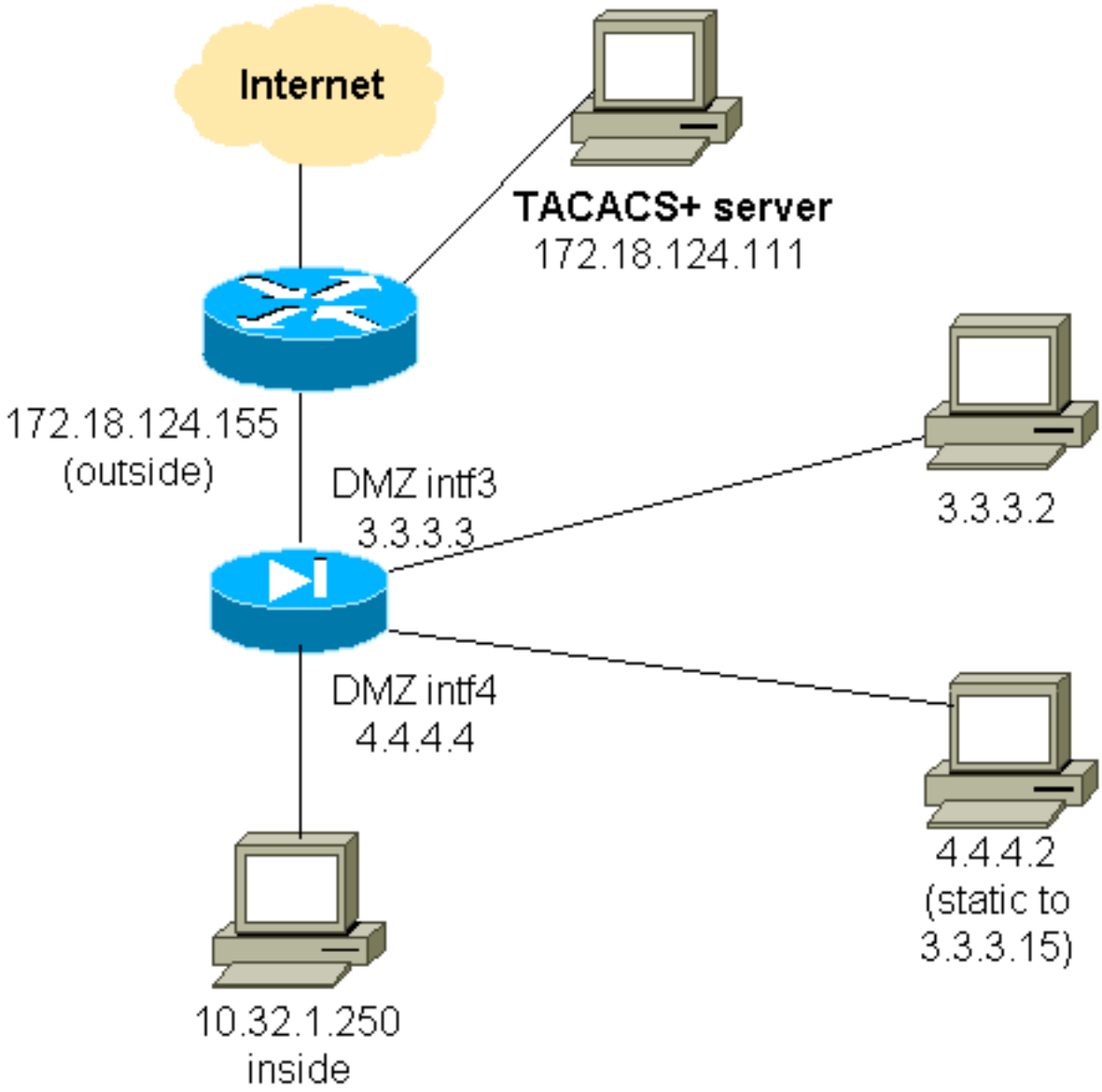
```
Thu Aug 24 08:06:09 2000 172.18.124.157 cse PIX 99.99.99.3
start task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
cmd=tcp/40-50
Thu Aug 24 08:06:17 2000 172.18.124.157 cse PIX 99.99.99.3
stop task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
cmd=tcp/40-50 elapsed_time=8 bytes_in=80 bytes_out=101
```

Autenticação no DMZ

Para autenticar usuários que vão de uma interface DMZ para outra, diga ao PIX para autenticar o tráfego das interfaces nomeadas. No PIX, a organização é assim:

```
least secure
PIX outside (security0) = 172.18.124.155
pix/intf3 (DMZ - security15) = 3.3.3.3 & device 3.3.3.2
pix/intf4 (DMZ - security20) = 4.4.4.4 & device 4.4.4.2 (static to 3.3.3.15)
PIX inside (security100) = 10.32.1.250
most secure
```

Diagrama de Rede



Configuração de PIX parcial

Autentique o tráfego Telnet entre pix/intf3 e pix/intf4, como demonstrado aqui.

Configuração de PIX parcial

```
  nameif ethernet0 outside security0
  nameif ethernet1 inside security100
  (nameif ethernet2 pix/intf2 security10)
  nameif ethernet3 pix/intf3 security15
  nameif ethernet4 pix/intf4 security20
  (nameif ethernet5 pix/intf5 security25)
  interface ethernet0 auto
  interface ethernet1 auto
  (interface ethernet2 auto shutdown)
  interface ethernet3 auto
  interface ethernet4 auto
  (interface ethernet5 auto shutdown)
  ip address outside 172.18.124.155 255.255.255.0
  ip address inside 10.32.1.250 255.255.255.0
  ip address pix/intf3 3.3.3.3 255.255.255.0
  ip address pix/intf4 4.4.4.4 255.255.255.0
  static (pix/intf4,pix/intf3) 3.3.3.15 4.4.4.2 netmask
255.255.255.255 0 0
```

```
  conduit permit tcp host 3.3.3.15 host 3.3.3.2
  aaa-server xway protocol tacacs+
  aaa-server xway (outside) host 172.18.124.111 timeout
5
  aaa authentication include telnet pix/intf4 4.4.4.0
255.255.255.0 3.3.3.0
  255.255.255.0 3.3.3.0 255.255.255.0 xway
  aaa authentication include telnet pix/intf3 4.4.4.0
255.255.255.0 3.3.3.0
  255.255.255.0 3.3.3.0 255.255.255.0 xway
!--- OR the new 5.2 feature allows these four statements
!--- to replace the previous two statements. !--- Note:
Do not mix the old and new verbiage.

  access-list 103 permit tcp 3.3.3.0 255.255.255.0
4.4.4.0 255.255.255.0 eq telnet
  access-list 104 permit tcp 4.4.4.0 255.255.255.0
3.3.3.0 255.255.255.0 eq telnet
  aaa authentication match 103 pix/intf3 xway
  aaa authentication match 104 pix/intf4 xway
```

Informações a serem coletadas se você abrir um caso de TAC

Se você ainda precisar de assistência após seguir as etapas de solução de problemas acima e quiser abrir um caso no Cisco TAC, inclua essas informações para a solução de problemas do seu PIX Firewall.

- Descrição do problema e detalhes relevantes de topologia
- Solucione problemas antes de abrir o caso
- Saída do comando **show tech-support**
- Saída do comando **show log** após a execução com o comando **logging buffered debugging** ou capturas de console que demonstram o problema (se disponível)

Anexe os dados coletados à sua ocorrência em formato de texto simples descompactado (.txt). Anexe informações ao seu caso carregando-as com a ajuda da Case Query Tool (somente clientes registrados) . Se você não puder acessar a Case Query Tool, envie as informações em um anexo de e-mail para attach@cisco.com com o número do caso na linha de assunto da sua mensagem.

Informações Relacionadas

- Cisco PIX Firewall Software
- Referências do comando Cisco Secure PIX Firewall
- Avisos de campo de produto de segurança (incluindo PIX)
- Solicitações de Comentários (RFCs)
- Cisco Secure Access Control Server for Windows
- Cisco Secure Access Control Server for Unix
- Sistema de controle de acesso do controlador de acesso de terminal (TACACS+)

- Remote Authentication Dial-In User Service (RADIUS)
- Suporte Técnico e Documentação - Cisco Systems