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

Índice

Introdução

O RAIO e a autenticação TACACS+ podem ser feitos para o FTP, o telnet, e as conexões de HTTP através do firewall PIX segura Cisco. A autenticação para outros menos protocolos comuns é feita geralmente para trabalhar. A autorização TACACS+ é apoiada. A autorização RADIUS não é apoiada. As mudanças no Authentication, Authorization, and Accounting (AAA) PIX 5.2 sobre a versão anterior incluem a lista de suporte de acesso de AAA para controlar quem são autenticados e os que recursos os acessos de usuário. Em PIX 5.3 e mais atrasado, a mudança do Authentication, Authorization, and Accounting (AAA) sobre versões anterior do código é que as portas RADIUS são configuráveis.

Nota: O PIX 6.x pode fazer esclarecer a passagem com o tráfego mas não para o tráfego destinated ao PIX.

Pré-requisitos

Requisitos

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Nota: Se você executa a versão de software 7.x PIX/ASA e mais tarde, refira configurar servidores AAA e o base de dados local.

Convenções

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

Autenticação, autorização e contabilidade

Estão aqui uma explicação de autenticação, uma autorização e uma contabilidade:

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

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

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

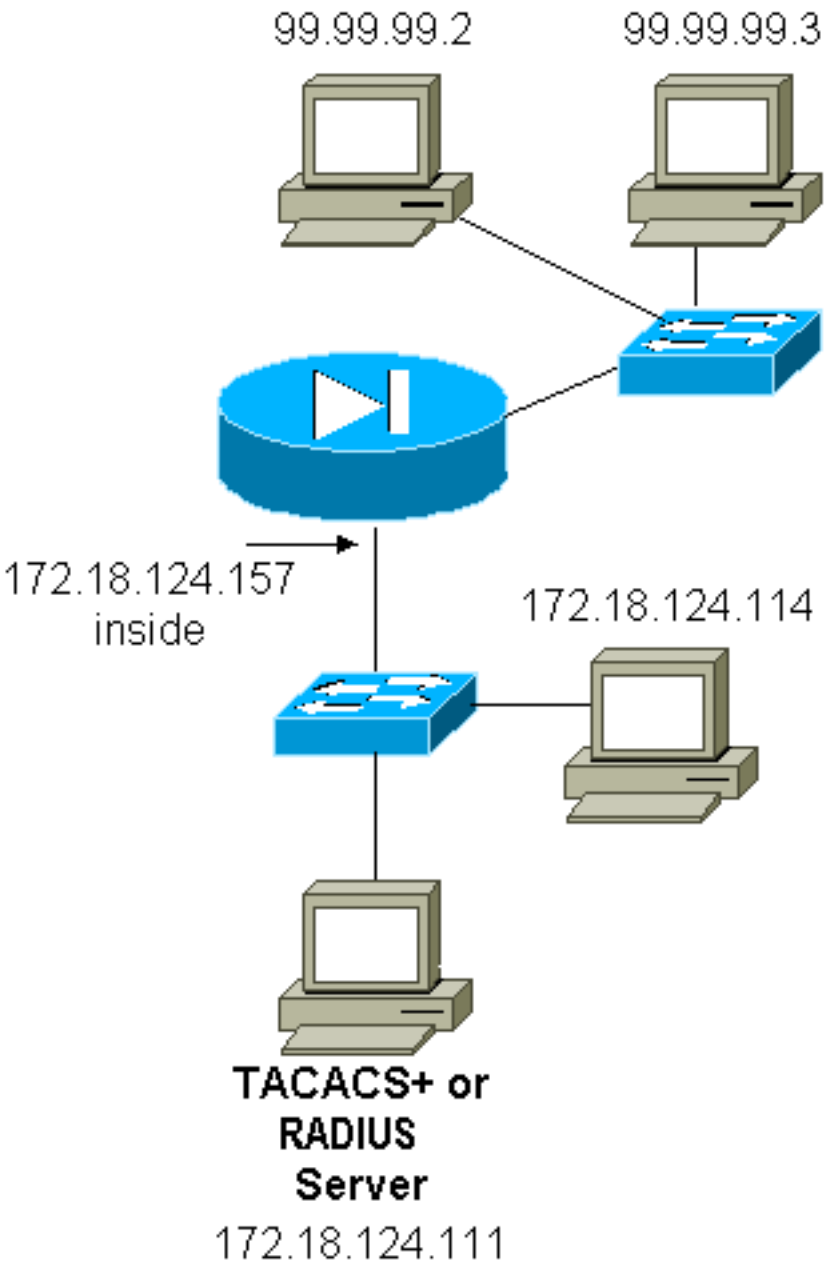
- Telnet – O usuário vê um prompt de nome de usuário ativado e, em seguida, a solicitação para a senha. Se a autenticação (e autorização) for bem-sucedida no PIX/servidor, o usuário está pronto para obter nome de usuário e senha pelo host de destino.
- **FTP** — O usuário vê uma alerta de nome de usuário vir acima. O usuário precisa inserir local_username@remote_username para nome de usuário e local_password@remote_password para senha. O PIX envia o “local_username” e o “local_password” ao servidor de segurança local. Se a autenticação (e a autorização) são bem sucedidas no PIX/server, o “remote_username” e o “remote_password” estão passados ao servidor FTP de destino além.
- **HTTP** — Um indicador é indicado na requisição de nome de usuário de navegador e na senha. Se a autenticação (e autorização) for concluída com sucesso, o usuário chega ao web site de destino. Mantenha na mente que os *navegadores põem em esconderijo nomes de usuário e senha.* Se parece que o PIX deve cronometrar para fora uma conexão de HTTP mas não faz assim, é provável que a reautenticação ocorre realmente com o navegador “tiro” o nome de usuário oculto e a senha ao PIX. O PIX para a frente isto ao Authentication Server. O Syslog e/ou o server PIX debugam mostras este fenômeno. Se o telnet e o FTP parecem trabalhar “normalmente”, mas as conexões de HTTP não fazem, esta é a razão.

Etapas de depuração

- Certifique-se dos trabalhos da configuração de PIX antes que você adicione a autenticação de AAA e a autorização. Se você é incapaz de passar o tráfego antes que você institua a authentication e autorização, você é incapaz de fazer tão mais tarde.
- Habilite algum tipo de registro no PIX.Emita o **comando logging console debug** girar sobre a eliminação de erros do console de registro.**Nota:** Não use a eliminação de erros do console de registro pesadamente em um sistema 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 de servidor de TACACS segura de Cisco UNIX

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

Configuração do servidor segura dos RADIUS UNIX de Cisco

Nota: Adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT e a chave PIX à lista do servidor do acesso de rede (NAS) com a ajuda do GUI avançado.

```
user=bill {
radius=Cisco {
check_items= {
```

```
2="foo"
}
reply_attributes= {
6=6
}
}
}
```

Windows RADIUS seguro de Cisco

Use estas etapas para estabelecer Cisco que o Windows RADIUS seguro separa.

1. Obtenha uma senha na **seção de instalação de usuário**.
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 Windows seguro TACACS+

O usuário obtém uma senha na seção Configuração de Usuário.

Configuração de servidor Livingston RADIUS

Nota: Adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT PIX e a chave aos *clientes* arquiva.

- fature o User-service-type = o Usuário Shell do " foo" de Password=

Configuração de servidor Merit RADIUS

Nota: Adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT PIX e a chave aos *clientes* arquiva.

- 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). Em PIX 5.3 e mais atrasado, a autenticação RADIUS e as portas de relatório podem ser mudadas a algo a não ser o padrão 1645/1646 com estes comandos:

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

Exemplos de depuração de autenticação de PIX

Veja passos de debugging para obter informações sobre de como girar sobre debugar. Estes são exemplos de um usuário em 99.99.99.2 que inicie o tráfego a 172.18.124.114 interno (99.99.99.99) e vice-versa. O tráfego de entrada é TACACS-autenticado e de partida Raio-é autenticado.

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 o “erro: Número máximo de tentativas excedidas.”

```
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 o “erro: Número máximo de tentativas excedidas.”

```
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 o pedido para o username, a seguir a senha, tem três oportunidades de entrar nestes, e se mal sucedido, vê o “erro: Número máximo de tentativas excedidas.”

```
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 username, a seguir a senha, a seguir o “servidor Radius falhado,” e então finalmente “erro: Número máximo de tentativas excedidas.”

```
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 quer permitir que todos os usuários autenticados executem todas as operações (HTTP, FTP, e telnet) com o PIX, a seguir a autenticação é suficiente e a autorização não é precisada. Contudo, se você quer permitir algum subconjunto dos serviços aos usuários determinados ou limitar usuários de ir às sites determinado, a autorização é precisada. A autorização RADIUS é inválida para o tráfego com o PIX. A autorização TACACS+ é válida neste caso.

Se a autenticação passa e a autorização está ligada, o PIX envia o comando que o usuário está fazendo ao server. Por exemplo, o “HTTP 1.2.3.4." na versão 5.2 do PIX, autorização TACACS+ é usado conjuntamente com Listas de acesso para controlar onde os usuários vão.

Se você quer executar a autorização para HTTP (sites visitados), use o software tal como Websense desde que um único site pode ter um grande número endereços IP de Um ou Mais Servidores Cisco ICM NT associados com ele.

Configuração do servidor – Autenticação mais autorização

Configuração de servidor de TACACS segura de Cisco UNIX

```
  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 Windows seguro TACACS+

Termine estas etapas para estabelecer um server seguro de Cisco Windows TACACS+.

1. Clique **comandos deny unmatched ios na** parte inferior da instalação de grupo.
2. Clique o **comando add/edit new (FTP, HTTP, telnet)**.Por exemplo, se você quer permitir o telnet a um local 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). Clique então o **comando editing do revestimento**.
3. Execute etapa 2 para cada um dos comandos permitidos (por exemplo, telnet, HTTP, e FTP).
4. Adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT PIX na seção de configuração de NAS com a ajuda do 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

Comandos Add exigir a 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
```

A característica 5.2 nova permite que esta indicação conjuntamente com a lista de acessos

previamente definida 101 substitua as três indicações precedentes. As expressões novas e antigas não devem ser misturadas.

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

Exemplos de depuração de autenticação e autorização de PIX

A boa autenticação e a autorização sucedem - 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 igualmente vê erro da mensagem “: 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 atrasado, defina Listas de acesso no PIX. Aplique-os em uma base do usuário per. baseada no perfil de usuário no server. O TACACS+ exige autenticação e autorização. O RADIUS exige apenas a autenticação. Neste exemplo, a autenticação externa e a autorização ao TACACS+ são mudadas. Uma lista de acessos no PIX estabelece-se.

Nota: Na versão de PIX 6.0.1 e mais atrasado, se você usa o RAIO, as Listas de acesso são executadas incorporando a lista ao atributo de IETF RADIUS padrão 11 (ID de filtro) [CSCdt50422]. Neste exemplo, o atributo 11 é ajustado a 115 no lugar de fazer a verbosidade específico de fornecedor de "acl=115".

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

Nota: A versão 2.1 do freeware TACACS+ não reconhece a verbosidade de "acl".

Configuração do servidor segura de Cisco UNIX TACACS+

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

Cisco Windows seguro TACACS+

A fim adicionar a autorização ao PIX controlar onde o usuário vai com Listas de acesso, verifique o **shell/executivo**, verifique a **caixa de lista de controle de acesso**, e preencha o número (combina o access list number no PIX).

Cisco Secure UNIX RADIUS

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

Windows RADIUS seguro de Cisco

RADIUS/Cisco é o tipo de dispositivo. As necessidades de usuário do “pixa” um username, uma senha, e uma verificação e um "acl=115" na caixa retangular Cisco/radius onde diz o par AV 009\001 (específico de fornecedor).

Saída

O usuário externo “pixa” com o "acl=115" no perfil autentica e autoriza. O server passa abaixo do acl=115 ao PIX, e o PIX mostra este:

```
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 a 99.99.99.3 (ou a todo o endereço IP de Um ou Mais Servidores Cisco ICM NT exceto 99.99.99.2, porque há um implícito nega), o usuário vê este:

```
Error: acl authorization denied
```

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

No Software Release 6.2 e Mais Recente do PIX Firewall, as Listas de acesso são definidas em um Access Control Server (ACS) para transferir ao PIX após a autenticação. Isto trabalha somente com o protocolo de raio. Não é necessário configurar a lista de acesso no próprio PIX. Um molde do grupo é aplicado aos usuários múltiplos.

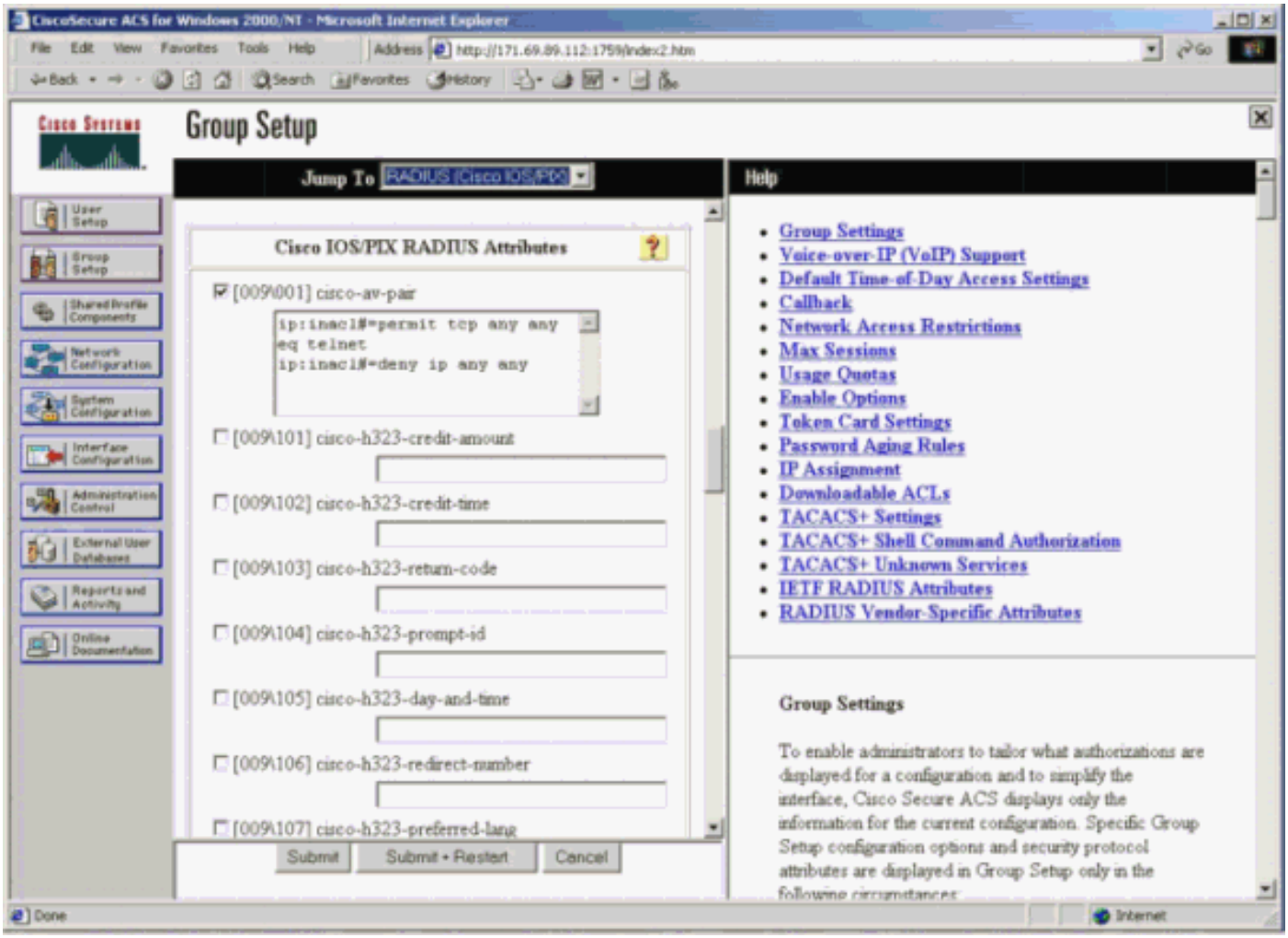
Nas versões anterior, a lista de acessos é definida no PIX. Em cima da autenticação, o ACS

empurrou o nome da lista de acessos para o PIX. A nova versão permite que o ACS empurre a lista de acessos diretamente para o PIX.

Nota: Se o Failover ocorre, a tabela do uauth não é usuários copiados reauthenticated. A lista de acessos é transferida outra vez.

Instalação do ACS

Clique a **instalação de grupo** e selecione o tipo de dispositivo do **RAIO (Cisco IOS/PIX)** para estabelecer uma conta de usuário. Atribua um username (“cse”, neste exemplo) e a senha para o usuário. Da lista de atributos, selecione a opção para configurar vendedor-AV-**pares [009\001]**. Defina a lista de acessos como ilustrado neste exemplo:



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

- Permite somente o telnet e nega o 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 o telnet e permite o 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

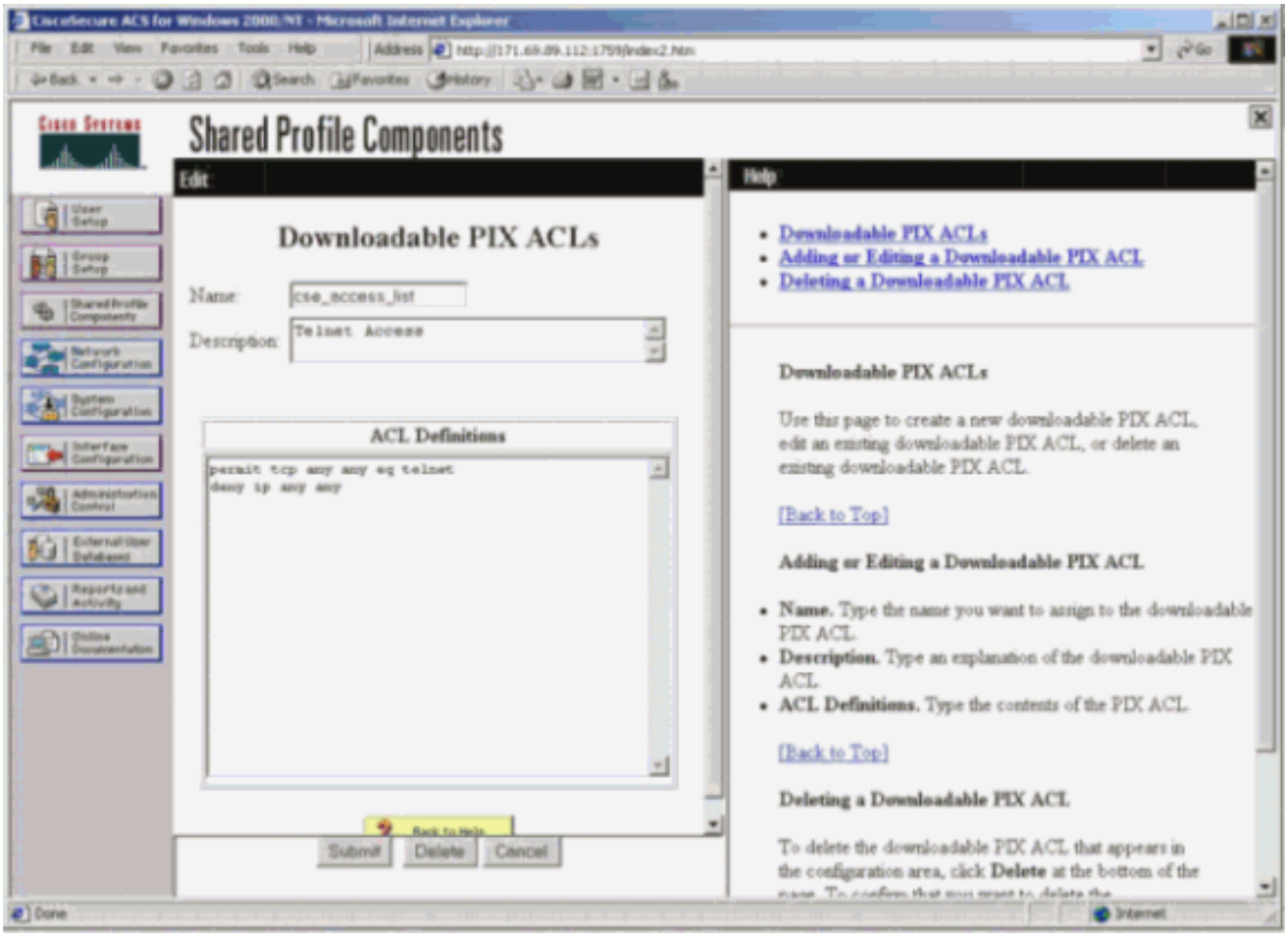
No ACS versão 3.0, o componente de perfil compartilhado permite que o usuário crie um modelo de lista de acesso e defina o nome do modelo para especificar usuários ou grupos. O nome de molde pode ser usado com tantos como usuários ou grupos como necessário. Isto elimina a necessidade de configurar Listas de acesso idênticas para cada usuário.

Nota: Se o Failover ocorre, o uauth não está copiado ao PIX secundário. Na comutação classificada, a sessão é sustentada. Contudo, a nova conexão deve ser reauthenticated e a lista de acessos deve ser transferida outra vez.

Usando perfis compartilhados

Termine estas etapas quando você usa perfis compartilhados.

1. Clique em Interface Configuration.
2. Verifique o **nível de usuário ACL carregável** e/ou o Grupo-**nível ACL carregável**.
3. Clique **componentes de perfil compartilhado**. Clique o **nível de usuário ACL carregável**.
4. Defina os ACLs que podem ser descarregados via download.
5. Clique a **instalação de grupo**. Sob ACL carregável, atribua a lista de acessos PIX à lista de acessos criada mais
   cedo.



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

- Permite somente o telnet e nega o 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 o telnet e permite o 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 a contabilidade

TACACS (AuthInbound=tacacs)

Adicionar este 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 os novos recursos em 5.2 para definir o que deve ser explicado por Listas de acesso.

aaa accounting match 101 outside AuthInbound

Nota: A lista de acessos 101 é definida separadamente.

RAIO (AuthOutbound=radius)

Adicionar este 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 os novos recursos em 5.2 para definir o que deve ser explicado por Listas de acesso.

aaa accounting match 101 outside AuthOutbound

Nota: A lista de acessos 101 é definida separadamente.

Nota: Os registros de contabilidade podem ser gerados para sessões administrativas no PIX que parte do código PIX 7.0.

Exemplos de relatórios

- Exemplo de relatório TACACS para o telnet de 99.99.99.2 fora a 172.18.124.114 para 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 a conexão de 172.18.124.114 para dentro a 99.99.99.2

fora de (telnet) e a 99.99.99.3 fora (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 decide que um origem específica ou um destino não precisam a autenticação, a autorização, ou explicar, emita estes 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

Nota: Você já tem os **comandos include**.

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

Ou, com os novos recursos em 5.2, defina o que você quer 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 exclui uma caixa da autenticação e você tem a autorização sobre, você deve igualmente excluir a caixa da autorização.

Sessões máx. e usuários que fez login da vista

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. Contudo, isto não trabalha bem para o HTTP. Neste exemplo, uma configuração de rede diferente é usada, mas os conceitos são os mesmos.

Usuário Telnets com o PIX, autenticando na maneira.

```
(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
```

Porque o server não viu um registro do “começo” mas nenhum registro da “parada”, neste momento, o server mostra que o usuário do “telnet” está entrado. Se o usuário tenta uma outra conexão que exija a autenticação (talvez de um outro PC), e se as sessões máx. estão ajustadas a "1" no server para este usuário (que supõe as sessões máx. dos suportes de servidor), a conexão está recusada pelo server. O usuário vai aproximadamente seu telnet ou negócio FTP no host de destino, a seguir nas saídas (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. Está aqui um exemplo de HTTP onde o usuário consulta de 171.68.118.100 a 9.9.9.25 com o 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 é entrado ao site. A conexão não está aberta quando o usuário está lendo o página da web. As sessões máx. ou os usuários que fez login da vista não trabalham aqui. Isto é porque o tempo de conexão (o tempo entre “construído” e o “Teardown”) no HTTP é demasiado curto. O registro “start” (iniciar) e “stop” (parar) é sub-segundo. Não há nenhum registro do “começo” sem um registro da “parada” desde que os registros ocorrem virtualmente no mesmo instante. Há ainda um registro do “começo” e da “parada” enviado ao server para cada transação se o uauth está ajustado para 0 ou algo maior. Contudo, as sessões máx. e os usuários que fez login da vista não trabalham devido às naturezas da conexão de HTTP.

Interface de usuário

Mude os usuários imediatos veem

Se você tem o comando:

auth-prompt prompt PIX515B

então os usuários que atravessam o PIX veem esta alerta.

PIX515B

Personalize os usuários da mensagem veem

Se você tem os comandos:

auth-prompt accept "GOOD_AUTHENTICATION" auth-prompt reject "BAD_AUTHENTICATION"
então os usuários veem uma mensagem sobre o status de autenticação em um login bem-sucedido/falha no login.

```
  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 TACACS+/autorização está ligada, esta está controlada em uma base do usuário per. Este perfil de usuário estabelece-se para controlar o intervalo (este está no programa gratuito de servidor TACACS+ e os intervalos realizam-se nos 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 fim de dois minutos:

Timeout absoluto - a sessão obtém rasgada para baixo:

```
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

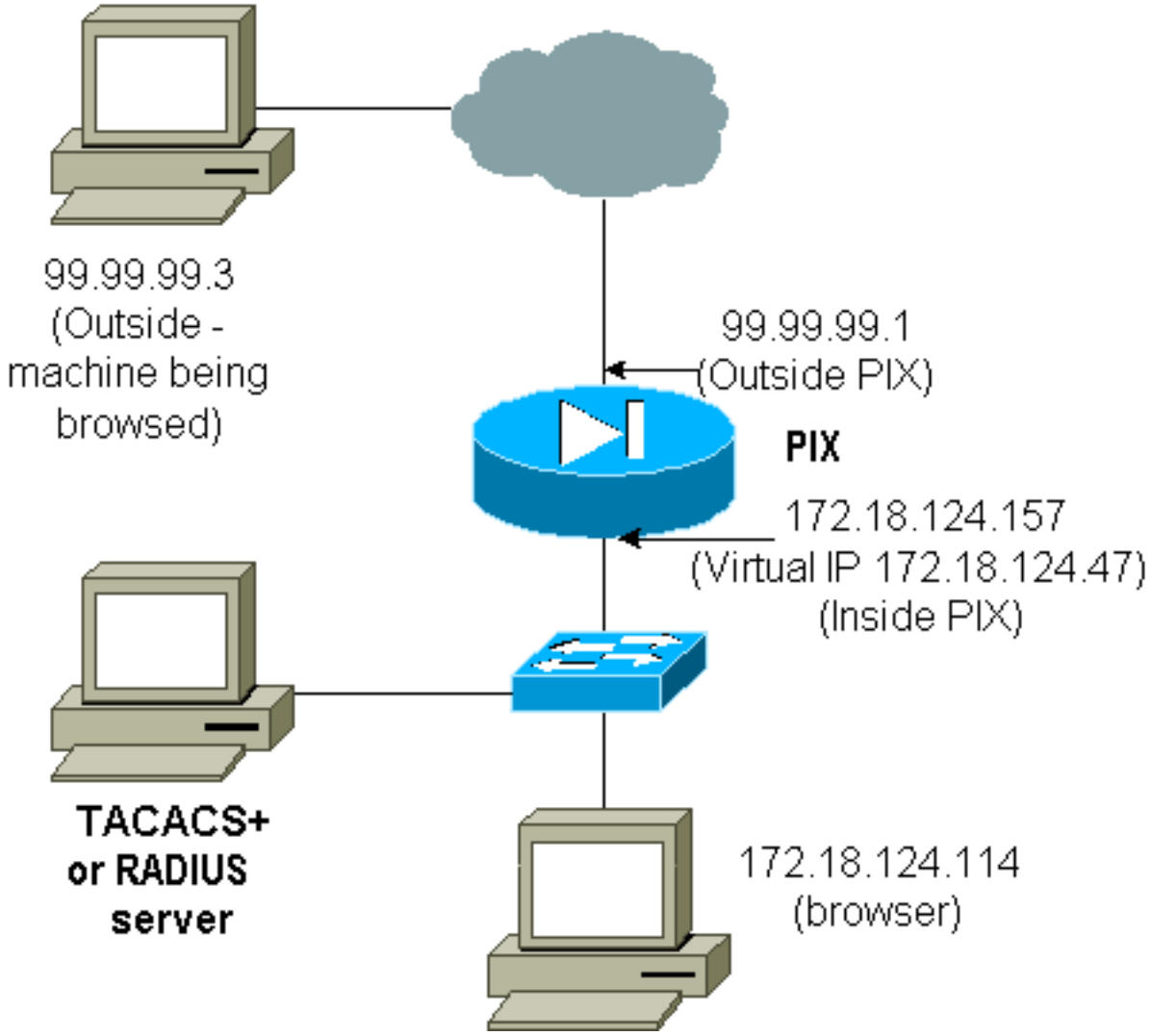
Se a autenticação é exigida em locais fora do PIX assim como no PIX próprio, o comportamento incomum do navegador está observado às vezes, desde que os navegadores põem em esconderijo o nome de usuário e senha.

A fim evitar isto, execute o HTTP virtual adicionando um endereço do RFC 1918 (um endereço irrastreável no Internet, mas válido e original para a rede interna PIX) à configuração de PIX no formato.

virtual http #.#.#.# <warn>
Quando o usuário tenta sair do PIX, a autenticação é necessária. Se o parâmetro de advertência estiver presente, o usuário recebe uma mensagem redirecionada. A autenticação é boa para a durante o tempo do uauth. Como indicado na documentação, não ajuste a duração do **comando**

timeout uauth aos segundos 0 com HTTP virtual. isso evita conexões de HTTP ao servidor da Web real.

Nota: O HTTP e os endereços IP telnet virtuais virtuais devem ser incluídos nas **instruções de autenticação aaa**. Neste exemplo, especificar 0.0.0.0 inclui estes endereços.



Na configuração de PIX adicionar este comando.

```
virtual http 172.18.124.47
```

O usuário aponta o navegador em 99.99.99.3. Esta mensagem é indicada.

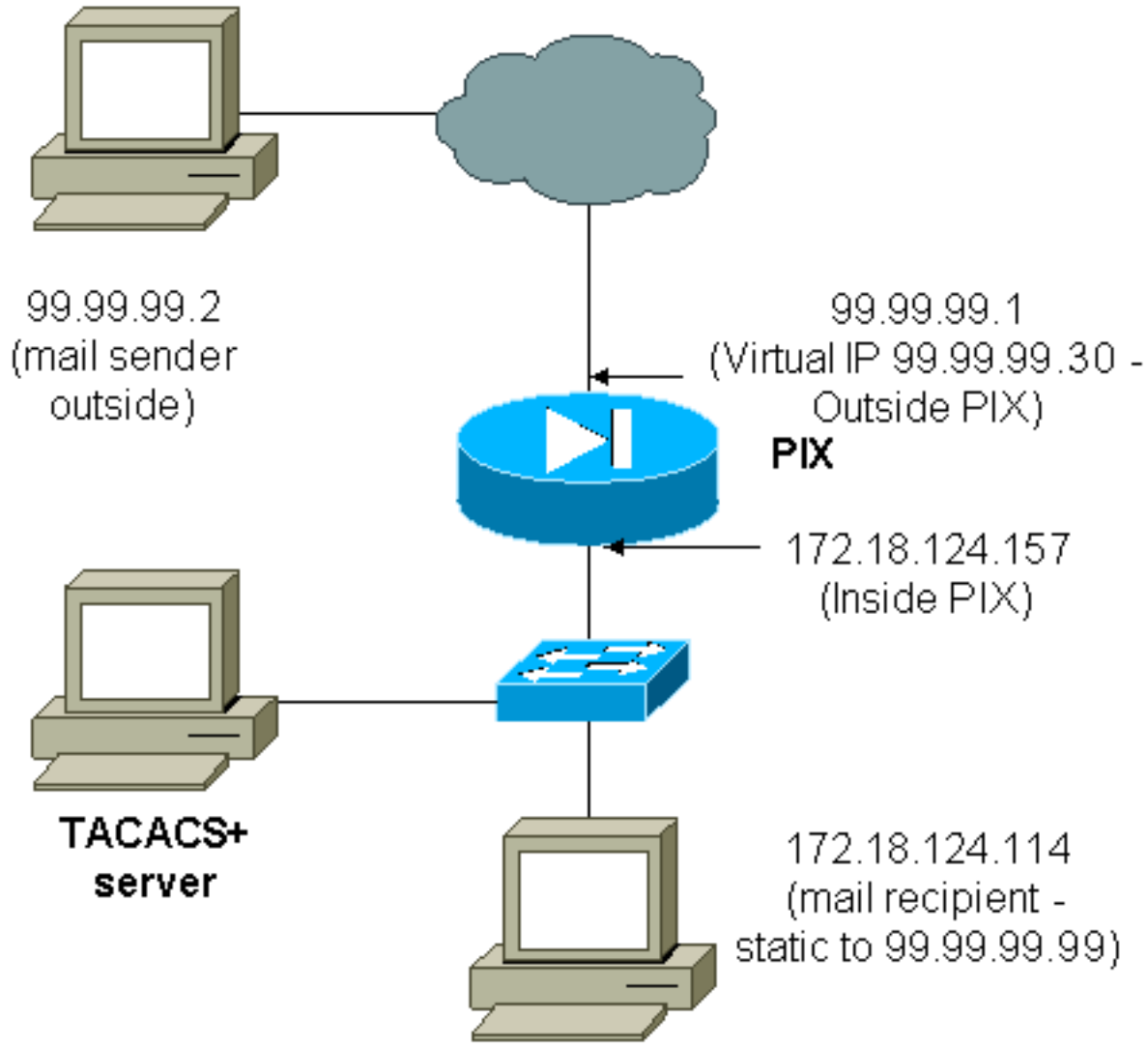
```
Enter username for PIX515B (IDXXX) at 172.18.124.47
```

Após a autenticação, o tráfego é reorientado a 99.99.99.3.

Telnet Virtual

Nota: O HTTP e os endereços IP telnet virtuais virtuais devem ser incluídos nas **instruções de autenticação aaa**. Neste exemplo, especificar 0.0.0.0 inclui estes endereços.

Entrada de Telnet Virtual



Não é uma ótima ideia autenticar o correio de entrada desde que um indicador não é indicado para que o correio seja enviado a de entrada. Use o **comando exclude** pelo contrário. Mas para o objetivo de ilustração, estes 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 freeware TACACS+):

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


user = pixuser {
login = cleartext "pixuser"
service = exec {
```

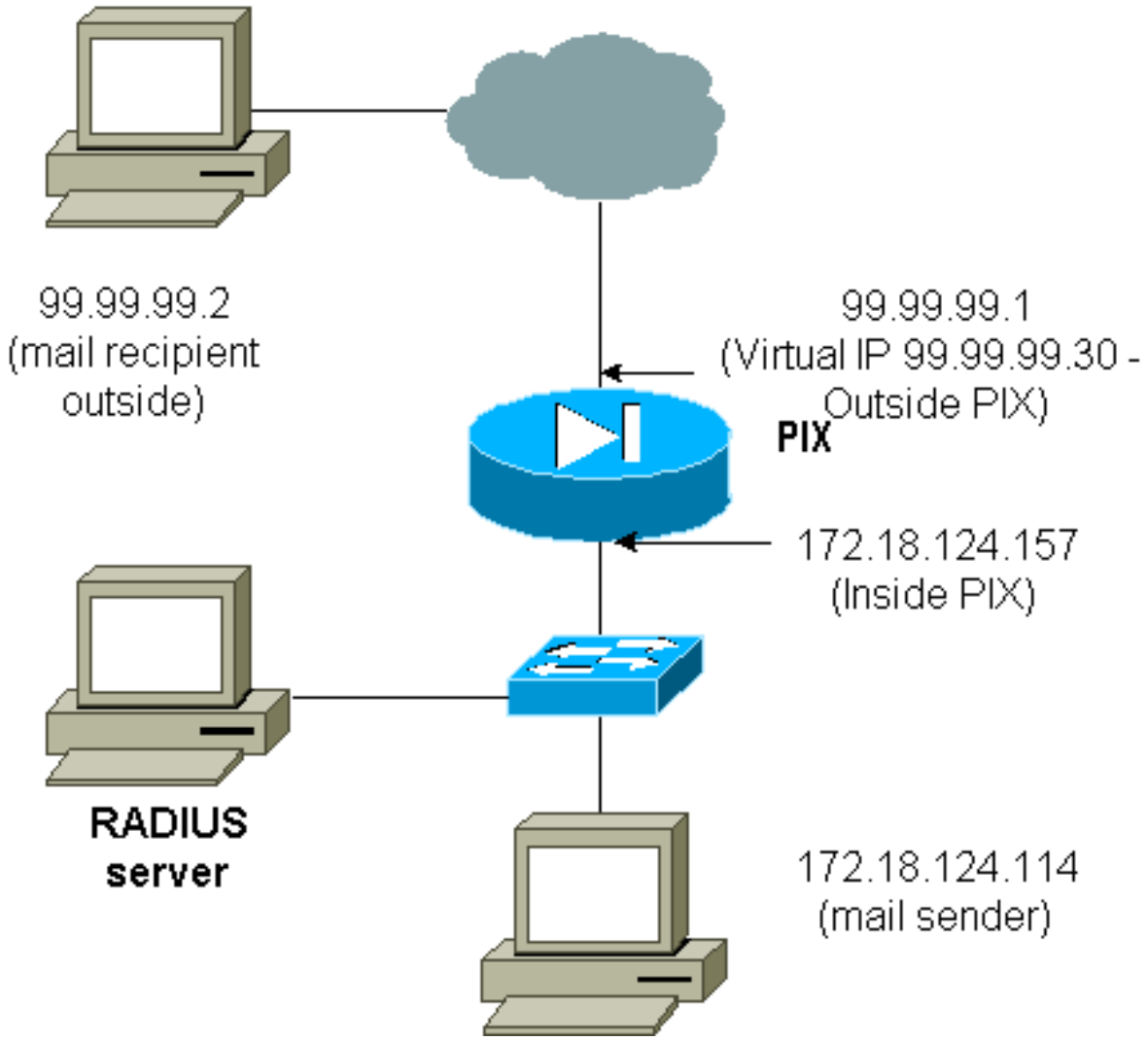
```
  }
  cmd = telnet {
  permit .*
  }
  }
```

Se somente a autenticação está ligada, ambos os usuários enviam o correio de entrada após a autenticação em um telnet ao endereço IP 99.99.99.30. Se a autorização é permitida, o usuário “cse” Telnets a 99.99.99.30, e incorpora o username TACACS+/senha. As gotas da conexão Telnet. O usuário “cse” envia então o correio a 99.99.99.99 (172.18.124.114). A autenticação sucede para o usuário “pixuser”. Contudo, quando o PIX envia o pedido de autorização para cmd=tcp/25 e cmd-arg=172.18.124.114, o pedido falha, segundo as indicações desta 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 ótima ideia autenticar o correio de entrada desde que um indicador não é indicado para que o correio seja enviado a de entrada. Use o **comando exclude** pelo contrário. Mas para o objetivo de ilustração, estes comandos são adicionados.

Não é uma ótima ideia autenticar o correio de partida desde que um indicador não é indicado para que o correio seja enviado a de partida. Use o **comando exclude** pelo contrário. Mas para fins da ilustração, estes 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.
```

A fim enviar do interior o correio a fora, traga acima um comando prompt no host de correio e o telnet a 99.99.99.30. Isto abre o furo para que o correio vá completamente. O correio é enviado de 172.18.124.114 a 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. Isto 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

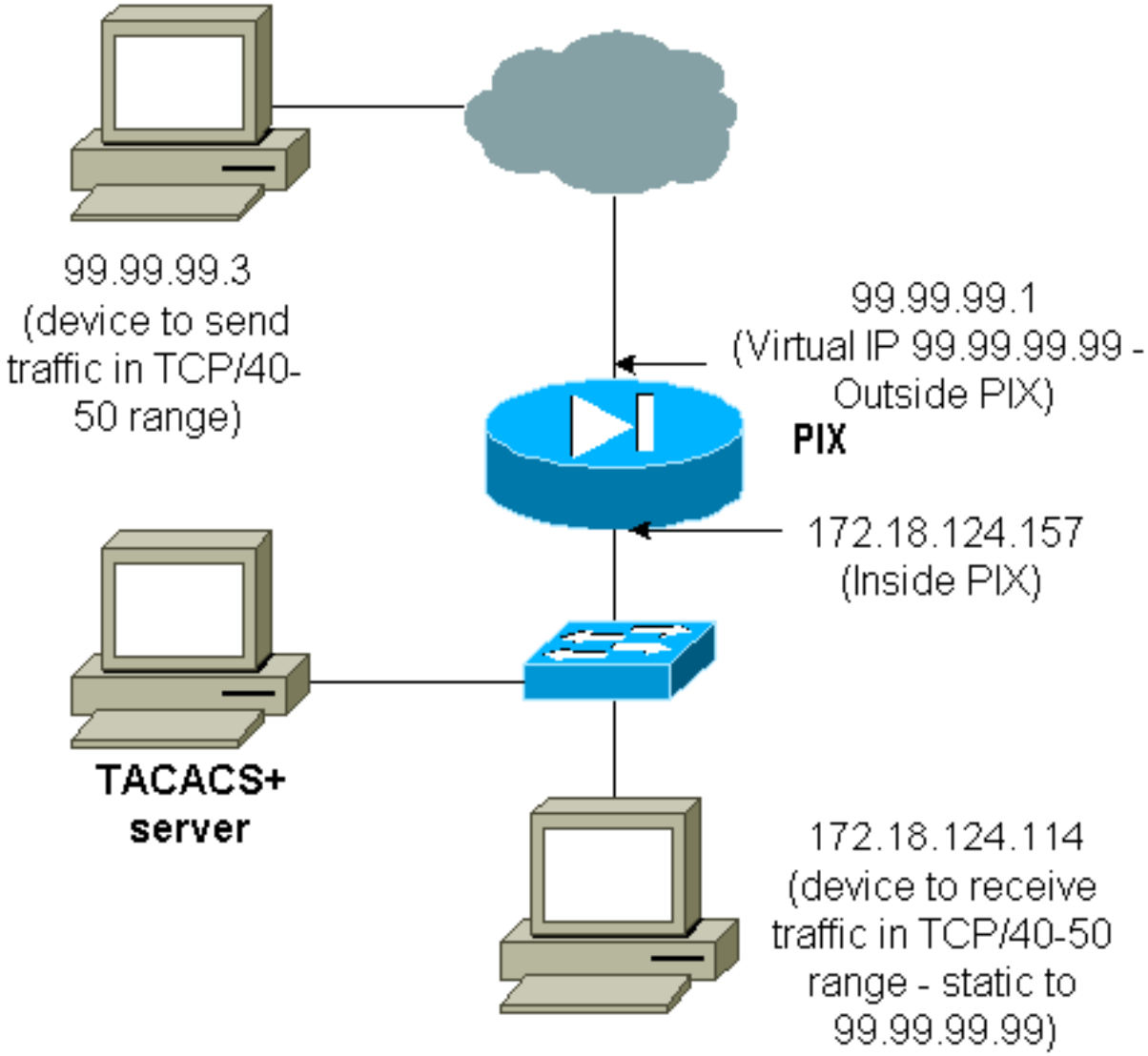
```
   pixfirewall#109001: Auth start for user 'cse' from 172.18.124.114/32863 to 99.99.99.30/23
109005: Authentication succeeded for user 'cse' from 172.18.124.114/32863 to 99.99.99.30/23 on
interface inside
```

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 está configurado no PIX, e a autorização está configurada para uma faixa de porta, o usuário abre o furo com 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 porta.

```
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 de 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 na escala da porta 40-50 com o PIX para 99.99.99.99 (172.18.124.114), cmd=tcp/40-50 é enviado ao server TACACS+ com cmd-

arg=172.18.124.114 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 que você se certifica de trabalhos do telnet virtual permitir o tráfego TCP/40-50 ao host dentro da rede, adicionar esclarecer este tráfego com estes 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+

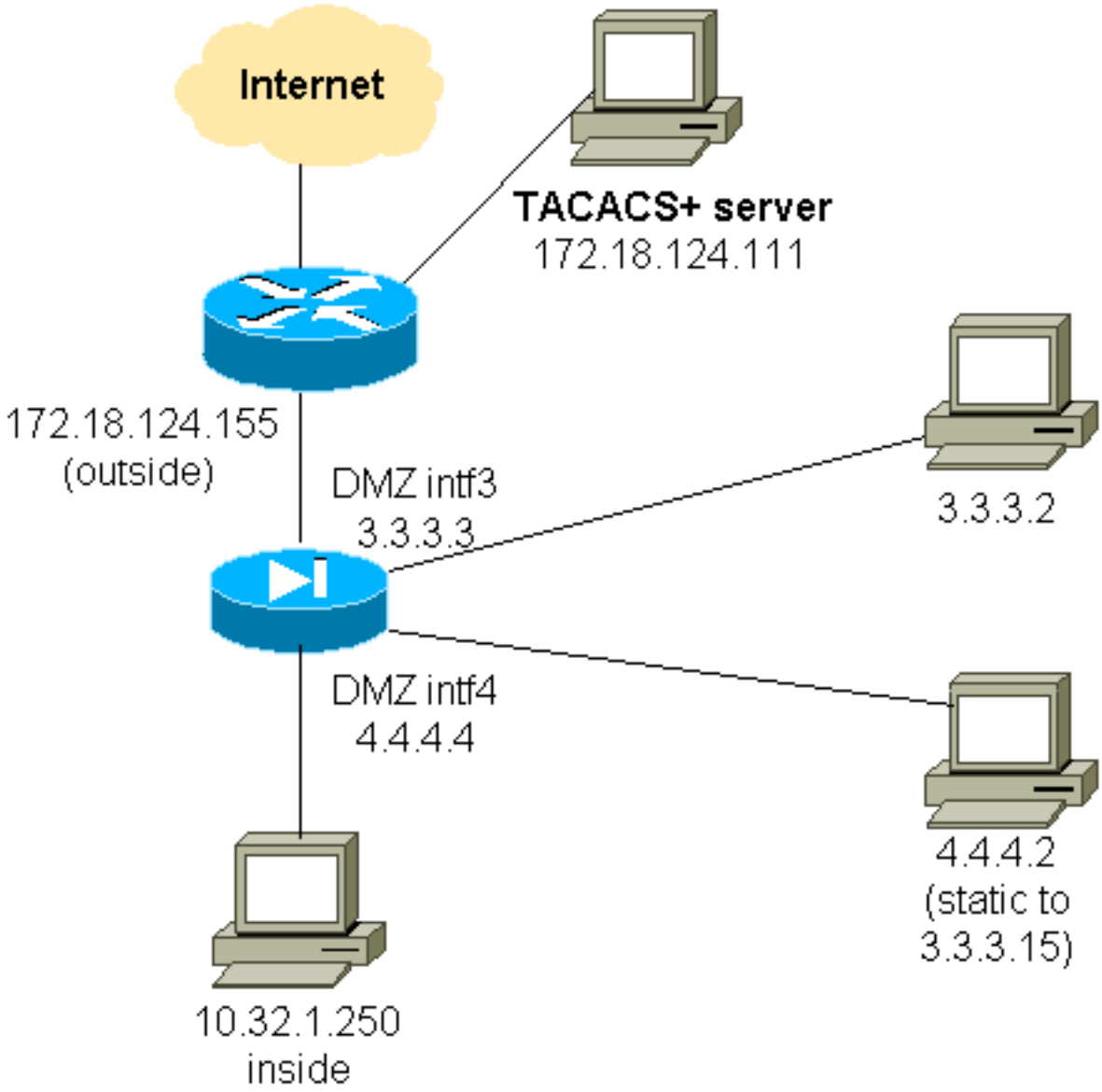
```
Thu Aug 24 08:06:09 2000 172.18.124.157 cse PIX 99.99.99.3
start task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
cmd=tcp/40-50
Thu Aug 24 08:06:17 2000 172.18.124.157 cse PIX 99.99.99.3
stop task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
cmd=tcp/40-50 elapsed_time=8 bytes_in=80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

Autenticação no DMZ

A fim autenticar os usuários que vão de uma relação DMZ a outra, diga o PIX para autenticar o tráfego para as interfaces nomeada. No PIX, o arranjo é como este:

```
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 do 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 precisa o auxílio após ter seguido os passos de Troubleshooting acima e o quer abrir um caso com o tac Cisco, seja certo incluir esta informação para pesquisar defeitos seu PIX Firewall.
• Descrição do problema e detalhes relevantes de topologia • Pesquise defeitos antes que você abra o caso • Saída do **comando show tech-support** • Saída do **comando show log** depois que você é executado 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 a informação a seu caso transferindo arquivos pela rede o com a ajuda da ferramenta do Case Query (clientes registrados somente). Se você é incapaz de alcançar a ferramenta do Case Query, envie a informação em um anexo de Email a attach@cisco.com com seu número de caso na linha de assunto de 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
- Terminal Access Controller Access Control System (TACACS+)
- Remote Authentication Dial-In User Service (RADIUS)
- Suporte Técnico e Documentação - Cisco Systems