Verificatie, autorisatie en accounting van gebruikers uitvoeren via PIX versies 5.2 en hoger

Inhoud

Inleiding

RADIUS- en TACACS+ verificatie kunnen worden uitgevoerd voor FTP, telnet en HTTP-verbindingen via de Cisco Secure PIX-firewall. Verificatie voor andere minder gebruikelijke protocollen wordt meestal uitgevoerd om te werken. De TACACS+-vergunning wordt ondersteund. RADIUS-autorisatie wordt niet ondersteund. Veranderingen in PIX 5.2 authenticatie, autorisatie en accounting (AAA) via de eerdere versie omvatten ondersteuning van AAA toegangslijst om te controleren wie geauthentificeerd is en welke bronnen de gebruiker toegang heeft. In PIX 5.3 en later is de verificatie, autorisatie en accounting (AAA) verandering in eerdere versies van code dat de RADIUS poorten configureerbaar zijn.

OPMERKING: PIX 6.x kan wel verantwoordelijk zijn voor doorgifte door het verkeer, maar niet voor verkeer dat naar de PIX wordt overgeheveld.

Voorwaarden

Vereisten

Er zijn geen specifieke voorwaarden van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- Cisco Secure PIX-firewall softwareversies 5.2.0.205 en 5.2.0.207

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

N.B.: Als u PIX/ASA software versie 7.x en later gebruikt, raadpleeg dan AAA-servers en de Local Database.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Verificatie, autorisatie en accounting

Hier is een verklaring voor verificatie, autorisatie en accounting:

- Verificatie is wie de gebruiker is.
- autorisatie is wat de gebruiker doet.
- Verificatie is geldig zonder vergunning.
- Vergunning is niet geldig zonder echtheidscontrole.
- Accounting is wat de gebruiker heeft gedaan.

Wat de gebruiker ziet met verificatie/autorisatie op

Wanneer de gebruiker probeert van binnen naar buiten te gaan (of omgekeerd) met authenticatie/autorisatie op:

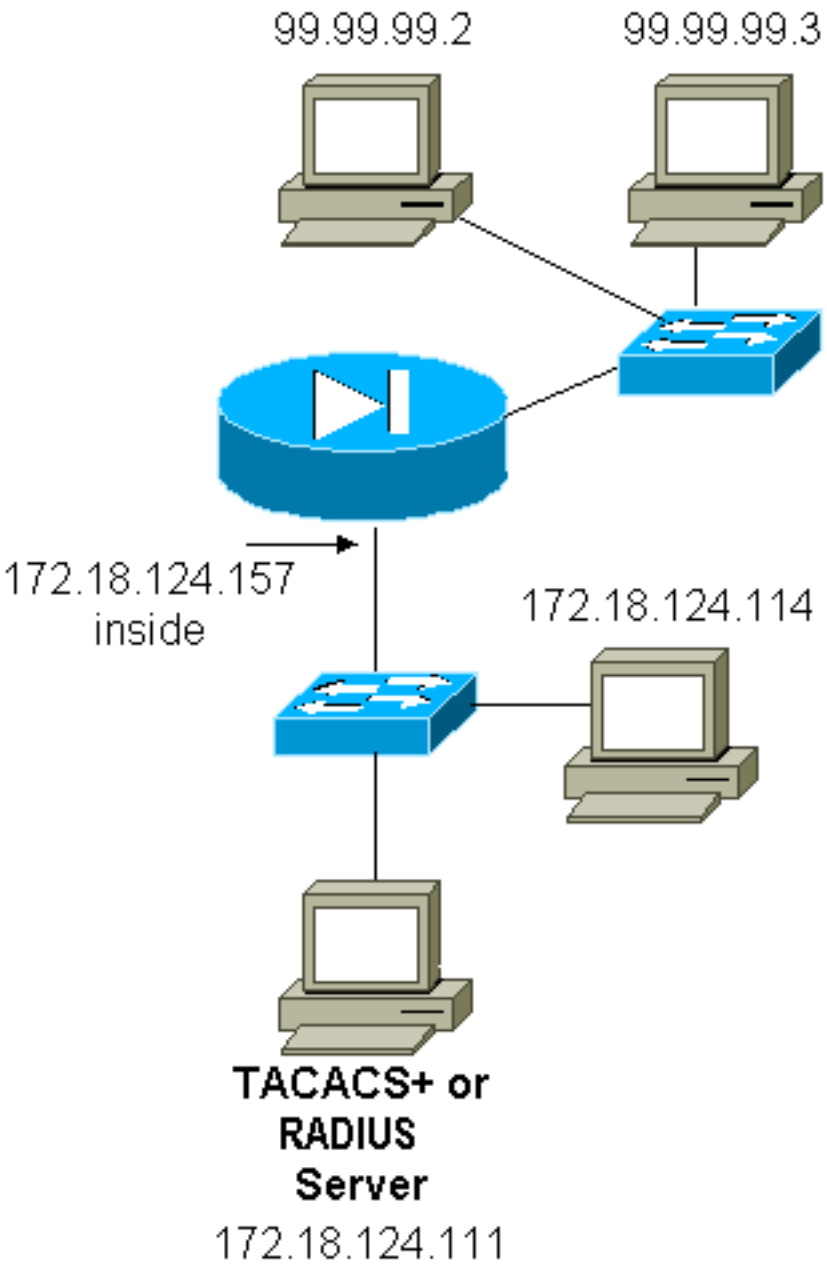
- **Telnet**-De gebruiker ziet een gebruikersnaam voor het wachtwoord verschijnen en een verzoek om een wachtwoord. Als verificatie (en autorisatie) succesvol is op de PIX/server, wordt de gebruiker voor gebruikersnaam en wachtwoord gevraagd door de doelhost.
- **FTP**-De gebruiker ziet een gebruikersnaam voor de melding verschijnen. De gebruiker moet "local_username@remote_username" voor gebruikersnaam en "local_password@remote_password" voor wachtwoord invoeren. De PIX stuurt de "local_gebruikersnaam" en "local_password" naar de lokale beveiligingsserver. Als verificatie (en autorisatie) succesvol is op de PIX/server, worden de "Remote_gebruikersnaam" en "Remote_password" doorgegeven naar de bestemmFTP server.
- **HTTP**-A venster wordt in de browser weergegeven met het verzoek om gebruikersnaam en wachtwoord. Als authenticatie (en autorisatie) succesvol is, arriveert de gebruiker op de bestemmingspruct. Houd in gedachten dat *browsers gebruikersnamen en wachtwoorden in het geheugen onderbrengen.* Als blijkt dat de PIX een HTTP-verbinding moet uitweiden maar dit niet doet, is het waarschijnlijk dat er een nieuwe verificatie plaatsvindt met de browser "schietend" de gecached gebruikersnaam en wachtwoord op de PIX. De PIX stuurt dit naar de authenticatieserver. PIX syslog en/of server debug toont dit fenomeen. Als telnet en FTP "normaal" lijken te werken, maar HTTP-verbindingen niet, is dit de reden.

Afluisterstappen

- Zorg ervoor dat de PIX-configuratie werkt voordat u AAA-verificatie en -autorisatie toevoegt. Indien u niet in staat bent om het verkeer door te geven voordat u de echtheidscontrole en de autorisatie instelt, kunt u dit achteraf niet meer doen.
- Laat wat houtkap in de PIX toe.Geef de **houtkapconsole uit** opdracht om het foutoptreden van de houtkapconsole aan te zetten.**Opmerking:** Gebruik de houtkapconsole niet voor het foutoptreden op een zwaar geladen systeem.Gebruik de **houtkapmonitor** opdracht om een Telnet-sessie te loggen.Het registreren van gebufferde debugging kan worden gebruikt, en dan de opdracht **tonen registreren** uitvoeren.Vastlegging kan ook naar een syslogserver worden verzonden en daar worden onderzocht.
- Zet de debugging aan op de TACACS+ of RADIUS servers.

Alleen verificatie

Netwerkdiagram



Setup servers - alleen verificatie

Cisco Secure UNIX-TACACS-serverconfiguratie

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

Cisco Secure UNIX-RADIUS-serverconfiguratie

OPMERKING: Voeg het PIX IP-adres en de sleutel toe aan de NAS-lijst (Network Access Server) met behulp van de geavanceerde GUI.

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

Cisco Secure Windows RADIUS

Gebruik deze stappen om een Cisco Secure Windows RADIUS-server in te stellen.

1. Wachtwoord verkrijgen in het gedeelte **Gebruikersinstelling**.
2. Stel eigenschap 6 (servicetype) in op **aanmelding** of **administratie** in uit het gedeelte **Groepsinstallatie**.
3. Voeg het PIX IP-adres toe in het gedeelte **NAS Configuration** van de GUI.

Cisco Secure Windows TACACS+

De gebruiker krijgt een wachtwoord in het gedeelte **Gebruikersinstelling**.

Configuratie van Livingston RADIUS-server

OPMERKING: Voeg PIX IP-adres en -toets toe aan het *clientbestand*.

- wachtwoord voor wet="foo" gebruiker-service-type = Shell-gebruiker

Configuratie van RADIUS-server Merken

OPMERKING: Voeg PIX IP-adres en -toets toe aan het *clientbestand*.

- Wachtwoord voor biljet="foo" Service-type = Shell-gebruiker

Configuratie van TACACS+ vriesserver

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

PIX Eerste configuratie - alleen verificatie

PIX Eerste configuratie - alleen verificatie

`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
```

Configureerbare RADIUS-poorten (5.3 en later)

Sommige RADIUS-servers gebruiken RADIUS-poorten anders dan 1645/1646 (gewoonlijk 1812/1813). In PIX 5.3 en hoger kunnen de RADIUS-verificatie en -accounting poorten worden gewijzigd in iets anders dan standaard 1645/1646 met deze opdrachten:

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

PIX-verificatie debug-voorbeelden

Zie Debugging Stappen voor informatie over hoe te om het debuggen aan te zetten. Dit zijn

voorbeelden van een gebruiker op 99.99.99.2 die het verkeer initieert naar 172.18.124.114 (99.99.99.99) en omgekeerd. Het inkomende verkeer is TACACS-geauthentiseerd en het uitgaande is RADIUS-geauthentiseerd.

Succesvolle verificatie - TACACS+ (inkomende versie)

```
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)
```

Onsuccesvolle verificatie door slechte gebruikersnaam/wachtwoord - TACACS+ (inkomende versie). De gebruiker ziet "Fout: Max. aantal overschrijdingen."

```
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
```

Server die niet op PIX spreekt - TACACS+ (inkomende). Gebruiker ziet éénmaal een gebruikersnaam en PIX vraagt nooit om een wachtwoord (dit is te zien op telnet). Gebruiker ziet "Fout: Max. aantal overschrijdingen."

```
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
```

Goede authenticatie - RADIUS (uitgaande)

```
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
```

Slechte verificatie (gebruikersnaam of wachtwoord) - RADIUS (uitgaande). Gebruiker ziet een aanvraag voor een gebruikersnaam en Wachtwoord heeft drie mogelijkheden om deze in te voeren. Als dit niet lukt, zie "Fout: Max. aantal overschrijdingen."

```
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
```

Pingable maar daemon-down server, pingable server of key/client-mismatch van de server zullen niet communiceren met PIX - RADIUS (uitgaande). Gebruiker ziet Gebruikersnaam, dan wachtwoord, dan "RADIUS-server is mislukt" en tenslotte "Fout: Max. aantal overschrijdingen."

```
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
```

Verificatie plus autorisatie

Als u alle geauthenticeerde gebruikers wilt toestaan om alle bewerkingen (HTTP, FTP en telnet) door de PIX uit te voeren, is verificatie voldoende en autorisatie niet nodig. Als u echter bepaalde deeldiensten aan bepaalde gebruikers wilt toestaan of de gebruikers wil beperken tot bepaalde locaties, is een vergunning nodig. RADIUS-autorisatie is niet geldig voor verkeer door de PIX. De TACACS+-vergunning is in dit geval geldig.

Als de authenticatie passeert en de autorisatie is geactiveerd, verstuurt de PIX de opdracht die de gebruiker aan de server doet. Bijvoorbeeld "http 1.2.3.4". In versie 5.2 van PIX wordt de TACACS+-vergunning gebruikt in combinatie met toegangslijsten om te controleren waar de gebruikers naartoe gaan.

Als u een vergunning voor HTTP wilt implementeren (bezochte websites), gebruikt u software zoals WebSense, aangezien één enkele website een groot aantal IP-adressen aan deze website kan gekoppeld hebben.

Setup servers - Verificatie en autorisatie

Cisco Secure UNIX-TACACS-serverconfiguratie

```
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+

Voltooi deze stappen om een Cisco Secure Windows TACACS+ server in te stellen.

1. Klik op **Deny niet-afgesloten IOS-opdrachten** onder in de groepsinstellingen.
2. Klik op **Toevoegen/Bewerken Nieuwe opdracht (FTP, HTTP, telnet)**.Als u bijvoorbeeld telnet aan een specifieke site ("telnet 1.2.3.4") wilt toestaan, is de opdracht **telnet**. Het argument is *1.2.3.4.* Vul na het invullen van "opdracht=**telnet**" het IP-adres(en) van de vergunning in in de woordenschat (bijvoorbeeld "vergunning 1.2.3.4"). Als alle telnetten moeten worden toegestaan, is de opdracht nog **telnet**, maar klik op **Sta alle niet vermelde argumenten toe**. Klik vervolgens op **Bewerken opdracht voltooien**.
3. Voer stap 2 uit voor elk van de toegestane opdrachten (bijvoorbeeld telnet, HTTP en FTP).
4. Voeg het PIX IP-adres toe in het gedeelte NAS Configuration met de hulp van de GUI.

Configuratie van TACACS+ vriesserver

```
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 .*
   }
   }
```

PIX-configuratie - Toelevering

Voeg opdrachten toe om toestemming te vereisen:

```
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
```

Met de nieuwe 5.2-functie kan deze verklaring in combinatie met de eerder gedefinieerde toegangslijst 101 de vorige drie verklaringen vervangen. Het oude en nieuwe gemiddelde moet niet worden gemengd.

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

PIX-verificatie en -autorisatie debug-voorbeelden

Goede verificatie en autorisatie slagen - 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)
```

Goede authenticatie maar autorisatie faalt - TACACS+. Gebruiker ziet ook het bericht "Fout: autorisatie geweigerd."

```
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
```

Functie nieuwe toegangslijst

In PIX-softwarerelease 5.2 en hoger definieert u toegangslijsten in de PIX. Pas ze toe op basis van het gebruikersprofiel op de server. Voor TACACS+ is verificatie en autorisatie vereist. RADIUS vereist alleen verificatie. In dit voorbeeld worden de uitgaande verificatie en de vergunning voor TACACS+ gewijzigd. Er wordt een toegangslijst in de PIX opgesteld.

Opmerking: In PIX versie 6.0.1 en later, als u RADIUS gebruikt, worden de toegangslijsten geïmplementeerd door de lijst in te voeren in standaard RADIUS-kenmerk 11 (filter-ID) [CSCdt50422]. In dit voorbeeld wordt eigenschap 11 ingesteld op 115 in plaats van de verkoper-specifieke "acl=115"-gemiddelde te doen.

PIX-configuratie

```
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
```

serverprofielen

Opmerking: De 2.1-versie van de TACACS+-software herkent het "acl"-woordenboek niet.

Cisco Secure UNIX-serverconfiguratie voor TACACS+

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

Cisco Secure Windows TACACS+

Als u toestemming aan de PIX wilt toevoegen om te controleren waar de gebruiker gaat met toegangslijsten, **shell/exec** controleren, het vakje **Access Control List** controleren en het nummer invullen (komt overeen met het toegangslijstnummer in de PIX).

Cisco Secure UNIX-RADIUS

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

Cisco Secure Windows RADIUS

RADIUS/Cisco is het apparaattype. De "pixels"-gebruiker heeft een gebruikersnaam, een wachtwoord en een controle en "acl=115" nodig in het rechthoekige Cisco/RADIUS-vak waarin staat dat 009\001 AV-paar (leverancierspecifiek).

Uitvoer

De uitgaande gebruiker "pixels" met "acl=115" in het profiel wordt geauthentiseerd en geautoriseerd. De server passeert acl=115 naar de PIX en de PIX toont dit:

```
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
```

Wanneer de gebruiker "elfa" probeert te gaan naar 99.99.9.3 (of welk IP-adres dan ook behalve

99.9.99.2, omdat er een impliciete ontkenning is) ziet de gebruiker dit:

```
Error: acl authorization denied
```

Nieuwe downloadbare toegangslijst per gebruiker, versie 6.2

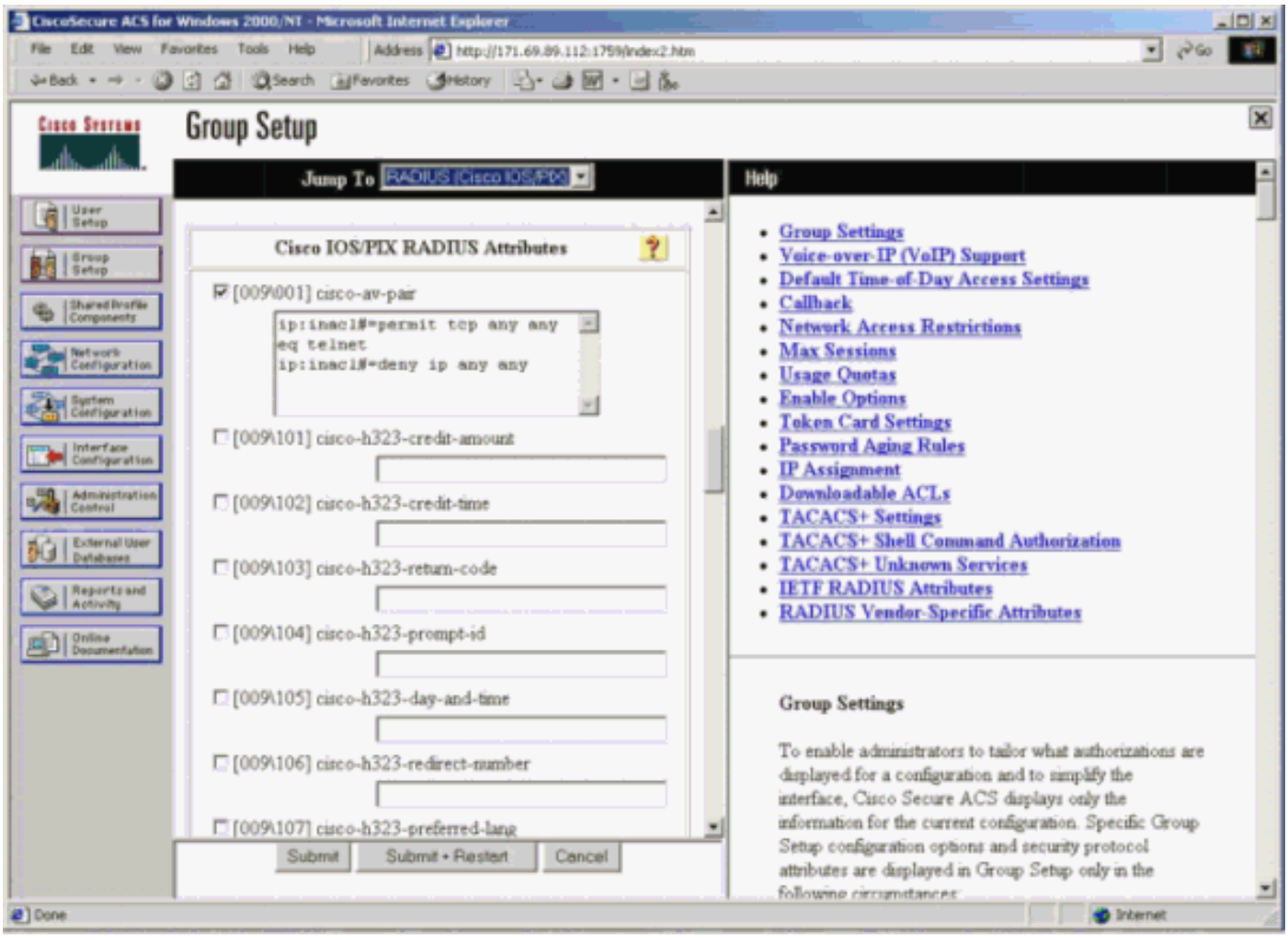
In softwarerelease 6.2 en later van de PIX-firewall worden toegangslijsten gedefinieerd op een toegangscontroleserver (ACS) die kan worden gedownload naar de PIX na verificatie. Dit werkt alleen met het RADIUS-protocol. Het is niet nodig om de toegangslijst in de PIX zelf te configureren. Een groepssjabloon is van toepassing op meerdere gebruikers.

In eerdere versies wordt de toegangslijst gedefinieerd in de PIX. Bij verificatie werd de naam van de toegangslijst door het ACS naar de PIX gedrukt. Met de nieuwe versie kunnen ACS de toegangslijst rechtstreeks naar de PIX duwen.

Opmerking: Als failover optreedt, wordt de automatische tabel niet gekopieerd. Gebruikers worden niet opnieuw geauthentiseerd. De toegangslijst wordt opnieuw gedownload.

ACS Instellen

Klik op **Group Setup** en selecteer het **RADIUS**-apparaattype **(Cisco IOS/PIX)** om een gebruikersaccount in te stellen. Pas een gebruikersnaam ("case", in dit voorbeeld) en een wachtwoord aan voor de gebruiker. Selecteer in de lijst Eigenschappen de optie om **[009\001]** ***verkoper-av*-paar** te configureren. Bepaal de toegangslijst zoals in dit voorbeeld wordt geïllustreerd:



PIX-uitwerpselen: Geldige verificatie en gedownloade toegangslijst

- Hiermee staat alleen telnet toe en ontkent u ander verkeer.

```
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)
```

  Uitvoer vanuit de opdracht **tonen**

```
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
```

  Uitvoer uit de opdracht **toegangslijst tonen**.

```
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)
```

- Ontkent alleen telnet en staat ander verkeer toe.

```
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
```

  Uitvoer vanuit de opdracht **tonen**

```
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
```

  Uitvoer uit de opdracht **toegangslijst tonen**.

```
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)
```

Nieuwe downloadbare toegangslijst per gebruiker met ACS 3.0

In ACS versie 3.0 kan de gedeelde profielcomponent de gebruiker een toegangslijstsjabloon

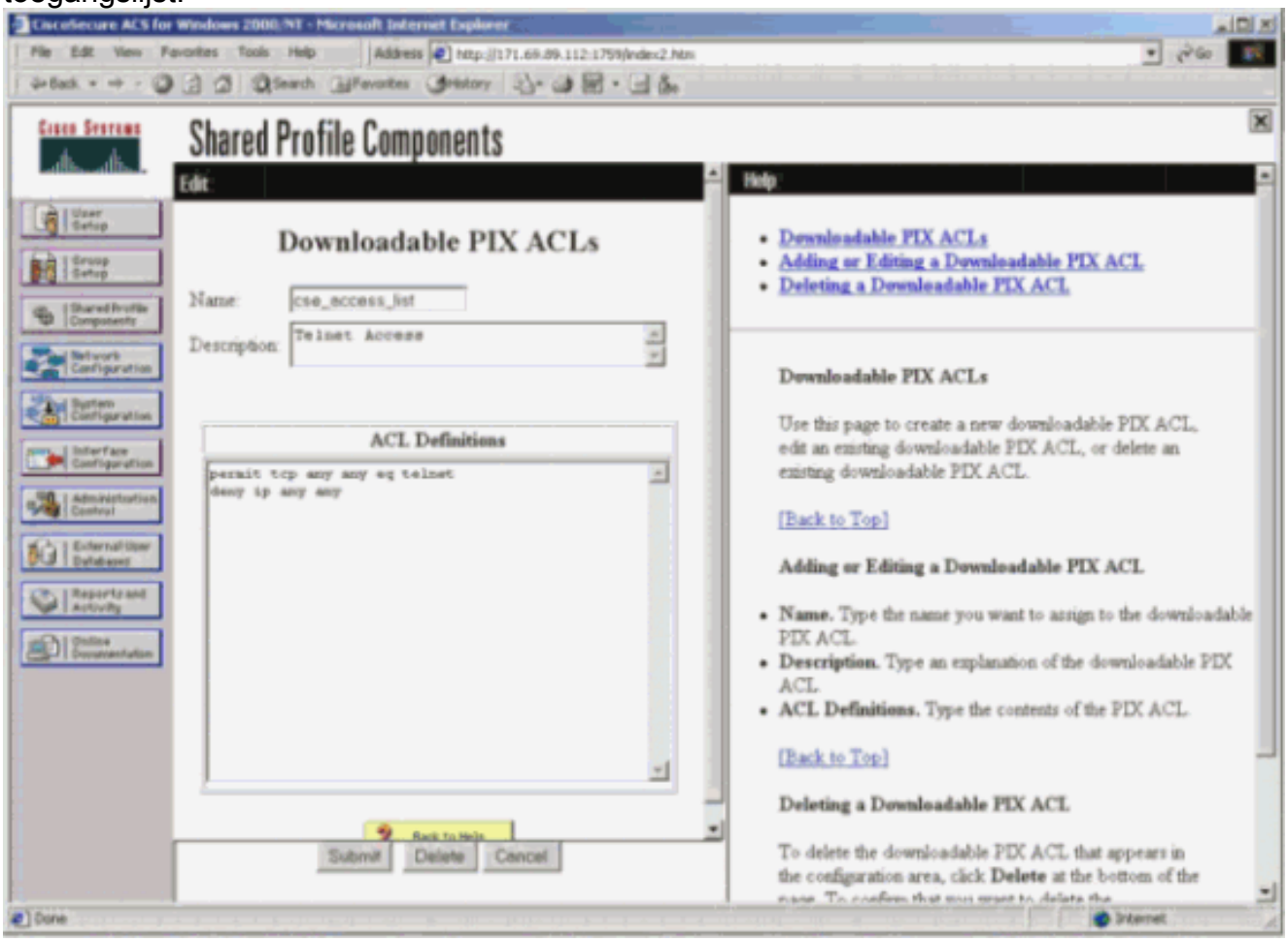
maken en de sjabloonnaam definiëren voor specifieke gebruikers of groepen. De sjabloonnaam kan indien nodig met zoveel gebruikers of groepen worden gebruikt. Dit heft de noodzaak op om identieke toegangslijsten voor elke gebruiker te configureren op.

Opmerking: Als failover optreedt, wordt uauth niet gekopieerd naar de secundaire PIX. Bij de stateful failover blijft de sessie behouden. De nieuwe verbinding moet echter opnieuw worden geauthentiseerd en de toegangslijst moet opnieuw worden gedownload.

Gedeelde profielen gebruiken

Voltooi deze stappen wanneer u gedeelde profielen gebruikt.

1. Klik op **Interface Configuration**.
2. Controleer **op gebruikersniveau downloadbare ACL's** en/of **gekleurde ACL's op groepsniveau**.
3. Klik op **Gedeelde profielen**. Klik op **USER-Level Downloadbare ACL's**.
4. Defineert de downloadbare ACL's.
5. Klik op **Groepsinstallatie**. Onder Downloadbare ACL's, toewijzen u de PIX-toegangslijst aan de eerder gemaakte
   toegangslijst.



PIX-uitwerpselen: Geldige verificatie en gedownloade toegangslijst met gedeelde profielen

- Hiermee staat alleen telnet toe en ontkent u ander verkeer.

```
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)
```

Uitvoer vanuit de opdracht **tonen**

```
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#
```

Uitvoer uit de opdracht **toegangslijst tonen**.

```
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
```

- Ontkent alleen telnet en staat ander verkeer toe.

```
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
```

Uitvoer vanuit de opdracht **tonen**

```
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
```

Uitvoer uit de opdracht **toegangslijst tonen**.

```
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#
```

Voeg accounting toe

PIX-configuratie - accounting voor add

TACACS (AuthInbound=tacacs)

Voeg deze opdracht toe.

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

Of gebruik de nieuwe optie in 5.2 om te definiëren wat door toegangslijsten moet worden verklaard.

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

Opmerking: Toegangslijst 101 wordt afzonderlijk gedefinieerd.

RADIUS (AutoOutbound=straal)

Voeg deze opdracht toe.

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

Of gebruik de nieuwe optie in 5.2 om te definiëren wat door toegangslijsten moet worden verklaard.

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

Opmerking: Toegangslijst 101 wordt afzonderlijk gedefinieerd.

Opmerking: Boekhoudkundige bestanden kunnen worden gegenereerd voor administratieve sessies op de PIX vanaf de PIX 7.0-code.

Boekhoudkundige voorbeelden

- TACACS-boekhoudingsvoorbeeld voor telnet van 99.99.99.2 buiten tot 172.18.124.114 binnenin (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
```

- RADIUS-accounting voorbeeld voor verbinding van 172.18.124.114 binnen tot 99.9.99.2

buiten (telnet) en 99.99.93 buiten (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
```

Gebruik van de opdracht tot uitsluiting

In dit netwerk, als u besluit dat een bepaalde bron of bestemming geen authenticatie, vergunning, of accounting nodig heeft, geef deze opdrachten uit.

```
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
```

OPMERKING: U hebt de opdrachten al opgenomen.

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

Of, met de nieuwe optie in 5.2, definieer wat u wilt uitsluiten.

```
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
```

Opmerking: Indien u een doos van de echtheidscontrole uitsluit en u een vergunning heeft, moet u ook het vakje van de vergunning uitsluiten.

Max. sessies en inloggebruikers bekijken

Sommige TACACS+- en RADIUS-servers hebben 'max-sessie' of 'view inloggebruikers'-functies. De mogelijkheid om max-sessies te doen of inloggebruikers te controleren is afhankelijk van accounting records. Wanneer er een accounting "start"-record is gegenereerd maar geen "stop"-opname, veronderstelt de TACACS+ of RADIUS-server dat de persoon nog aangemeld is (dwz, de gebruiker heeft een sessie door de PIX). Dit werkt goed voor telnet en FTP verbindingen vanwege de aard van de verbindingen. Dit werkt echter niet goed voor HTTP. In dit voorbeeld wordt een andere netwerkconfiguratie gebruikt, maar de concepten zijn hetzelfde.

Gebruikerstelnetten door de PIX, die onderweg authentiek verklaren.

```
(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
```

Omdat de server een "start" record maar geen "stop" record heeft gezien, toont de server op dit moment aan dat de "telnet"-gebruiker is aangemeld. Als de gebruiker een andere verbinding probeert die verificatie vereist (wellicht van een andere PC), en als max-sessies worden ingesteld op "1" op de server voor deze gebruiker (ervan uitgaande dat de server max-sessies ondersteunt), wordt de verbinding geweigerd door de server. De gebruiker gaat over hun telnet of FTP-activiteiten op de doelhost en sluit vervolgens af (brengt tien minuten door).

```
(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
```

Of de auth 0 is (dat wil zeggen, elke keer echt maken) of meer (voor één keer en niet opnieuw tijdens de auteperiode echt maken), de accounting record wordt voor elke benaderde site bijgesneden.

HTTP werkt anders vanwege de aard van het protocol. Hier is een voorbeeld van HTTP waarin de gebruiker doorbladert van 17.68.18.100 naar 9.9.9.25 door de 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
```

De gebruiker leest de gedownload webpagina. Het beginrecord wordt om 16:35:34 gepost en het stoprecord om 16:35:35. Dit download duurde één seconde (dat wil zeggen dat er minder dan een seconde was tussen het begin en het einde). De gebruiker is niet aangemeld bij de website. De verbinding is niet geopend wanneer de gebruiker de webpagina leest. Max-sessies of weergave-inloggebruikers werken hier niet. Dit komt doordat de verbindingstijd (de tijd tussen de "Built" en "Teardown") in HTTP te kort is. Het start- en stop-record is sub-seconde. Er is geen "start"-record zonder "stop" record aangezien de records vrijwel op hetzelfde moment plaatsvinden. Er wordt nog steeds een 'start'- en 'stop'-record naar de server gestuurd voor elke transactie, ongeacht of de auth is ingesteld voor 0 of iets groters. Max-sessies en inloggebruikers bekijken werken echter niet vanwege de aard van HTTP-verbindingen.

Gebruikersinterface

Zie de snelle gebruikers wijzigen

Als u de opdracht hebt:

```
auth-prompt prompt PIX515B
```

dan zien gebruikers die door de PIX gaan deze aanwijzing.

```
PIX515B
```

De gebruikers van het bericht aanpassen Zie

Als u de opdrachten hebt:

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

dan zien gebruikers een bericht over de authenticatiestatus op een mislukte/succesvolle inlognaam.

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

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

Uitgangspunten per gebruiker en absolute tijden

De PIX **timeout Uauth** opdracht controleert hoe vaak herauthenticatie vereist is. Indien de verificatie/vergunning van TACACS+ is ingeschakeld, wordt dit gecontroleerd op basis van een individuele gebruiker. Dit gebruikersprofiel is ingesteld om de tijdelijke versie te controleren (dit staat op de TACACS+-server en de tijdelijke versie is in minuten).

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

Na verificatie/vergunning:

```
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
```

Na twee minuten:

De absolute time-out sessie wordt afgebroken:

```
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)
```

Virtuele HTTP-uitgang

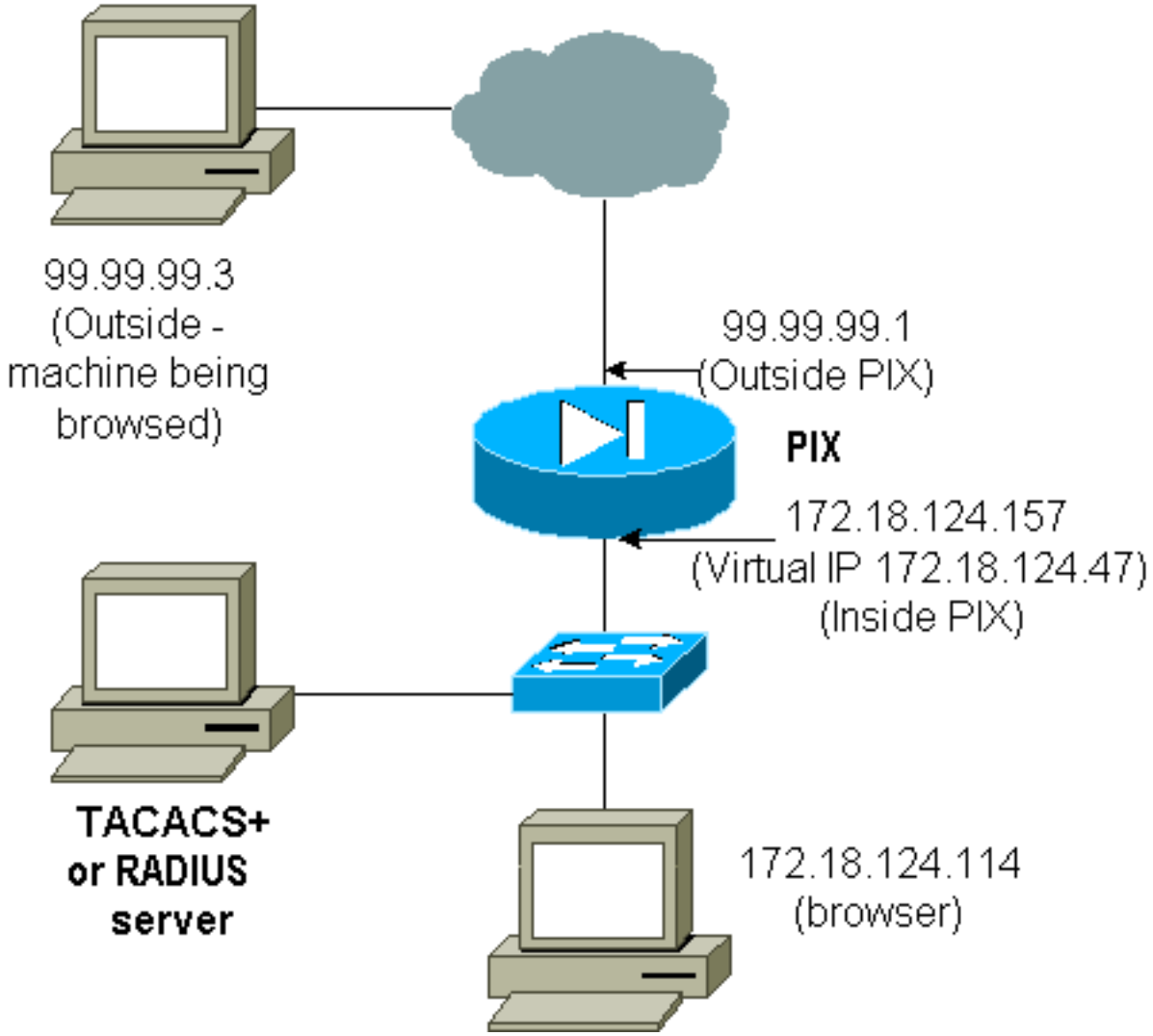
Als verificatie vereist is op sites buiten de PIX en op de PIX zelf, wordt ongebruikelijk browser gedrag soms waargenomen, aangezien browsers de gebruikersnaam en het wachtwoord in het geheugen plaatsen.

Om dit te voorkomen, dient u virtueel HTTP te implementeren door een RFC 1918- adres (een adres dat onrouteerbaar is op het internet, maar geldig en uniek is voor het PIX-netwerk) toe te voegen aan de PIX-configuratie in het formaat.

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

Wanneer de gebruiker buiten de PIX probeert te gaan, is een echtheidscontrole vereist. Als de waarschuwingsparameter aanwezig is, ontvangt de gebruiker een bericht om te sturen. De authenticatie is goed voor de tijdsduur in de auth. Zoals aangegeven in de documentatie, stelt u de opdrachtduur van de **tijdelijke versie** niet in op 0 seconden met virtueel HTTP. Dit voorkomt HTTP-verbindingen naar de echte webserver.

Opmerking: De virtuele HTTP- en virtuele IP-adressen van telnet moeten worden opgenomen in de **AAA-verificatie-**verklaringen. In dit voorbeeld omvat het specificeren van 0.0.0.0 deze adressen.



Voeg deze opdracht toe in de PIX-configuratie.

```
virtual http 172.18.124.47
```

De gebruiker wijst de browser aan op 9.9.99.3. Dit bericht wordt weergegeven.

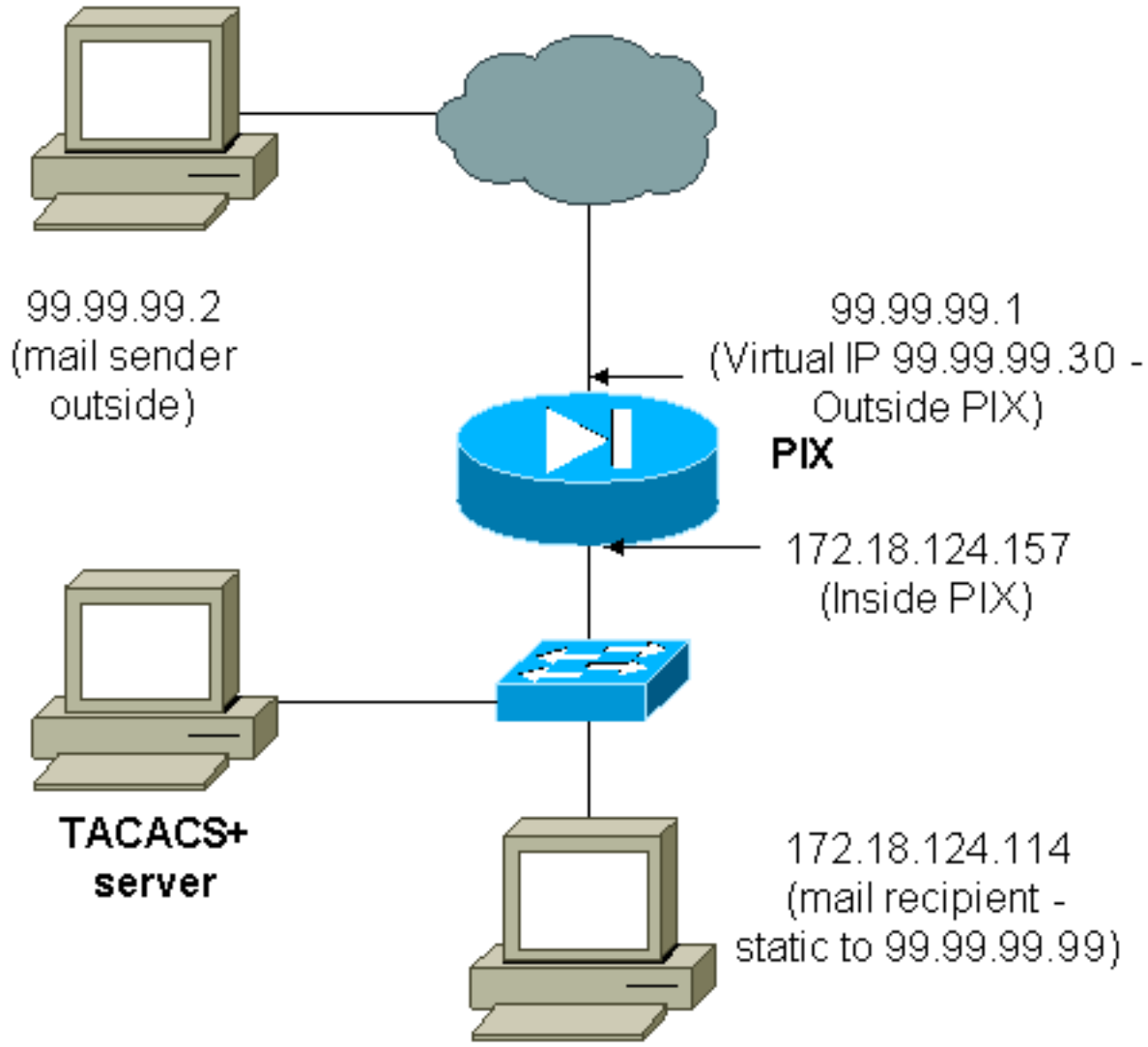
```
Enter username for PIX515B (IDXXX) at 172.18.124.47
```

Na verificatie wordt het verkeer omgeleid naar 99.99.99.3.

Virtueel telnet

Opmerking: De virtuele HTTP- en virtuele IP-adressen van telnet moeten worden opgenomen in de **AAA-verificatie-**verklaringen. In dit voorbeeld omvat het specificeren van 0.0.0.0 deze adressen.

Virtueel telnet inkomend



Het is geen goed idee om e-mail te bevestigen binnenkomend aangezien een venster niet voor post wordt weergegeven om binnenkomend te worden verzonden. Gebruik in plaats daarvan de opdracht **afsluiten**. Maar deze opdrachten worden ter illustratie toegevoegd.

```
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
```

De gebruikers (dit is TACACS+ software):

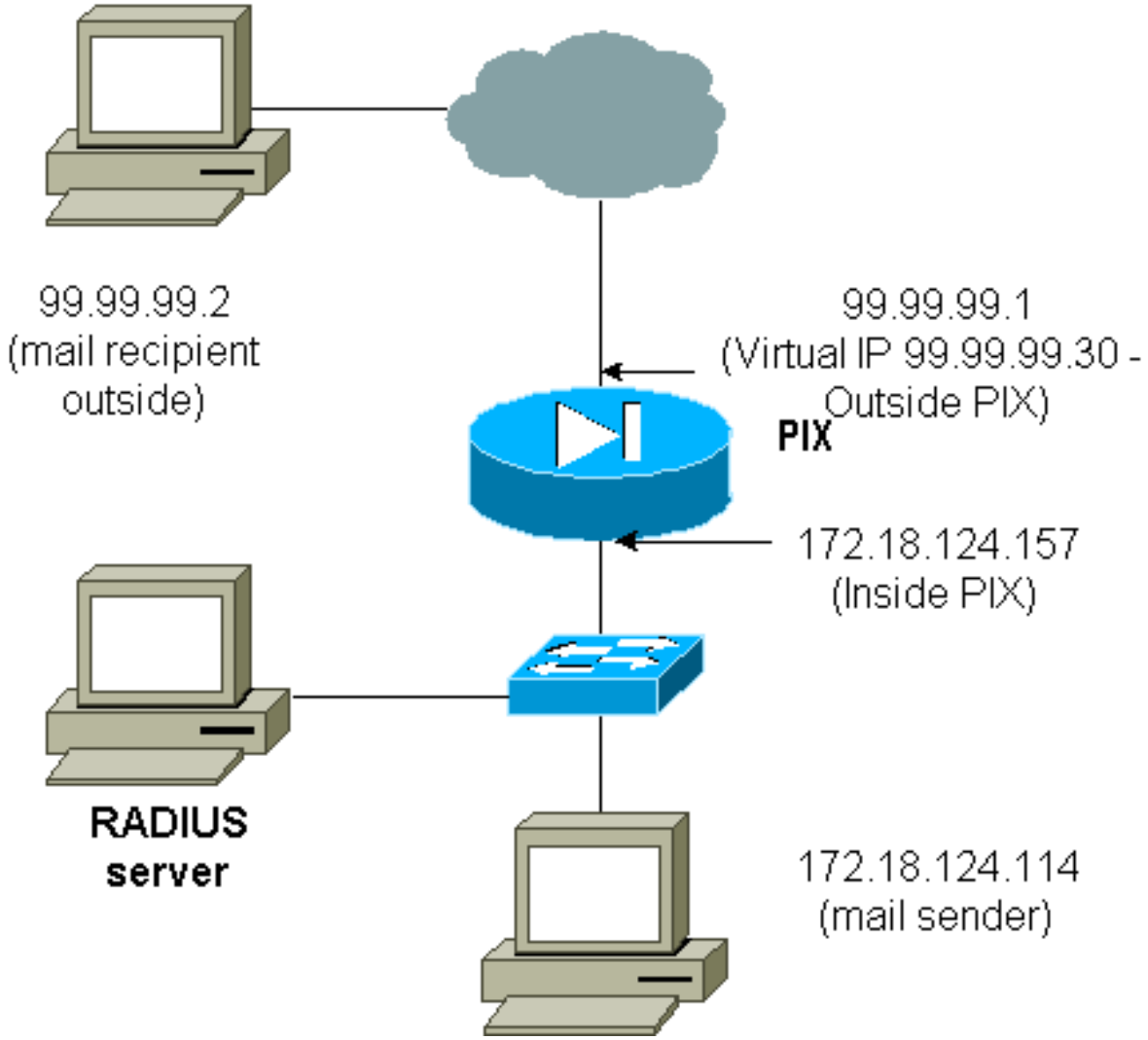
```
  user = cse {
  default service = permit
  login = cleartext "csecse"
  }


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

Als slechts authenticatie is ingeschakeld, verzenden beide gebruikers inkomende e-mail nadat ze op een telnet zijn geauthentificeerd naar IP-adres 99.99.30. Als autorisatie is ingeschakeld, sturen gebruikers "cse"-telnetten naar 99.99.30 en voeren zij de gebruikersnaam/het wachtwoord voor TACACS+ in. De Telnet-verbinding daalt. De gebruiker "cse" stuurt de post naar 99.99.99.99 (172.18.124.114). Verificatie volgt op gebruiker "elfuser". Wanneer de PIX echter het vergunningsverzoek voor cmd=tcp/25 en cmd-arg=172.18.124.114 verstuurt, ontbreekt het verzoek, zoals in deze output wordt getoond.

```
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
```

Uitgaande virtuele telnet



Het is geen goed idee om e-mail te bevestigen binnenkomend aangezien een venster niet voor post wordt weergegeven om binnenkomend te worden verzonden. Gebruik in plaats daarvan de opdracht **afsluiten**. Maar deze opdrachten worden ter illustratie toegevoegd.

Het is geen goed idee om e-mail te authentiseren uitgestuurd aangezien een venster niet voor e-mail wordt weergegeven om uitgestuurd. Gebruik in plaats daarvan de opdracht **afsluiten**. Maar ter illustratie worden deze opdrachten toegevoegd.

```
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.
```

Als u e-mail van binnen naar buiten wilt verzenden, plaatst u een opdrachtmelding op de posthost en telnet op 9.9.99.30. Dit opent het gat voor e-mail om door te gaan. De post wordt verzonden van 172.18.124.114 tot 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
```

Vastlegging virtueel telnet

Wanneer gebruikers net naar het virtuele IP-adres van telnet tellen, **toont** de opdracht Geluid uit de **show** de tijd dat het gat open is. Als de gebruikers willen voorkomen dat het verkeer door gaat nadat hun sessies zijn beëindigd (wanneer de tijd in de auth blijft), moeten ze opnieuw telnet aan het virtuele IP-adres van telnet. Dit beukt de sessie af. Dit voorbeeld illustreert dit.

De eerste echtheidscontrole

```
 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
```

Na de eerste verificatie

```
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
```

De tweede echtheidscontrole

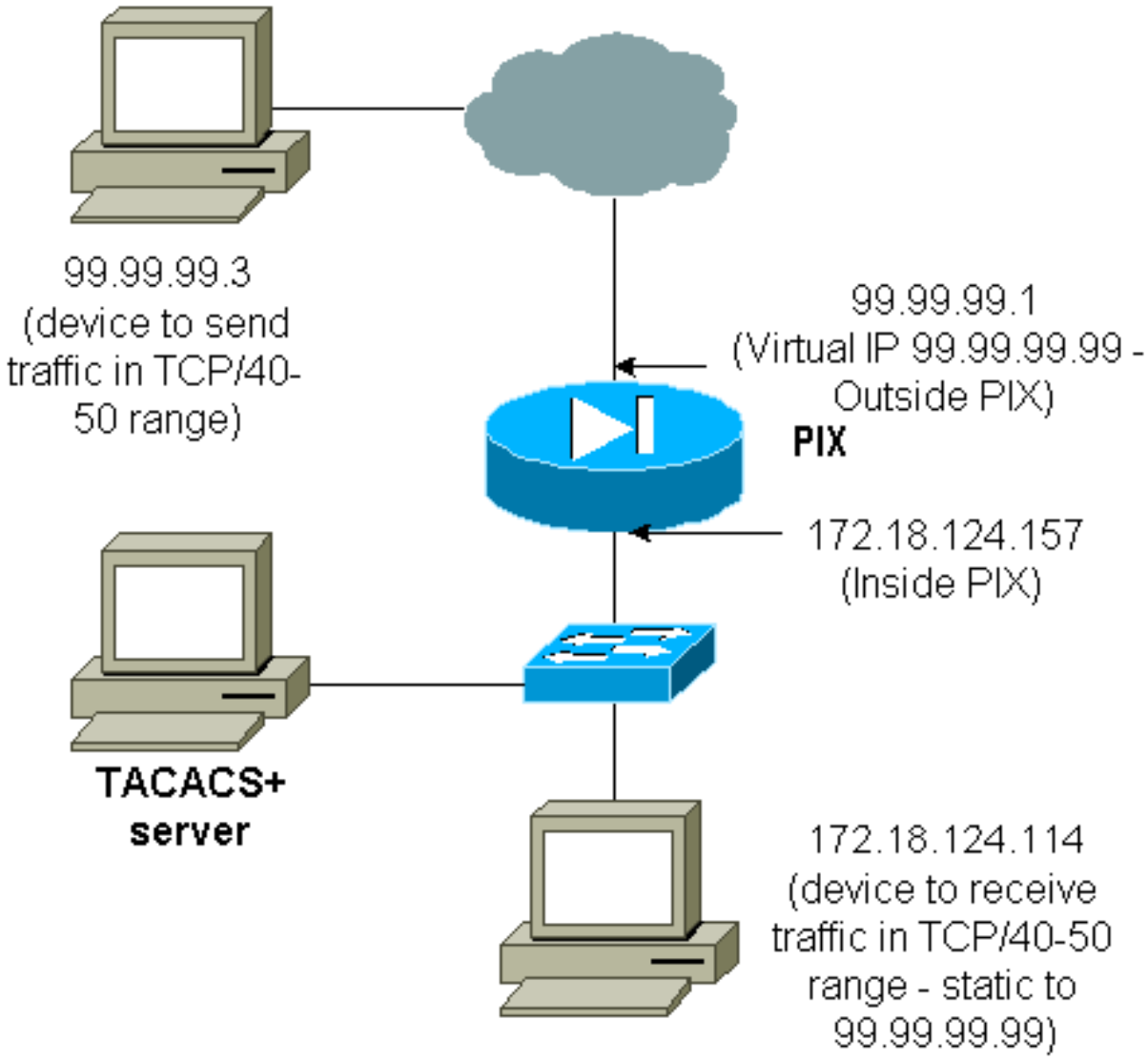
```
pixfirewall# 109001: Auth start for user 'cse'
   from 172.18.124.114/32863 to    99.99.99.30/23
109005: Authentication succeeded for user 'cse'
   from 172.18.124.114/32863 to    99.99.99.30/23
   on interface inside
```

[Na de tweede echtheidscontrole](#)

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

Poortautorisatie

Netwerkdiagram



Een vergunning is toegestaan voor havenfaciliteiten. Als virtueel telnet op de PIX is geconfigureerd en de licentie is ingesteld voor een heel scala aan poorten, opent de gebruiker het gat met virtueel telnet. Als er een vergunning voor een poortbereik is en het verkeer in dat bereik de PIX raakt, stuurt de PIX de opdracht naar de TACACS+ server voor goedkeuring. Dit voorbeeld toont inkomende vergunningen op een havengebied.

```
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
```

Configuratievoorbeeld TACACS+ server (freware):

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

De gebruiker moet eerst telnet naar het virtuele IP-adres 99.99.99.99. Na verificatie, wanneer een gebruiker probeert om TCP-verkeer in het poort 40-50-bereik door PIX naar 99.99.99 (172.18.124.114) te duwen, cmd=tcp/4 0-50 wordt naar de TACACS+ server verzonden met cmd-arg=172.18.124.114, zoals hier wordt geïllustreerd:

```
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
```

AAA-accounting voor verkeer anders dan HTTP, FTP en telnet

Nadat u ervoor hebt gezorgd dat het virtuele telnet werkt om TCP/40-50 verkeer aan de host in het netwerk toe te staan, voeg accounting voor dit verkeer met deze opdrachten toe.

```
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
```

Voorbeeld van TACACS+-boekhoudbescheiden

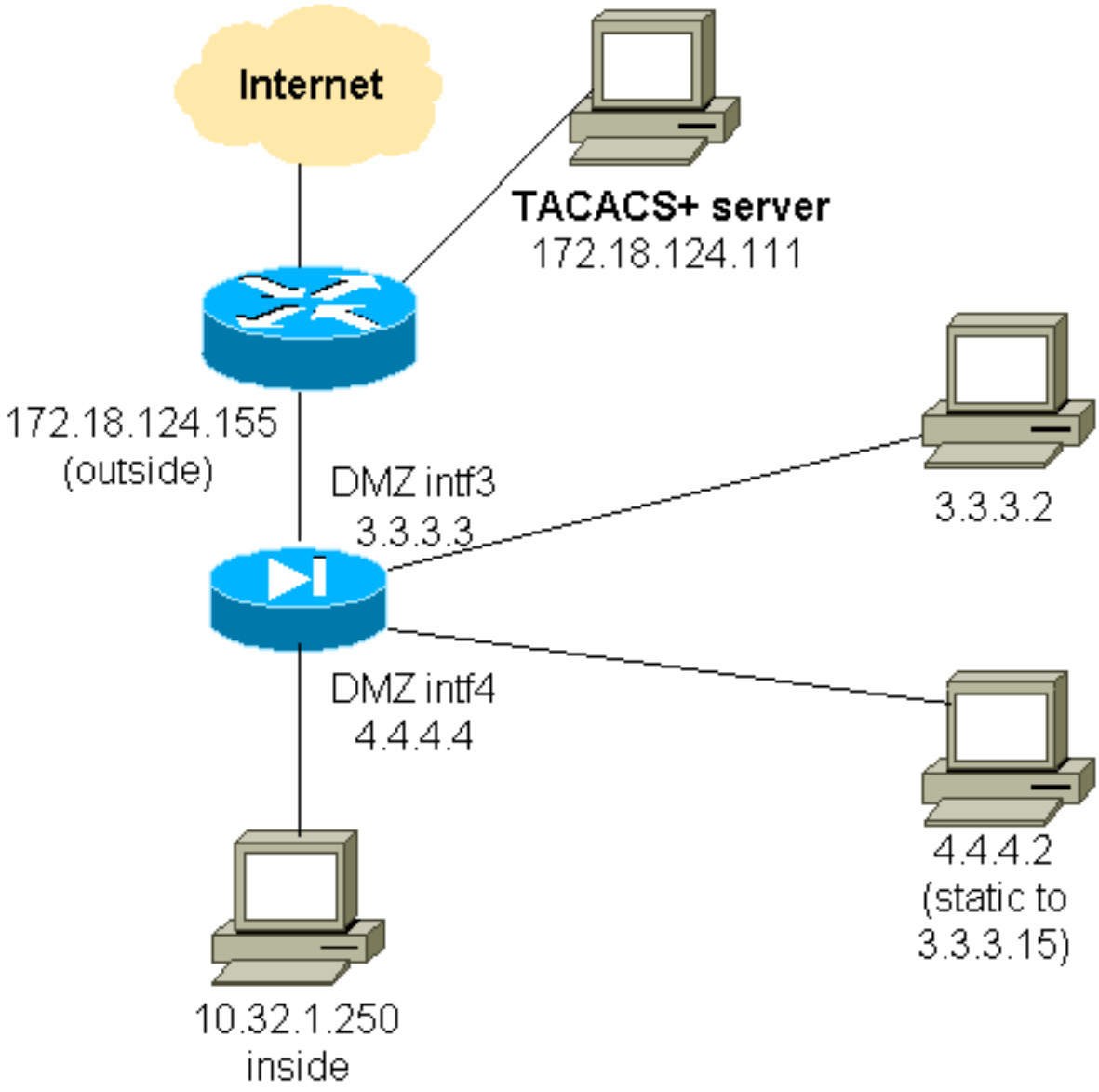
```
Thu Aug 24 08:06:09 2000 172.18.124.157 cse PIX 99.99.99.3
start task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
cmd=tcp/40-50
Thu Aug 24 08:06:17 2000 172.18.124.157 cse PIX 99.99.99.3
stop task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
cmd=tcp/40-50 elapsed_time=8 bytes_in=80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

Verificatie via DMZ

Om gebruikers die van één interface DMZ naar een andere gaan voor authentiek te verklaren, vertel de PIX om verkeer voor de genoemde interfaces te authentiseren. Op de PIX is de regeling als volgt:

```
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
```

Netwerkdiagram



Configuratie van gedeeltelijke PIX

Verifieer Telnet-verkeer tussen pix/intf3 en pix/intf4, zoals hier wordt aangetoond.

Configuratie van gedeeltelijke PIX

```
  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
```

Te verzamelen informatie als u een TAC-case opent

Als u nog steeds assistentie nodig hebt nadat u de bovenstaande stappen voor het oplossen van problemen hebt gevolgd en u een case wilt openen met Cisco TAC, zorg er dan voor dat u deze informatie bevat voor het oplossen van uw PIX-firewall.

- Probleembeschrijving en relevante topologgegevens
- Probleemoplossing voordat u de case opent
- Uitvoer vanuit de opdracht **Tech-support**
- Uitvoer van het bevel van het **showlogbestand** nadat u met de **houtkap gebufferde** opdracht hebt uitgevoerd, of console vangt die het probleem (indien beschikbaar) aantoont

Hang de verzamelde gegevens aan uw case in een niet-zipped, onbewerkte tekstformaat (.txt). Hang informatie aan uw case door deze te uploaden met de hulp van het Case Query Tool (alleen geregistreerde klanten). Als u geen toegang hebt tot de Case Query Tool, verstuur de informatie in een e-mailbijlage naar attach@cisco.com met uw casenummer in de onderwerpregel of uw bericht.

Gerelateerde informatie

- Cisco PIX-firewallsoftware
- Opdrachtreferenties van Cisco Secure PIX-firewall
- Security meldingen uit het veld (inclusief PIX)
- Verzoeken om opmerkingen (RFC's)
- Cisco Secure Access Control Server voor Windows
- Cisco Secure Access Control Server voor UNIX
- Terminal Access Control-systeem (TACACS+)

- Inbelservice voor externe verificatie (RADIUS)
- Technische ondersteuning en documentatie – Cisco Systems