PIX 5.1.x configureren: TACACS+ en RADIUS

Inhoud

Inleiding

RADIUS- en TACACS+-verificatie kunnen worden uitgevoerd voor FTP-, telnet- en HTTP-verbindingen. Verificatie voor andere minder gebruikelijke protocollen kan gewoonlijk aan het werk worden gemaakt. de TACACS+-vergunning wordt ondersteund; RADIUS-autorisatie is dat niet. Veranderingen in PIX 5.1 verificatie, autorisatie en accounting (AAA) ten opzichte van de vorige versie omvatten uitgebreide verificatie (xauth)— verificatie van IPSec-tunnels van Cisco Secure VPN-client 1.1.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Conventies

Zie de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

Verificatie vs. autorisatie

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

Stel dat je honderd gebruikers binnen hebt en je wilt dat slechts zes van deze gebruikers FTP, telnet of HTTP buiten het netwerk kunnen doen. U zou de PIX vertellen om uitgaande verkeer te authentiseren en alle zes gebruikers id's op de TACACS+/RADIUS-beveiligingsserver te geven. Met eenvoudige authenticatie, zouden deze zes gebruikers geauthentificeerd kunnen worden met gebruikersnaam en wachtwoord, en dan weg kunnen gaan. De andere 94 gebruikers konden niet weggaan. De PIX vraagt gebruikers om een gebruikersnaam/wachtwoord, geeft vervolgens hun gebruikersnaam en wachtwoord door aan de TACACS+/RADIUS-beveiligingsserver en afhankelijk van de reactie opent of ontkent de verbinding. Deze zes gebruikers kunnen FTP, telnet of HTTP doen.

Maar stel dat *één* van deze zes gebruikers, "Festus", niet vertrouwd is. U zou Festus willen

toestaan om FTP te doen, maar niet HTTP of telnet naar buiten. Dat betekent dat we *vergunningen* moeten *geven*, dat wil zeggen dat we moeten toestaan *wat* gebruikers kunnen doen naast het authentiseren van wie ze zijn. Dit geldt alleen voor TACACS+. Als we *toestemming* toevoegen aan PIX, stuurt PIX eerst de gebruikersnaam en het wachtwoord van Festus naar de beveiligingsserver en stuurt hij vervolgens een autorisatieverzoek om de beveiligingsserver te vertellen wat "*commando*" Festus probeert te doen. Als de server goed is ingesteld, kan Festus "ftp 1.2.3.4" toestaan, maar zou hij de mogelijkheid om HTTP of telnet ergens anders te ontzeggen hebben.

Wat de gebruiker ziet met verificatie/autorisatie op

Wanneer men probeert van binnen naar buiten te gaan (of omgekeerd) met authenticatie/vergunning 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 het programma verschijnen. De gebruiker moet **local_username@remote_username** invoeren voor de gebruikersnaam en **local_password@remote_password** voor het wachtwoord. PIX verstuurt de local_gebruikersnaam en local_password naar de lokale beveiligingsserver, en als verificatie (en autorisatie) succesvol is op de PIX/server, worden de Remote_gebruikersnaam en het Remote_password doorgegeven naar de doelFTP server.
- **HTTP** - Er wordt een venster weergegeven in de browser waarin een gebruikersnaam en wachtwoord wordt gevraagd. Als authenticatie (en autorisatie) succesvol is, arriveert de gebruiker op de bestemmingspruct. Houd in gedachten dat *browsers gebruikersnamen en wachtwoorden in het geheugen plaatsen*. Als het lijkt dat PIX een HTTP-verbinding moet afstemmen maar dit niet doet, is het waarschijnlijk dat er een nieuwe verificatie plaatsvindt met de browser die de gecached gebruikersnaam en wachtwoord naar de PIX stuurt, die dit dan doorstuurt naar de verificatieserver. PIX syslog en/of server debug toont dit fenomeen. Als telnet en FTP normaal lijken te werken maar HTTP connecties niet, is dit waarom.
- **Tunnel** - Wanneer u probeert om IPSec-verkeer naar het netwerk te tunnellen met de VPN-client en -toets in, wordt een grijze doos voor "Gebruikersverificatie voor nieuwe verbinding" weergegeven voor een gebruikersnaam/wachtwoord.**Opmerking:** Deze verificatie wordt ondersteund vanaf de Cisco Secure VPN-client 1.1. Als het **Help > About** menu versie 2.1.x of hoger niet toont, werkt dit niet.

Security Server-configuraties gebruikt voor alle scenario's

Cisco Secure UNIX-TACACS-serverconfiguratie

In deze sectie, wordt u voorgesteld met de informatie om uw veiligheidsserver te configureren.

Zorg ervoor dat u het PIX IP-adres of de volledig-gekwalificeerde domeinnaam en -toets in het CSU.cfg-bestand hebt.

```
user = ddunlap {
password = clear "rtp"
```

```
default service = permit
}

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

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

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

Cisco Secure UNIX-RADIUS-serverconfiguratie

Gebruik de GUI om het PIX IP-adres en de toets aan de NAS-lijst (Network Access Server) toe te voegen.

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

Cisco Secure ACS voor Windows 2.x RADIUS

Gebruik deze stappen om Cisco Secure ACS voor Windows 2.x RADIUS te configureren.

1. Wachtwoord verkrijgen in het vak User Setup GUI.
2. Stel eigenschap 6 (servicetype) in op **aanmelding** of **administratie** in vanuit het gedeelte GUI-instelling.
3. Voeg het PIX IP adres toe in de sectie GUI van de NAS Configuration.

Gemakkelijk ACS+ TACACS+

De EasyACS-documentatie beschrijft instellingen.

1. Klik in het groepsgedeelte op **Shell-exec** om extra bevoegdheden te geven.
2. Als u toestemming aan de PIX wilt toevoegen, klikt u op **Deny niet-afgesloten IOS-opdrachten** onder in de groepsinstellingen.
3. Selecteer **Toevoegen/Bewerken nieuwe opdracht** voor elke opdracht die u wilt toestaan, bijvoorbeeld, **Telnet**.
4. Als telnetting op specifieke locaties is toegestaan, vul dan het IP-adres(sen) in in het argument gedeelte in het formulier "vergunning #.#.#". Anders, om Telnetting toe te staan, klik **staat alle niet-beursgenoteerde argumenten toe**.
5. Klik op **Bewerken opdracht Voltooien**.
6. Voer stappen 1 door 5 uit voor elk van de toegestane opdrachten (bijvoorbeeld telnet, HTTP of FTP).
7. Voeg de PIX IP toe in de sectie NAS Configuration GUI.

Cisco Secure 2.x TACACS+

De gebruiker verkrijgt een wachtwoord in de sectie User Setup GUI.

1. Klik in het groepsgedeelte op **Shell-exec** om extra bevoegdheden te geven.
2. Als u toestemming aan de PIX wilt toevoegen, klikt u onder in de groepsinstelling op **Deny niet-afgesloten IOS-opdrachten**.
3. Selecteer **Toevoegen/Bewerken nieuwe opdracht** voor elke opdracht die u wilt toestaan (bijvoorbeeld **Telnet**).
4. Om telnetting op specifieke plaatsen toe te staan, voer het IP adres in het argument gedeelte in het formulier "vergunning #.#.#.#" in. Om telnetting aan om het even welke website toe te staan, klik **staat alle niet vermelde argumenten toe**.
5. Klik op **Bewerken opdracht Voltooien**.
6. Voer stappen 1 door 5 uit voor elk van de toegestane opdrachten (bijvoorbeeld telnet, HTTP of FTP).
7. Zorg ervoor dat het PIX IP-adres is toegevoegd in het gedeelte NAS Configuration GUI.

Configuratie van Livingston RADIUS-server

Voeg het PIX IP-adres en de toets aan het Clientbestand toe.

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

Configuratie van RADIUS-server Merken

Voeg het PIX IP-adres en de toets aan het Clientbestand toe.

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

Configuratie van TACACS+ vriesserver

```
key = "cisco"
user = adminuser {
login = cleartext "all"
default service = permit
```

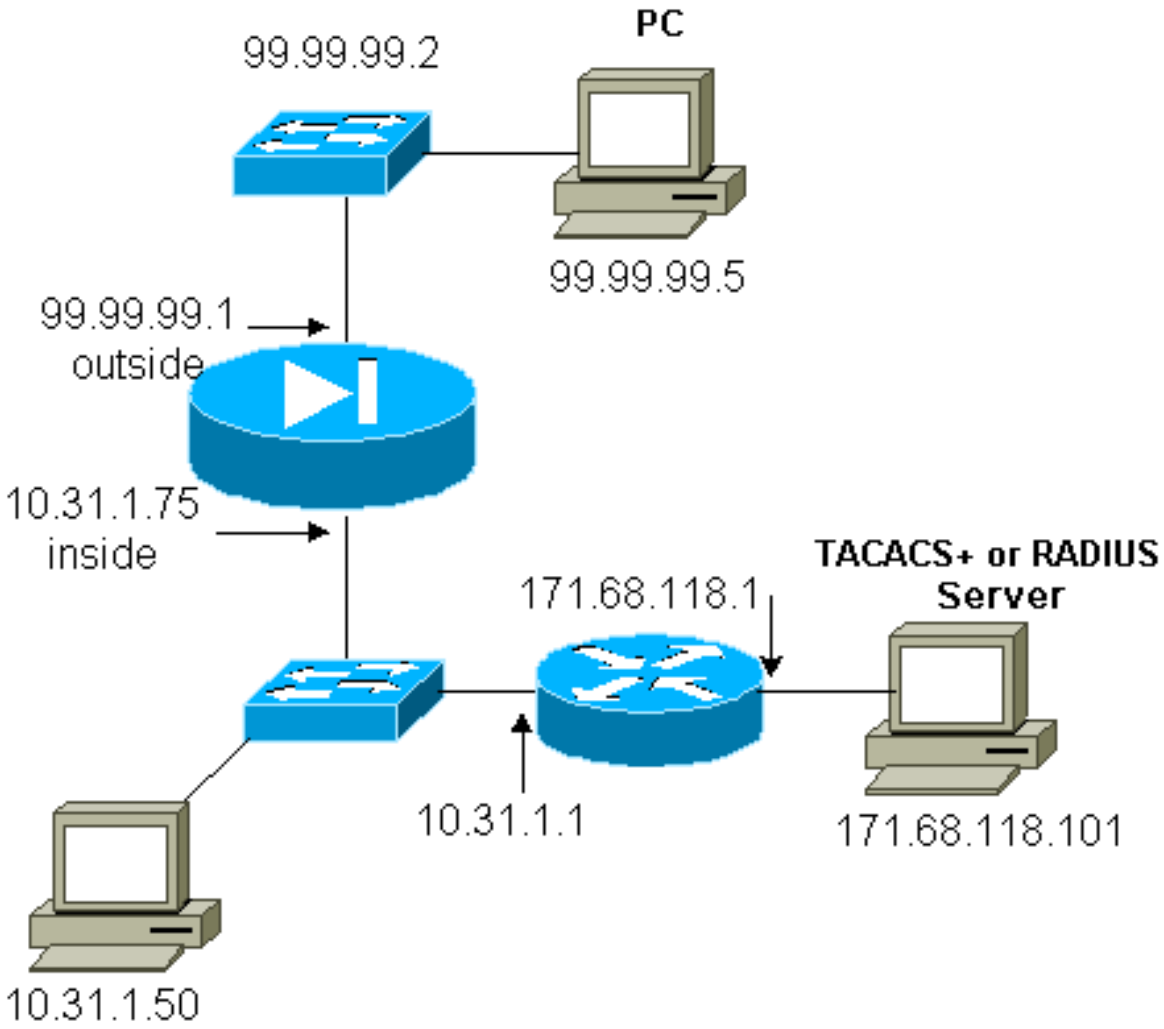
```
}

user = can_only_do_telnet {
login = cleartext "telnetonly"
cmd = telnet {
permit .*
}
}

user = httponly {
login = cleartext "httponly"
cmd = http {
permit .*
}
}

user = can_only_do_ftp {
login = cleartext "ftponly"
cmd = ftp {
permit .*
}
}
```

Afluisterstappen

N.B.: Bepaalde **show** opdrachten worden ondersteund door de Output Tolk Tool (alleen geregistreerde klanten), waardoor u een analyse van **show** opdrachtoutput kunt bekijken.

- Zorg ervoor dat de PIX-configuratie werkt voordat u AAA toevoegt. Indien u geen verkeer kan doorgeven voordat u een echtheidscontrole en een vergunning instelt, kunt u dit achteraf niet meer doen.
- Inloggen in de PIX inschakelen.Het debuggen van de Logging dient niet gebruikt te worden op een zwaar geladen systeem.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 (alle servers hebben deze optie).

Netwerkdiagram



PIX-configuratie

```
PIX Version 5.1(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 pix/intf2 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix3
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
names
pager lines 24
no logging timestamp
no logging standby
logging console debugging
no logging monitor
no logging buffered
no logging trap
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
```

```
mtu outside 1500
mtu inside 1500
mtu pix/intf2 1500
ip address outside 99.99.99.1 255.255.255.0
ip address inside 10.31.1.75 255.255.255.0
ip address pix/intf2 127.0.0.1 255.255.255.255
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address pix/intf2 0.0.0.0
arp timeout 14400
global (outside) 1 99.99.99.7-99.99.99.10 netmask
255.255.255.0
nat (inside) 1 10.31.1.0 255.255.255.0 0 0
static (inside,outside) 99.99.99.99 10.31.1.50 netmask
255.255.255.255 0 0
conduit permit icmp any any
conduit permit tcp any any
conduit permit udp any any
route outside 0.0.0.0 0.0.0.0 99.99.99.2 1
route inside 171.68.118.0 255.255.255.0 10.31.1.1 1
route inside 171.68.120.0 255.255.255.0 10.31.1.1 1
timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00
udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server AuthInbound protocol tacacs+
aaa-server AuthInbound (inside) host 171.68.118.101
cisco timeout 5
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 171.68.118.101
cisco timeout 5
aaa authentication include telnet outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication include telnet inbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authentication include http outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication include http inbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthInbound
aaa authentication include ftp outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication include ftp inbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthInbound
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
telnet timeout 5
terminal width 80
Cryptochecksum:b26b560b20e625c9e23743082484caca
: end
[OK]
```

Verificatie Debug Voorbeelden van PIX

In dit deel worden monsters van de echtheidscontroles voor verschillende scenario's getoond.

Inkomend

De externe gebruiker op 99.99.99.2 initieert verkeer naar binnen 10.31.1.50 (99.99.99.99) en is geauthentificeerd door TACACS (dat wil zeggen, de lijst van de inkomende gebruikersserver "AuthInbound" die TACACS server 171.68.10 omvat 1).

PIX-debug - goede verificatie - TACACS+

Het onderstaande voorbeeld toont een PIX-debug met goede authenticatie:

```
109001: Auth start for user '???' from
    99.99.99.2/11008 to 10.31.1.50/23
109011: Authen Session Start: user 'cse', sid 4
109005: Authentication succeeded for user 'cse'
    from 10.31.1.50/23 to 99.99.99.e
302001: Built inbound TCP connection 10 for
    faddr 99.99.99.2/11008 gaddr 99.99.)
```

PIX Debug - bad Authentication (gebruikersnaam of wachtwoord) - TACACS+

Het onderstaande voorbeeld toont een PIX-debug met slechte authenticatie (gebruikersnaam of wachtwoord). De gebruiker ziet drie gebruikersnaam/wachtwoordtypen, gevolgd door dit bericht: `Fout: max aantal overschrijdingen.`

```
109001: Auth start for user '???' from
     99.99.99.2/11010 to 10.31.1.50/23
  109006: Authentication failed for user '' from
     10.31.1.50/23 to 99.99.99.2/11010 on
     interface outside
```

PIX Debug - Can Ping Server, geen respons - TACACS+

Het voorbeeld hieronder toont een PIX debug waar de server pingable is maar niet met PIX spreekt. De gebruiker ziet de gebruikersnaam eenmaal, maar de PIX vraagt nooit om een wachtwoord (dit is op telnet). De gebruiker ziet `fout: Max. aantal overschrijdingen.`

```
109001: Auth start for user '???' from 99.99.99.2/11011
     to 10.31.1.50/23
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
  109006: Authentication failed for user '' from 10.31.1.50/23
     to 99.99.99.2/11011 on interface outside
```

PIX Debug - Kan geen Ping Server - TACACS+

Het voorbeeld hieronder toont een PIX debug waar de server niet pingable is. De gebruiker ziet de gebruikersnaam eenmaal, maar de PIX vraagt nooit om een wachtwoord (dit is op telnet). De

volgende berichten worden weergegeven: `Time-out bij TACACS+ server` en `fout: Max. aantal probeert te overschrijden` (een webserver is in de configuratie aangevallen).

```
111005: console end configuration: OK
  109001: Auth start for user '???' from
     99.99.99.2/11012 to 10.31.1.50/23
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109006: Authentication failed for user '' from
     10.31.1.50/23 to 99.99.99.2/11012 on interface
     outside
```

PIX-debug - goede verificatie - RADIUS

Het onderstaande voorbeeld toont een PIX-debug met goede authenticatie:

```
109001: Auth start for user '???' from
     10.31.1.50/11008 to 99.99.99.2/23
  109011: Authen Session Start: user 'pixuser', sid 8
  109005: Authentication succeeded for user
     'pixuser' from 10.31.1.50/11008 to
     99.99.99.2/23 on interface inside
  302001: Built outbound TCP connection 16 for faddr
     99.99.99.2/23 gaddr 99.99.99.99/11008
     laddr 10.31.1.50/11008 (pixuser)
```

PIX Debug - bad Authentication (gebruikersnaam of wachtwoord) - RADIUS

Het onderstaande voorbeeld toont een PIX-debug met slechte authenticatie (gebruikersnaam of wachtwoord). De gebruiker ziet het verzoek om een gebruikersnaam en wachtwoord en heeft drie mogelijkheden om deze in te voeren. Wanneer de bewerking geen resultaat heeft, verschijnt het volgende bericht: `Fout: max aantal overschrijdingen`.

```
109001: Auth start for user '???' from 10.31.1.50/11010
     to 99.99.99.2/23
  109006: Authentication failed for user ''
     from 10.31.1.50/11010 to 99.99.99.2/23
     on interface inside
```

PIX Debug - Can Ping Server, Daemon Down - RADIUS

Het voorbeeld hieronder toont een PIX debug waar de server pingable is, maar de daemon is beneden en zal niet met PIX communiceren. De gebruiker ziet een gebruikersnaam, dan een wachtwoord, de `RADIUS-server is mislukt` bericht en de `fout: Max. aantal overschrijdingen.` foutmelding.

```
109001: Auth start for user '???' from 10.31.1.50/11011
     to 99.99.99.2/23
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  1ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
```

```
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  09002: Auth from 10.31.1.50/11011 to 99.99.99.2/23
     failed (server 171.68.118.101 failed) on interface inside
  109002: Auth from 10.31.1.50/11011 to 99.99.99.2/23 failed
     (server 171.68.118.101 failed) on interface inside
  109002: Auth from 10.31.1.50/11011 to 99.99.99.2/23 failed
     (server 171.68.118.101 failed) on interface inside
  109006: Authentication failed for user '' from 10.31.1.50/11011
     to 99.99.99.2/23 on interface inside
```

PIX Debug - is niet in staat om server of Key/Client Mismatch te openen - RADIUS

Het onderstaande voorbeeld toont een PIX-debug waar de server niet pingable is of wanneer er een fout-match Client/key is. De gebruiker ziet een gebruikersnaam, wachtwoord, de `Time-out bij het RADIUS-`serverbericht en de `fout: Max. aantal pogingen overschreden` bericht dat een server met een bellengenerator is ingeburgerd in de configuratie).

```
109001: Auth start for user '???' from 10.31.1.50/11012
     to 99.99.99.2/23
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109006: Authentication failed for user '' from 10.31.1.50/11012
     to 99.99.99.2/23 on interface inside
```

Toestemming toevoegen

Indien u besluit een vergunning toe te voegen, aangezien de vergunning niet geldig is zonder echtheidscontrole, moet u een vergunning voor dezelfde bron- en doelgroep vragen.

```
aaa authorization telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authorization http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authorization ftp inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

Let op dat u geen toestemming voor uitgaande verkeer toevoegt, omdat het uitgaande verkeer met RADIUS is geauthentiseerd en de RADIUS-licentie niet geldig is.

Verificatie en autorisatie Debug Voorbeelden van PIX

PIX debug - goede verificatie en succesvolle autorisatie - TACACS+

Het onderstaande voorbeeld toont een PIX-debug met goede authenticatie en succesvolle autorisatie:

```
109001: Auth start for user '???' from 99.99.99.2/11016
   to 10.31.1.50/23
109011: Authen Session Start: user 'cse', Sid 11
109005: Authentication succeeded for user 'cse'
   from 10.31.1.50/23 to 99.99.99.2/11016 on interface outside
109011: Authen Session Start: user 'cse', Sid 11
```

```
109007: Authorization permitted for user 'cse' from
   99.99.99.2/11016 to 10.31.1.50/23 on interface outside
302001: Built inbound TCP connection 19 for faddr 99.99.99.2/11016
   gaddr 99.99.99.99/23 laddr 10.31.1.50/23 (cse)
```

PIX debug - goede verificatie, mislukte autorisatie - TACACS+

Het onderstaande voorbeeld toont het PIX-debug met goede authenticatie maar heeft geen toestemming gekregen. Hier ziet de gebruiker ook de `berichtfout: Vergunning geweigerd`.

```
109001: Auth start for user '???' from
    99.99.99.2/11017 to 10.31.1.50/23
109011: Authen Session Start: user 'httponly',
   Sid 12
109005: Authentication succeeded for user 'httponly'
   from 10.31.1.50/23 to 99.99.99.2/11017 on
   interface outside
109008: Authorization denied for user 'httponly' from
   10.31.1.50/23 to 99.99.99.2/11017 on interface outside
```

Boekhouding toevoegen

TACACS+

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

Uitvoer van TACACS+ software:

```
Tue Feb 22 08:52:20 2000  10.31.1.75 cse PIX
   99.99.99.2 start task_id=0x14
   foreign_ip=99.99.99.2 local_ip=10.31.1.50
   cmd=telnet
Tue Feb 22 08:52:25 2000  10.31.1.75 cse PIX
   99.99.99.2 stop task_id=0x14
   foreign_ip=99.99.99.2 local_ip=10.31.1.50
   cmd=telnet elapsed_time=5
   bytes_in=39 bytes_out=126
```

RADIUS

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

RADIUS-uitvoer samenvoegen:

```
Tue Feb 22 08:56:17 2000
        Acct-Status-Type = Start
        NAS-IP-Address = 10.31.1.75
        Login-IP-Host = 10.31.1.50
        Login-TCP-Port = 23
```

```
        Acct-Session-Id = 0x00000015
        User-Name = pixuser

        Tue Feb 22 08:56:24 2000
        Acct-Status-Type = Stop
        NAS-IP-Address = 10.31.1.75
        Login-IP-Host = 10.31.1.50
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000015
        Username = pixuser
        Acct-Session-Time = 6
        Acct-Input-Octets = 139
        Acct-Output-Octets = 36
```

Gebruik van uitsluitende opdracht

Als we een andere host buiten ons netwerk toevoegen (99.99.99.100) en deze host wordt vertrouwd, kunt u deze host uitsluiten van verificatie en autorisatie met de volgende opdrachten:

```
aaa authentication exclude telnet inbound 0.0.0.0 0.0.0.0 99.99.99.100
 255.255.255.255 AuthInbound

aaa authorization exclude telnet inbound 0.0.0.0 0.0.0.0 99.99.99.100 255.255.255.255
AuthInbound
```

Maximum aantal sessies en ingesloten gebruikers 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 niet goed voor HTTP vanwege de aard van de verbinding. In het volgende voorbeeld wordt een andere netwerkconfiguratie gebruikt, maar de concepten zijn hetzelfde.

Gebruikersletters door de PIX, voor authentiek onderweg

```
   171.68.118.100/1200 to 9.9.9.25 /23
  (pix) 109011: Authen Session Start: user
     'cse', Sid 3
  (pix) 109005: Authentication succeeded for user
     'cse' from 171.68.118.100/12 00 to 9.9.9.25/23
  (pix) 302001: Built TCP connection 5 for faddr
     9.9.9.25/23 gaddr 9.9.9.10/12 00
     laddr 171.68.118.100/1200 (cse)
  (server start account) Sun Nov 8 16:31:10 1998
     rtp-pinecone.rtp.cisco.com cse
  PIX 171.68.118.100 start task_id=0x3 foreign_ip=9.9.9.25
     local_ip=171.68.118.100 cmd=telnet
```

Omdat de server een begin record maar geen stop record heeft gezien, toont de server op dit punt in de tijd aan dat de gebruiker van het telnet is aangemeld. Als de gebruiker een andere verbinding probeert die verificatie vereist (wellicht van een andere PC), en als max-sessies zijn 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-bedrijf op de doelhost en sluit vervolgens af (besteedt daar tien minuten aan):

```
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. Hieronder zie je een voorbeeld van HTTP:

De gebruiker bladert van 171.68.118.100 tot 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). Is de gebruiker nog steeds aangemeld bij de website en is de verbinding nog open wanneer de gebruiker de webpagina leest? Neen. Zullen de maximum sessies of de weergave van ingelogde gebruikers hier werken? Nee, omdat de verbindingstijd (de tijd tussen de "Built" en "Teardown") in HTTP te kort is. Het begin- en stoprecord is subseconde. Er is geen beginrecord zonder stop record, aangezien de records vrijwel op hetzelfde moment plaatsvinden. Er wordt nog steeds begin- en stop record verzonden naar de server voor elke transactie, ongeacht of de auth is ingesteld op 0 of iets groters. Max-sessies en inloggebruikers bekijken werken echter niet vanwege de aard van HTTP-verbindingen.

Verificatie en inschakelen van de PIX zelf

De vorige discussie gaat over het authenticeren van het telnet (en HTTP, FTP) verkeer door de PIX. Verzeker telnet aan de PIX werkt zonder Verificatie op:

```
telnet 10.31.1.5 255.255.255.255
passwd ww
```

Voeg dan de opdracht toe om gebruikers Telnetting aan PIX voor authentiek te verklaren:

```
aaa authentication telnet console AuthInbound
```

Wanneer gebruikers Telnet aan PIX, worden ze gevraagd naar het Telnet-wachtwoord (**WW**). De PIX vraagt ook om de gebruikersnaam en het wachtwoord voor TACACS+ of RADIUS. In dit geval aangezien de AuthInbound serverlijst wordt gebruikt, vraagt PIX om de TACACS+ gebruikersnaam en het wachtwoord.

Als de server uit is, kunt u de PIX benaderen door **PIX** in te voeren voor de gebruikersnaam en vervolgens het wachtwoord inschakelen (**om *het* wachtwoord *in te schakelen*).** Met deze opdracht:

```
aaa authentication enable console AuthInbound
```

De gebruiker wordt gevraagd om een gebruikersnaam en wachtwoord voor de TACACS- of RADIUS-server. In dit geval aangezien de AuthInbound serverlijst wordt gebruikt, vraagt PIX om de TACACS+ gebruikersnaam en het wachtwoord.

Aangezien het verificatiepakket waarmee u een verbinding kunt maken, hetzelfde is als het authenticatiepakket voor inloggen, kunnen de gebruikers, als ze met TACACS of RADIUS in kunnen loggen, via TACACS of RADIUS met dezelfde gebruikersnaam/wachtwoord een verbinding maken. Dit probleem is toegewezen aan Cisco bug-ID CSCdm47044 (alleen geregistreerde klanten).

Als de server uit is, kunt u PIX inschakelen en de modus inschakelen door **PIX** in te voeren voor de gebruikersnaam en het wachtwoord door de PIX in te schakelen (**geef *het* wachtwoord *op* wat *dan ook*).** Als u *het* ***wachtwoord invoert wat*** niet in de PIX-configuratie voorkomt, voert u **pix** in voor de gebruikersnaam en drukt u op **ENTER**. Als het wachtwoord wordt ingesteld maar niet bekend, moet er een wachtwoordterugzetschijf worden gebouwd om het wachtwoord te herstellen.

De snelle gebruikers wijzigen

Als u de opdracht hebt:

```
auth-prompt PIX_PIX_PIX
```

gebruikers die door de PIX gaan, zien de volgende volgorde:

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

Bij aankomst op de eindbestemming zagen gebruikers de Username: en wachtwoord: Dit wordt aangegeven door het doelvak. Deze melding beïnvloedt alleen gebruikers die *door* de PIX gaan, niet de PIX.

Toelichting: Er zijn geen boekhoudkundige gegevens bijgesneden voor toegang tot de PIX.

De gebruikers van het bericht aanpassen Zie over succes/falen

Als u de opdrachten hebt:

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

dan zien gebruikers de volgende volgorde op een mislukte/succesvolle inloging door de PIX:

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

Uitgangspunten per gebruiker en absolute tijden

Deze functie werkt momenteel niet en het probleem is toegewezen aan Cisco bug ID CSCdp93492 (alleen geregistreerde klanten).

Virtuele HTTP

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

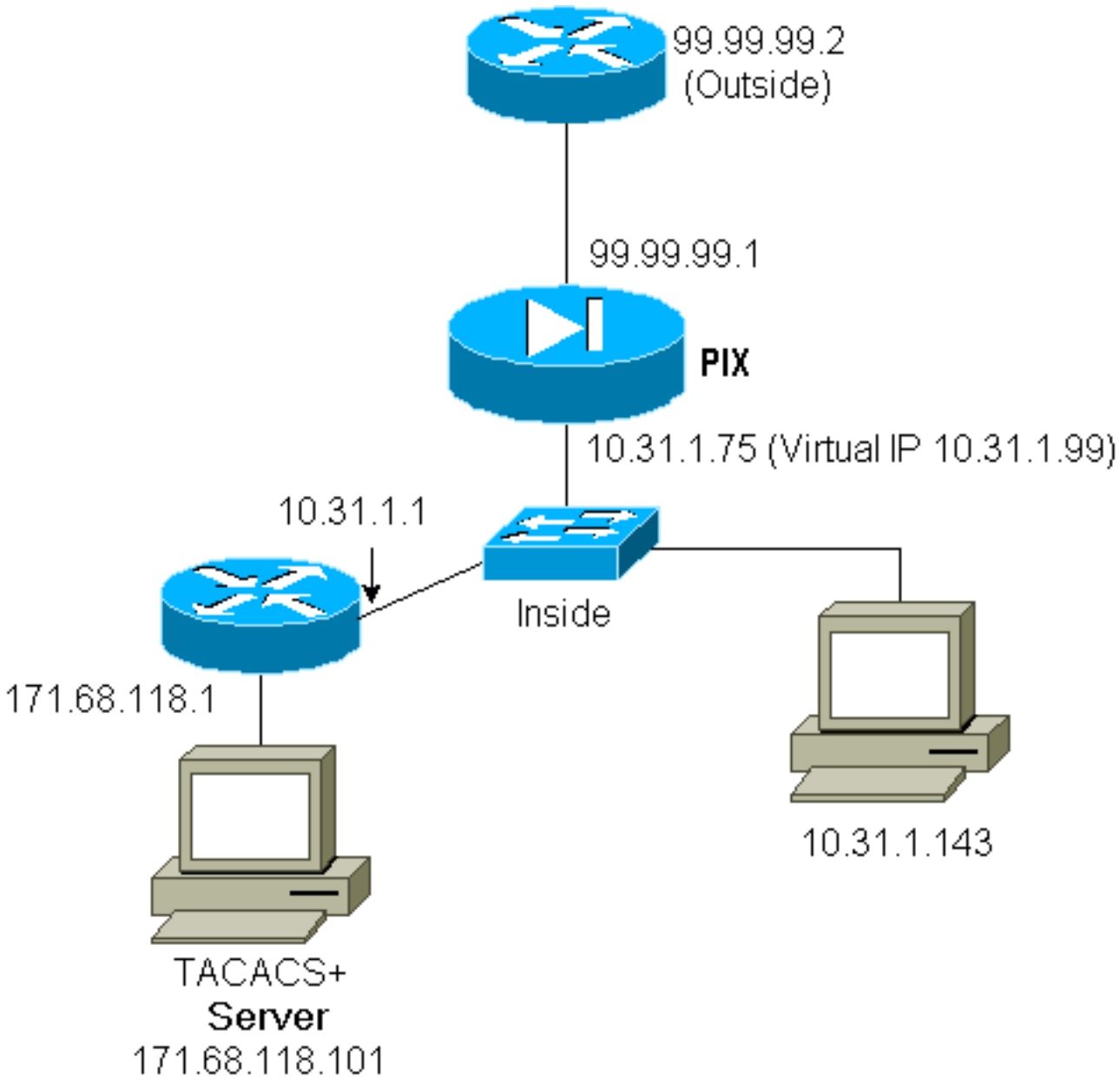
Om dit te vermijden, kunt u virtueel HTTP implementeren door een RFC 1918- adres toe te voegen (dat is een adres dat onrouteerbaar is op het internet, maar geldig en uniek is voor het PIX-netwerk) aan de PIX-configuratie met de volgende opdracht:

```
virtual http #.#.#.# [warn]
```

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. Stel, zoals aangegeven in de documentatie, de opdrachtduur van de **tijdelijke versie** niet in op 0 seconden met virtuele HTTP; dit voorkomt HTTP -

verbindingen naar de echte webserver.

Virtueel HTTP-uitgaande voorbeeld



PIX-configuratie virtueel HTTP-uitgang:

```
ip address outside 99.99.99.1 255.255.255.0
ip address inside 10.31.1.75 255.255.255.0
global (outside) 1 99.99.99.7-99.99.99.10 netmask 255.255.255.0
timeout uauth 01:00:00
aaa authentication include http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa-server RADIUS protocol radius
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 5
virtual http 10.31.1.99
```

Virtueel telnet

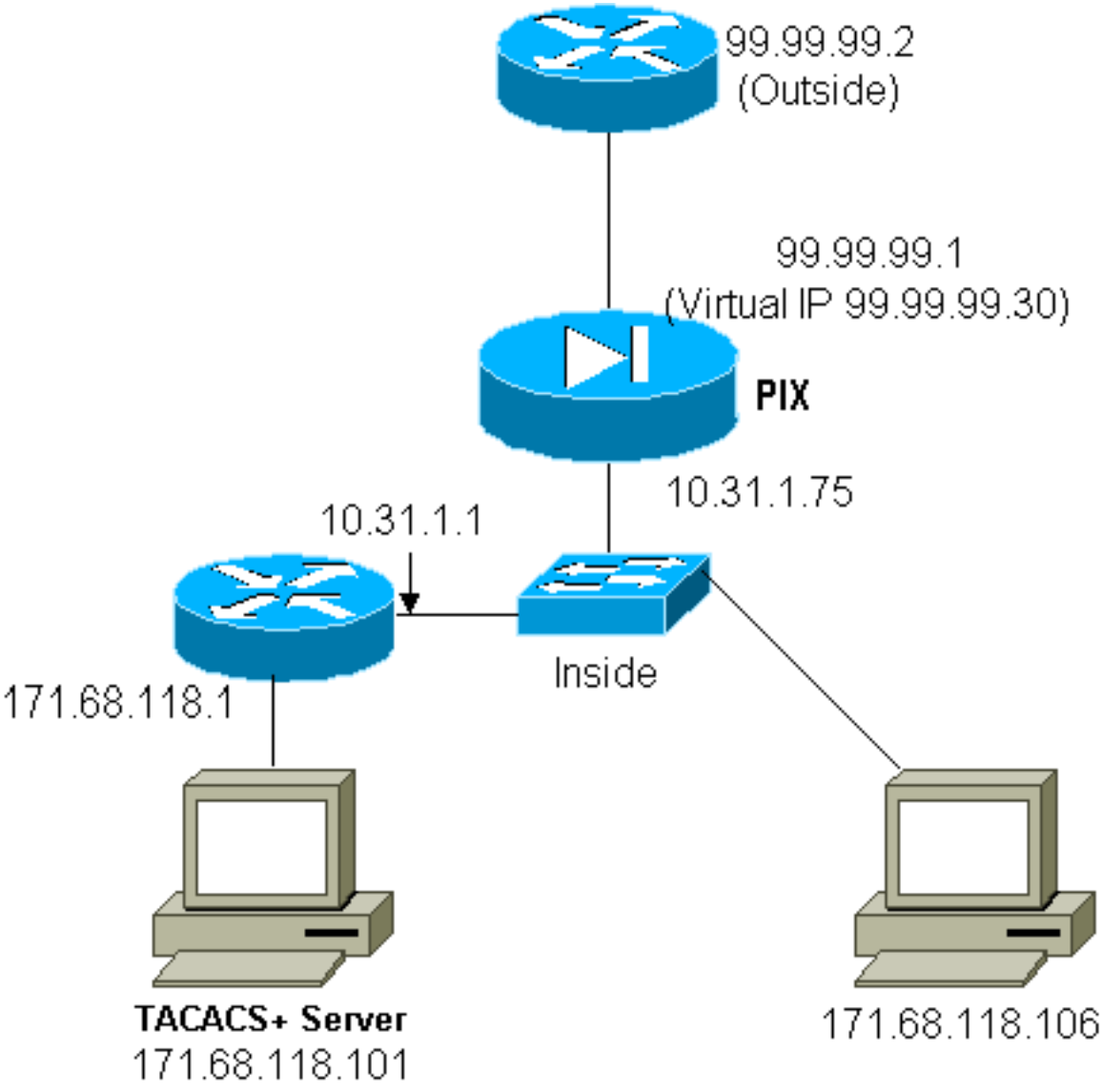
Het is mogelijk om de PIX te vormen om alle inkomende en uitgaande te authentiseren, maar het is geen goed idee omdat sommige protocollen, zoals post, niet gemakkelijk echt bevonden zijn. Wanneer een mailserver en client proberen via de PIX te communiceren wanneer al het verkeer via de PIX is geauthentiseerd, toont PIX syslogg voor onauthentiek verklaarde protocollen berichten zoals:

```
109013: User must authenticate before using
    this service
109009: Authorization denied from 171.68.118.106/49
    to 9.9.9.10/11094    (not authenticated)
```

Maar als er echt een noodzaak is om een of ander soort ongebruikelijke service te authenticeren, kan dit gedaan worden door gebruik te maken van de **virtuele telnet** opdracht. Deze opdracht maakt verificatie mogelijk naar het virtuele IP-adres van telnet. Na deze authenticatie kan het verkeer voor de ongebruikelijke service naar de echte server gaan.

In dit voorbeeld, wil u TCP poort 49 verkeer om van buiten host 99.99.99.2 naar binnen host 171.68.118.106 te stromen. Aangezien dit verkeer niet echt authentiek is, moet u een virtueel telnet instellen. Voor virtueel telnet moet er een bijbehorende statische installatie zijn. Hier zijn zowel 99.99.99.20 als 171.68.118.20 virtuele adressen.

Virtueel telnet inkomend



PIX-configuratie virtueel telnet inkomend

```
ip address outside 99.99.99.1 255.255.255.0
ip address inside 10.31.1.75 255.255.255.0
static (inside,outside) 99.99.99.20 171.68.118.20 netmask 255.255.255.255 0 0
static (inside,outside) 99.99.99.30 171.68.118.106 netmask 255.255.255.255 0 0
conduit permit tcp host 99.99.99.20 eq telnet any
conduit permit tcp host 99.99.99.30 eq tacacs any
aaa-server TACACS+ protocol tacacs+
aaa-server Incoming protocol tacacs+
aaa-server Incoming (inside) host 171.68.118.101 cisco timeout 5
aaa authentication include telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Incoming
aaa authentication include tcp/49 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Incoming
virtual telnet 99.99.99.20
```

PIX debug virtueel telnet ingesloten

De gebruiker moet op 99.99.99.2 eerst een authenticatie uitvoeren door Telnetting op het adres 99.99.20 op PIX:

```
109001: Auth start for user '???' from
    99.99.99.2/22530 to 171.68.118.20/23
 109011: Authen Session Start: user 'cse', Sid 13
 109005: Authentication succeeded for user
    'cse' from 171.68.118.20/23 to
    99.99.99.2/22530 on interface outside
```

Na de succesvolle authenticatie toont de **show** uauth opdracht de gebruiker "tijd op de meter":

```
pixfirewall# show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
user 'cse' at 99.99.99.2, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

En wanneer het apparaat om 99.99.99.2 TCP/49 verkeer naar het apparaat wil sturen om 171.68.118.106:

```
302001: Built inbound TCP connection 16
    for faddr 99.99.99.2/11054 gaddr
    99.99.99.30/49 laddr 171.68.118.106/49 (cse)
```

Er kan een vergunning worden toegevoegd:

```
aaa authorization include tcp/49 inbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

zodat wanneer TCP/49-verkeer via de PIX wordt geprobeerd, de PIX-zoekopdracht ook naar de server wordt gestuurd:

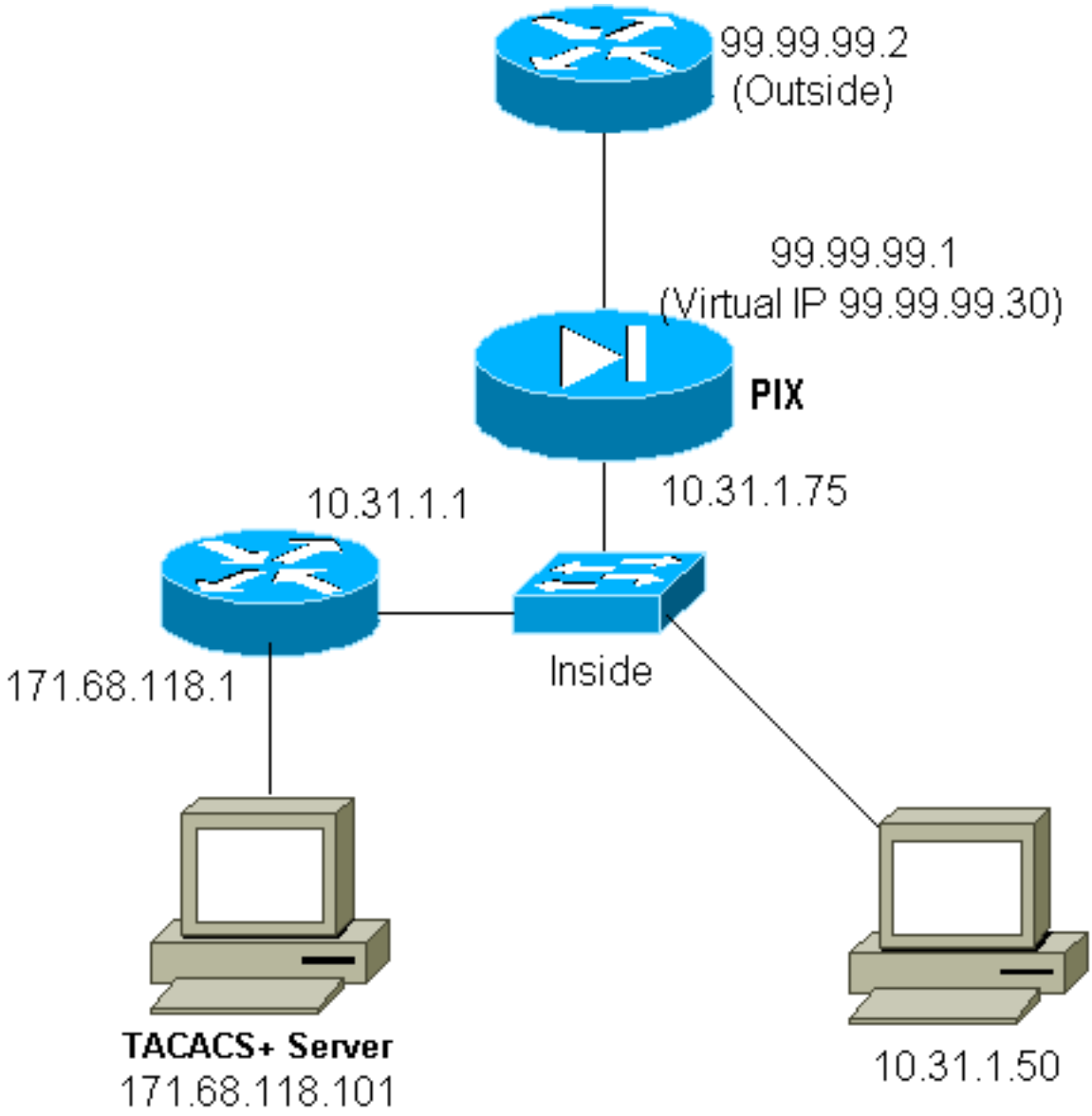
```
109007: Authorization permitted for user 'cse'
    from 99.99.99.2/11057 to 171.68.118.106/49
    on interface outside
```

Op de TACACS+ server wordt dit gezien als:

```
service=shell,
  cmd=tcp/49,
  cmd-arg=171.68.118.106
```

Uitgaande virtuele telnet

Aangezien het uitgaande verkeer standaard is toegestaan, is er geen statisch geluid vereist voor het gebruik van virtueel telnet. In het volgende voorbeeld, de binnengebruiker op 10.31.1.50 Telnetten aan virtueel 99.99.99.30 en authentificeert; De Telnet-verbinding wordt onmiddellijk verbroken. Zodra echt geauthentiseerd, wordt het TCP-verkeer toegestaan van 10.31.1.50 naar de server op 99.99.99.2:



PIX-configuratie virtueel telnet uit:

```
ip address outside 99.99.99.1 255.255.255.0
ip address inside 10.31.1.75 255.255.255.0
global (outside) 1 99.99.99.7-99.99.99.10 netmask 255.255.255.0
timeout uauth 0:05:00 absolute
aaa-server RADIUS protocol radius
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 5
aaa authentication include telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication include tcp/49 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
virtual telnet 99.99.99.30
```

Opmerking: Er is geen vergunning aangezien dit RADIUS is.

PIX Debug Virtual Telnet-uitgang:

```
109001: Auth start for user '???' from 10.31.1.50/11034
    to 99.99.99.30/23
 109011: Authen Session Start: user 'pixuser', Sid 16
 109005: Authentication succeeded for user 'pixuser'
    from 10.31.1.50/11034 to 99.99.99.30/23 on interface
    inside
 302001: Built outbound TCP connection 18 for faddr
    99.99.99.2/49 gaddr 99.99.99.8/11036 laddr
    10.31.1.50/11036 (pixuser)
 302002: Teardown TCP connection 18 faddr 99.99.99.2/49
    gaddr 99.99.99.8/11036 laddr 10.31.1.50/11036
    duration 0:00:02 bytes 0 (pixuser)
```

Vastlegging virtueel telnet

Wanneer gebruikers net naar het virtuele IP-adres van telnet tellen, toont de **show** Uauth-opdracht hun uauth. Als de gebruikers willen voorkomen dat het verkeer door gaat nadat hun sessies zijn beëindigd wanneer er tijd in de auth is, moeten ze opnieuw telnet aan het virtuele IP-adres van telnet. Dit beukt de sessie af.

Na eerste authenticatie:

```
 pix3# show uauth
                         Current    Most Seen
 Authenticated Users       1          2
 Authen In Progress        0          1
 user 'pixuser' at 10.31.1.50, authenticated
    absolute   timeout: 0:05:00
    inactivity timeout: 0:00:00
 pix3# 109001: Auth start for user 'pixuser' from
    10.31.1.50/11038 to 99.99.99.30/23
 109005: Authentication succeeded for user 'pixuser'
    from 10.31.1.50/11038 to 99.99.99.30/23 on
    interface inside
```

Na tweede echtheidscontrole (d.w.z. het gat is gesloten):

```
 pix3# show uauth
                         Current    Most Seen
 Authenticated Users       0          2
```

```
Authen In Progress        0          1
```

Poortautorisatie

Vergunning is toegestaan voor poortbereik (zoals TCP/30-100). Als virtueel telnet is ingesteld op PIX en een machtiging voor een verzameling poorten, nadat het gat is geopend met virtueel telnet, geeft de PIX een opdracht Tcp**/30-100** uit aan de TACACS+ server voor goedkeuring:

```
static (inside,outside) 99.99.99.75 10.31.1.50 netmask 255.255.255.255 0 0
conduit permit tcp host 99.99.99.75 host 99.99.99.2
static (inside,outside) 99.99.99.75 10.31.1.50 netmask 255.255.255.255 0 0
virtual telnet 99.99.99.75
aaa authentication include any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authorization include tcp/30-100 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
virtual telnet 99.99.99.30
```

Configuratie van TACACS+ Freeware-server:

```
user = anyone {
         login = cleartext "anyone"
         cmd = tcp/30-100 {
         permit 10.31.1.50
         }
         }
```

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

Nadat we er zeker van waren dat virtueel telnet werkte om TCP/49-verkeer naar de host in het netwerk toe te staan, besloten we dat we dit wilden verwerken, dus voegden we eraan toe:

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

Dit leidt tot een vermindering van de boekhoudkundige gegevens wanneer het tcp/49-verkeer doorgaat (dit voorbeeld komt uit de TACACS+-vrijeware):

```
Sun Feb 27 05:24:44 2000 10.31.1.75 cse PIX
    99.99.99.2 start task_id=0x14 foreign_ip=99.99.99.2 local_ip=171.68.118.106
    cmd=tcp/49
```

Uitgebreide verificatie (Xauth)

Configuraties van voorbeelden

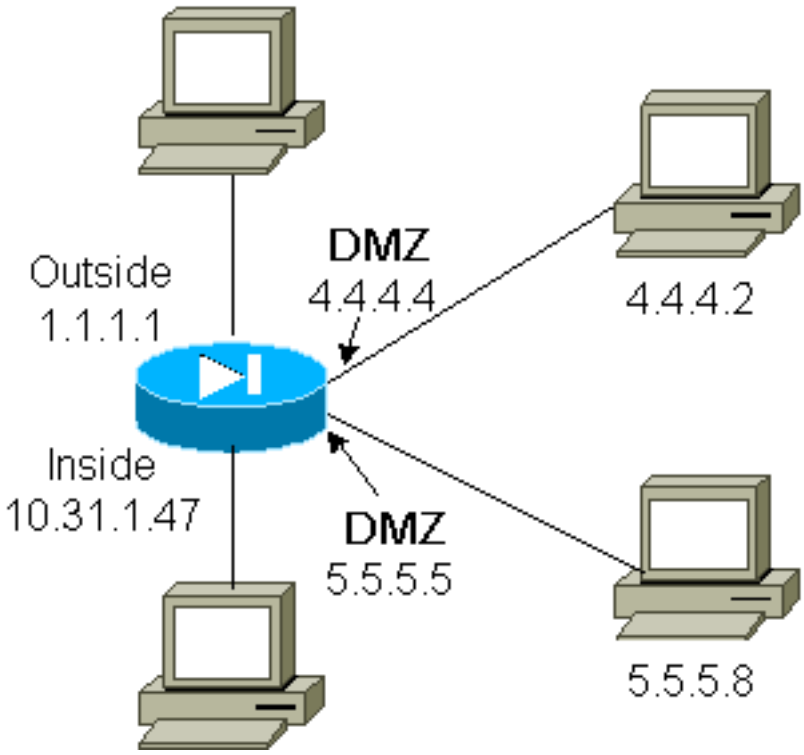
- Beëindiging van IPSec-tunnels op meerdere Cisco beveiligde PIX-firewallinterfaces met Xauth
- IPsec tussen Cisco Secure PIX-firewall en een VPN-client met uitgebreide verificatie

Verificatie via DMZ

Om gebruikers die van één interface DMZ naar een andere gaan voor de authenticatie te verklaren, vertel de PIX om verkeer voor de genoemde interfaces voor de authenticatie te zorgen. In onze PIX is de regeling:

```
least secure

PIX outside (security0) = 1.1.1.1

pix/intf4 (DMZ - security20) = 4.4.4.4 & device 4.4.4.2

pix/intf5 (DMZ - security25) = 5.5.5.5 & device 5.5.5.8

(static to 4.4.4.15)

PIX inside (security100) = 10.31.1.47

 most secure
```

Netwerkdiagram



PIX-configuratie

We willen Telnet-verkeer tussen pix/intf4 en pix/intf5 authentiek uiten:

```
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
ip address outside 1.1.1.1 255.255.255.0
ip address inside 10.31.1.47 255.255.255.0
(ip address pix/intf2 127.0.0.1 255.255.255.255
ip address pix/intf3 127.0.0.1 255.255.255.255)
```

```
ip address pix/intf4 4.4.4.4 255.255.255.0
ip address pix/intf5 5.5.5.5 255.255.255.0
static (pix/intf5,pix/intf4) 4.4.4.15 5.5.5.8 netmask 255.255.255.255 0 0
aaa authentication telnet pix/intf4 5.5.5.0 255.255.255.0
4.4.4.0 255.255.255.0 AuthInbound
aaa authentication telnet pix/intf5 5.5.5.0 255.255.255.0
4.4.4.0 255.255.255.0 AuthInbound
aaa-server TACACS+ protocol tacacs+
aaa-server AuthInbound protocol tacacs+
aaa-server AuthInbound (inside) host 171.68.118.101 cisco timeout 5
```

Xauth-accounting

Als de opdracht **snelverbinding-ipsec**, niet de **voor systeem bestemde ipsec pl-compatibele** opdracht, in PIX met breedte is ingesteld, is accounting geldig voor TCP-verbindingen, maar niet voor ICMP of UDP.

Gerelateerde informatie

- PIX-productondersteuningspagina
- PIX-opdracht
- RADIUS-ondersteuningspagina
- Verzoeken om opmerkingen (RFC's)
- Cisco Secure UNIX-ondersteuningspagina
- Cisco Secure ACS voor Windows-ondersteuningspagina
- Technische ondersteuning - Cisco-systemen