PIX 5.0.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 TCP protocollen kan gewoonlijk gemaakt worden om te werken.

De TACACS+-vergunning wordt ondersteund. RADIUS-autorisatie is dat niet. Veranderingen in de PIX 5.0 authenticatie, autorisatie en accounting (AAA) via de vorige versie omvatten AAA accounting voor verkeer anders dan HTTP, FTP en telnet.

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

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

Verificatie vs. autorisatie

- Verificatie is wie de gebruiker is.
- autorisatie is wat de gebruiker kan doen.
- Verificatie *is* geldig zonder vergunning.
- De vergunning is *niet* geldig zonder echtheidscontrole.

Als voorbeeld, neem aan dat u 1-honderd gebruikers binnen hebt en u wilt slechts zes van deze gebruikers hebben om FTP, telnet, of HTTP buiten het netwerk te kunnen doen. Vertel de PIX om uitgaande verkeer te authentiseren en geef alle zes gebruikers-IDs op de TACACS+/RADIUS-beveiligingsserver. Met eenvoudige *authenticatie*, kunnen deze zes gebruikers geauthentiseerd worden met gebruikersnaam en wachtwoord, en dan naar buiten gaan. De andere 94 gebruikers kunnen niet de straat op. De PIX vraagt gebruikers om een gebruikersnaam/wachtwoord en geeft vervolgens hun gebruikersnaam en wachtwoord door aan de TACACS+/RADIUS-beveiligingsserver. Afhankelijk van de reactie, opent of ontkent het de verbinding. Deze zes gebruikers kunnen FTP, telnet of HTTP doen.

Aan de andere kant, neem aan dat *een* van deze drie gebruikers, "Terry," niet te vertrouwen is. U zou Terry willen toestaan om FTP te doen, maar niet HTTP of telnet aan de buitenkant. Dat betekent dat je *toestemming* moet geven. Dat wil zeggen, autoriseren *wat* gebruikers kunnen doen naast het authentiseren *van wie* ze zijn. Wanneer u *toestemming* aan de PIX toevoegt, stuurt de PIX eerst Terry's gebruikersnaam en wachtwoord naar de beveiligingsserver en stuurt u vervolgens een autorisatieverzoek om de beveiligingsserver te vertellen wat "*commando*" Terry probeert te doen. Als de server goed is ingesteld, kan Terry worden toegestaan om "FTP 1.2.3.4" maar wordt de mogelijkheid ontzegd om "HTTP" of "telnet" overal te gebruiken.

Wat de gebruiker ziet met verificatie/autorisatie op

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

- **Telnet** - De gebruiker ziet een gebruikersbenaming snelle weergave, gevolgd door 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" voor gebruikersnaam en "local_password@remote_password" voor wachtwoord invoeren. 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 "Remote_password" doorgegeven naar de bestemming FTP server.
- **HTTP** - Een venster dat in de browser wordt weergegeven en dat om een gebruikersnaam en wachtwoord vraagt. 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 het lijkt dat PIX een HTTP-verbinding zou moeten afstemmen maar dit niet doet, is het waarschijnlijk dat er een nieuwe verificatie plaatsvindt met de browser die de gecached gebruikersnaam en wachtwoord opslaat naar de PIX, die dit

dan doorstuurt naar de verificatieserver. PIX syslog en/of server debug zullen dit fenomeen laten zien. Als telnet en FTP normaal lijken te werken maar HTTP connecties niet, is dit waarom.

Security Server-configuraties gebruikt voor alle scenario's

Cisco Secure UNIX-TACACS-serverconfiguratie

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 grafische gebruikersinterface (GUI) om de PIX IP 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 Windows 2.x RADIUS

Ga als volgt te werk:

1. Wachtwoord verkrijgen in het vak User Setup GUI.
2. Stel eigenschap 6 (servicetype) in op Aanmelden of Beheers vanuit het gedeelte Group Setup GUI.
3. Voeg PIX IP toe in de NAS Configuration GUI.

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 u telnet aan specifieke sites wilt toestaan, specificeert u de IP(en) in het argument gedeelte in het formulier "vergunning #.#.#". Om telnet aan alle plaatsen 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 krijgt een wachtwoord in de sectie GUI van de gebruikersinstelling.

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 u telnet aan specifieke sites wilt toestaan, specificeert u de licentie IP(s) in de argument-rechthoek (bijvoorbeeld "licentie 1.2.3.4"). Om telnet aan alle plaatsen toe te staan, klik **staat alle niet beursgenoteerde argumenten toe**.
5. Klik op **opdracht Bewerken**.
6. Voer de vorige stappen uit voor elk van de toegestane opdrachten (bijvoorbeeld telnet, HTTP en/of FTP).
7. Voeg de PIX IP toe in de sectie NAS Configuration GUI.

Configuratie van Livingston RADIUS-server

Voeg de PIX IP en de sleutel aan clientbestand toe.

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

Configuratie van RADIUS-server Merken

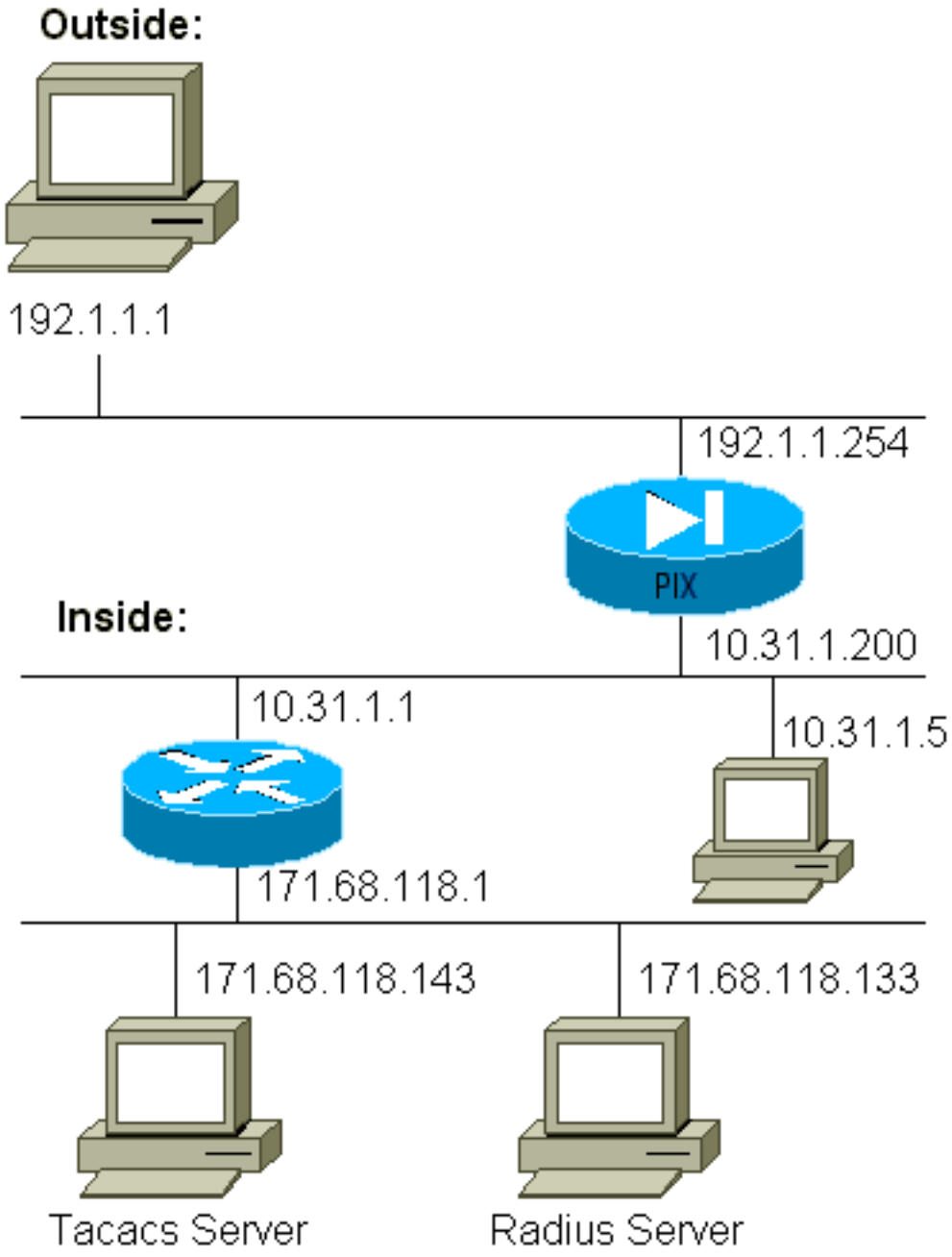
Voeg de PIX IP en de sleutel aan het clientbestand toe.

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

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

- Zorg ervoor dat de PIX-configuraties werken 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.
- Registratie in PIX inschakelenDe opdracht **voor het** foutherstellen van de **houtkapconsole** *mag niet* op een zwaar geladen systeem worden gebruikt.De **houtkapgebufferde** opdracht kan worden gebruikt. Uitvoer van de opdrachten **show logging** of **logging** kan naar een server worden verzonden en onderzocht.
- Zorg ervoor dat het debuggen is voor de TACACS+ of RADIUS servers. Alle servers hebben deze optie.

Netwerkdiagram



PIX-configuratie

```
pix-5# write terminal
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pixfirewall
 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
 name 1.1.1.1 abcd
 name 1.1.1.2 a123456789
 name 1.1.1.3 a123456789123456
 pager lines 24
 logging timestamp
 no logging standby
```

```
 logging console debugging
 no logging monitor
 logging buffered debugging
 no logging trap
 logging facility 20
 logging queue 512
 interface ethernet0 auto
 interface ethernet1 auto
 mtu outside 1500
 mtu inside 1500
 ip address outside 192.1.1.254 255.255.255.0
 ip address inside 10.31.1.200 255.255.255.0
 no failover
 failover timeout 0:00:00
 failover ip address outside 0.0.0.0
 failover ip address inside 0.0.0.0
 arp timeout 14400
 global (outside) 1 192.1.1.10-192.1.1.20 netmask
255.255.255.0
 static (inside,outside) 192.1.1.25 171.68.118.143
netmask 255.255.255.255 0 0
 static (inside,outside) 192.1.1.30 10.31.1.5 netmask
255.255.255.255 0 0
 conduit permit tcp any any
 conduit permit icmp any any
 conduit permit udp any any
 no rip outside passive
 no rip outside default
 no rip inside passive
 no rip inside default
 route inside 171.68.118.0 255.255.255.0 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 0:00:00 absolute
 aaa-server TACACS+ protocol tacacs+
 aaa-server RADIUS protocol radius
 aaa-server AuthInbound protocol tacacs+
 aaa-server AuthInbound (inside) host 171.68.118.143
cisco timeout 5
 aaa-server AuthOutbound protocol radius
 aaa-server AuthOutbound (inside) host 171.68.118.133
cisco timeout 5
 aaa authentication telnet outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound
 aaa authentication telnet inbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthInbound
 aaa authentication http outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound
 aaa authentication http inbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 AuthInbound
 aaa authentication ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 AuthOutbound
 aaa authentication 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
 telnet timeout 5
 terminal width 80
 Cryptochecksum:fef4bfc9801d7692dce0cf227fe7859b
 : end
```

Verificatie Debug Voorbeelden van PIXAverificatie Debug Voorbeelden van PIX

In deze debug-voorbeelden:

Uitgaand

De interne gebruiker om 10.31.1.5 initieert verkeer naar buiten 192.1.1.1 en is authentiek door TACACS+. De lijst AutoOutbound van het verkeer gebruikt server die "AuthOutbound" bevat RADIUS-server 171.68.118.133.

Inkomend

De externe gebruiker start op 192.1.1.1 verkeer naar binnen 10.31.1.5 (192.1.1.30) en is geauthentiseerd door TACACS. De lijst van het inkomende verkeer gebruikt server "AuthInbound" die TACACS server 171.68.118.143 omvat).

PIX-debug - goede verificatie - TACACS+

Dit voorbeeld toont een PIX debug met goede authenticatie:

```
pixfirewall# 109001: Auth start for user "???" from 192.1.1.1/13155
    to 10.31.1.5/23
 109011: Authen Session Start: user 'pixuser', sid 6
 109005: Authentication succeeded for user 'pixuser' from 10.31.1.5/23
    to 192.1.1.1/13155
 109012: Authen Session End: user 'pixuser', Sid 6, elapsed 1 seconds
 302001: Built inbound TCP connection 6 for faddr 192.1.1.1/13155
    gaddr 192.1.1.30/23 laddr 10.31.1.5/23 (pixuser)
```

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

Dit voorbeeld toont PIX debug met slechte authenticatie (gebruikersnaam of wachtwoord). De gebruiker ziet vier gebruikersnaam/wachtwoordgroepen en het bericht "`Fout: max aantal overschrijdingen`."

```
pixfirewall# 109001: Auth start for user '???' from 192.1.1.1/13157
    to 10.31.1.5/23
 109006: Authentication failed for user '' from 10.31.1.5/23
    to 192.1.1.1/13157
```

PIX debug - Kan Ping Server, geen respons - TACACS+

Dit voorbeeld toont PIX debug waar de server kan worden gepeld maar niet met PIX spreekt. De gebruiker ziet een gebruikersnaam eenmaal, maar PIX vraagt nooit om een wachtwoord (dit is op telnet). De gebruiker ziet "`Fout: Max. aantal overschrijdingen.`"

```
Auth start for user '???' from 192.1.1.1/13159 to
    10.31.1.5/23
 pixfirewall# 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13159
    failed (server 171.68.118.143 failed)
```

```
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13159 failed
    (server 171.68.118.143 failed)
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13159 failed
    (server 171.68.118.143 failed)
 109006: Authentication failed for user '' from 10.31.1.5/23
    to 192.1.1.1/13159
```

PIX Debug - Kan geen Ping Server - TACACS+

Dit voorbeeld toont een PIX debug waar de server niet pingable is. De gebruiker ziet een gebruikersnaam maar de PIX vraagt nooit om een wachtwoord (dit is op telnet). Deze berichten worden weergegeven: "`Time-out bij TACACS+ server`" en "`fout: Max. aantal probeert te overschrijden`" (we hebben in de configuratie een server met belletjes aangezet).

```
109001: Auth start for user '???' from 192.1.1.1/13158
    to 10.31.1.5/23
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed
    (server 171.68.118.143 failed)
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed
    (server 171.68.118.143 failed)
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed
    (server 171.68.118.143 failed)
 109006: Authentication failed for user '' from 10.31.1.5/23
    to 192.1.1.1/13158
```

PIX-debug - goede verificatie - RADIUS

Dit voorbeeld toont een PIX debug met goede authenticatie:

```
109001: Auth start for user '???' from 10.31.1.5/11074
    to 192.1.1.1/23
 109011: Authen Session Start: user 'pixuser', Sid 7
 109005: Authentication succeeded for user 'pixuser'
    from 10.31.1.5/11074 to 192.1.1.1/23
 109012: Authen Session End: user 'pixuser', Sid 7,
    elapsed 1 seconds
 302001: Built outbound TCP connection 7 for faddr 192.1.1.1/23
    gaddr 192.1.1.30/11074 laddr 10.31.1.5/11074 (pixuser)
```

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

Dit voorbeeld toont een PIX debug met slechte authenticatie (gebruikersnaam of wachtwoord). De gebruiker ziet een verzoek om gebruikersnaam en wachtwoord. De gebruiker heeft drie mogelijkheden voor een succesvol gebruikersnaam/wachtwoord.

```
- 'Error: max number of tries exceeded'
 pixfirewall# 109001: Auth start for user '???' from
    192.1.1.1/13157 to 10.31.1.5/23
 109001: Auth start for user '???' from 10.31.1.5/11075
    to 192.1.1.1/23
 109002: Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109002: Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109002: Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11075
    to 192.1.1.1/23
```

Ping Debug - Can Ping Server, Daemon Down - RADIUS

Dit voorbeeld toont een PIX debug waar de server pingable is, maar de daemon is beneden en zal niet met PIX communiceren. De gebruiker ziet Gebruikersnaam, wachtwoord en de berichten "`RADIUS-server is mislukt`" en "`Fout: Max. aantal overschrijdingen.`"

```
pixfirewall# 109001: Auth start for user '???'
    from 10.31.1.5/11076 to 192.1.1.1/23
 109002: Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109002: Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109002: Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11076
    to 192.1.1.1/23
```

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

Dit voorbeeld geeft een PIX-debug op plaatsen waar de server niet pingable is of waar een key/client-mismatch is. De gebruiker ziet Gebruikersnaam, wachtwoord en de berichten "`Time-out bij RADIUS-server`" en "`Fout: Max. aantal probeert te overschrijden`" (een server met een bellengenerator is in de configuratie aangevallen).

```
109001: Auth start for user '???' from 10.31.1.5/11077
    to 192.1.1.1/23
 109002: Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed
    (server 100.100.100.100 failed)
 109002: Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed
    (server 100.100.100.100 failed)
 109002: Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed
    (server 100.100.100.100 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11077
    to 192.1.1.1/23
```

Toevoegen autorisatie

Indien u besluit een vergunning toe te voegen, zult u een vergunning voor dezelfde bron- en doelgroep nodig hebben (aangezien de vergunning niet geldig is zonder echtheidscontrole):

```
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
```

Merk op dat er geen vergunning voor "uitgaande" is toegevoegd omdat het uitgaande verkeer met RADIUS is geauthentiseerd en de RADIUS-vergunning niet geldig is.

Verificatie en autorisatie Debug Voorbeelden van PIX

PIX debug - goede verificatie en succesvolle autorisatie - TACACS+

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

```
109011: Authen Session Start: user 'pixuser', Sid 8
 109007: Authorization permitted for user 'pixuser'
    from 192.1.1.1/13160 to 10.31.1.5/23
 109012: Authen Session End: user 'pixuser', Sid 8,
    elapsed 1 seconds
 302001: Built inbound TCP connection 8 for faddr 192.1.1.1/13160
    gaddr 192.1.1.30/23 laddr 10.31.1.5/23 (pixuser)
```

PIX debug - goede verificatie, mislukte autorisatie - TACACS+

Dit voorbeeld toont een PIX-debug met goede authenticatie maar met een mislukte autorisatie. Hier ziet de gebruiker ook het bericht "`Fout: Vergunning geweigerd.`"

```
109001: Auth start for user '???' from 192.1.1.1/13162
    to 10.31.1.5/23
 109011: Authen Session Start: user 'userhttp', Sid 10
 109005: Authentication succeeded for user 'userhttp'
    from 10.31.1.5/23 to 192.1.1.1/13162
 109008: Authorization denied for user 'userhttp'
    from 10.31.1.5/23 to 192.1.1.1/13162
 109012: Authen Session End: user 'userhttp', Sid 10,
    elapsed 1 seconds
 302010: 0 in use, 2 most used
```

Voeg accounting toe

TACACS+

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

Debug kijkt hetzelfde of accounting aan of uit is. Ten tijde van het "Built" wordt echter een "start"-boekhouding verstuurd. Op het tijdstip van de "Teardown" wordt een "stop" - boekhouding verstuurd.

De TACACS+ accounting records lijken op deze uitvoer (deze zijn van Cisco Secure NT, vandaar de comma-toegewezen indeling):

```
04/26/2000,01:31:22,pixuser,Default Group,192.1.1.1,
  start,,,,,,,0x2a,,PIX,10.31.1.200,telnet,6,
  Login,1,,,1,,,,,,,,,,,local_ip=10.31.1.5 foreign_ip=192.1.1.1,
  ,, ,,,,,,,,,zekie,,,,,,,,^
04/26/2000,01:31:26,pixuser,Default Group,192.1.1.1,stop,4,
  ,36,82,,,0x2a,,PIX,10.31.1.200,telnet,6,
  Login,1,,,1,,,,,,,,,,,local_ip=10.31.1.5 foreign_ip=192.1.1. 1,
  ,,,,,,,,,,,zekie,,,,,,,,
```

RADIUS

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

Debug ziet er hetzelfde uit of accounting aan of uit is. Ten tijde van het "Built" wordt echter een

"start"-boekhouding verstuurd. Op het tijdstip van de "Teardown" wordt een "stop" - boekhouding verstuurd.

RADIUS-accounting records lijken op deze uitvoer (deze zijn van Cisco Secure UNIX); Degenen in Cisco Secure NT kunnen daarentegen komma-delimated zijn):

```
radrecv: Request from host a1f01c8 code=4, id=18, length=65
Acct-Status-Type = Start
Client-Id = 10.31.1.200
Login-Host = 10.31.1.5
Login-TCP-Port = 23
Acct-Session-Id = "0x0000002f"
User-Name = "pixuser"
Sending Accounting Ack of id 18 to a1f01c8 (10.31.1.200)
radrecv: Request from host a1f01c8 code=4, id=19, length=83
Acct-Status-Type = Stop
Client-Id = 10.31.1.200
Login-Host = 10.31.1.5
Login-TCP-Port = 23
Acct-Session-Id = "0x0000002f"
Username = "pixuser"
Acct-Session-Time = 7
```

Gebruik van behalve Opdracht

Als we in ons netwerk bepalen dat een bepaalde bron en/of bestemming geen verificatie, autorisatie of accounting nodig heeft, kunnen we zoiets doen als deze output:

```
aaa authentication except inbound 192.1.1.1 255.255.255.255
   0.0.0.0 0.0.0.0 AuthInbound
```

Indien u een doos van de authenticatie "uitzondert" en toestemming heeft, moet u dit ook doen behalve het vak van de vergunning.

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"-record is, veronderstelt de TACACS+ of RADIUS-server dat de persoon nog is inlogd (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 deze voorbeelduitvoer wordt een andere netwerkconfiguratie gebruikt, maar de concepten zijn hetzelfde.

De gebruiker Telnetjes door de PIX, authentiek op weg:

```
(pix) 109001: Auth start for user '???' from 171.68.118.100/1200
    to 9.9.9.25 /23
(pix) 109011: Authen Session Start: user 'cse', Sid 3
```

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

Aangezien de server een "start"-record maar geen "stop"-record (op dit moment) heeft gezien, toont de server 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 verder met het telnet of FTP-bedrijf op de doelhost en sluit vervolgens af (besteedt 10 minuten daar):

```
(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 (elke keer authenticeren) of meer (opnieuw authenticeren tijdens de auteperiode), wordt een accounting record voor elke benaderde site bijgesneden.

HTTP werkt anders vanwege de aard van het protocol. Deze output toont 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 gepost om 16:35:34, en het stoprecord gepost om 16:35:35. Deze 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 tijdens het lezen van de webpagina? 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 start- en stop-record is sub-seconde. Er zal geen "start"-record zijn zonder "stop" record, aangezien de records vrijwel op hetzelfde moment plaatsvinden. Er wordt nog steeds "start"- 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 beschreven het authenticeren van het telnet (en HTTP, FTP) verkeer *door* de PIX. We zorgen ervoor dat net *op* de PIX werkt *zonder* verificatie op:

```
telnet 10.31.1.5 255.255.255.255 passwd ww
```

```
aaa authentication telnet console AuthInbound
```

Wanneer gebruikers Telnet aan PIX, worden ze gevraagd naar het Telnet-wachtwoord (**ww**). Vervolgens vraagt de PIX ook om de TACACS+ (in dit geval, omdat de "AuthInbound"-serverlijst wordt gebruikt) of de gebruikersnaam en het wachtwoord voor de RADIUS-verbinding. Als de server uit is, kunt u PIX invoeren door de gebruikersnaam op te geven en vervolgens het wachtwoord inschakelen (**om het wachtwoord *in* te stellen, wat dan ook** ook**) om toegang te krijgen.**

Met deze opdracht:

```
aaa authentication enable console AuthInbound
```

de gebruiker wordt gevraagd om een gebruikersnaam en een wachtwoord, die naar de TACACS (in dit geval, aangezien de "AuthInbound"-serverlijst wordt gebruikt, gaat het verzoek naar de TACACS-server) of de RADIUS-server. 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).

Verificatie op de seriële console

De opdracht **AuthInbound**-console **van de** authenticatie vereist verificatie om toegang te hebben tot de seriële console van de PIX.

Wanneer de gebruiker configuratieopdrachten uit de console uitvoert, worden de syslogberichten doorgesneden (ervan uitgaande dat de PIX is ingesteld om syslog op debug-niveau naar een syslog-host te verzenden). Dit is een voorbeeld van wat op de syslogserver wordt weergegeven:

```
logmsg: pri 245, flags 0, from [10.31.1.200.2.2], msg Nov 01 1999
 03:21:14: %PIX-5-111008: User 'pixuser' executed the 'logging' command.
```

Verander de roep die gebruikers zien

Als je de **auth-prompt PIX_PIX_PIX** opdracht hebt, zien gebruikers die door de PIX gaan deze volgorde:

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

Bij aankomst in het ultieme doelvak wordt de "Gebruikersnaam:" en "Wachtwoord:"-melding weergegeven. Deze melding heeft alleen gevolgen voor gebruikers die *door* de PIX gaan, niet *voor* de PIX.

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

De berichtgebruikers Zie Informatie over succes/falen aanpassen

Als u de opdrachten hebt:

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

gebruikers zien deze volgorde op een mislukte/succesvolle inloging via de PIX:

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

Uitgangspunten per gebruiker en absolute tijden

De inactiviteitstiptijden en de absolute waarde kunnen per gebruiker worden verstuurd vanaf de TACACS+ server. Als alle gebruikers in uw netwerk de zelfde "timeout auth" moeten hebben, voer dit niet uit! Maar als je verschillende gebruikers nodig hebt, blijf dan lezen.

In dit voorbeeld wordt de **timeout optie 3:00:00** opdracht gebruikt. Als een persoon echt is geworden, hoeft dit niet voor drie uur opnieuw te worden geauthentificeerd. Als u echter een gebruiker met dit profiel instelt en in de PIX een TACACS AAA-*vergunning* hebt, hebben de ongebruikte en absolute tijden in het gebruikersprofiel voorrang op de timeout in de PIX voor die gebruiker. Dit betekent niet dat de Telnet-sessie door de PIX wordt losgekoppeld na de stationaire/absolute time-out. Het controleert alleen of herauthenticatie plaatsvindt.

Dit profiel is afkomstig van TACACS+ software:

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

Voer na verificatie een **show uauth** opdracht uit op PIX:

```
pix-5# show uauth
                        Current    Most Seen
 Authenticated Users       1          1
 Authen In Progress        0          1
 user 'timeout' at 10.31.1.5, authorized to:
    port 11.11.11.15/telnet
    absolute   timeout: 0:02:00
    inactivity timeout: 0:01:00
```

Nadat de gebruiker één minuut niets heeft gedaan, toont het debug op de PIX:

```
109012: Authen Session End: user 'timeout', Sid 19, elapsed 91 seconds
```

De gebruiker moet opnieuw echt verklaren wanneer het naar de zelfde doelgastheer of een andere gastheer terugkeert.

Virtuele HTTP

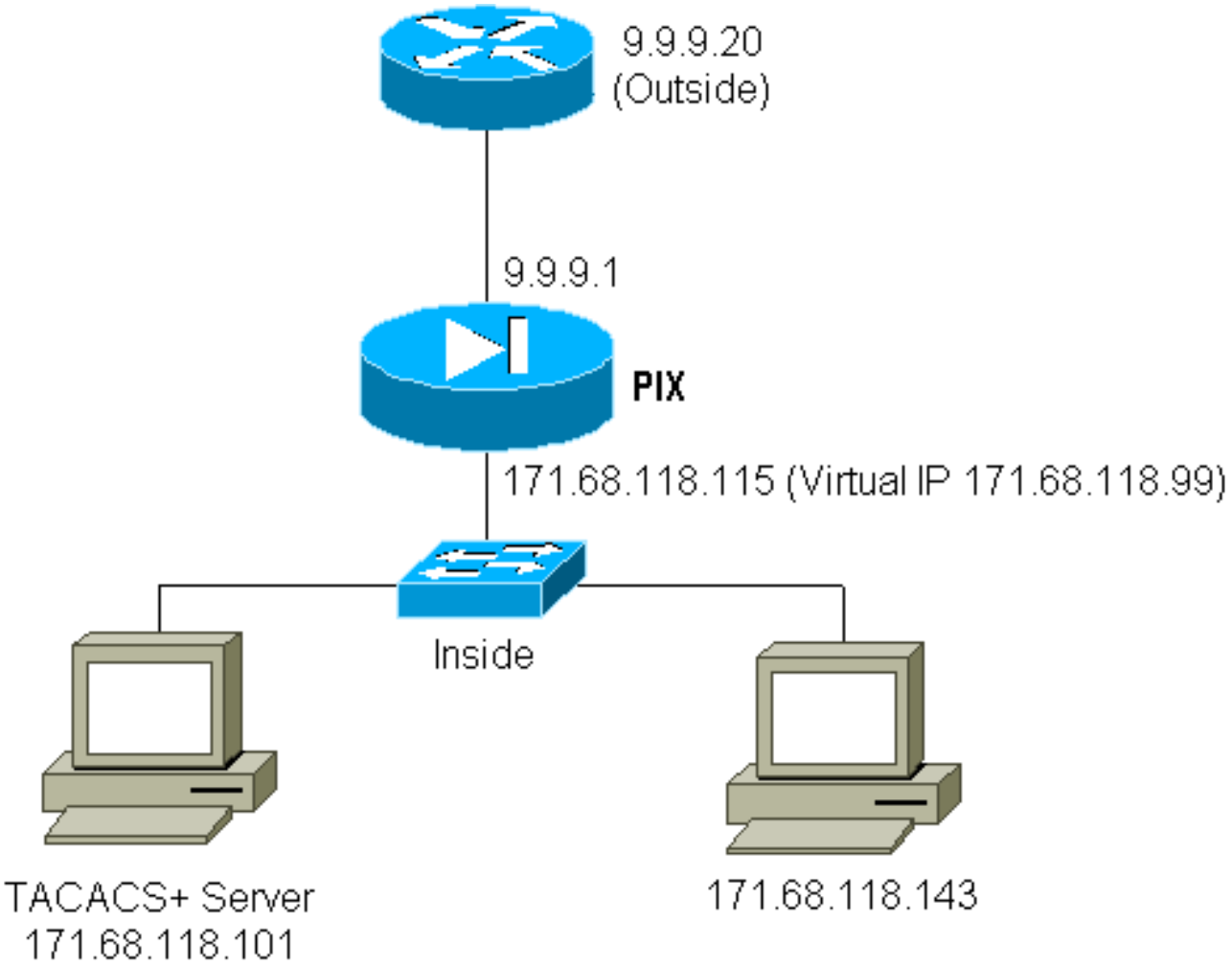
Als verificatie vereist is op sites buiten de PIX, zowel als op de PIX zelf, kan ongebruikelijk browser gedrag soms worden waargenomen aangezien browsers de gebruikersnaam en het wachtwoord in het geheugen plaatsen.

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

Virtueel HTTP-uitgaande diagram



PIX-configuratie virtueel HTTP-uitgang

```
ip address outside 9.9.9.1 255.255.255.0
 ip address inside 171.68.118.115 255.255.255.0
 global (outside) 1 9.9.9.5-9.9.9.9 netmask 255.0.0.0
 timeout uauth 01:00:00
 aaa-server TACACS+ protocol tacacs+
 aaa-server AuthOutbound protocol tacacs+
 aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 10
 aaa authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
 virtual http 171.68.118.99
 auth-prompt THIS_IS_PIX_5
```

Virtueel telnet

Het is mogelijk om de PIX te vormen om al binnen en uitgaande verkeer authentiek te verklaren, maar het is geen goed idee om dit te doen. Dit komt doordat bepaalde protocollen, zoals "mail", niet makkelijk geauthentiseerd zijn. Wanneer een mailserver en client proberen via de PIX te communiceren wanneer al het verkeer door de PIX is geauthentiseerd, toont PIX syslog voor niet-echt te verklaren protocollen berichten zoals:

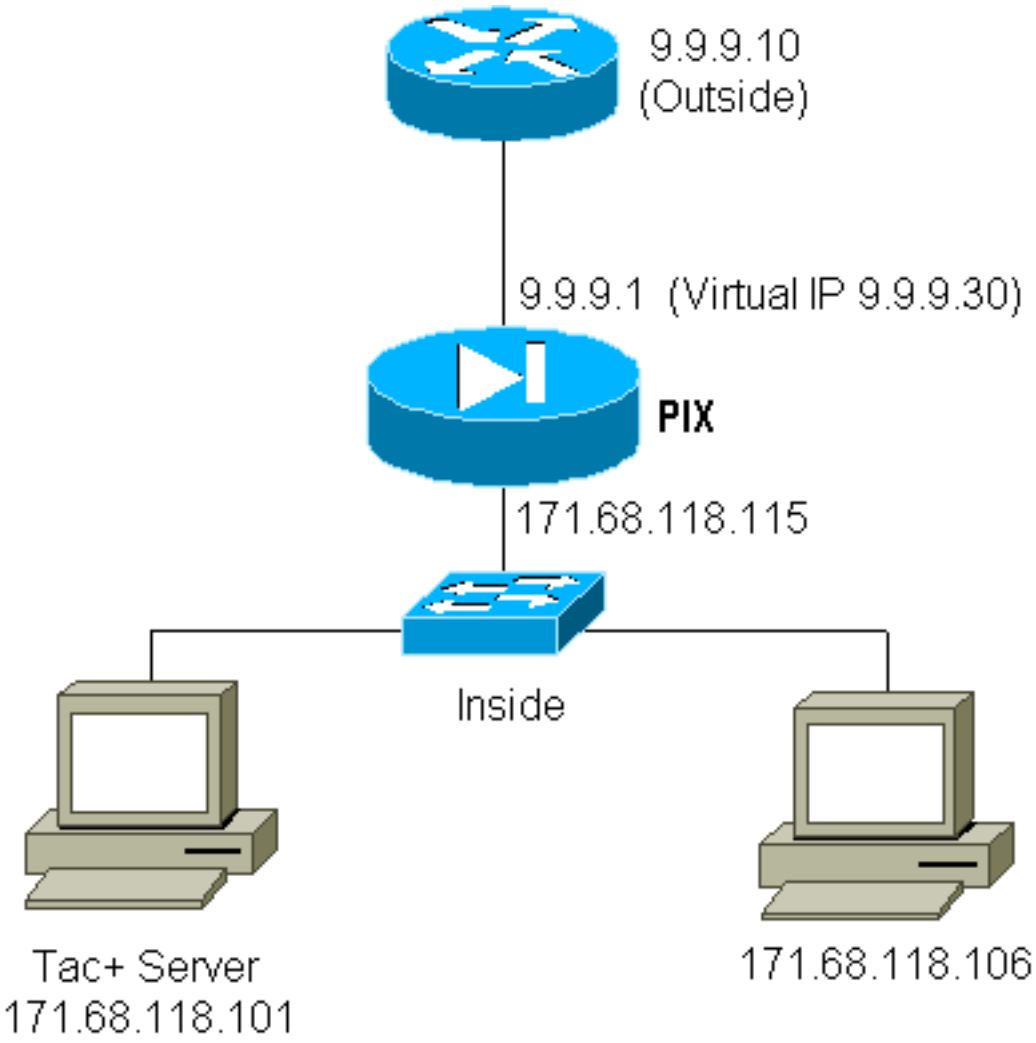
```
109001: Auth start for user '???' from 9.9.9.10/11094
    to 171.68.118.106/25
 109009: Authorization denied from 171.68.118.106/49 to
    9.9.9.10/11094 (not authenticated
```

Aangezien e-mail en sommige andere diensten niet interactief genoeg zijn om authentiek te verklaren, is één oplossing het gebruik van de **behalve** opdracht voor authenticatie/vergunning (alle behalve bron/bestemming van de postserver/client voor authenticatie authentiek).

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

In dit voorbeeld willen we TCP poort 49-verkeer van buiten host 9.9.9.10 naar binnen host 171.68.118.106. Omdat dit verkeer niet echt authentiek is, zetten we een virtueel telnet op. Voor inkomende virtuele telnet, moet er een verbonden statisch zijn. Op dit punt zijn zowel 9.9.9.20 als 17.68.118.20 virtuele adressen.

Virtueel telnet-binnendiagram



PIX-configuratie virtueel telnet inkomend

```
ip address outside 9.9.9.1 255.255.255.0
 ip address inside 171.68.118.115 255.255.255.0
 static (inside,outside) 9.9.9.20 171.68.118.20 netmask 255.255.255.255 0 0
 static (inside,outside) 9.9.9.30 171.68.118.106 netmask 255.255.255.255 0 0
 conduit permit tcp host 9.9.9.20 eq telnet any
 conduit permit tcp host 9.9.9.30 eq tacacs any
```

```
 aaa-server TACACS+ protocol tacacs+
 aaa-server AuthInbound protocol tacacs+
 aaa-server AuthInbound (inside) host 171.68.118.101 cisco timeout 5
 AAA authentication any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
 virtual telnet 9.9.9.20
```

Configuratie van virtuele telnet voor TACACS+ servers

```
user = pinecone {
default service = permit
        login = cleartext "pinecone"
service = exec {
        timeout = 10
        idletime = 10
        }
}
```

PIX debug virtueel telnet ingesloten

De gebruiker moet op 9.9.9.10 eerst authentiek verklaren door Telnetting aan het adres 9.9.9.20 op PIX:

```
pixfirewall# 109001: Auth start for user '???' from 9.9.9.10/11099
    to 171.68.118.20/23
 109011: Authen Session Start: user 'pinecone', Sid 13
 109005: Authentication succeeded for user 'pinecone'
    from 171.68.118.20/23 to 9.9.9.10/1470
```

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

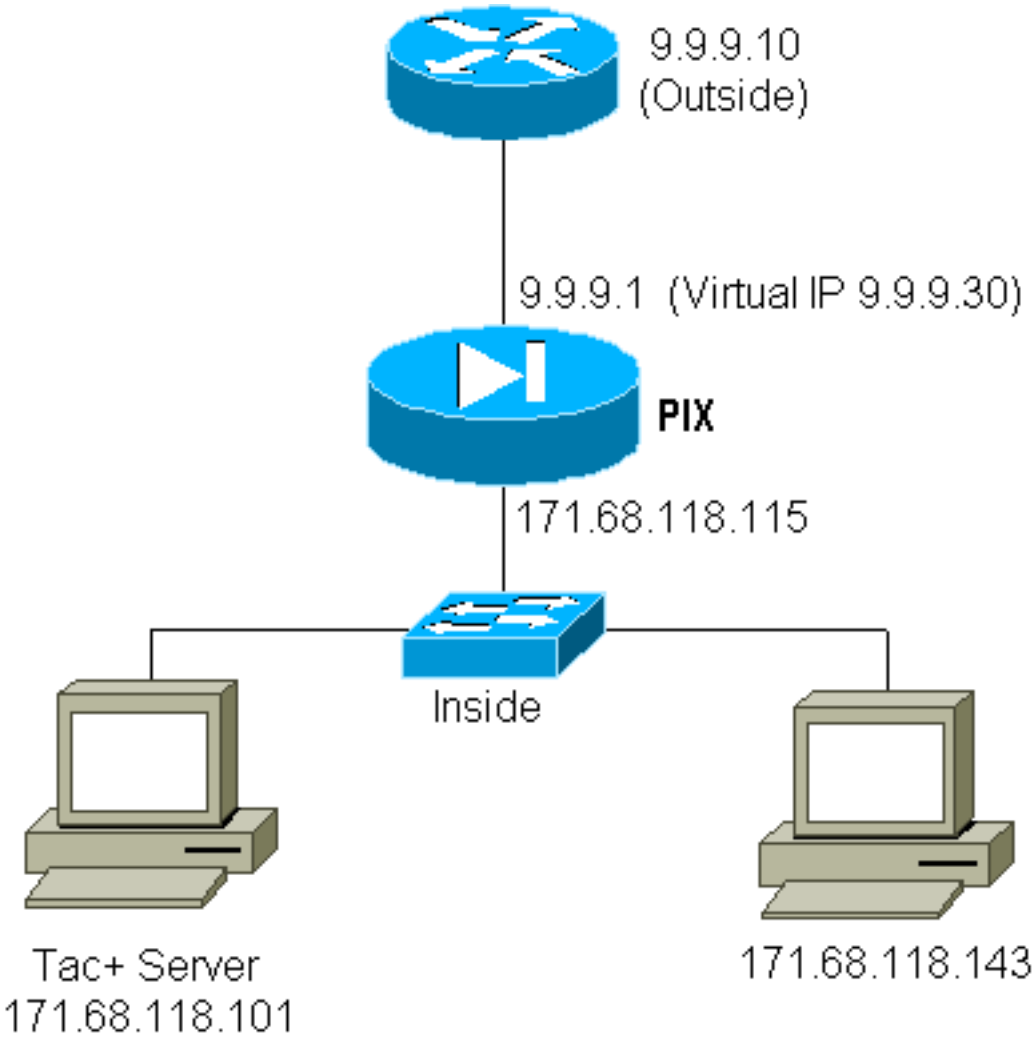
```
pixfirewall# show uauth
                         Current    Most Seen
 Authenticated Users       1          1
 Authen In Progress        0          1
 user 'pinecone' at 9.9.9.10, authenticated
    absolute   timeout: 0:10:00
    inactivity timeout: 0:10:00
```

Hier wil het apparaat om 9.9.9.10 TCP/49-verkeer naar het apparaat sturen om 17.18.106:

```
pixfirewall# 109001: Auth start for user 'pinecone' from 9.9.9.10/11104
     to 171.68.118.20/23
 109011: Authen Session Start: user 'pinecone', Sid 14
 109005: Authentication succeeded for user 'pinecone' from 171.68.118.20/23
     to 9.9.9.10/1470
 302001: Built TCP connection 23 for faddr 9.9.9.10/11104 gaddr 9.9.9.30/49
  laddr 171.68.118.106/49 (pinecone)
 302002: Teardown TCP connection 23 faddr 9.9.9.10/11104 gaddr 9.9.9.30/49
  laddr 171.68.118.106/49 duration 0:00:10 bytes 179 (pinecone)
```

Uitgaande virtuele telnet

Aangezien het uitgaande verkeer standaard is toegestaan, is er geen statisch geluid vereist voor het gebruik van virtueel telnet. In dit voorbeeld, de binnengebruiker op 171.68.118.143 Telnetten aan virtueel 9.9.9.30 en authenticeert. De Telnet-verbinding wordt onmiddellijk verbroken. Zodra echt geauthentiseerd is, wordt het TCP-verkeer toegestaan van 171.68.118.143 naar de server op 9.9.10:



PIX-configuratie virtueel telnet

```
ip address outside 9.9.9.1 255.255.255.0
 ip address inside 171.68.118.115 255.255.255.0
 global (outside) 1 9.9.9.5-9.9.9.9 netmask 255.0.0.0
 timeout uauth 00:05:00
 aaa-server TACACS+ protocol tacacs+
 aaa-server AuthOutbound protocol tacacs+
 aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 10
 AAA authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
 virtual telnet 9.9.9.30
```

PIX debug virtueel telnet

```
109001: Auth start for user '???' from 171.68.118.143/1536
     to 9.9.9.30/23
 109011: Authen Session Start: user 'timeout_143', Sid 25
 109005: Authentication succeeded for user 'timeout_143' from
    171.68.118.143/1536 to 9. 9.9.30/23
 302001: Built TCP connection 46 for faddr 9.9.9.10/80 gaddr
    9.9.9.30/1537 laddr 171.68 .118.143/1537 (timeout_143)
 304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
 302001: Built TCP connection 47 for faddr 9.9.9.10/80 gaddr
    9.9.9.30/1538 laddr 171.68 .118.143/1538 (timeout_143)
 302002: Teardown TCP connection 46 faddr 9.9.9.10/80 gaddr
    9.9.9.30/1537 laddr 171.68. 118.143/1537 duration 0:00:03
```

```
    bytes 625 (timeout_143)
 304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
 302002: Teardown TCP connection 47 faddr 9.9.9.10/80 gaddr
    9.9.9.30/1538 laddr 171.68. 118.143/1538 duration 0:00:01
    bytes 2281 (timeout_143)
 302009: 0 in use, 1 most used
```

Vastlegging virtueel telnet

Wanneer de gebruiker Telnetten aan de virtuele IP van het telnet, de opdracht van de **show** toont de uauth.

Als de gebruiker verkeer na het einde van de sessie wil voorkomen (wanneer er tijd in de auth is) moet de gebruiker opnieuw telnet naar de virtuele telnet IP. Dit beukt de sessie af.

Poortautorisatie

U kunt een vergunning voor een groot aantal havens nodig hebben. In dit voorbeeld was verificatie nog steeds vereist voor alle uitgaande poorten, maar alleen autorisatie was vereist voor TCP poorten 23-49.

PIX-configuratie

```
AAA authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
AAA authorization tcp/23-49 outbound 0.0.0.0 0.0.0.0
   0.0.0.0 0.0.0.0 AuthOutbound
```

Toen het telnet van 171.68.118.143 tot 9.9.9.10 werd gedaan, kwam de authenticatie en vergunning voor omdat Telnet poort 23 in het bereik van 23-49 ligt.

Als een HTTP-sessie wordt uitgevoerd van 171.68.118.143 tot 9.9.9.10, moet je nog steeds authenticeren, maar de PIX vraagt de TACACS+ server niet om HTTP te autoriseren omdat 80 niet binnen het bereik van 23-49 ligt.

Configuratie van TACACS+ vriesserver

```
user = telnetrange {
        login = cleartext "telnetrange"
        cmd = tcp/23-49 {
        permit 9.9.9.10
        }
        }
```

Merk op dat PIX "`cmd=tcp/23-49`" en "`cmd-arg=9.9.9.10`" naar de TACACS+ server stuurt.

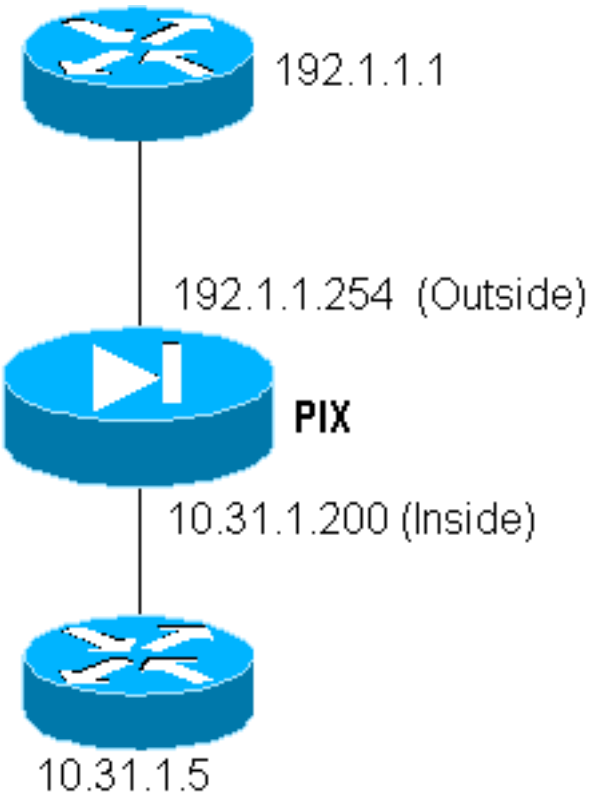
Debug in de PIX

```
109001: Auth start for user '???' from 171.68.118.143/1051
    to 9.9.9.10/23
 109011: Authen Session Start: user 'telnetrange', Sid 0
 109005: Authentication succeeded for user 'telnetrange'
```

```
   from 171.68.118.143/1051 to 9. 9.9.10/23
109011: Authen Session Start: user 'telnetrange', Sid 0
109007: Authorization permitted for user 'telnetrange'
   from 171.68.118.143/1051 to 9.9 .9.10/23
302001: Built TCP connection 0 for faddr 9.9.9.10/23
   gaddr 9.9.9.5/1051 laddr 171.68.1 18.143/1051 (telnetrange)
109001: Auth start for user '???' from 171.68.118.143/1105
   to 9.9.9.10/80
109001: Auth start for user '???' from 171.68.118.143/1110
   to 9.9.9.10/80
109011: Authen Session Start: user 'telnetrange', Sid 1
109005: Authentication succeeded for user 'telnetrange'
   from 171.68.118.143/1110 to 9. 9.9.10/80
302001: Built TCP connection 1 for faddr 9.9.9.10/80 gaddr 9.9.9.5/1110
 laddr 171.68.1 18.143/1110 (telnetrange)
302001: Built TCP connection 2 for faddr 9.9.9.10/80 gaddr 9.9.9.5/1111
 laddr 171.68.1 18.143/1111 (telnetrange)
302002: Teardown TCP connection 1 faddr 9.9.9.10/80 gaddr 9.9.9.5/1110
 laddr 171.68.11 8.143/1110 duration 0:00:08 bytes 338 (telnetrange)
304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
302002: Teardown TCP connection 2 faddr 9.9.9.10/80 gaddr 9.9.9.5/1111
 laddr 171.68.11 8.143/1111 duration 0:00:01 bytes 2329 (telnetrange)
```

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

PIX-softwareversie 5.0 wijzigt de functie voor verkeersaccounting. Boekhoudkundige records kunnen nu worden gesneden voor verkeer anders dan HTTP, FTP en telnet, nadat de verificatie is voltooid.



Aan TFTP-exemplaar van een bestand van de externe router (192.1.1.1) naar de interne router (10.31.1.5) voegt u virtueel telnet toe om een gat voor het TFTP-proces te openen:

```
virtual telnet 192.1.1.30
static (inside,outside) 192.1.1.30 10.31.1.5 netmask 255.255.255.255 0 0
conduit permit udp any any
AAA authentication udp/69 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
AAA authorization udp/69 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
AAA accounting udp/0 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

Daarna, net van de buitenrouter op 192.1.1.1 tot virtuele IP 192.1.1.30 en authentiek aan het virtuele adres dat UDP toestaat om de PIX te verplaatsen. In dit voorbeeld werd het **fotoflitsproces van** het **fototoestel** van buiten naar binnen gestart:

```
302006: Teardown UDP connection for faddr 192.1.1.1/7680
    gaddr 192.1.1.30/69 laddr 10.31.1.5/69
```

Voor elke **flitser van het kopieer** op de PIX (er waren drie tijdens deze IOS kopie) wordt een boekhoudkundig record bijgesneden en naar de authenticatieserver gestuurd. Hieronder zie je een voorbeeld van een TACACS-record op Cisco Secure Windows):

```
Date,Time,Username,Group-Name,Caller-Id,Acct-Flags,elapsed_time,
    service,bytes_in,bytes_out,paks_in,paks_out,
    task_id,addr,NAS-Portname,NAS-IP-Address,cmd
 04/28/2000,03:08:26,pixuser,Default Group,192.1.1.1,start,,,,,,,
    0x3c,,PIX,10.31.1.200,udp/69
```

Gerelateerde informatie

- PIX-opdracht
- PIX-productondersteuningspagina