Configuraties van PIX, TACACS+ en RADIUS-monsters: 4,4,x

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. Wijzigingen in PIX 4.4.1 authenticatie, autorisatie en accounting (AAA) ten opzichte van de vorige versie omvatten: AAA servergroepen en failover, authenticatie voor toegang tot en seriële console, en accepteer en verwerp onmiddellijke berichten.

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.
- Vergunning is niet geldig zonder echtheidscontrole.

Stel dat u 100 gebruikers binnen hebt en u wilt slechts 6 van deze gebruikers om FTP, telnet, of HTTP buiten het netwerk te kunnen doen. U zou de PIX vertellen om uitgaande verkeer te authentiseren en alle 6 gebruikers IDs op de TACACS+/RADIUS-beveiligingsserver te geven. Met eenvoudige authenticatie zouden deze 6 gebruikers geauthentiseerd kunnen worden met gebruikersnaam en wachtwoord, en dan weg kunnen. De overige 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 6 gebruikers kunnen FTP, telnet of HTTP doen.

Maar veronderstel 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 er een vergunning moet komen, dat wil zeggen dat er toestemming moet worden gegeven voor wat de gebruikers kunnen doen, naast het authentiseren van wie ze zijn. Als we toestemming aan de PIX toevoegen, stuurt de PIX eerst Terry's gebruikersnaam en wachtwoord naar de beveiligingsserver en stuurt hij 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" te gebruiken, maar zou Terry de mogelijkheid om HTTP of telnet overal te ontkennen ontzegd worden.

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 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 - 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 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 de reden.

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 geavanceerde 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 NT2.x RADIUS

Voer de volgende stappen uit.

1. Wachtwoord verkrijgen in de sectie User Setup GUI.
2. Selecteer in het gedeelte GUI voor groepsinstallatie de optie Eigenschappen 6 (servicetype) op Aanmelden of Beheers.
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 exec privileges 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 de nieuwe opdracht **Toevoegen/Bewerken** 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 tot en met 5 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.

Cisco Secure 2.x TACACS+

De gebruiker krijgt een wachtwoord in het gedeelte Gebruikersinstelling van de 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 op **Deny niet-afgesloten IOS-opdrachten** onder in de groepsinstellingen.
3. Selecteer **Toevoegen/Bewerken** voor elke opdracht die u wilt toestaan (bijvoorbeeld telnet).
4. Als u telnet aan specifieke locaties wilt toestaan, specificeert u de licentie IP(s) in de argument rechthoek (bijvoorbeeld "sta 1.2.3.4" toe). 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.

Configuratie van Livingston RADIUS-server

Voeg de PIX IP en de sleutel aan het 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
```

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"
```

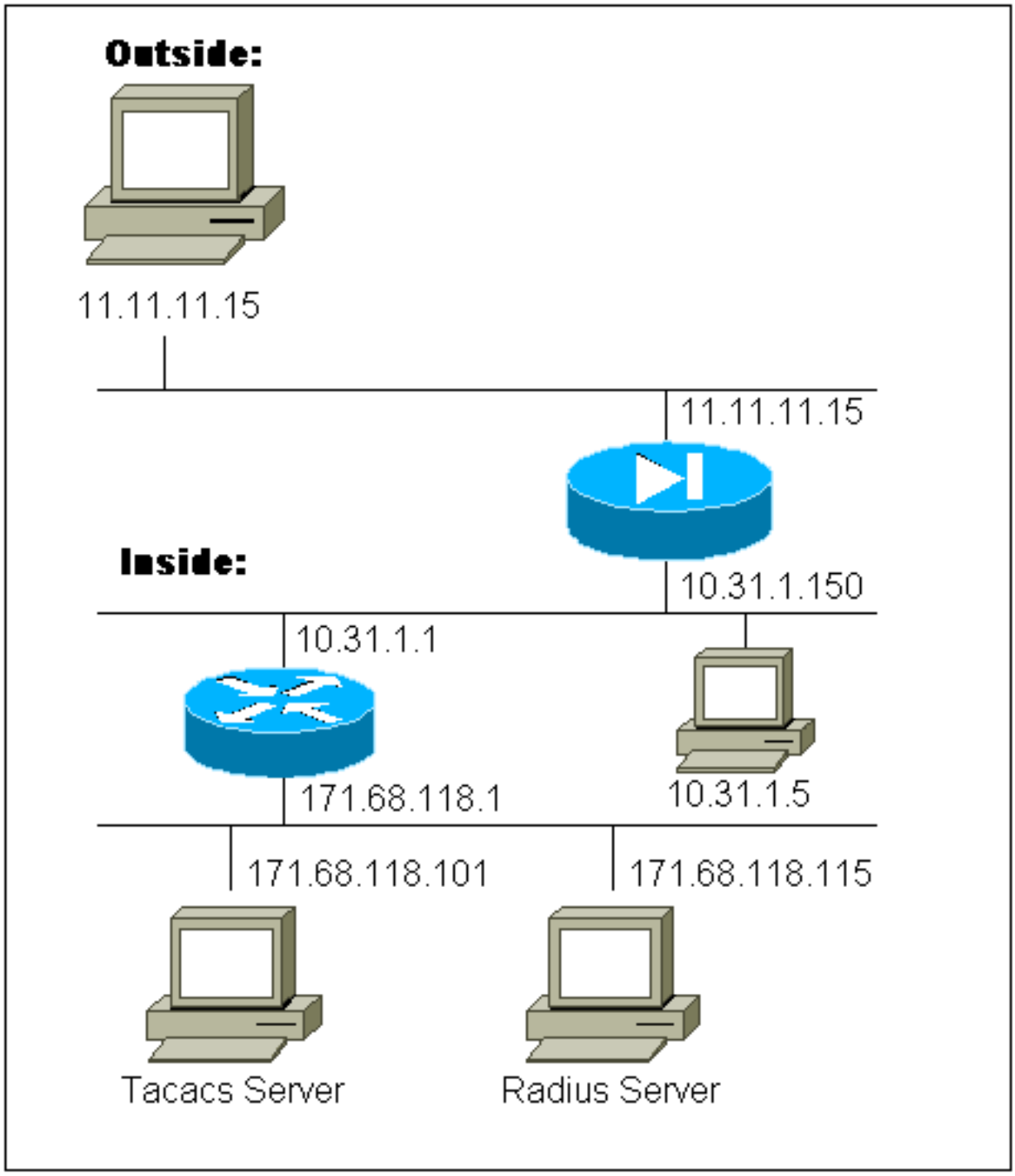
```
cmd = http {
permit .*
}
}

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

Afluisterstappen

- Zorg ervoor dat de PIX-configuraties werken voordat ze verificatie, autorisatie en accounting (AAA) toevoegen.Indien u geen verkeer kan doorgeven voordat u een echtheidscontrole en een vergunning instelt, kunt u dit achteraf niet meer doen.
- Meld in PIX inschakelen:De opdracht **het** foutopzetten van de **houtkapconsole** moet 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
 Building configuration...
 : Saved
 :
 PIX Version 4.4(1)
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 nameif ethernet2 pix/intf2 security10
 nameif ethernet3 pix/intf3 security15
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pix-5
 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
 logging console debugging
 no logging monitor
 no logging buffered
 logging trap debugging
 logging facility 20
 interface ethernet0 auto
 interface ethernet1 auto
 interface ethernet2 auto
 interface ethernet3 auto
 mtu outside 1500
 mtu inside 1500
 mtu pix/intf2 1500
 mtu pix/intf3 1500
 ip address outside 11.11.11.1 255.255.255.0
 ip address inside 10.31.1.150 255.255.255.0
 ip address pix/intf2 127.0.0.1 255.255.255.255
 ip address pix/intf3 127.0.0.1 255.255.255.255
 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
 failover ip address pix/intf3 0.0.0.0
 arp timeout 14400
 global (outside) 1 11.11.11.10-11.11.11.14 netmask
255.255.255.0
 static (inside,outside) 11.11.11.20 171.68.118.115
netmask 255.255.255.255 0 0
 static (inside,outside) 11.11.11.21 171.68.118.101
netmask 255.255.255.255 0 0
 static (inside,outside) 11.11.11.22 10.31.1.5 netmask
255.255.255.255 0 0
 conduit permit icmp any any
 conduit permit tcp any any
 no rip outside passive
 no rip outside default
 no rip inside passive
 no rip inside default
 no rip pix/intf2 passive
 no rip pix/intf2 default
 no rip pix/intf3 passive
 no rip pix/intf3 default
 route inside 0.0.0.0 0.0.0.0 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
!
!--- For any given list, multiple AAA servers can !---
be configured. They will be !--- tried sequentially if
any one of them is down. ! aaa-server Outgoing protocol
tacacs+ aaa-server Outgoing (inside) host 171.68.118.101
cisco timeout 10 aaa-server Incoming protocol radius
aaa-server Incoming (inside) host 171.68.118.115 cisco
timeout 10 aaa authentication ftp outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa authentication http
outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa
```

```
authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 Outgoing aaa authentication ftp inbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa authentication http
inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa
authentication telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 Incoming no snmp-server location no snmp-server
contact snmp-server community public no snmp-server
enable traps telnet timeout 5 terminal width 80
Cryptochecksum:b287a37a676262275a4201cac52399ca : end
```

Verificatie Debug Voorbeelden van PIX

In deze debug-voorbeelden:

Uitgaand

Binnengebruiker op 10.31.1.5 initieert verkeer naar buiten 11.11.15 en is authentiek door TACACS+ (uitgaande traffic use server list "OutDoorgaand", die TACACS server 171.68.118.101 omvat).

Inkomend

Buitengebruiker op 11.11.15 initieert het verkeer naar binnen 10.31.1.5 (11.11.11.22) en is geauthentiseerd door RADIUS (de lijst van inkomende verkeerserver "Inkomend" die RADIUS-server 171.68.118.115 omvat).

PIX-debug - goede verificatie - TACACS+

Het onderstaande voorbeeld toont PIX debug met goede authenticatie:

```
109001: Auth start for user '???' from 10.31.1.5/11004 to 11.11.11.15/23
 109011: Authen Session Start: user 'ddunlap', sid 3
 109005: Authentication succeeded for user 'ddunlap'
 from 10.31.1.5/11004 to 11.11.11.15/23
 109012: Authen Session End: user 'ddunlap', sid 3, elapsed 1 seconds
 302001: Built outbound TCP connection 4 for faddr 11.11.11.15/23 gaddr
11.11.11.22/11004 laddr 10.31.1.5/11004
```

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

Het onderstaande voorbeeld toont PIX debug met slechte authenticatie (gebruikersnaam of wachtwoord). De gebruiker ziet vier gebruikersnaam/wachtwoordsets. Het volgende bericht verschijnt: "Fout: max aantal overschrijdingen".

```
109001: Auth start for user '???' from 10.31.1.5/11005 to 11.11.11.15/23
 109006: Authentication failed for user '' from 10.31.1.5/11005 to 11.11.11.15/23
```

PIX debug - Kan pingen, maar geen respons - TACACS+

Het onderstaande voorbeeld toont PIX debug voor een pingable server die niet met PIX spreekt. De gebruiker ziet de gebruikersnaam eenmaal, en PIX vraagt nooit om een wachtwoord (dit is op telnet).

```
'Error: Max number of tries exceeded'
 109001: Auth start for user '???' from 10.31.1.5/11006 to 11.11.11.15/23
 109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
 (server 171.68.118.101 failed)
 109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
 (server 171.68.118.101 failed)
 304006: URL Server 171.68.118.101 not responding, trying 171.68.118.101
 109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
 (server 171.68.118.101 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11006 to 11.11.11.15/23
```

PIX-debug - kan geen Ping Server - TACACS+

Het onderstaande voorbeeld toont PIX debug voor een server die niet pingable is. De gebruiker ziet de gebruikersnaam eenmaal. PIX vraagt nooit om een wachtwoord (dit is gebaseerd op telnet). Het volgende bericht verschijnt: "Time-out bij TACACS+ server" en "Fout: Max. aantal probeert te overschrijden" (de configuratie in dit voorbeeld geeft een nepserver aan).

```
109001: Auth start for user '???' from 10.31.1.5/11007 to 11.11.11.15/23
 109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
 (server 171.68.118.199 failed)
 109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
 (server 171.68.118.199 failed)
 304006: URL Server 171.68.118.199 not responding, trying 171.68.118.199
 109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
 (server 171.68.118.199 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11007 to 11.11.11.15/23
```

PIX-debug - goede verificatie - RADIUS

Het onderstaande voorbeeld toont PIX debug met goede authenticatie:

```
109001: Auth start for user '???' from 11.11.11.15/11003 to 10.31.1.5/23
 109011: Authen Session Start: user 'adminuser', sid 4
 109005: Authentication succeeded for user 'adminuser'
 from 10.31.1.5/23 to 11.11.11.15/11003
 109012: Authen Session End: user 'adminuser', sid 4, elapsed 1 seconds
 302001: Built inbound TCP connection 5 for faddr
 11.11.11.15/11003 gaddr 11.11.11.22/23 laddr 10.31.1.5/23
```

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

Het onderstaande voorbeeld toont PIX debug met slechte authenticatie (gebruikersnaam of wachtwoord). De gebruiker ziet een verzoek om gebruikersnaam en wachtwoord. Als een van de twee verkeerd is, wordt het bericht "Onjuist wachtwoord" vier keer weergegeven. De gebruiker is losgekoppeld. Dit probleem is toegewezen aan bug-ID #CSCdm46934.

```
'Error: Max number of tries exceeded'
 109001: Auth start for user '???' from 11.11.11.15/11007 to 10.31.1.5/23
 109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11007
```

PIX Debug - Deamon Down communiceert niet met PIX - RADIUS

Het onderstaande voorbeeld toont PIX debug met een pingable server, maar daemon is omlaag. De server communiceert niet met PIX. De gebruiker ziet een gebruikersnaam, gevolgd door een

wachtwoord. De volgende berichten worden weergegeven: "RADIUS-server mislukt" en "Fout: Max. aantal overschrijdingen overschreden".

```
109001: Auth start for user '???' from 11.11.11.15/11008 to 10.31.1.5/23
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
 (server 171.68.118.115 failed)
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
 (server 171.68.118.115 failed)
 304006: URL Server 171.68.118.115 not responding, trying 171.68.118.115
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
 (server 171.68.118.115 failed)
 109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11008
```

PIX Debug - kan geen server of Key/Client-Mismatch pingen - RADIUS

Het voorbeeld hieronder toont PIX debug voor een server die niet pingable is of waar een zeer belangrijke/cliënt mismatch is. De gebruiker ziet gebruikersnaam en wachtwoord. De volgende berichten worden weergegeven: "Time-out bij RADIUS-server" en "Fout: Max. aantal probeert te overschrijden" (de server in de configuratie is alleen voor een doel bedoeld).

```
109001: Auth start for user '???' from 11.11.11.15/11009 to 10.31.1.5/23
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
 (server 171.68.118.199 failed)
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
 (server 171.68.118.199 failed)
 304006: URL Server 171.68.118.199 not responding, trying 171.68.118.199
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
 (server 171.68.118.199 failed)
 109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11009
```

Toestemming toevoegen

Aangezien een vergunning zonder echtheidscontrole niet geldig is, zullen we een vergunning voor dezelfde bron- en doelgroep nodig hebben:

```
aaa authorization ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
aaa authorization http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
aaa authorization telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

uitgaand

Let op dat we geen autorisatie voor 'inkomend' toevoegen omdat inkomend verkeer geauthentificeerd is met RADIUS en de RADIUS-autorisatie niet geldig

Verificatie en autorisatie Debug Voorbeelden van PIX

PIX Debug met goede verificatie en succesvolle autorisatie - TACACS+

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

```
109001: Auth start for user '???' from 10.31.1.5/11002 to 11.11.11.15/23
 109011: Authen Session Start: user 'can_only_do_telnet', sid 7
 109005: Authentication succeeded for user 'can_only_do_telnet'
 from 10.31.1.5/11002 to 11.11.11.15/23
 109011: Authen Session Start: user 'can_only_do_telnet', sid 7
 109007: Authorization permitted for user 'can_only_do_telnet'
 from 10.31.1.5/11002 to 11.11.11.15/23
 109012: Authen Session End: user 'can_only_do_telnet', sid 7,
 elapsed 1 seconds
 302001: Built outbound TCP connection 6 for faddr 11.11.11.15/23
 gaddr 11.11.11.22/11002 laddr 10.31.1.5/11002 (can_only_do_telnet)
```

PIX debug - goede verificatie, mislukte autorisatie - TACACS+

Het onderstaande voorbeeld toont PIX debug met goede authenticatie maar heeft geen vergunning gekregen:

Hier ziet de gebruiker ook het bericht "Fout: Vergunning geweigerd"

```
109001: Auth start for user '???' from 10.31.1.5/11000 to 11.11.11.15/23
 109011: Authen Session Start: user 'can_only_do_ftp', sid 5
 109005: Authentication succeeded for user 'can_only_do_ftp'
 from 10.31.1.5/11000 to 11.11.11.15/23
 109008: Authorization denied for user 'can_only_do_ftp' from
 10.31.1.5/11000 to 11.11.11.15/23
 109012: Authen Session End: user 'can_only_do_ftp', sid 5, elapsed 33 seconds
```

Boekhouding toevoegen

TACACS+

aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing

Debug zal er hetzelfde uitzien of accounting aan of uit is. Ten tijde van het "Built" zal er echter een "start"-boekhouding worden verstuurd. Ten tijde van de "Teardown" wordt een "stop"-boekhouding verstuurd.

De boekhoudgegevens van TACACS+ lijken op het volgende (deze zijn van Cisco Secure UNIX); De functies in Cisco Secure NT kunnen daarentegen door de komma worden gedefinieerd):

```
Thu Jun  3 10:41:50 1999 10.31.1.150 can_only_do_telnet
 PIX 10.31.1.5 start task_id=0x7 foreign_ip=11.11.11.15
local_ip=10.31.1.5  cmd=telnet
Thu Jun  3 10:41:55 1999 10.31.1.150 can_only_do_telnet PIX 10.31.1.5
 stop task_id=0x7 foreign_ip=11.11.11.15
local_ip=10.31.1.5 cmd=telnet elapsed_time=4 bytes_in=74 bytes_out=27
```

RADIUS

aaa accounting any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming

Debug zal er hetzelfde uitzien 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 boekhouding van RADIUS ziet er als volgt uit: (deze komen van Cisco Secure UNIX; De functies in Cisco Secure NT kunnen daarentegen door de komma worden gedefinieerd):

```
10.31.1.150adminuser -- start server=rtp-evergreen.rtp.cisco.com
time=14:53:11 date=06/3/1999 task_id=0x00000008
 Thu Jun  3 15:53:11 1999
         Acct-Status-Type = Start
         Client-Id = 10.31.1.150
         Login-Host = 10.31.1.5
         Login-TCP-Port = 23
         Acct-Session-Id = "0x00000008"
         User-Name = "adminuser"
 10.31.1.150 adminuser -- stop server=rtp-evergreen.rtp.cisco.com
time=14:54:24 date=06/ 3/1999 task_id=0x00000008
 Thu Jun  3 15:54:24 1999
         Acct-Status-Type = Stop
         Client-Id = 10.31.1.150
         Login-Host = 10.31.1.5
         Login-TCP-Port = 23
         Acct-Session-Id = "0x00000008"
         User-Name = "adminuser"
         Acct-Session-Time = 73
         Acct-Input-Octets = 27
         Acct-Output-Octets = 73
```

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 het volgende doen:

```
aaa authentication except outbound 10.31.1.60 255.255.255.255
11.11.11.15 255.255.255.255 Outgoing
aaa authorization except outbound 10.31.1.60 255.255.255.255
11.11.11.15 255.255.255.255 Outgoing
```

Indien u "uitzonderingen" maakt op de ip-adressen van de authenticatie en u een vergunning heeft, moet u deze ook van de autorisatie uitsluiten!

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 (dat wil zeggen, 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.

De gebruiker telnet 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
```

Omdat de server een "start"-record maar geen "stop"-record heeft gezien (op dit moment in de tijd), zal de server laten zien 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 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 verder met haar telnet of FTP-bedrijf op de doelhost en verlaat zich vervolgens (brengt 10 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 (elke keer authenticeren) of meer (opnieuw authenticeren tijdens de auteperiode), wordt een accounting record voor elke benaderde site bijgesneden.

HTTP werkt echter 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 begin van het record gepost om 16:35:34, en het stoprecord gepost om 16:35:35. Deze download duurde één seconde (dat wil zeggen: tussen het begin en het einde was er minder dan

een seconde) . 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 was gericht op het authenticeren van het telnet (en HTTP, FTP) verkeer door de PIX. In het onderstaande voorbeeld zorgen we ervoor dat het telnet aan de pix werkt zonder verificatie op:

```
telnet 10.31.1.5 255.255.255.255
passwd ww
```

Vervolgens voegen we de opdracht toe om gebruikers telnetting voor authentiek te verklaren aan PIX:

```
aaa authentication telnet console Outgoing
```

Wanneer gebruikers telnet aan PIX, worden zij voor het wachtwoord van het telnet ("ww") gevraagd. PIX vraagt in dit geval ook om TACACS+ (aangezien de "Outitting" serverlijst wordt gebruikt) of de gebruikersnaam en het wachtwoord van de RADIUS.

```
aaa authentication enable console Outgoing
```

Met deze opdracht wordt de gebruiker gevraagd om een gebruikersnaam en wachtwoord voor de TACACS- of RADIUS-server. In dit geval, aangezien de "Uitgaande" serverlijst wordt gebruikt, gaat het verzoek naar de TACACS server. Aangezien het verificatiepakket waarmee u een verbinding kunt maken hetzelfde is als het authenticatiepakket voor inloggen, kan de gebruiker via TACACS of RADIUS met dezelfde gebruikersnaam/wachtwoord schakelen, ervan uitgaande dat de gebruiker in kan loggen op de PIX met TACACS of RADIUS. Dit probleem is toegewezen aan bug-ID #CSCdm47044.

Als de server uit is, kan de gebruiker toegang krijgen tot de PIX-modus door "PIX" in te voeren voor de gebruikersnaam en de normale instelling maakt een wachtwoord uit de PIX-instelling mogelijk ("Geef het wachtwoord los"). Als "laat het wachtwoord toe wat" niet in de PIX-configuratie is, moet de gebruiker "PIX" voor de gebruikersnaam invoeren en op de ENTER-toets drukken. Als het wachtwoord wordt ingesteld maar niet bekend, moet u een wachtwoord terugzetten om het wachtwoord opnieuw te kunnen instellen.

Verificatie op de seriële console

De opdracht **van de** echtheidscontrole **seriële console** vereist verificatie om toegang te hebben tot

de seriële console van de PIX. Wanneer de gebruiker configuratieopdrachten uit de console uitvoert, worden de syslog-berichten doorgesneden (als de PIX is ingesteld om syslog op debug-niveau naar een syslog-host te verzenden). Hieronder zie je een voorbeeld van de syslog server:

```
Jun  5 07:24:09 [10.31.1.150.2.2] %PIX-5-111008: User 'cse' executed
the 'hostname' command.
```

De snelle gebruikers wijzigen

Als we het bevel hebben:

```
auth-prompt THIS_IS_PIX_5
```

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

```
THIS_IS_PIX_5 [at which point one would enter the username]
 Password:[at which point one would enter the password]
```

en dan, bij aankomst in het ultieme doelvak, de "Gebruikersnaam:" en "Wachtwoord:" navraag het doelvak wordt aangeboden.

Deze melding beïnvloedt alleen gebruikers die door de PIX gaan, niet door 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 we de opdrachten hebben:

```
auth-prompt accept "You're allowed through the pix"
auth-prompt reject "You blew it"
```

Gebruikers zien het volgende bij een mislukt/succesvol inloggen via de PIX:

```
THIS_IS_PIX_5
 Username: asjdkl
 Password:
 "You blew it"
 "THIS_IS_PIX_5"
 Username: cse
 Password:
 "You're allowed through the pix"
```

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 dan stel deze niet in! Maar als je verschillende gebruikers nodig hebt, lees dan op.

In ons voorbeeld op de PIX, gebruiken we de **time-out** opdracht **3:00:00**. Dit betekent dat als een persoon echt is, hij gedurende 3 uur niet meer hoeft te controleren. Maar als we een gebruiker met het volgende profiel opzetten en een TACACS AAA-vergunning hebben in de PIX, dan hebben de ongebruikte en absolute tijden in het gebruikersprofiel de time-out-uauth in de PIX voor die gebruiker omzeilen. Dit betekent niet dat de Telnet-sessie door de PIX wordt losgekoppeld na de stationaire/absolute time-out. Het controleert alleen of herauthenticatie plaatsvindt.

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

Geef na verificatie een **show uauth** commandoopdracht op in de 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 zal opnieuw authentiek moeten verklaren wanneer het terugkeren naar de zelfde doelgastheer of een andere gastheer.

Virtuele HTTP

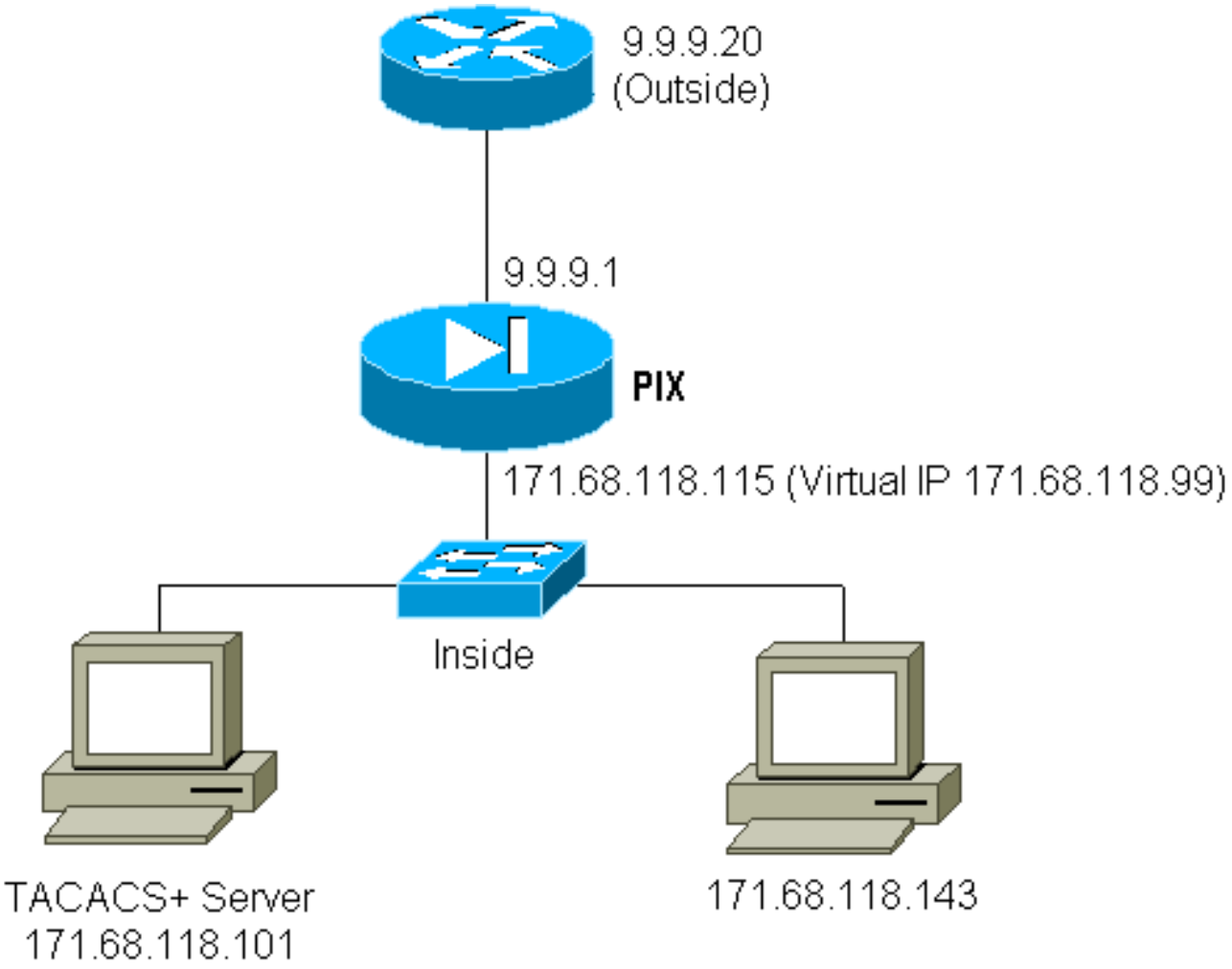
Als verificatie vereist is op sites buiten de PIX, zowel als op de PIX zelf, kan ongebruikelijk browser gedrag soms worden waargenomen aangezien browsers de gebruikersnaam en het wachtwoord in het geheugen plaatsen.

Om dit te vermijden, kunt u virtueel HTTP implementeren door een RFC 1918- adres toe te voegen (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 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 Outgoing protocol tacacs+
 aaa-server Outgoing (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 Outgoing
 virtual http 171.68.118.99
 auth-prompt THIS_IS_PIX_5
```

Virtueel telnet

Het configureren van de PIX om al inkomende en uitgaande verkeer te authenticeren is geen goed idee omdat sommige protocollen, zoals "e-mail" niet makkelijk geauthentiseerd zijn. Wanneer een mailserver en client proberen via de PIX te communiceren wanneer al het verkeer via de PIX is geauthentiseerd, zal de PIX-slang voor niet-authentiek verklaarde protocollen berichten zoals tonen:

```
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
```

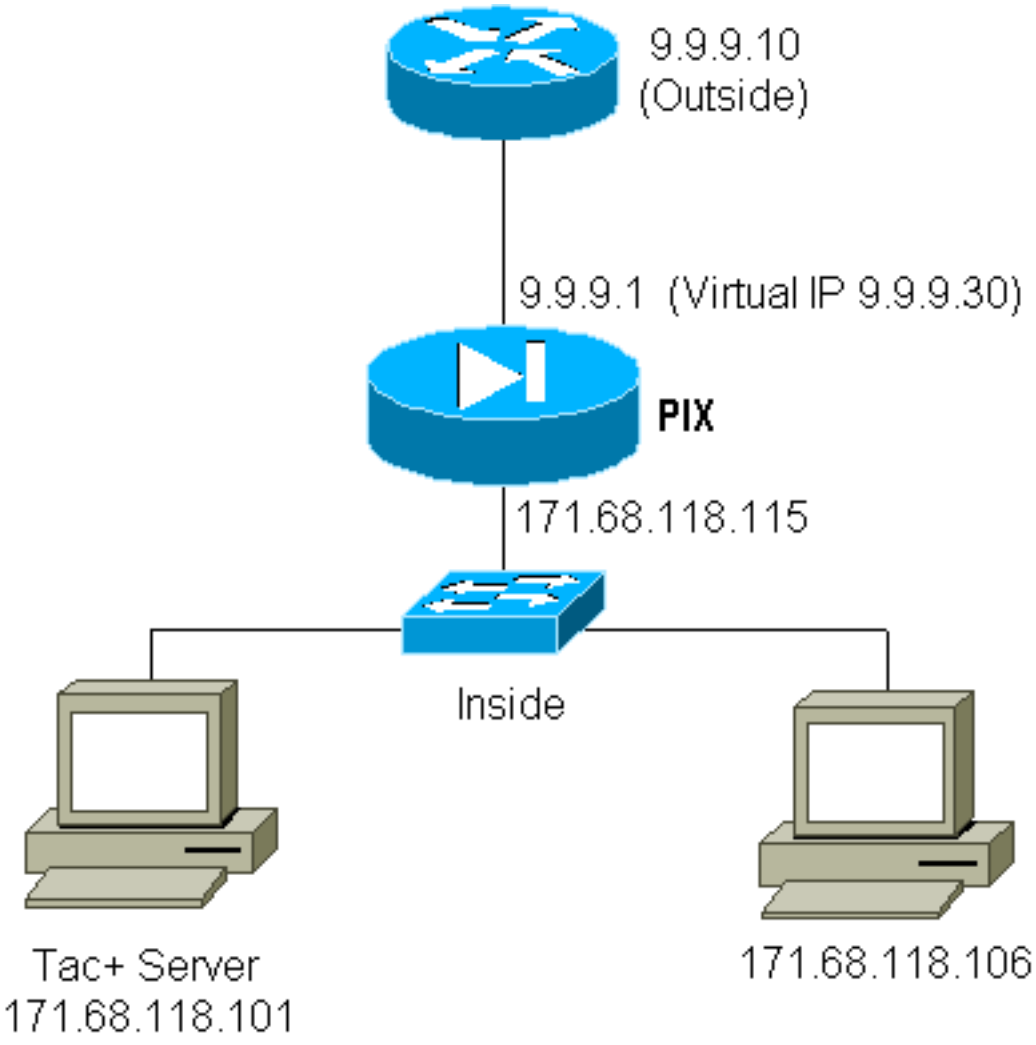
Aangezien e-mail en sommige andere diensten niet interactief genoeg zijn om authentiek te

verklaren, is één oplossing het gebruik van de **behalve** opdracht voor authenticatie/vergunning (alle behalve bron/bestemming van de postserver/client voor authenticatie authentiek).

Maar als er echt een noodzaak is om een of ander soort ongewone service te authenticeren, kan dit gedaan worden door gebruik te maken 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 die aan de virtuele IP is gekoppeld.

In ons voorbeeld willen we TCP poort 49-verkeer laten stromen van buiten host 9.9.9.10 naar binnen host 171.68.118.106. Aangezien dit verkeer niet echt authentiek is, hebben we virtueel telnet opgezet.

Virtueel telnet inkomend:



PIX-configuratie virtueel telnet inkomende:

```
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) 9.9.9.30 171.68.118.106 netmask 255.255.255.255 0 0
 conduit permit tcp host 9.9.9.30 host 9.9.9.10
 aaa-server TACACS+ protocol tacacs+
 aaa-server Incoming protocol tacacs+
 aaa-server Incoming (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 Incoming
 virtual telnet 9.9.9.30
```

Configuratie virtuele telnet van gebruikers van TACACS+ servers inkomende:

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

PIX Debug virtueel telnet inkomende:

De gebruiker moet op 9.9.9.10 eerst authenticeren door te tellen naar het 9.9.9.30 adres op PIX:

```
pixfirewall# 109001: Auth start for user '???' from 9.9.9.10/11099
 to 171.68.118.106/23
 109011: Authen Session Start: user 'pinecone', sid 13
 109005: Authentication succeeded for user 'pinecone' from
 171.68.118.106/23 to 9.9.9.10/11099
```

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

```
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
```

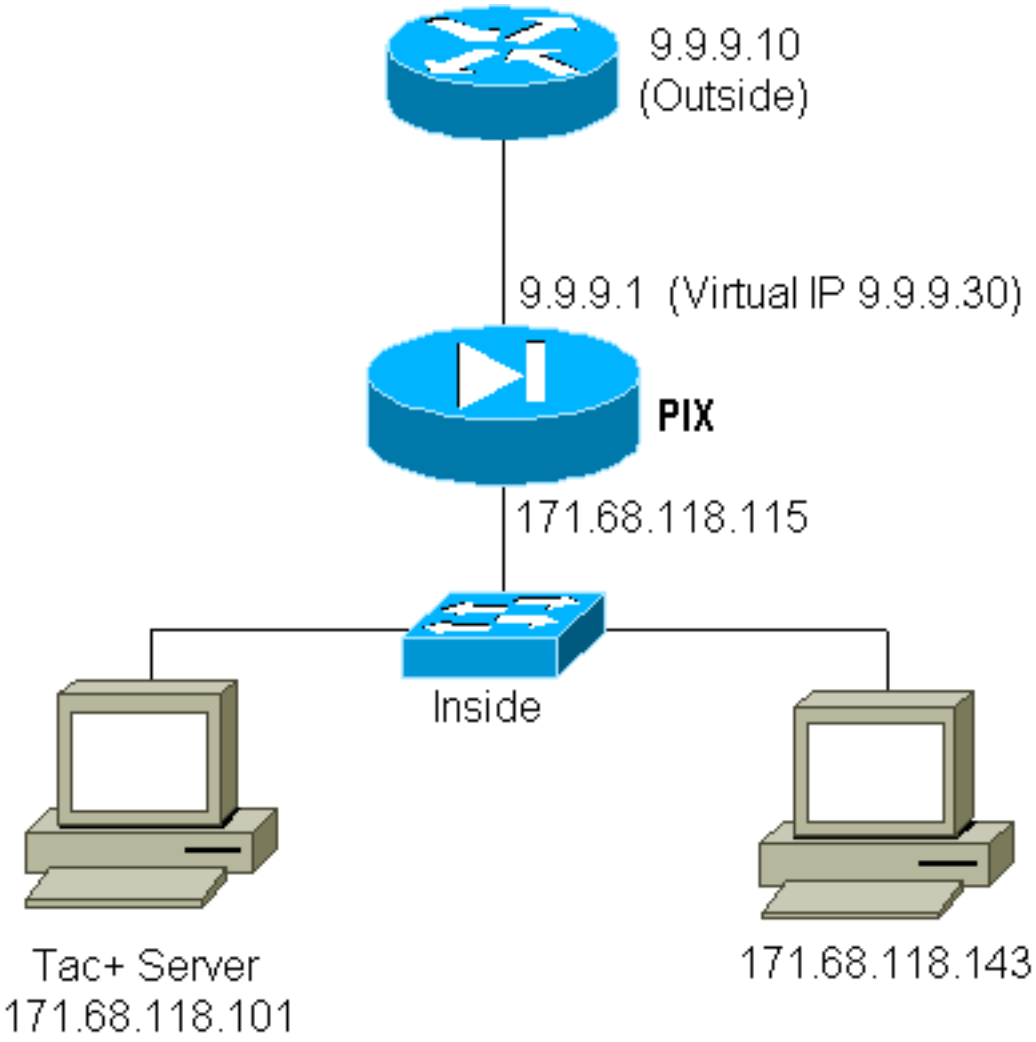
En wanneer het apparaat om 9.9.9.10 TCP/49 verkeer naar het apparaat wil sturen om 171.68.118.106:

```
pixfirewall# 109001: Auth start for user 'pinecone'
 from 9.9.9.10/11104 to 171.68.118.106/49
 109011: Authen Session Start: user 'pinecone', sid 14
 109007: Authorization permitted for user 'pinecone' from 9.9.9.10/11104
 to 171.68.118.106/49
 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)
```

Virtueel telnet uit:

Aangezien het uitgaande verkeer standaard is toegestaan, is er geen statisch geluid vereist voor het gebruik van virtueel telnet. In het volgende voorbeeld, zal de binnengebruiker op 171.68.118.143 telnet naar virtueel 9.9.9.30 en authentiek verklaren. 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 uit:

```
 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 Outgoing protocol tacacs+
 aaa-server Outgoing (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 Outgoing
 virtual telnet 9.9.9.30
```

PIX Debug Virtual Telnet-uitgang:

```
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** auth toont zijn uauth. Als de gebruiker verkeer wil verhinderen om door te gaan nadat zijn sessie is beëindigd (wanneer er tijd in de auth is achtergebleven) moet hij 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 het volgende voorbeeld was authenticatie nog vereist voor alle uitgaande poorten, maar autorisatie is alleen 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 Outgoing
aaa authorization tcp/23-49 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
```

Dus toen we telnet van 171.68.118.143 tot 9.9.9.10, kwam de authenticatie en vergunning voor omdat Telnet poort 23 in het bereik van 23-49 ligt. Als we een HTTP-sessie doen van 171.68.118.143 tot 9.9.9.10, moeten we 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)
```

Gerelateerde informatie

- Productondersteuning voor Cisco PIX-firewall
- Opdrachtreferenties van Cisco Secure PIX-firewall