Configuraties van PIX-, TACACS+- en RADIUS-voorbeelden: 4.2.x

Inhoud

Inleiding

RADIUS- en TACACS+-verificatie kan worden uitgevoerd voor FTP-, Telnet- en HTTP-verbindingen. De TACACS+-autorisatie wordt ondersteund, de RADIUS-autorisatie niet.

De syntaxis voor verificatie is in PIX-software 4.2.2 enigszins gewijzigd. In dit document wordt de syntaxis gebruikt voor softwareversies 4.2.2.

Voorwaarden

Vereisten

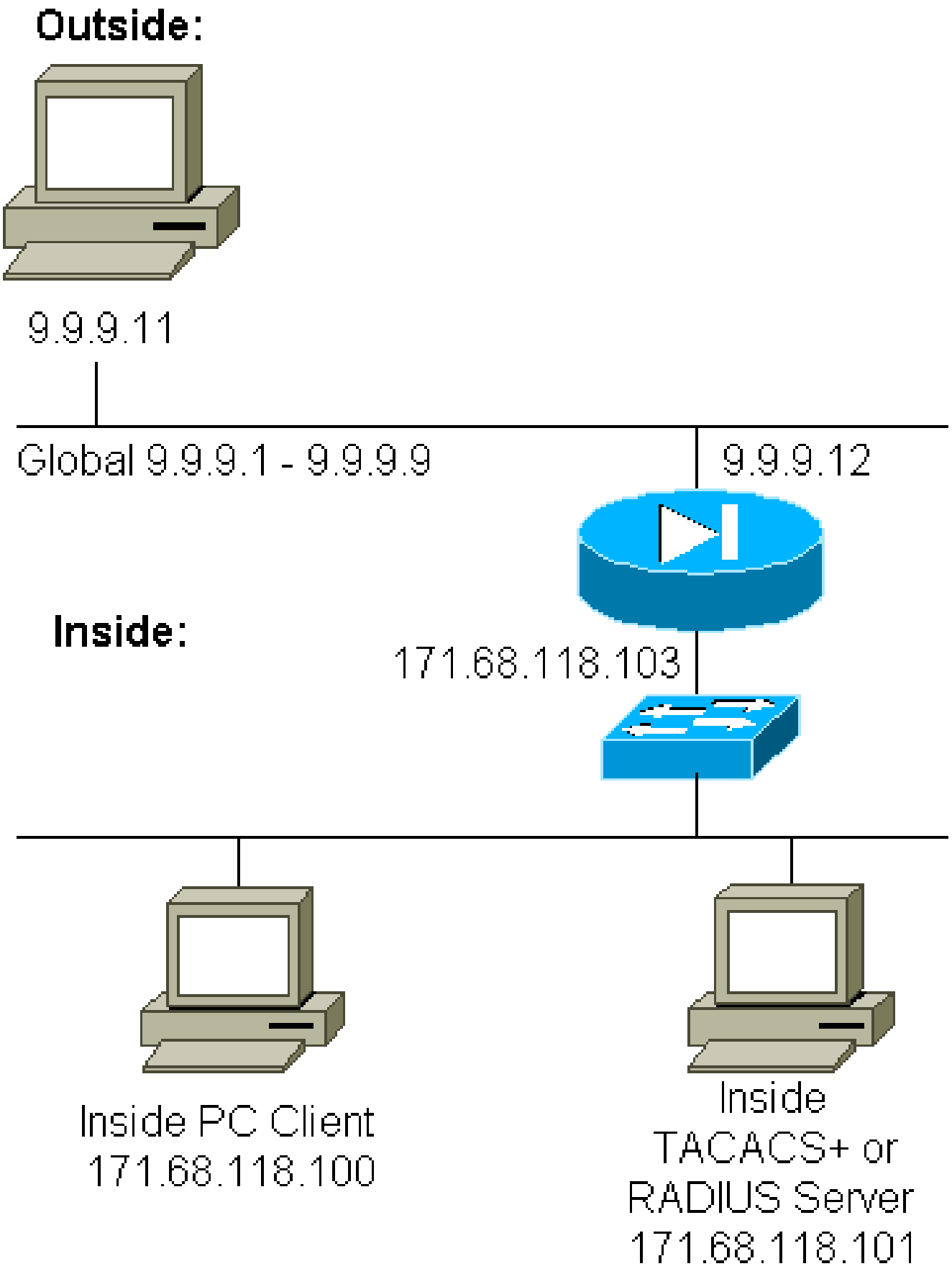
Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

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

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



PIX-configuratie
<#root>

```
pix2#
write terminal

Building configuration
: Saved
:
PIX Version 4.2(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd OnTrBUG1TpOedmkr encrypted
hostname pix2
fixup protocol http 80
fixup protocol smtp 25
no fixup protocol ftp 21
no fixup protocol h323 1720
no fixup protocol rsh 514
no fixup protocol sqlnet 1521
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  0.0.0.0
names
pager lines 24
logging console debugging
no logging monitor
logging buffered debugging
logging trap debugging
logging facility 20
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
ip address outside 9.9.9.12 255.255.255.0
ip address inside 171.68.118.103 255.255.255.0
ip address  0.0.0.0 0.0.0.0
arp timeout 14400
global (outside) 1 9.9.9.1-9.9.9.9 netmask 255.0.0.0
static (inside,outside) 9.9.9.10 171.68.118.100 netmask 255.255.255.255 0 0
conduit permit icmp any any
conduit permit tcp host 9.9.9.10 eq telnet any
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
timeout xlate 3:00:00 conn 1:00:00 udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:00:00 absolute
!
!--- The next entry depends on whether TACACS+ or RADIUS is used.

!
tacacs-server (inside) host 171.68.118.101 cisco timeout 5
radius-server (inside) host 171.68.118.101 cisco timeout 10

!
!--- The focus of concern is with hosts on the inside network !--- accessing a particular outside host

!
```

```
aaa authentication any outbound 171.68.118.0 255.255.255.0 9.9.9.11
   255.255.255.255 tacacs+|radius

!

!--- It is possible to be less granular and authenticate !--- all outbound FTP, HTTP, Telnet traffic w

aaa authentication ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   tacacs+|radius
aaa authentication http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   tacacs+|radius
aaa authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   tacacs+|radius
!

!--- Accounting records are sent for !--- successful authentications to the TACACS+ or RADIUS server.

!
aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius
!
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
telnet 171.68.118.100 255.255.255.255
mtu outside 1500
mtu inside 1500
mtu  1500
Smallest mtu: 1500
floodguard 0
tcpchecksum silent
Cryptochecksum:be28c9827e13baf89a937c617cfe6da0
: end
[OK]
```

Conventies

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

Verificatie versus autorisatie

- Verificatie is wie de gebruiker is.
- Machtiging is wat de gebruiker kan doen.
- Verificatie is geldig zonder machtiging.
- De autorisatie is niet geldig zonder authenticatie.

Neem bijvoorbeeld aan dat je honderd gebruikers hebt en dat je maar zes van deze gebruikers wilt laten doen met FTP, Telnet of HTTP buiten het netwerk. Vertel de PIX om uitgaand verkeer te authenticeren en alle zes gebruikers-ID's op de TACACS+/RADIUS security server te geven. Met eenvoudige authenticatie, deze zes gebruikers kunnen worden geverifieerd met gebruikersnaam

en wachtwoord, en vervolgens uitgaan. De andere 94 gebruikers kunnen niet uitgaan. De PIX vraagt gebruikers om gebruikersnaam/wachtwoord en geeft vervolgens hun gebruikersnaam en wachtwoord door aan de TACACS+/RADIUS-beveiligingsserver. Afhankelijk van het antwoord wordt de verbinding geopend of ontkend. Deze zes gebruikers kunnen FTP, Telnet of HTTP gebruiken.

Ga er echter vanuit 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 naar buiten. Dit betekent dat je toestemming moet toevoegen. Dat wil zeggen, toestaan wat gebruikers kunnen doen naast het verifiëren wie ze zijn. Wanneer u toestemming aan de PIX toevoegt, stuurt de PIX eerst Terry's gebruikersnaam en wachtwoord naar de beveiligingsserver en stuurt dan een autorisatieverzoek dat de beveiligingsserver vertelt 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 krijgt hij niet de mogelijkheid om "HTTP" of "Telnet" te gebruiken waar dan ook.

Wat de gebruiker ziet met verificatie/autorisatie op

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

- Telnet - De gebruiker ziet een gebruikersbenamingprompt, gevolgd door een verzoek om wachtwoord. Als verificatie (en autorisatie) op de PIX/server succesvol is, wordt de gebruiker door de doelhost om gebruikersnaam en wachtwoord gevraagd.
- FTP - De gebruiker ziet een gebruikersnaam en prompt verschijnen. De gebruiker moet "local_username@remote_username" voor gebruikersnaam en "local_password@remote_password" voor wachtwoord invoeren. PIX stuurt de "local_username" en "local_password" naar de lokale security server, en als authenticatie (en autorisatie) succesvol is op de PIX / server, worden de "remote_username" en "remote_password" doorgegeven aan de bestemming FTP server.
- HTTP - Er wordt een venster weergegeven in de browser die een gebruikersnaam en wachtwoord aanvraagt. Als de verificatie (en autorisatie) succesvol is, arriveert de gebruiker bij de doelwebsite. Houd in gedachten dat browsers gebruikersnaam en wachtwoord cachen. Als het lijkt dat de PIX zou moeten zijn timing uit een HTTP verbinding maar niet doet dit, is het waarschijnlijk dat re-authenticatie daadwerkelijk plaatsvindt met de browser "schieten" de gecachede gebruikersnaam en wachtwoord op de PIX. Dit wordt vervolgens doorgestuurd naar de verificatieserver. PIX syslog en/of server debugs tonen dit fenomeen. Als Telnet en FTP normaal lijken te werken, maar HTTP verbindingen niet, is dit de reden.

Serverconfiguraties voor alle scenario's

Als in de TACACS+ serverconfiguratievoorbeelden alleen verificatie is ingeschakeld, werken de gebruikers "all", "telnet only", "httponly" en "ftponly" allemaal. In de voorbeeld van de RADIUS-serverconfiguratie werkt gebruiker "all".

Wanneer de vergunning aan PIX wordt toegevoegd, naast het verzenden van de

gebruikersbenaming en het wachtwoord naar de TACACS+ authentificatieserver, verzendt PIX bevelen (Telnet, HTTP, of FTP) naar de server TACACS+. De TACACS+ server controleert vervolgens of die gebruiker geautoriseerd is voor die opdracht.

In een later voorbeeld geeft de gebruiker op 171.68.118.100 de opdracht Telnet 9.9.9.11 uit. Wanneer dit bij PIX wordt ontvangen, gaat PIX de gebruikersbenaming, het wachtwoord, en de opdracht voor verwerking over tot de TACACS+ server.

Zo met vergunning op naast authentificatie, kan de gebruiker "telnet slechts" de handelingen van Telnet door PIX uitvoeren. Gebruikers 'httponly' en 'ftponly' kunnen echter geen Telnet-bewerkingen via de PIX uitvoeren.

(Ook hier wordt de autorisatie niet ondersteund met RADIUS vanwege de aard van de protocolspecificatie).

Configuratie van Cisco Secure UNIX-TACACS+ server

Cisco Secure 2.x

- Gebruikersstanza's worden hier weergegeven.
- Voeg het PIX IP-adres of de volledig gekwalificeerde domeinnaam en sleutel toe aan CSU.cfg.

```
user = all {
password = clear "all"
default service = permit
}

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

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

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

```
    }
    }
```

Configuratie van Cisco Secure UNIX RADIUS-server

Gebruik de geavanceerde grafische gebruikersinterface (GUI) om de PIX IP en sleutel toe te voegen aan de lijst van de netwerktoegangsserver (NAS). Het gebruikersstandpunt verschijnt zoals hier te zien is:

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

Cisco Secure NT 2.x RADIUS-software

De sectie Sample Configurations van de online- en webdocumentatie van CiscoSecure 2.1 beschrijft de instellingen; kenmerk 6 (Service-Type) is Login of Administratief.

Voeg het IP van de PIX toe in het gedeelte NAS Configuration met behulp van de GUI.

EasyACS TACACS+

De EasyACS-documentatie bevat setup-informatie.

1. Klik in het groepsvak op Shell exec (om exec-rechten te geven).
2. Als u een licentie aan de PIX wilt toevoegen, klikt u onder in de groepsinstallatie op Niet-overeenkomende IOS-opdrachten weigeren.
3. Selecteer Add/Edit voor elke opdracht die u wilt toestaan (bijvoorbeeld Telnet).
4. Als u Telnet wilt toestaan op bepaalde sites, voert u de IP(s) in het gedeelte met argumenten in. Als u Telnet wilt toestaan voor alle sites, klikt u op Toestaan voor alle niet-vermelde argumenten.
5. Klik op Bewerkingsopdracht voltooien.
6. Voer stap 1 tot en met 5 uit voor elk van de toegestane opdrachten (Telnet, HTTP en/of FTP, bijvoorbeeld).
7. Voeg het IP van de PIX toe in het gedeelte NAS Configuration met behulp van de GUI.

Cisco Secure NT-2.x - TACACS+

De documentatie van Cisco Secure 2.x biedt setup-informatie.

1. Klik in het groepsvak op Shell exec (om exec-rechten te geven).
2. Als u een licentie aan de PIX wilt toevoegen, klikt u onder in de groepsinstallatie op Niet-overeenkomende IOS-opdrachten weigeren.
3. Selecteer onderaan het aanvinkvakje voor opdracht en voer de opdracht in die u wilt toestaan (bijvoorbeeld Telnet).
4. Als u Telnet aan specifieke plaatsen wilt toestaan, ga IP in de argumentsectie (bijvoorbeeld, "vergunning 1.2.3.4") in. Om Telnet aan alle plaatsen toe te staan, klik op Niet vermelde argumenten toestaan.
5. Klik op Verzenden.
6. Voer stap 1 tot en met 5 uit voor elk van de toegestane opdrachten (Telnet, FTP en/of HTTP bijvoorbeeld).
7. Voeg het IP van de PIX toe in het gedeelte NAS Configuration met behulp van de GUI.

Configuratie van Livingston RADIUS-server

Voeg de PIX IP en sleutel toe aan het clientbestand.

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

Configuratie van Merit RADIUS-server

Voeg de PIX IP en sleutel toe aan het clientbestand.

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

Configuratie van TACACS+ Freeware-server

```
# Handshake with router--PIX needs 'tacacs-server host #.#.#.# cisco':
key = "cisco"

user = all {
default service = permit
login = cleartext "all"
}

user = telnetonly {
```

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

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

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

Debugging stappen

- Zorg ervoor dat de PIX-configuraties werken voordat u verificatie, autorisatie en accounting (AAA) toevoegt.
    - Als u geen verkeer kunt doorgeven voordat u de AAA instelt, kunt u dit nadien niet meer doen.
- Aanmelden bij PIX inschakelen:
    - De opdracht debuggen van de logboekconsole mag niet worden gebruikt op een zwaar geladen systeem.
    - De opdracht logging buffered debugging kan worden gebruikt. De output van de opdrachten logboekregistratie of logboekregistratie kan vervolgens naar een syslogserver worden verzonden en worden onderzocht.
- Zorg ervoor dat de debugging is ingeschakeld voor de TACACS+ of RADIUS-servers. Alle servers hebben deze optie.

Verificatie Debug Voorbeelden van PIX

PIX Debug - goede verificatie - RADIUS

Dit is een voorbeeld van een PIX debug met goede verificatie:

```
109001: Auth start for user '???' from 171.68.118.100/1116 to 9.9.9.11/23
 109011: Authen Session Start: user 'bill', sid 1
 109005: Authentication succeeded for user 'bill'
   from 171.68.118.100/1116 to 9.9.9.11/23
```

```
 109012: Authen Session End: user 'bill', sid 1, elapsed 1 seconds
 302001: Built TCP connection 1 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1116
   laddr 171.68.118.100/1116 (bill)
```

PIX Debug - slechte verificatie (gebruikersnaam of wachtwoord) - RADIUS

Dit is een voorbeeld van een PIX debug met slechte verificatie (gebruikersnaam of wachtwoord). De gebruiker ziet vier gebruikersnaam/wachtwoordreeksen. De melding "Fout: max. aantal pogingen overschreden" wordt weergegeven.

N.B.: Als dit een FTP-poging is, is één poging toegestaan. Voor HTTP zijn oneindig veel herhalingen toegestaan.

```
109001: Auth start for user '???' from 171.68.118.100/1132 to 9.9.9.11/23
 109006: Authentication failed for user '' from
   171.68.118.100/1132 to 9.9.9.11/23
```

PIX Debug - Server Down - RADIUS

Dit is een voorbeeld van een PIX debug met de server down. De gebruiker ziet de gebruikersnaam eenmaal. De server "hangt" en vraagt om een wachtwoord (drie keer).

```
109001: Auth start for user '???' from 171.68.118.100/1151 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1151 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1151 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
```

PIX Debug - goede verificatie - TACACS+

Dit is een voorbeeld van een PIX debug met goede verificatie:

```
109001: Auth start for user '???' from 171.68.118.100/1200 to 9.9.9.11/23
 109011: Authen Session Start: user 'cse', sid 3
 109005: Authentication succeeded for user 'cse'
   from 171.68.118.100/1200 to 9.9.9.11/23
 109012: Authen Session End: user 'cse', sid 3, elapsed 1 seconds
 302001: Built TCP connection 3 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1200
  laddr 171.68.118.100/1200 (cse)
```

PIX Debug - Slechte verificatie (gebruikersnaam of wachtwoord) - TACACS+

Dit is een voorbeeld van een PIX debug met slechte verificatie (gebruikersnaam of wachtwoord).

De gebruiker ziet vier gebruikersnaam/wachtwoordreeksen. De melding "Fout: max. aantal pogingen overschreden" wordt weergegeven.

N.B.: Als dit een FTP-poging is, is één poging toegestaan. Voor HTTP zijn oneindig veel herhalingen toegestaan.

```
109001: Auth start for user '???' from 171.68.118.100/1203 to 9.9.9.11/23
 109006: Authentication failed for user ''
   from 171.68.118.100/1203 to 9.9.9.11/23
```

PIX Debug - Server Down - TACACS+

Dit is een voorbeeld van een PIX debug met de server down. De gebruiker ziet de gebruikersnaam eenmaal. Er wordt onmiddellijk de melding "Fout: Max. aantal pogingen overschreden" weergegeven.

```
109001: Auth start for user '???' from 171.68.118.100/1212 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109006: Authentication failed for user '' from 171.68.118.100/1212 to 9.9.9.11/23
```

Toevoegende vergunning

Omdat de vergunning zonder authentificatie ongeldig is, wordt de vergunning vereist voor de zelfde bron en de bestemming:

<#root>

```
aaa authorization any outbound 171.68.118.0 255.255.255.0 9.9.9.11
   255.255.255.255 tacacs+|radius
```

Of, als alle drie de uitgaande diensten oorspronkelijk voor authentiek werden verklaard:

<#root>

```
aaa authorization http outbound 0.0.0.0 0.0.0.0 0.0.0.0
   0.0.0.0 tacacs+|radius
aaa authorization ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0
   0.0.0.0 tacacs+|radius
aaa authorization telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
```

```
   0.0.0.0 tacacs+|radius
```

Verificatie en autorisatie Debug voorbeelden van PIX

PIX Debug - goede verificatie en autorisatie - TACACS+

Dit is een voorbeeld van een PIX debug met goede verificatie en autorisatie:

```
109001: Auth start for user '???' from 171.68.118.100/1218 to 9.9.9.11/23
 109011: Authen Session Start: user 'telnetonly', sid 5
 109005: Authentication succeeded for user 'telnetonly' from
   171.68.118.100/1218 to 9.9.9.11/23
 109011: Authen Session Start: user 'telnetonly', sid 5
 109007: Authorization permitted for user 'telnetonly' from
   171.68.118.100/1218 to 9.9.9.11/23
 109012: Authen Session End: user 'telnetonly', sid 5, elapsed 1 seconds
 302001: Built TCP connection 4 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1218
   laddr 171.68.118.100/1218 (telnetonly)
```

PIX Debug - goede verificatie, maar falen in autorisatie - TACACS+

Dit is een voorbeeld van een PIX debug met goede authenticatie maar falen in autorisatie:

```
109001: Auth start for user '???' from 171.68.118.100/1223 to 9.9.9.11/23
 109011: Authen Session Start: user 'httponly', sid 6
 109005: Authentication succeeded for user 'httponly'
   from 171.68.118.100/1223 to 9.9.9.11/23
 109008: Authorization denied for user 'httponly'
   from 171.68.118.100/1223 to 9.9.9.11/23
```

PIX Debug - slechte verificatie, autorisatie niet geprobeerd - TACACS+

Dit is een voorbeeld van een PIX debug met authenticatie en autorisatie, maar autorisatie niet geprobeerd vanwege slechte authenticatie (gebruikersnaam of wachtwoord). De gebruiker ziet vier gebruikersnaam/wachtwoordreeksen. De melding "Fout: max. aantal pogingen overschreden." wordt weergegeven

N.B.: Als dit een FTP-poging is, is één poging toegestaan. Voor HTTP zijn oneindig veel herhalingen toegestaan.

```
109001: Auth start for user '???' from 171.68.118.100/1228 to 9.9.9.11/23
 109006: Authentication failed for user '' from 171.68.118.100/1228
   to 9.9.9.11/23
```

PIX Debug - Verificatie/autorisatie, server omlaag - TACACS+

Dit is een voorbeeld van een PIX debug met authenticatie en autorisatie. De server is defect. De gebruiker ziet gebruikersnaam eenmaal. Direct wordt "Fout: Max. aantal pogingen overschreden." weergegeven.

```
109001: Auth start for user '???' from 171.68.118.100/1237 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109006: Authentication failed for user '' from 171.68.118.100/1237
   to 9.9.9.11/23
```

Accounting toevoegen

TACACS +

<#root>

aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0: tacacs+

Debug ziet er hetzelfde uit of accounting aan of uit is. Ten tijde van de "Built" wordt echter een "start" accounting record verstuurd. Ten tijde van de "Teardown" wordt ook een "stop"-accounting record gestuurd:

```
109011: Authen Session Start: user 'telnetonly', sid 13
 109005: Authentication succeeded for user 'telnetonly'
   from 171.68.118.100/1299 to 9.9.9.11/23
 109011: Authen Session Start: user 'telnetonly', sid 13
 109007: Authorization permitted for user 'telnetonly'
   from 171.68.118.100/1299 to 9.9.9.11/23
 109012: Authen Session End: user 'telnetonly', sid 13, elapsed 1 seconds
 302001: Built TCP connection 11 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1299
  laddr 171.68.118.100/1299 (telnetonly)
 302002: Teardown TCP connection 11 faddr 9.9.9.11/23 gaddr 9.9.9.10/1299
  laddr 171.68.118.100/1299 duration 0:00:02 bytes 112
```

De TACACS+ accounting records zien er als deze uitvoer uit (deze zijn van Cisco Secure UNIX; de records in Cisco Secure Windows kunnen in plaats daarvan door komma's worden gescheiden):

```
Tue Sep 29 11:00:18 1998 redclay cse PIX 171.68.118.103
   start task_id=0x8 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet
 Tue Sep 29 11:00:36 1998 redclay cse PIX 171.68.118.103
   stop task_id=0x8 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet elapsed_time=17
   bytes_in=1198 bytes_out=62
 Tue Sep 29 11:02:08 1998 redclay telnetonly PIX 171.68.118.103
   start task_id=0x9 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet
 Tue Sep 29 11:02:27 1998 redclay telnetonly PIX 171.68.118.103
   stop task_id=0x9 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet elapsed_time=19
   bytes_in=2223 bytes_out=64
```

De velden worden hier uitgesplitst:

```
DAY MO DATE TIME YEAR NAME_OF_PIX USER SENDER PIX_IP START/STOP
   UNIQUE_TASK_ID DESTINATION SOURCE
   SERVICE <TIME> <BYTES_IN> <BYTES_OUT>
```

RADIUS

<#root>

aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 radius

Debug ziet er hetzelfde uit of accounting aan of uit is. Ten tijde van de "Built" wordt echter een "start" accounting record verstuurd. Ten tijde van de "Teardown" wordt ook een "stop"-accounting record gestuurd:

```
109001: Auth start for user '???' from 171.68.118.100/1316 to 9.9.9.11/23
 109011: Authen Session Start: user 'bill', sid 16
 109005: Authentication succeeded for user 'bill'
   from 171.68.118.100/1316 to 9.9.9.11/23
 109012: Authen Session End: user 'bill', sid 16, elapsed 1 seconds
 302001: Built TCP connection 14 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1316
  laddr 171.68.118.100/1316 (bill)
 302002: Teardown TCP connection 14 faddr 9.9.9.11/23 gaddr 9.9.9.10/1316
  laddr 171.68.118.100/1316 duration 0:00:03 bytes 112
```

RADIUS-accounting records zien er zo uit als deze uitvoer (deze komen van Cisco Secure UNIX; de records in Cisco Secure Windows zijn kommagescheiden):

```
Mon Sep 28 10:47:01 1998
Acct-Status-Type = Start
Client-Id = 171.68.118.103
Login-Host = 171.68.118.100
Login-TCP-Port = 23
Acct-Session-Id = "0x00000004"
User-Name = "bill"

Mon Sep 28 10:47:07 1998
Acct-Status-Type = Stop
Client-Id = 171.68.118.103
Login-Host = 171.68.118.100
Login-TCP-Port = 23
Acct-Session-Id = "0x00000004"
User-Name = "bill"
Acct-Session-Time = 5
```

De velden worden hier uitgesplitst:

```
Acct-Status-Type = START or STOP
Client-ID = IP_OF_PIX
Login_Host = SOURCE_OF_TRAFFIC
Login-TCP-Port = #
Acct-Session-ID = UNIQUE_ID_PER_RADIUS_RFC
User-name = <whatever>
<Acct-Session-Time = #>
```

Max. aantal sessies en ingelogde gebruikers bekijken

Sommige TACACS- en RADIUS-servers hebben "max-sessie"- of "view login users"-functies. De mogelijkheid om max-sessies te doen of de ingelogde gebruikers te controleren is afhankelijk van de boekhouding. Wanneer er een accounting "start" record gegenereerd maar geen "stop" record is, gaat de TACACS of RADIUS server ervan uit dat de persoon nog steeds ingelogd is (dat wil zeggen; heeft een sessie via PIX). Dit werkt goed voor Telnet en FTP verbindingen vanwege de aard van de verbindingen. Een voorbeeld:

De gebruiker Telnets van 171.68.118.100 tot 9.9.9.25 door PIX, die op de weg voor authentiek verklaren:

```
(pix) 109001: Auth start for user '???' from 171.68.118.100/1200
   to 9.9.9.25/23
(pix) 109011: Authen Session Start: user 'cse', sid 3
(pix) 109005: Authentication succeeded for user 'cse' from 171.68.118.100/12
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 heeft gezien, maar geen "stop"-record (op dit moment), toont de server aan dat de "Telnet"-gebruiker is ingelogd. Als de gebruiker een andere verbinding probeert waarvoor verificatie nodig is (wellicht vanaf een andere pc) en als max-sessies voor deze gebruiker is ingesteld op "1" op de server, wordt de verbinding door de server geweigerd.

De gebruiker gaat over zaken op de doelhost, en gaat dan weg (besteedt er 10 minuten).

```
(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 uauth 0 is (dat wil zeggen elke keer authenticeren) of meer (eenmalig en niet opnieuw authenticeren tijdens de wachtperiode), er zal een boekhoudkundige record knippen voor elke site die wordt benaderd.

Maar HTTP werkt anders vanwege de aard van het protocol. Hierna volgt een voorbeeld:

De gebruiker bladert van 171.68.118.100 tot 9.9.9.25 via 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 een gedownloade webpagina.

Let op de tijd. Deze download duurde een seconde (er was minder dan een seconde tussen de start en de stop record). Is de gebruiker nog steeds ingelogd op de website en is de verbinding nog steeds open? Nee.

Zullen max-sessies of inloggebruikers bekijken hier werken? Nee, omdat de verbindingstijd in HTTP te kort is. De tijd tussen "Built" en "Teardown" (de "start" en "stop" record) is subseconde. Er zal geen "start" record zijn zonder een "stop" record, omdat de records op vrijwel hetzelfde moment plaatsvinden. Voor elke transactie wordt nog steeds een start- en stop-record naar de server verzonden, ongeacht of de auth is ingesteld op 0 of iets groters. Echter, de max-sessies en de weergave ingelogde gebruikers werken niet vanwege de aard van HTTP verbindingen.

Gebruik van de opdracht Opslaan

In ons netwerk, als we besluiten dat een uitgaande gebruiker (171.68.118.100) niet hoeft te worden geverifieerd, kunnen we dit doen:

<#root>

```
aaa authentication any outbound 171.68.118.0 255.255.255.0 9.9.9.11
   255.255.255.255 tacacs+
aaa authentication except outbound 171.68.118.100 255.255.255.255 9.9.9.11
   255.255.255.255 tacacs+
```

Verificatie naar de PIX zelf

De vorige discussie gaat over het verifiëren van Telnet- (en HTTP-, FTP-) verkeer via de PIX. Met 4.2.2 kunnen Telnet-verbindingen naar de PIX ook worden geverifieerd. Hier, bepalen wij IPs van dozen die Telnet aan PIX kunnen:

<#root>

```
telnet 171.68.118.100 255.255.255.255
```

Typ vervolgens het Telnet-wachtwoord: wachtwoord ww.

Voeg de nieuwe opdracht toe om gebruikers Telnetting te verifiëren aan de PIX:

<#root>

```
aaa authentication telnet console tacacs+|radius
```

Wanneer gebruikers Telnet naar de PIX vragen, wordt om het Telnet-wachtwoord ("ww")

gevraagd. PIX vraagt ook om de TACACS+ of RADIUS gebruikersnaam en wachtwoord.

De prompt voor gebruikers wijzigen Zie

Als u de opdracht toevoegt: auth-prompt YOU_ARE_AT_THE_PIX, zullen gebruikers die door de PIX gaan de volgorde zien:

```
YOU_ARE_AT_THE_PIX [at which point you enter the username]
 Password:[at which point you enter the password]
```

Bij aankomst op de eindbestemming worden de "Gebruikersnaam:" en "Wachtwoord:"-vragen weergegeven. Deze prompt heeft alleen invloed op gebruikers die door de PIX gaan, niet naar de PIX.

Opmerking: er zijn geen boekhoudkundige gegevens geknipt voor toegang tot de PIX.

Gerelateerde informatie

- Productondersteuning voor Cisco PIX-firewall-software
- Referenties voor Cisco Secure PIX-firewall-opdracht
- Requests for Comments (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.