Authentifizierung, Autorisierung und Abrechnung von Benutzern über PIX Version 5.2 und höher

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Authentifizierung, Autorisierung und Abrechnung
Was der Benutzer mit Authentifizierung/Autorisierung auf
Debugschritte
Nur Authentifizierung
Netzwerkdiagramm
Server-Setup - Nur Authentifizierung
Konfigurierbare RADIUS-Ports (5.3 und höher)
Debugbeispiele für die PIX-Authentifizierung
Authentication Plus-Autorisierung
Server-Setup - Authentifizierung plus Autorisierung
PIX-Konfiguration - Hinzufügen von Autorisierung
Debugbeispiele für PIX-Authentifizierung und -Autorisierung
Neue Funktion für die Zugriffsliste
PIX-Konfiguration
Serverprofile
Neue benutzerspezifische herunterladbare Zugriffsliste mit Version 6.2
Accounting hinzufügen
PIX-Konfiguration - Hinzufügen von Accounting
Buchhaltungsbeispiele
Verwendung des Befehls "exclude"
Max. Sitzungen und Anzeige der angemeldeten Benutzer
Benutzeroberfläche
Benutzer auffordern anzeigen
Anpassen der angezeigten Nachricht
Leerlauf- und absolute Timeouts pro Benutzer
Ausgehendes virtuelles HTTP
Virtuelles Telnet
Virtual Telnet Inbound
Virtuelles Telnet - Ausgehend
Logout für virtuelles Telnet
Port-Autorisierung

Netzwerkdiagramm
AAA-Abrechnung für Datenverkehr außer HTTP, FTP und Telnet
Beispiel für TACACS+-Accounting-Datensätze
Authentifizierung auf der DMZ
Netzwerkdiagramm
Partielle PIX-Konfiguration
Informationen, die beim Öffnen eines TAC-Tickets gesammelt werden müssen
Zugehörige Informationen

Einführung

Die RADIUS- und TACACS+-Authentifizierung kann für FTP-, Telnet- und HTTP-Verbindungen über die Cisco Secure PIX Firewall erfolgen. Die Authentifizierung für andere, weniger häufig verwendete Protokolle wird normalerweise zum Arbeiten durchgeführt. Die TACACS+-Autorisierung wird unterstützt. Die RADIUS-Autorisierung wird nicht unterstützt. Änderungen bei PIX 5.2 Authentication, Authorization, Accounting (AAA) gegenüber der früheren Version beinhalten die Unterstützung von AAA-Zugriffslisten, um zu kontrollieren, wer authentifiziert ist und auf welche Ressourcen der Benutzer zugreift. In PIX 5.3 und höher ist die Änderung von Authentication, Authorization, Accounting (AAA) gegenüber früheren Codeversionen darin, dass die RADIUS-Ports konfigurierbar sind.

Hinweis: PIX 6.x kann den Datenverkehr durch den PIX abrechnen, jedoch nicht den Datenverkehr, der an den PIX gerichtet ist.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine besonderen Voraussetzungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- Cisco Secure PIX Firewall Software Versionen 5.2.0.205 und 5.2.0.207

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hinweis: Wenn Sie die PIX/ASA-Software Version 7.x oder höher ausführen, lesen Sie Informationen zum Konfigurieren von AAA-Servern und zur lokalen Datenbank.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Authentifizierung, Autorisierung und Abrechnung

Hier eine Erklärung zur Authentifizierung, Autorisierung und Abrechnung:

- Die Authentifizierung ist der Benutzer.
- Autorisierung ist, was der Benutzer tut.
- Die Authentifizierung ist ohne Autorisierung gültig.
- Die Autorisierung ist ohne Authentifizierung ungültig.
- Die Abrechnung ist das, was der Benutzer getan hat.

Was der Benutzer mit Authentifizierung/Autorisierung auf

Wenn der Benutzer versucht, von innen nach außen (oder umgekehrt) mit Authentifizierung/Autorisierung zu wechseln:

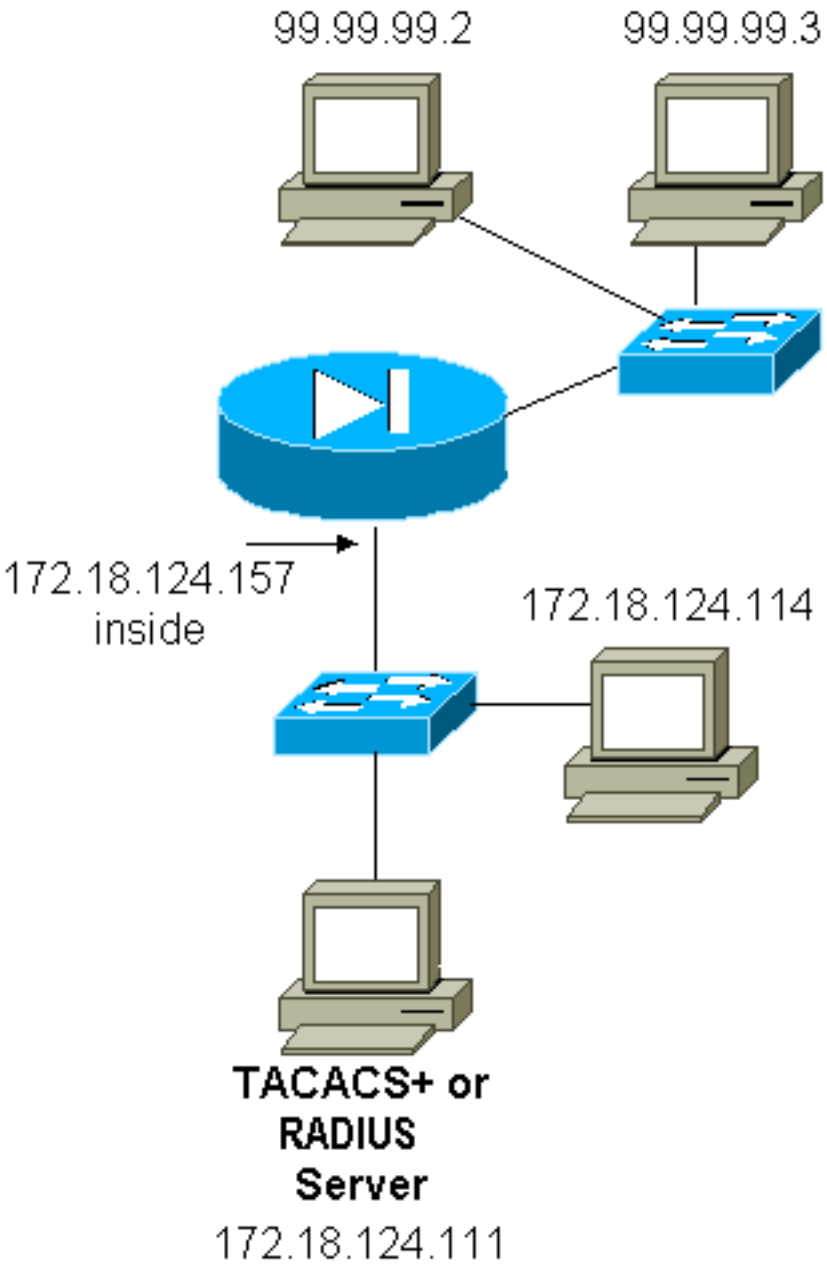
- **Telnet** - Der Benutzer sieht eine Eingabeaufforderung für einen Benutzernamen und dann eine Kennwortanfrage. Wenn die Authentifizierung (und Autorisierung) auf dem PIX/Server erfolgreich ist, wird der Benutzer vom Zielhost nach Benutzername und Kennwort gefragt.
- **FTP**: Der Benutzer sieht eine Eingabeaufforderung für einen Benutzernamen. Der Benutzer muss "local_username@remote_username" als Benutzernamen und "local_password@remote_password" als Kennwort eingeben. Der PIX sendet den Befehl "local_username" und den Befehl "local_password" an den lokalen Sicherheitsserver. Wenn die Authentifizierung (und Autorisierung) auf dem PIX/Server erfolgreich ist, werden der "remote_username" und "remote_password" über die Grenzen hinaus an den Ziel-FTP-Server übergeben.
- **HTTP**: Im Browser wird ein Fenster angezeigt, in dem Benutzername und Kennwort angefordert werden. Wenn die Authentifizierung (und Autorisierung) erfolgreich ist, erreicht der Benutzer die Ziel-Website darüber hinaus. Beachten Sie, dass *Browser Benutzernamen und Kennwörter zwischenspeichern.* Wenn es scheint, dass das PIX eine HTTP-Verbindung auslöst, dies aber nicht tut, ist es wahrscheinlich, dass die erneute Authentifizierung tatsächlich mit dem Browser "schießen" den zwischengespeicherten Benutzernamen und das Kennwort auf den PIX. Das PIX leitet dies an den Authentifizierungsserver weiter. Dieses Phänomen zeigt PIX Syslog und/oder Server-Debugging. Wenn Telnet und FTP scheinbar "normal" funktionieren, HTTP-Verbindungen jedoch nicht, ist dies der Grund.

Debugschritte

- Stellen Sie sicher, dass die PIX-Konfiguration funktioniert, bevor Sie AAA-Authentifizierung und -Autorisierung hinzufügen. Wenn Sie keinen Datenverkehr weiterleiten können, bevor Sie Authentifizierung und Autorisierung einleiten, können Sie dies nachher nicht tun.
- Aktivieren Sie eine Protokollierung im PIX.Führen Sie den **Debugging-**Befehl der **Protokollierungskonsole aus**, um das Debuggen der Protokollierungskonsole zu aktivieren.**Hinweis:** Verwenden Sie kein Protokollierungskonsolendebuggen auf einem stark ausgelasteten System.Verwenden Sie den Befehl **logging monitor debug**, um eine Telnet-Sitzung zu protokollieren.Das gepufferte Debugging für die Protokollierung kann verwendet werden. Anschließend kann der Befehl **show logging** ausgeführt werden.Die Protokollierung kann auch an einen Syslog-Server gesendet und dort überprüft werden.
- Aktivieren Sie das Debuggen auf den TACACS+- oder RADIUS-Servern.

Nur Authentifizierung

Netzwerkdiagramm



Server-Setup - Nur Authentifizierung

Cisco Secure UNIX TACACS-Serverkonfiguration

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

Cisco Secure UNIX RADIUS-Serverkonfiguration

Hinweis: Fügen Sie die PIX-IP-Adresse und den PIX-Schlüssel zur Liste des Network Access

Servers (NAS) mithilfe der erweiterten Benutzeroberfläche hinzu.

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

Cisco Secure Windows RADIUS

Mithilfe dieser Schritte können Sie einen Cisco Secure Windows RADIUS-Server einrichten.

1. Rufen Sie ein Kennwort im Abschnitt **User Setup (Benutzereinrichtung)** ab.
2. Legen Sie im Abschnitt **Gruppeneinrichtung** das Attribut 6 (Servicetyp) auf **Anmelden** oder **Verwaltung fest**.
3. Fügen Sie die PIX-IP-Adresse im Abschnitt "**NAS-Konfiguration**" der GUI hinzu.

Cisco Secure Windows TACACS+

Der Benutzer erhält ein Kennwort im Abschnitt **User Setup (Benutzereinrichtung)**.

Konfiguration des Livingston RADIUS-Servers

Hinweis: Fügen Sie der *Client*-Datei PIX-IP-Adresse und -Schlüssel hinzu.

- Bill Password="foo" User-Service Type = Shell-User

RADIUS-Serverkonfiguration vermerken

Hinweis: Fügen Sie der *Client*-Datei PIX-IP-Adresse und -Schlüssel hinzu.

- Bill Password="foo" Service Type = Shell-User

TACACS+ Freeware Server-Konfiguration

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

Erstkonfiguration für PIX - nur Authentifizierung

Erstkonfiguration für PIX - nur Authentifizierung
`PIX Version 5.2(0)205`

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd OnTrBUG1Tp0edmkr encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
!
!--- These lines are necessary !--- if the new feature
in 5.2 is used to define which !--- target/source IP
addresses are to be authenticated. access-list 101
permit tcp any any eq telnet
access-list 101 permit tcp any any eq ftp
access-list 101 permit tcp any any eq www
!
pager lines 24
logging on
no logging timestamp
no logging standby
logging console debugging
no logging monitor
no logging buffered
logging trap debugging
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 10baset
mtu outside 1500
mtu inside 1500
ip address outside 99.99.99.1 255.255.255.0
ip address inside 172.18.124.157 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
global (outside) 1 99.99.99.10-99.99.99.20 netmask
255.255.255.0
nat (inside) 1 172.18.124.0 255.255.255.0 0 0
static (inside,outside) 99.99.99.99 172.18.124.114
netmask 255.255.255.255 0 0
conduit permit tcp any any
conduit permit udp any any
conduit permit icmp any any
route inside 172.18.0.0 255.255.0.0 172.18.124.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h323 0:05:00
si p 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
!
!--- For the purposes of illustration, the TACACS+
process is used !--- to authenticate inbound users and
RADIUS is used to authenticate outbound users. aaa-
```

```
server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server AuthInbound protocol tacacs+
aaa-server AuthInbound (inside) host 172.18.124.111
cisco timeout 5
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 172.18.124.111
cisco timeout 5
!
!--- The next six statements are used to authenticate
all inbound !--- and outbound FTP, Telnet, and HTTP
traffic. aaa authentication include ftp outside 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authentication include telnet outside 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authentication include http outside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0
   AuthInbound
aaa authentication include http inside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0
   AuthOutbound
aaa authentication include telnet inside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0
   AuthOutbound
aaa authentication include ftp inside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0
   AuthOutbound
!
!--- OR the new 5.2 feature allows these two statements
in !--- conjunction with access-list 101 to replace the
previous six statements. !--- Note: Do not mix the old
and new verbiage.

aaa authentication match 101 outside AuthInbound
aaa authentication match 101 inside AuthOutbound
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
no sysopt route dnat
isakmp identity hostname
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:5882f514247589d784a0d74c800907b8
: end
```

Konfigurierbare RADIUS-Ports (5.3 und höher)

Einige RADIUS-Server verwenden andere RADIUS-Ports als 1645/1646 (in der Regel 1812/1813). In PIX 5.3 und höher können die RADIUS-Authentifizierungs- und Accounting-Ports mithilfe der folgenden Befehle in einen anderen Wert als den Standardwert 1645/1646 geändert werden:

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

Debugbeispiele für die PIX-Authentifizierung

Informationen zum Aktivieren des Debuggens finden Sie unter Debugschritte. Dies sind Beispiele für einen Benutzer mit der Nummer 99.99.99.2, der Datenverkehr mit der Adresse 172.18.124.114 (99.99.99.99) initiiert und umgekehrt. Eingehender Datenverkehr wird vom TACACS authentifiziert, und ausgehender Datenverkehr wird über RADIUS authentifiziert.

Erfolgreiche Authentifizierung: TACACS+ (eingehender Datenverkehr)

```
109001: Auth start for user '???' from 99.99.99.2/11003 to 172.18.124.114/23
109011: Authen Session Start: user 'cse', sid 2
109005: Authentication succeeded for user 'cse' from 172.18.124.114/23
  to 99.99. 99.2/11003 on interface outside
302001: Built inbound TCP connection 4 for faddr 99.99.99.2/11003
  gaddr 99.99.99 .99/23 laddr 172.18.124.114/23 (cse)
```

Fehlgeschlagene Authentifizierung aufgrund von ungültigem Benutzernamen/Kennwort - TACACS+ (eingehend). Der Benutzer sieht "Fehler: Die maximale Anzahl der Versuche wurde überschritten."

```
109001: Auth start for user '???' from 99.99.99.2/11004 to 172.18.1 24.114/23
109006: Authentication failed for user '' from 172.18.124.114/23
  to 99.99.99.2/1 1004 on interface outside
```

Server spricht nicht mit PIX - TACACS+ (eingehend). Der Benutzer sieht den Benutzernamen einmal und der PIX fragt nie nach einem Kennwort (dies ist auf Telnet). Benutzer sieht "Fehler: Die maximale Anzahl der Versuche wurde überschritten."

```
109001: Auth start for user '???' from 99.99.99.2/11005 to 172.18.124.114/23
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
  (server 172.18.12 4.111 failed) on interface outside
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
  (server 172.18.12 4.111 failed) on interface outside
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
  (server 172.18.12 4.111 failed) on interface outside
109006: Authentication failed for user '' from 172.18.124.114/23
  to 99.99.99.2/1 1005 on interface outside
```

Gute Authentifizierung - RADIUS (ausgehend)

```
109001: Auth start for user '???' from 172.18.124.114/35931 to 99.99.99.2/23
109011: Authen Session Start: user 'bill', Sid 0
109005: Authentication succeeded for user 'bill' from 172.18.124.114/35931
  to 99 .99.99.2/23 on interface inside
```

Schlechte Authentifizierung (Benutzername oder Kennwort) - RADIUS (ausgehend). Benutzer sieht die Anfrage für Benutzername und dann Kennwort, hat drei Möglichkeiten, diese einzugeben, und wenn nicht erfolgreich, siehe "Fehler: Die maximale Anzahl der Versuche wurde überschritten."

```
109001: Auth start for user '???' from 172.18.124.114/35932 to 99.99.99.2/23
109002: Auth from 172.18.124.114/35932 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109006: Authentication failed for user '' from 172.18.124.114/35932
```

```
  to 99.99.99. 2/23 on interface inside
```

Server-Pingable, aber Daemon Down, Server nicht Pingable oder Schlüssel/Client-Ungleichheit - kommuniziert nicht mit PIX - RADIUS (ausgehend). Benutzer sieht Benutzername, dann Kennwort, dann "RADIUS-Server fehlgeschlagen" und schließlich "Fehler: Die maximale Anzahl der Versuche wurde überschritten."

```
109001: Auth start for user '???' from 172.18.124.114/35933 to 99.99.99.2/23
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109006: Authentication failed for user '' from 172.18.124.114/35933
  to 99.99.99. 2/23 on interface inside
```

Authentication Plus-Autorisierung

Wenn alle authentifizierten Benutzer alle Operationen (HTTP, FTP und Telnet) über PIX ausführen möchten, ist eine Authentifizierung ausreichend, und eine Autorisierung ist nicht erforderlich. Wenn Sie jedoch bestimmten Benutzern einige Teilgruppen von Diensten erlauben oder Benutzer daran hindern möchten, bestimmte Sites aufzurufen, ist eine Autorisierung erforderlich. Die RADIUS-Autorisierung ist für Datenverkehr über den PIX nicht gültig. In diesem Fall ist die TACACS+-Autorisierung gültig.

Wenn die Authentifizierung erfolgreich verläuft und die Autorisierung aktiviert ist, sendet das PIX-System den Befehl, den der Benutzer an den Server ausführt. Beispiel: "http 1.2.3.4" In Version 5.2 von PIX wird die TACACS+-Autorisierung in Verbindung mit Zugriffslisten verwendet, um zu kontrollieren, wohin Benutzer gehen.

Wenn Sie die Autorisierung für HTTP (besuchte Websites) implementieren möchten, verwenden Sie Software wie Websense, da eine einzelne Website mit einer großen Anzahl von IP-Adressen verbunden sein kann.

Server-Setup - Authentifizierung plus Autorisierung

Cisco Secure UNIX TACACS-Serverkonfiguration

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

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

```
  }

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

Cisco Secure Windows TACACS+

Führen Sie diese Schritte aus, um einen Cisco Secure Windows TACACS+-Server einzurichten.

1. Klicken Sie unten im Group Setup (Gruppen-Setup) auf **Nicht übereinstimmende IOS-Befehle verweigern**.
2. Klicken Sie auf **Neuen Befehl hinzufügen/bearbeiten (FTP, HTTP, Telnet)**.Wenn Sie beispielsweise Telnet für einen bestimmten Standort zulassen möchten ("Telnet 1.2.3.4"), lautet der Befehl **telnet**. Das Argument ist *1.2.3.4*. Geben Sie nach dem Ausfüllen von "command=**telnet**" die IP-Adresse(n) "permit" im Argument-Rechteck ein (z. B. "permit 1.2.3.4"). Wenn alle Telnets zugelassen werden sollen, lautet der Befehl immer noch **telnet**, aber klicken Sie auf **Alle nicht aufgeführten Argumente zulassen**. Klicken Sie anschließend auf **Bearbeiten beenden**.
3. Führen Sie Schritt 2 für jeden der zulässigen Befehle aus (z. B. Telnet, HTTP und FTP).
4. Fügen Sie die PIX-IP-Adresse mithilfe der GUI im Abschnitt "NAS Configuration" (NAS-Konfiguration) hinzu.

TACACS+ Freeware Server-Konfiguration

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

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

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

PIX-Konfiguration - Hinzufügen von Autorisierung

Hinzufügen von Befehlen zum Anfordern der Autorisierung:

```
aaa authorization include telnet outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authorization include http outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authorization include ftp outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
```

Mit der neuen 5.2-Funktion kann diese Anweisung in Verbindung mit der zuvor definierten Zugriffsliste 101 die vorherigen drei Anweisungen ersetzen. Der alte und der neue Wortlaut sollten nicht gemischt werden.

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

Debugbeispiele für PIX-Authentifizierung und -Autorisierung

Gute Authentifizierung und Autorisierung erfolgreich - TACACS+

```
109001: Auth start for user '???' from
   99.99.99.2/11010 to 172.18.124.114/23
109011: Authen Session Start: user 'cse', Sid 3
109005: Authentication succeeded for user
   'cse' from 172.18.124.114/23 to 99.99.99.2/11010
   on interface outside
109011: Authen Session Start: user 'cse', Sid 3
109007: Authorization permitted for user 'cse'
   from 99.99.99.2/11010 to 172.18.1  24.114/23
   on interface outside
302001: Built inbound TCP connection 2 for faddr
   99.99.99.2/11010 gaddr 99.99.99.99/23 laddr
   172.18.124.114/23 (cse)
```

Gute Authentifizierung, aber Autorisierung schlägt fehl - TACACS+. Der Benutzer sieht außerdem die Meldung "Fehler: Autorisierung verweigert."

```
109001: Auth start for user '???' from
   99.99.99.2/11011 to 172.18.124.114/23
109011: Authen Session Start: user 'httponly', Sid 4
109005: Authentication succeeded for user 'httponly'
   from 172.18.124.114/23 to  9 9.99.99.2/11011
   on interface outside
109008: Authorization denied for user 'httponly'
   from 172.18.124.114/23 to 99.99.99.2/11011
   on interface outside
```

Neue Funktion für die Zugriffsliste

Definieren Sie in der PIX-Softwareversion 5.2 und höher Zugriffslisten auf dem PIX. Wenden Sie diese auf Benutzerbasis an, basierend auf dem Benutzerprofil auf dem Server. TACACS+ erfordert Authentifizierung und Autorisierung. RADIUS erfordert nur Authentifizierung. In diesem Beispiel werden die ausgehende Authentifizierung und Autorisierung für TACACS+ geändert. Es wird eine Zugriffsliste auf dem PIX eingerichtet.

Hinweis: Wenn Sie in PIX Version 6.0.1 und höher RADIUS verwenden, werden die Zugriffslisten

implementiert, indem Sie die Liste im IETF RADIUS-Attribut 11 (Filter-ID) [CSCdt50422] eingeben. In diesem Beispiel wird das Attribut 11 auf 115 festgelegt, anstatt das anbieterspezifische "acl=115"-Wort zu verwenden.

PIX-Konfiguration

```
access-list 115 permit tcp any host 99.99.99.2 eq telnet
access-list 115 permit tcp any host 99.99.99.2 eq www
access-list 115 permit tcp any host 99.99.99.2 eq ftp
access-list 115 deny tcp any host 99.99.99.3 eq www
access-list 115 deny tcp any host 99.99.99.3 eq ftp
access-list 115 deny tcp any host 99.99.99.3 eq telnet
```

Serverprofile

Hinweis: Die 2.1-Version der Freeware TACACS+ erkennt die Verbiage "acl" nicht.

Cisco Secure UNIX TACACS+-Serverkonfiguration

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

Cisco Secure Windows TACACS+

Um dem PIX eine Autorisierung hinzuzufügen, um zu steuern, wo der Benutzer Zugriffslisten erhält, aktivieren Sie **shell/exec**, aktivieren Sie das **Zugriffssteuerungslisten-**Feld, und füllen Sie die Nummer aus (entspricht der Zugriffslistennummer auf dem PIX).

Cisco Secure UNIX RADIUS

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

Cisco Secure Windows RADIUS

RADIUS/Cisco ist der Gerätetyp. Der "pixa"-Benutzer benötigt einen Benutzernamen, ein Kennwort und ein Häkchen sowie "acl=115" im rechteckigen Feld Cisco/RADIUS, in dem 009\001 AV-Pair (anbieterspezifisch) steht.

Ausgabe

Der ausgehende Benutzer "pixa" mit "acl=115" im Profil authentifiziert und autorisiert. Der Server übergibt das ACL=115 an das PIX, und das PIX zeigt Folgendes:

```
pixfirewall#show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          2
user 'pixa' at 172.18.124.114, authenticated
   access-list 115
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

Wenn der Benutzer "pixa" versucht, zu 99.99.99.3 zu wechseln (oder zu einer beliebigen IP-Adresse außer 99.99.99.2, da eine implizite Ablehnung vorliegt), sieht der Benutzer Folgendes:

```
Error: acl authorization denied
```

Neue benutzerspezifische herunterladbare Zugriffsliste mit Version 6.2

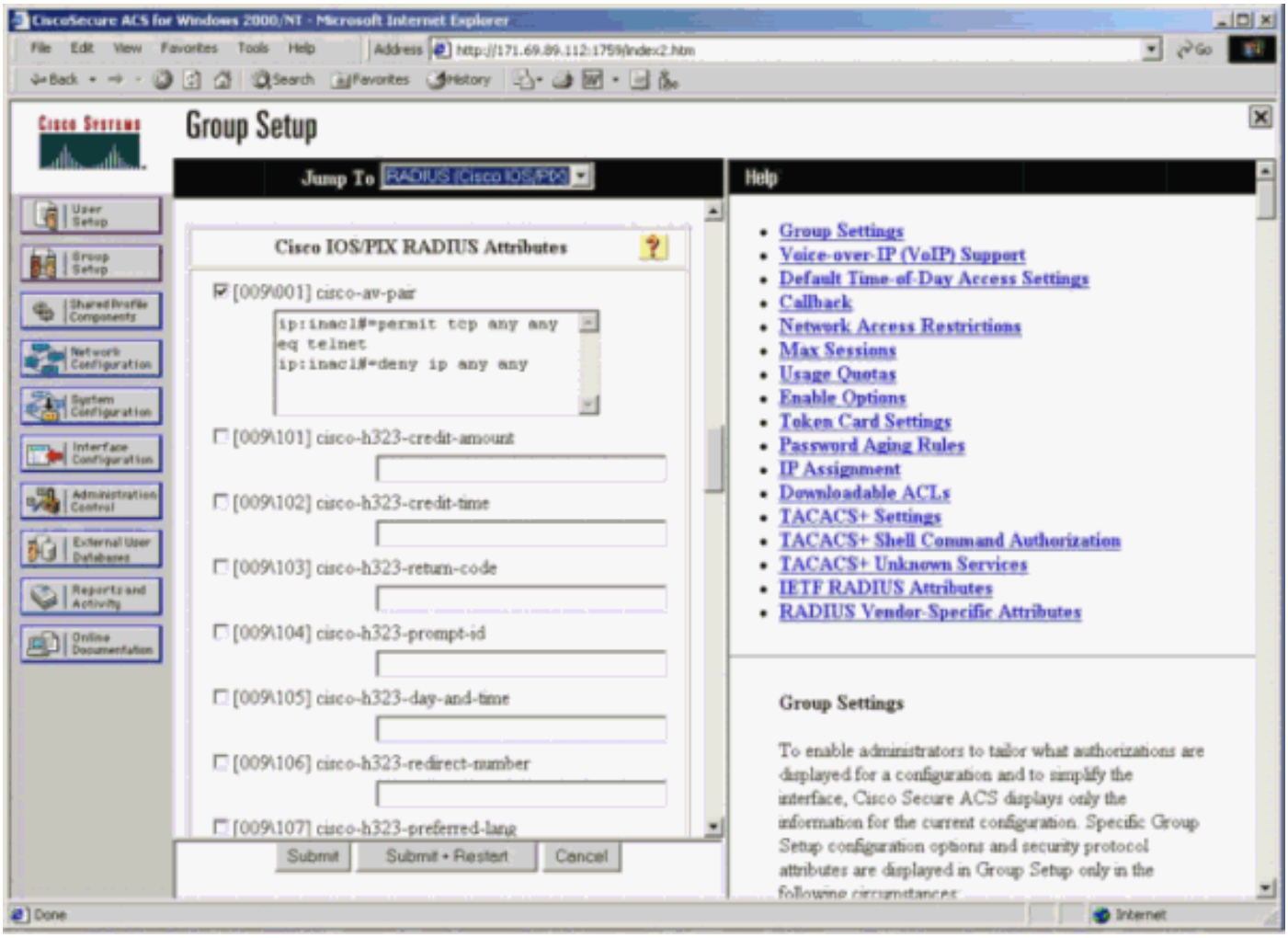
In der Softwareversion 6.2 und höher der PIX-Firewall werden Zugriffslisten auf einem Zugriffskontrollserver (ACS) definiert, die nach der Authentifizierung auf das PIX-System heruntergeladen werden können. Dies funktioniert nur mit dem RADIUS-Protokoll. Es ist nicht erforderlich, die Zugriffsliste auf dem PIX selbst zu konfigurieren. Eine Gruppenvorlage wird mehreren Benutzern zugeordnet.

In früheren Versionen wird die Zugriffsliste auf dem PIX definiert. Nach der Authentifizierung drückte der ACS den Namen der Zugriffsliste an das PIX-System weiter. Die neue Version ermöglicht es dem ACS, die Zugriffsliste direkt auf den PIX zu übertragen.

Hinweis: Wenn ein Failover auftritt, wird die Authentifizierungstabelle nicht kopiert. Benutzer werden erneut authentifiziert. Die Zugriffsliste wird erneut heruntergeladen.

ACS-Einrichtung

Klicken Sie auf **Group Setup**, und wählen Sie den **RADIUS (Cisco IOS/PIX)**-Gerätetyp aus, um ein Benutzerkonto einzurichten. Weisen Sie dem Benutzer einen Benutzernamen ("cse" in diesem Beispiel) und ein Kennwort zu. Wählen Sie in der Liste Attribute die Option zum Konfigurieren **[009\001]** ***Anbieter-Av*-Paar aus**. Definieren Sie die Zugriffsliste, wie in diesem Beispiel veranschaulicht:



PIX-Debugger: Gültige Authentifizierung und heruntergeladene Zugriffsliste

- Lässt nur Telnet zu und verweigert anderen Datenverkehr.

```
pix# 305011: Built dynamic TCP translation from inside:
  172.16.171.33/11063 to outside:172.16.171.201/1049
109001: Auth start for user '???' from 172.16.171.33/11063
   to 172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 10
109005: Authentication succeeded for user 'cse'
   from 172.16.171.33/11063
   to 172.16.171.202/23 on interface inside

302013: Built outbound TCP connection 123 for outside:
   172.16.171.202/23 (172.16.171.202/23) to inside:
   172.16.171.33/11063 (172.16.171.201/1049) (cse)
```

Ausgabe über den Befehl **show uauth**.

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list AAA-user-cse
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
```

Ausgabe über den Befehl **show access-list**.

```
pix#show access-list
access-list AAA-user-cse; 2 elements
access-list AAA-user-cse permit tcp any any eq telnet (hitcnt=1)
access-list AAA-user-cse deny ip any any (hitcnt=0)
```

- Verweigert nur Telnet und lässt anderen Datenverkehr zu.

```
pix# 305011: Built dynamic TCP translation from inside:
   172.16.171.33/11064 to outside:172.16.171.201/1050
109001: Auth start for user '???' from 172.16.171.33/11064 to
   172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 11
109005: Authentication succeeded for user 'cse'
   from 172.16.171.33/11064
   to 172.16.171.202/23 on interface inside
109015: Authorization denied (acl= AAA-user-cse) for user 'cse'
  from 172.16.171.33/11064 to 172.16.171.202/23 on interface inside
```

Ausgabe über den Befehl **show uauth**.

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list AAA-user-cse
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
```

Ausgabe über den Befehl **show access-list**.

```
pix#show access-list
access-list AAA-user-cse; 2 elements
access-list AAA-user-cse deny tcp any any eq telnet (hitcnt=1)
access-list AAA-user-cse permit ip any any (hitcnt=0)
```

Neue benutzerspezifische herunterladbare Zugriffsliste mit ACS 3.0

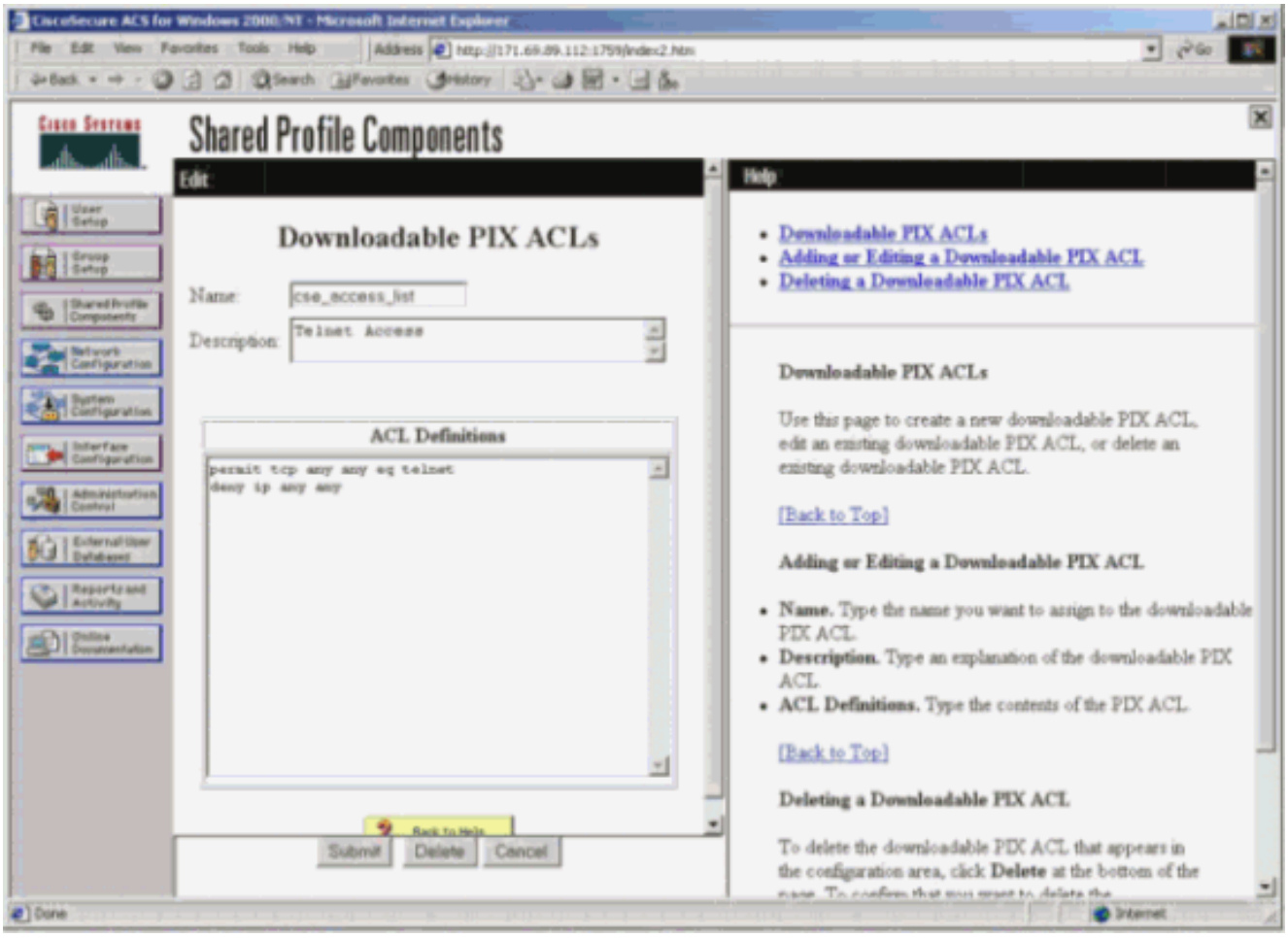
In ACS Version 3.0 kann der Benutzer mithilfe der Komponente für freigegebene Profile eine Vorlage für die Zugriffsliste erstellen und den Vorlagennamen für bestimmte Benutzer oder Gruppen definieren. Der Vorlagenname kann mit beliebig vielen Benutzern oder Gruppen verwendet werden. Dadurch müssen für jeden Benutzer keine identischen Zugriffslisten konfiguriert werden.

Hinweis: Wenn ein Failover auftritt, wird die Authentifizierung nicht auf den sekundären PIX kopiert. Beim Stateful Failover wird die Sitzung aufrechterhalten. Die neue Verbindung muss jedoch erneut authentifiziert werden, und die Zugriffsliste muss erneut heruntergeladen werden.

Verwenden freigegebener Profile

Führen Sie diese Schritte aus, wenn Sie freigegebene Profile verwenden.

1. Klicken Sie auf **Schnittstellenkonfiguration**.
2. Überprüfen Sie **die herunterladbaren ACLs** und/oder **herunterladbaren Zugriffskontrolllisten auf Gruppenebene**.
3. Klicken Sie auf **Komponenten freigegebener Profile**. Klicken Sie auf **Herunterladbare ACLs auf Benutzerebene**.
4. Definieren Sie die herunterladbaren ACLs.
5. Klicken Sie auf **Gruppeneinrichtung**. Weisen Sie unter "Herunterladbare ACLs" die PIX-Zugriffsliste der zuvor erstellten Zugriffsliste
   zu.



[PIX-Debugger: Gültige Authentifizierung und heruntergeladene Zugriffslisten mit freigegebenen Profilen]

- Lässt nur Telnet zu und verweigert anderen Datenverkehr.

```
pix# 305011: Built dynamic TCP translation from inside:
   172.16.171.33/11065 to outside:172.16.171.201/1051
109001: Auth start for user '???' from 172.16.171.33/11065 to
   172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 12
109005: Authentication succeeded for user 'cse' from
   172.16.171.33/11065 to 172.16.171.202/23 on interface inside
302013: Built outbound TCP connection 124 for outside:
   172.16.171.202/23 (172.16.171.202/23) to inside:
   172.16.171.33/11065 (172.16.171.201/1051) (cse)
```

Ausgabe über den Befehl **show uauth**.

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
pix# 111009: User 'enable_15' executed cmd: show uauth
pix#
```

Ausgabe über den Befehl **show access-list**.

```
pix#show access-list
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3; 2 elements
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3
   permit tcp any any eq telnet (hitcnt=1)
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3
```

```
   deny ip any any (hitcnt=0)
pix# 111009: User 'enable_15' executed cmd: show access-list
```

- Verweigert nur Telnet und lässt anderen Datenverkehr zu.

```
pix# 305011: Built dynamic TCP translation from inside:
   172.16.171.33/11066 to outside:172.16.171.201/1052
109001: Auth start for user '???' from 172.16.171.33/11066 to
   172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 13
109005: Authentication succeeded for user 'cse'
   from 172.16.171.33/11066
   to 172.16.171.202/23 on interface inside
109015: Authorization denied (acl=#ACSACL#-PIX-cse_access_list-3cff1dd6)
   for user 'cse' from 172.16.171.33/11066
   to 172.16.171.202/23 on interface inside
```

Ausgabe über den Befehl **show uauth**.

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
pix# 111009: User 'enable_15' executed cmd: show uauth
```

Ausgabe über den Befehl **show access-list**.

```
pix#show access-list
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6; 2 elements
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6
   deny tcp any any eq telnet (hitcnt=1)
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6
   permit ip any any (hitcnt=0)
pix# 111009: User 'enable_15' executed cmd: show access-listpix#
```

Accounting hinzufügen

PIX-Konfiguration - Hinzufügen von Accounting

TACACS (AuthInbound=tacacs)

Fügen Sie diesen Befehl hinzu.

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

Alternativ können Sie die neue Funktion in 5.2 verwenden, um festzulegen, welche Daten von Zugriffslisten erfasst werden sollen.

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

Hinweis: Die Zugriffsliste 101 ist separat definiert.

RADIUS (AuthOutbound=radius)

Fügen Sie diesen Befehl hinzu.

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

Alternativ können Sie die neue Funktion in 5.2 verwenden, um festzulegen, welche Daten von Zugriffslisten erfasst werden sollen.

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

Hinweis: Die Zugriffsliste 101 ist separat definiert.

Hinweis: Buchhaltungsdatensätze können für Verwaltungssitzungen auf dem PIX ab dem PIX 7.0-Code generiert werden.

Buchhaltungsbeispiele

- TACACS-Accounting-Beispiel für Telnet von 99.99.99.2 außerhalb von 172.18.124.114 inside (99.99.99.99).

```
172.18.124.157 pixuser PIX 99.99.99.2 start server=rtp-cherry
   time=10:36:16 date=08/23/2000 task_id=0x0 foreign_ip=99.99.99.2
   local_ip=172.18.124.114 cmd=telnet
172.18.124.157 pixuser PIX 99.99.99.2 stop server=rtp-cherry
   time=10:37:50 date=08/23/2000 task_id=0x0 foreign_ip=99.99.99.2
   local_ip=172.18.124.114
   cmd=telnet elapsed_time=94 bytes_in=61 bytes_out=254
```

- RADIUS-Accounting-Beispiel für die Verbindung von 172.18.124.114 innerhalb zu 99.99.99.2 außerhalb (Telnet) und 99.99.99.3 außerhalb (HTTP).

```
Sun Aug  6 03:59:28 2000
        Acct-Status-Type = Start
        NAS-IP-Address = 172.18.124.157
        Login-IP-Host = 172.18.124.114
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000004
        User-Name = cse
        Vendor-Specific = Source-IP=172.18.124.114
        Vendor-Specific = Source-Port=35937
        Vendor-Specific = Destination-IP=99.99.99.2
        Vendor-Specific = Destination-Port=23

Sun Aug  6 03:59:32 2000
        Acct-Status-Type = Stop
        NAS-IP-Address = 172.18.124.157
        Login-IP-Host = 172.18.124.114
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000004
         Username = cse
        Acct-Session-Time = 4
        Acct-Input-Octets = 101
        Acct-Output-Octets = 143
        Vendor-Specific = Source-IP=172.18.124.114
        Vendor-Specific = Source-Port=35937
        Vendor-Specific = Destination-IP=99.99.99.2
        Vendor-Specific = Destination-Port=23
```

```
    Sun Aug  6 04:05:02 2000
            Acct-Status-Type = Start
            NAS-IP-Address = 172.18.124.157
            Login-IP-Host = 172.18.124.114
            Login-TCP-Port = 80
            Username = cse
            Vendor-Specific = Source-IP=172.18.124.114
            Vendor-Specific = Source-Port=35949
            Vendor-Specific = Destination-IP=99.99.99.3
            Vendor-Specific = Destination-Port=80

    Sun Aug  6 04:05:02 2000
            Acct-Status-Type = Stop
            NAS-IP-Address = 172.18.124.157
            Login-IP-Host = 172.18.124.114
            Login-TCP-Port = 80
            Acct-Session-Id = 0x0000000a
            Username = cse
            Acct-Session-Time = 0
            Acct-Input-Octets = 1277
            Acct-Output-Octets = 310
            Vendor-Specific = Source-IP=172.18.124.114
            Vendor-Specific = Source-Port=35949
            Vendor-Specific = Destination-IP=99.99.99.3
            Vendor-Specific = Destination-Port=80
```

Verwendung des Befehls "exclude"

Wenn Sie in diesem Netzwerk entscheiden, dass eine bestimmte Quelle oder ein bestimmtes Ziel keine Authentifizierung, Autorisierung oder Abrechnung benötigt, geben Sie diese Befehle aus.

```
aaa authentication exclude telnet outside 172.18.124.114 255.255.255.255
  99.99.99.3 255.255.255.255 AuthInbound
aaa authorization exclude telnet outside 172.18.124.114 255.255.255.255
  99.99.99.3 255.255.255.255 AuthInbound
aaa accounting exclude telnet outside 172.18.124.114 255.255.255.255
  99.99.99.3 255.255.255.255 AuthInbound
```

Hinweis: Sie verfügen bereits über die **include**-Befehle.

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

Oder definieren Sie mit der neuen Funktion in 5.2, was Sie ausschließen möchten.

```
access-list 101 deny tcp host 99.99.99.3 host 172.18.124.114 eq telnet
access-list 101 deny tcp host 99.99.99.3 host 172.18.124.114 eq ftp
access-list 101 deny tcp host 99.99.99.3 host 172.18.124.114 eq www
access-list 101 permit tcp any any eq telnet
access-list 101 permit tcp any any eq www
access-list 101 permit tcp any any eq ftp
aaa authentication match 101 outside AuthInbound
aaa authorization match 101 outside AuthInbound
```

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

Hinweis: Wenn Sie ein Feld von der Authentifizierung ausschließen und über eine Autorisierung verfügen, müssen Sie das Feld auch von der Autorisierung ausschließen.

Max. Sitzungen und Anzeige der angemeldeten Benutzer

Einige TACACS+- und RADIUS-Server verfügen über die Funktionen "max-session" (max-session) oder "view login users" (Anzeige angemeldeter Benutzer). Die Möglichkeit, maximal Sitzungen durchzuführen oder angemeldete Benutzer zu überprüfen, hängt von den Accounting-Datensätzen ab. Wenn ein verbuchter "Start"-Datensatz generiert wird, aber kein "Stopp"-Datensatz vorhanden ist, geht der TACACS+- oder RADIUS-Server davon aus, dass die Person noch angemeldet ist (d. h. der Benutzer hat eine Sitzung über den PIX). Dies funktioniert aufgrund der Art der Verbindungen gut für Telnet- und FTP-Verbindungen. Dies funktioniert bei HTTP jedoch nicht gut. In diesem Beispiel wird eine andere Netzwerkkonfiguration verwendet, die Konzepte sind jedoch identisch.

Benutzer-Telnet über den PIX, wobei die Authentifizierung unterwegs erfolgt.

```
(pix) 109001: Auth start for user '???' from
        171.68.118.100/1200 to 9.9.9.25 /23
    (pix) 109011: Authen Session Start: user 'cse', Sid 3
    (pix) 109005: Authentication succeeded for user
        'cse' from 171.68.118.100/1200 to 9.9.9.25/23
    (pix) 302001: Built TCP connection 5 for
        faddr 9.9.9.25/23 gaddr 9.9.9.10/1200 laddr
        171.68.118.100/1200 (cse)
    (server start account) Sun Nov 8 16:31:10 1998
        rtp-pinecone.rtp.cisco.com cse
        PIX 171.68.118.100 start task_id=0x3
        foreign_ip=9.9.9.25
        local_ip=171.68.118.100 cmd=telnet
```

Da der Server einen "Start"-Datensatz, aber keinen "Stopp"-Datensatz gesehen hat, zeigt der Server zu diesem Zeitpunkt an, dass der "Telnet"-Benutzer angemeldet ist. Wenn der Benutzer eine andere Verbindung versucht, die eine Authentifizierung erfordert (möglicherweise von einem anderen PC aus), und wenn die maximale Sitzung auf dem Server für diesen Benutzer auf "1" festgelegt ist (vorausgesetzt, der Server unterstützt max-sessions), wird die Verbindung vom Server abgelehnt. Der Benutzer führt seine Telnet- oder FTP-Geschäfte auf dem Ziel-Host durch und beendet anschließend (verbringt dort zehn 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
```

Ob uauth 0 (d. h. jedes Mal authentifizieren) oder mehr (einmal und nicht wieder während des Authentifizierungszeitraums authentifizieren), ein Buchhaltungsdatensatz wird für jede Website, auf die zugegriffen wird, abgeschnitten.

HTTP funktioniert aufgrund der Art des Protokolls anders. Im Folgenden sehen Sie ein Beispiel für HTTP, bei dem der Benutzer durch das PIX von 171.68.118.100 bis 9.9.9.25 durchsucht.

```
(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
```

Der Benutzer liest die heruntergeladene Webseite. Der Startdatensatz wird um 16:35:34 und der Stoppdatensatz um 16:35:35 Uhr veröffentlicht. Dieser Download dauerte eine Sekunde (d.h. es gab weniger als eine Sekunde zwischen dem Start und dem Stopp Record). Der Benutzer ist nicht auf der Website angemeldet. Die Verbindung wird beim Lesen der Webseite nicht geöffnet. Max. Sitzungen oder Anzeigen angemeldeter Benutzer funktionieren hier nicht. Dies liegt daran, dass die Verbindungszeit (die Zeit zwischen "Built" und "Teardown") in HTTP zu kurz ist. Der Startdatensatz und der Stopp-Datensatz sind Sekundenbruchteile. Es gibt keinen "Start"-Datensatz ohne "Stopp"-Datensatz, da die Datensätze praktisch im selben Augenblick auftreten. Für jede Transaktion wird immer noch ein Start- und Stopp-Datensatz an den Server gesendet, unabhängig davon, ob die Authentifizierung auf 0 oder etwas Größeres festgelegt ist. Allerdings funktionieren maximale Sitzungen und die Ansicht angemeldeter Benutzer aufgrund der Art der HTTP-Verbindungen nicht.

Benutzeroberfläche

Benutzer auffordern anzeigen

Wenn Sie den Befehl besitzen:

auth-prompt prompt PIX515B

Benutzer, die den PIX durchlaufen, sehen diese Eingabeaufforderung.

```
PIX515B
```

Anpassen der angezeigten Nachricht

Wenn Sie über Befehle verfügen:

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

wird eine Meldung über den Authentifizierungsstatus bei fehlgeschlagener/erfolgreicher Anmeldung angezeigt.

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

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

Leerlauf- und absolute Timeouts pro Benutzer

Der PIX **Timeout**-Befehl steuert, wie oft eine erneute Authentifizierung erforderlich ist. Wenn die TACACS+-Authentifizierung/-Autorisierung aktiviert ist, wird diese auf Benutzerbasis gesteuert. Dieses Benutzerprofil ist so konfiguriert, dass es die Zeitüberschreitung steuert (dies ist auf dem Freeware-Server TACACS+, und die Zeitüberschreitungen liegen in Minuten vor).

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

Nach Authentifizierung/Autorisierung:

```
show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
user 'cse' at 99.99.99.3, authorized to:
   port 172.18.124.114/telnet
   absolute   timeout: 0:02:00
   inactivity timeout: 0:01:00
```

Nach zwei Minuten:

Absolute Zeitüberschreitung - Sitzung wird abgebrochen:

```
109012: Authen Session End: user 'cse', Sid 20, elapsed 122 seconds
302002: Teardown TCP connection 32 faddr 99.99.99.3/11025
   gaddr 99.99.99.99/23 l addr 172.18.124.114/23 duration 0:02:26
   bytes 7547 (TCP FINs)
```

Ausgehendes virtuelles HTTP

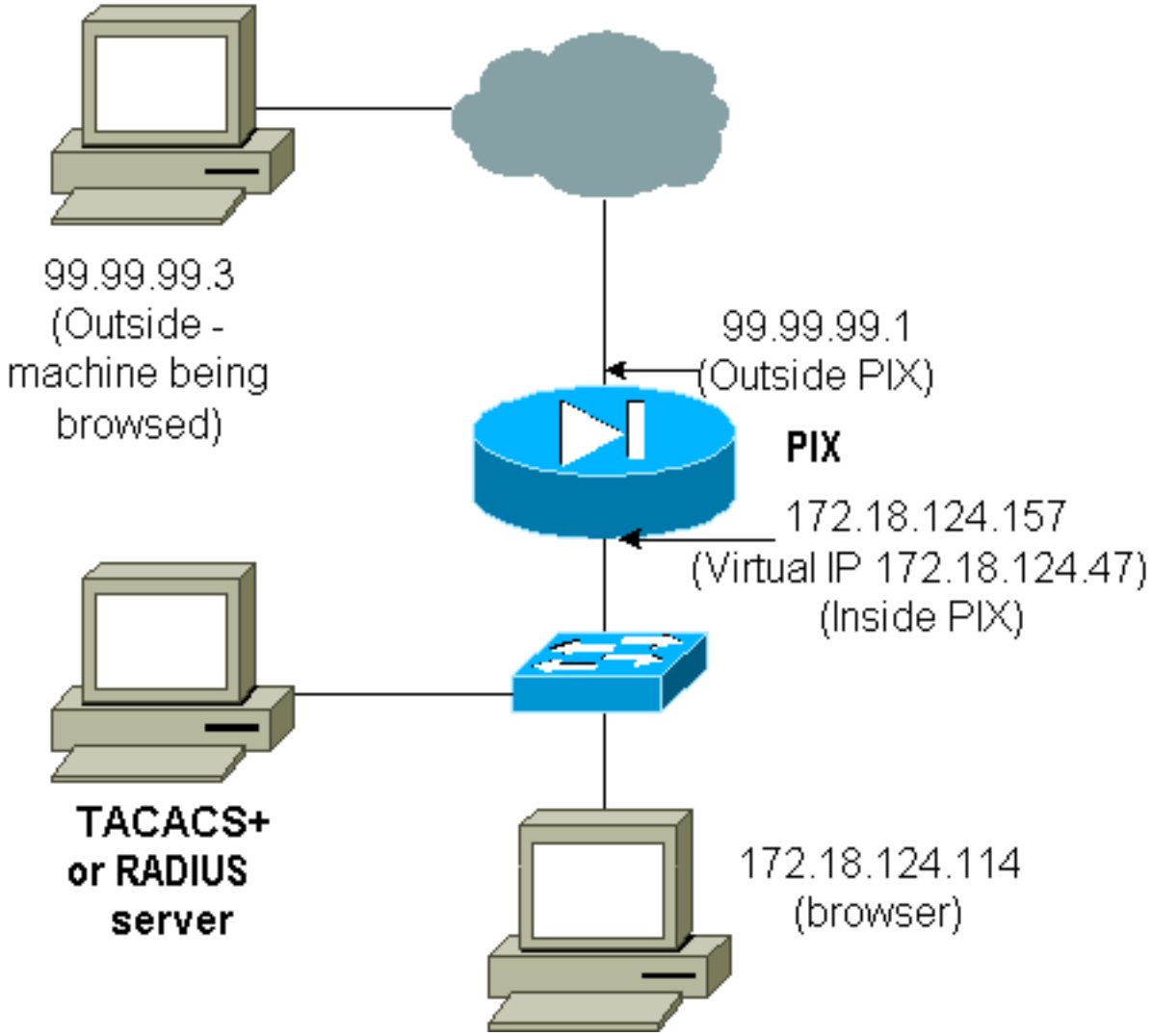
Wenn auf Sites außerhalb des PIX sowie auf dem PIX selbst eine Authentifizierung erforderlich ist, wird gelegentlich ein ungewöhnliches Browserverhalten beobachtet, da Browser den Benutzernamen und das Kennwort zwischenspeichern.

Um dies zu vermeiden, müssen Sie virtuelles HTTP implementieren, indem Sie der PIX-Konfiguration eine RFC 1918 -Adresse (eine Adresse, die im Internet nicht routbar ist, aber für das PIX-interne Netzwerk gültig und eindeutig ist) hinzufügen.

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

Wenn der Benutzer versucht, den PIX zu verlassen, ist eine Authentifizierung erforderlich. Wenn der Warn-Parameter vorhanden ist, erhält der Benutzer eine Umleitungsmeldung. Die Authentifizierung ist für die Dauer der Authentifizierung gut. Legen Sie, wie in der Dokumentation angegeben, bei virtuellem HTTP nicht die Dauer des **Timeout-**Befehls auf 0 Sekunden fest. Dadurch werden HTTP-Verbindungen zum echten Webserver verhindert.

Hinweis: Die virtuellen HTTP- und Telnet-IP-Adressen müssen in den **AAA-Authentifizierungsanweisungen** enthalten sein. In diesem Beispiel enthält die Angabe von 0.0.0.0 diese Adressen.



Fügen Sie in der PIX-Konfiguration diesen Befehl hinzu.

```
virtual http 172.18.124.47
```

Der Benutzer zeigt den Browser auf 99.99.99.3. Diese Meldung wird angezeigt.

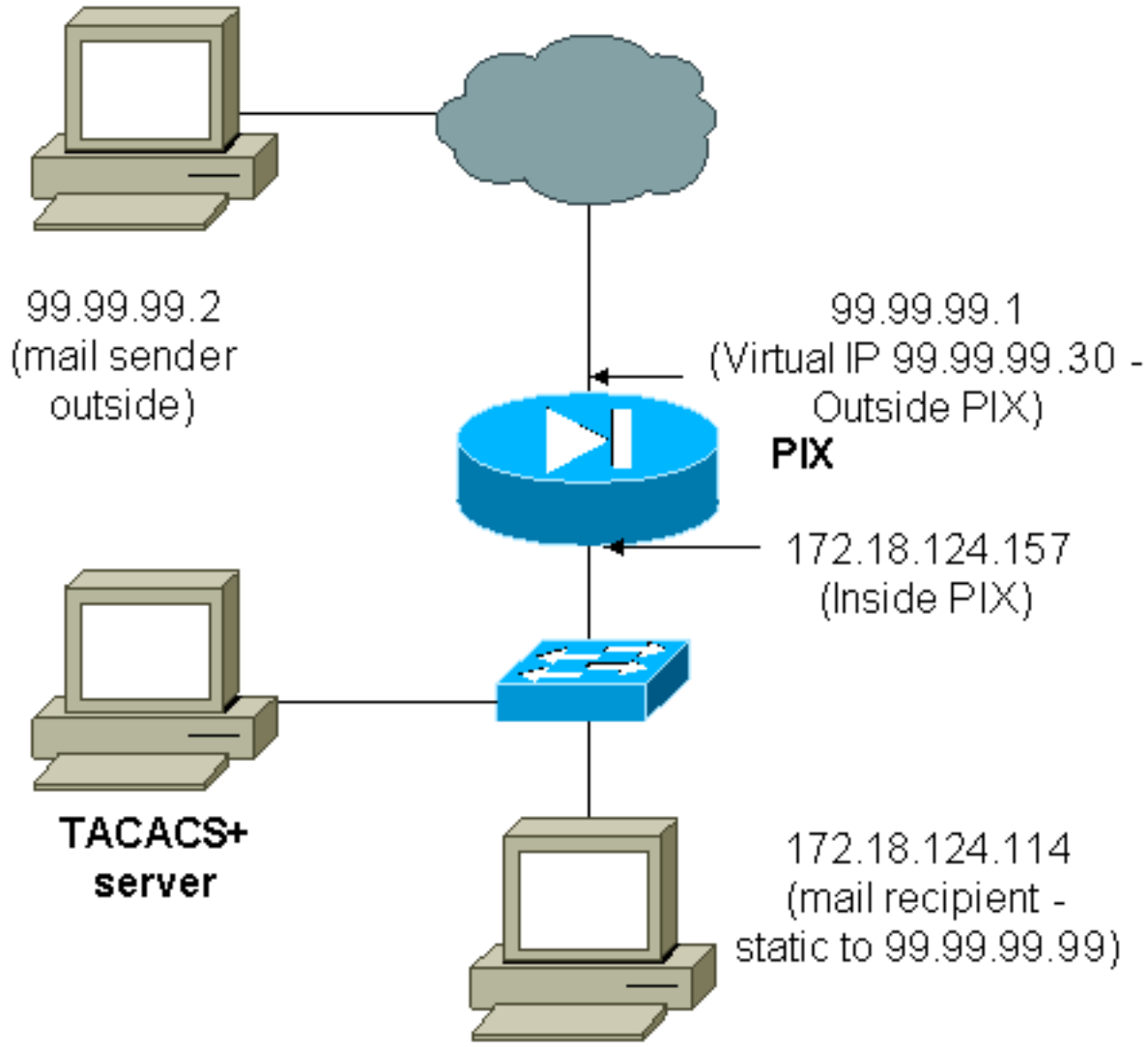
```
Enter username for PIX515B (IDXXX) at 172.18.124.47
```

Nach der Authentifizierung wird der Datenverkehr an 99.99.99.3 umgeleitet.

Virtuelles Telnet

Hinweis: Die virtuellen HTTP- und Telnet-IP-Adressen müssen in den **AAA-Authentifizierungsanweisungen** enthalten sein. In diesem Beispiel enthält die Angabe von 0.0.0.0 diese Adressen.

Virtual Telnet Inbound



Eingehende E-Mails sollten nicht authentifiziert werden, da ein Fenster nicht angezeigt wird, in dem eingehende E-Mails gesendet werden. Verwenden Sie stattdessen den Befehl **exclude**. Zur Veranschaulichung werden diese Befehle jedoch hinzugefügt.

```
aaa authentication include tcp/25 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authorization include tcp/25 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
!--- OR the new 5.2 feature allows these !--- four statements to perform the same function. !---
Note: The old and new verbiage should not be mixed.

access-list 101 permit tcp any any eq smtp
!--- The "mail" was a Telnet to port 25. access-list 101 permit tcp any any eq telnet
aaa authentication match 101 outside AuthInbound
aaa authorization match 101 outside AuthInbound
!
!--- plus ! virtual telnet 99.99.99.30
static (inside,outside) 99.99.99.30 172.18.124.30
   netmask 255.255.255.255 0 0
static (inside,outside) 99.99.99.99 172.18.124.114
   netmask 255.255.255.255 0 0
conduit permit tcp host 99.99.99.30 eq telnet any
conduit permit tcp host 99.99.99.99 eq telnet any
conduit permit tcp host 99.99.99.99 eq smtp any
```

Die Benutzer (dies ist TACACS+ Freeware):

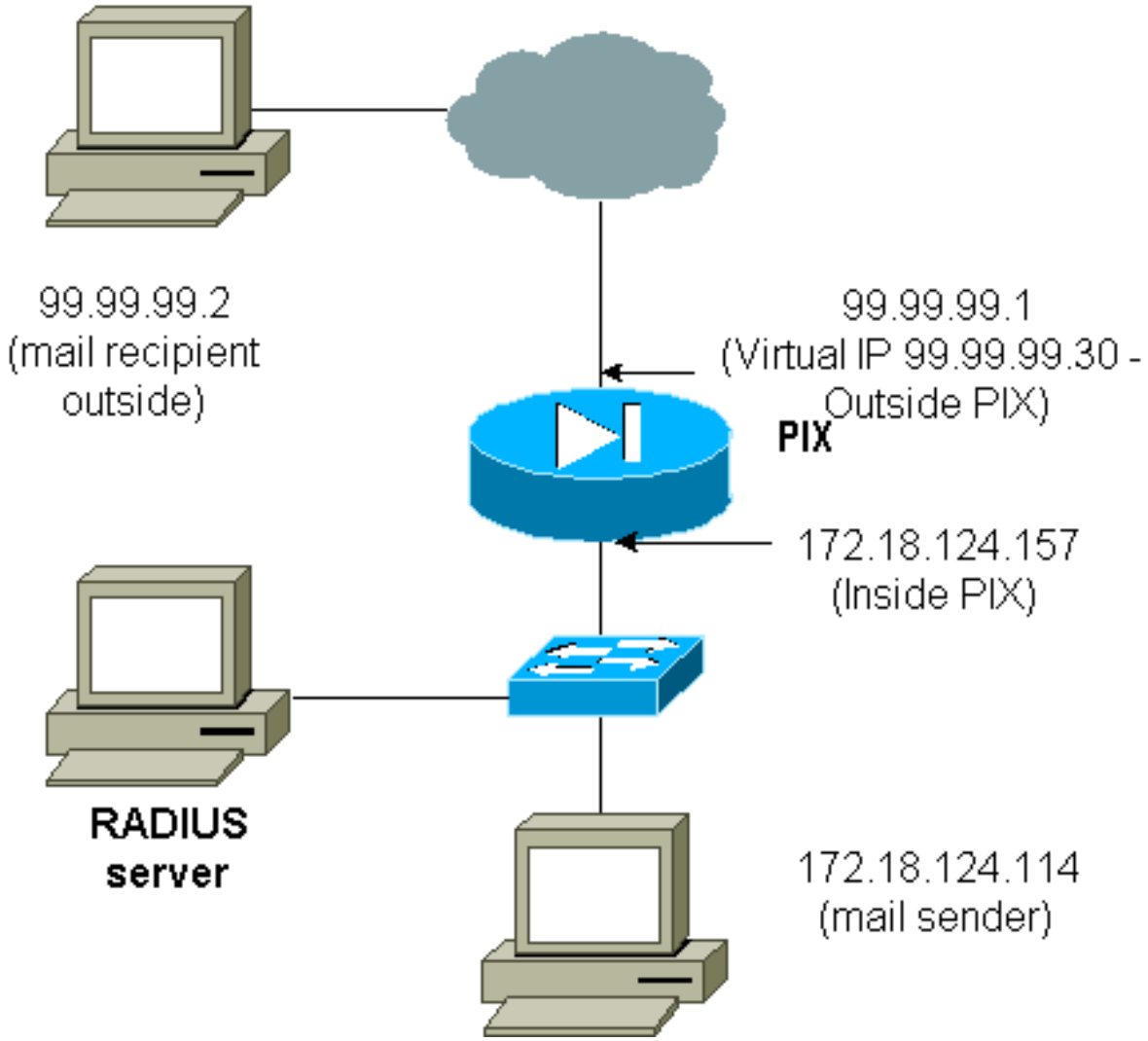
```
  user = cse {
  default service = permit
  login = cleartext "csecse"
  }


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

Wenn nur die Authentifizierung aktiviert ist, senden beide Benutzer eingehende E-Mails, nachdem sie sich bei einem Telnet an die IP-Adresse 99.99.30 authentifiziert haben. Wenn die Autorisierung aktiviert ist, geben Sie als Benutzer "cse" Telnets bis 99.99.99.30 ein und geben den TACACS+-Benutzernamen/das TACACS+-Kennwort ein. Die Telnet-Verbindung wird unterbrochen. Benutzer "cse" sendet dann E-Mail an 99.99.99.99 (172.18.124.114). Die Authentifizierung des Benutzers "pixuser" ist erfolgreich. Wenn das PIX jedoch die Autorisierungsanfrage für cmd=tcp/25 und cmd-arg=172.18.124.114 sendet, schlägt die Anforderung fehl, wie in dieser Ausgabe gezeigt.

```
109001: Auth start for user '???' from
   99.99.99.2/11036 to 172.18.124.114/23
109005: Authentication succeeded for user
   'cse' from 172.18.124.114/23 to
   99.99.99.2/11036 on interface outside

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

pixfirewall# 109001: Auth start for user '???' from
    99.99.99.2/11173 to 172.18.124.30/23
109011: Authen Session Start: user 'cse', sid 10
109005: Authentication succeeded for user 'cse' from 99.99.99.2/23
    to 172.18.124.30/11173 on interface outside
109011: Authen Session Start: user 'cse', sid 10
109007: Authorization permitted for user 'cse' from 99.99.99.2/11173
    to 172.18.124.30/23 on interface outside
109001: Auth start for user 'cse' from 99.99.99.2/11174 to
    172.18.124.114/25
109011: Authen Session Start: user 'cse', sid 10
109007: Authorization permitted for user 'cse' from 99.99.99.2/11174
    to 172.18.124.114/25 on interface outside
302001: Built inbound TCP connection 5 for faddr 99.99.99.2/11174
    gaddr 99.99.99.99/25 laddr 172.18.124.114/25 (cse)

pixfirewall# 109001: Auth start for user '???' from 99.99.99.2/11175
    to 172.18.124.30/23
109011: Authen Session Start: user 'pixuser', sid 11
```

```
109005: Authentication succeeded for user 'pixuser' from 99.99.99.2/23
    to 172.18.124.30/11175 on interface outside
109011: Authen Session Start: user 'pixuser', sid 11
109007: Authorization permitted for user 'pixuser' from 99.99.99.2/11175
    to 172.18.124.30/23 on interface outside
109001: Auth start for user 'pixuser' from 99.99.99.2/11176
    to 172.18.124.114/25
109008: Authorization denied for user 'pixuser' from 99.99.99.2/25
    to 172.18.124.114/11176 on interface outside
```

Virtuelles Telnet - Ausgehend



Eingehende E-Mails sollten nicht authentifiziert werden, da ein Fenster nicht angezeigt wird, in dem eingehende E-Mails gesendet werden. Verwenden Sie stattdessen den Befehl **exclude**. Zur Veranschaulichung werden diese Befehle jedoch hinzugefügt.

Es ist nicht empfehlenswert, ausgehende E-Mails zu authentifizieren, da kein Fenster angezeigt wird, in dem E-Mails nach außen gesendet werden können. Verwenden Sie stattdessen den Befehl **exclude**. Zur Veranschaulichung werden diese Befehle jedoch hinzugefügt.

```
aaa authentication include tcp/25 inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthOutbound
!--- OR the new 5.2 feature allows these three statements !--- to replace the previous
statements. !--- Note: Do not mix the old and new verbiage.

access-list 101 permit tcp any any eq smtp
```

```
access-list 101 permit tcp any any eq telnet
aaa authentication match 101 inside AuthOutbound
!
!--- plus ! virtual telnet 99.99.99.30
!--- The IP address on the outside of PIX is not used for anything else.
```

Um E-Mails von innen nach außen zu senden, rufen Sie eine Eingabeaufforderung auf dem Mailhost und Telnet auf 99.99.99.30. Dadurch wird das Loch geöffnet, in das die Post gehen kann. Die Post wird von 172.18.124.114 bis 99.99.99.2 gesendet:

```
   305002: Translation built for gaddr 99.99.99.99
      to laddr 172.18.124.114
   109001: Auth start for user '???' from
      172.18.124.114/32860 to 99.99.99.30/23
   109011: Authen Session Start: user 'cse', Sid 14
   109005: Authentication succeeded for user 'cse'
      from 172.18.124.114/32860 to    99.99.99.30/23
      on interface inside
   302001: Built outbound TCP connection 22 for faddr
      99.99.99.2/25 gaddr 99.99.99.99/32861
      laddr 172.18.124.114/32861 (cse)

pixfirewall#show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
user 'cse' at 172.18.124.114, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

Logout für virtuelles Telnet

Wenn Benutzer Telnet zur virtuellen Telnet-IP-Adresse wechseln, zeigt der Befehl **show uauth** die Zeit an, zu der das Loch geöffnet ist. Wenn die Benutzer verhindern möchten, dass Datenverkehr nach Abschluss der Sitzungen weitergeleitet wird (wenn die Zeit in der Warteschlange verbleibt), müssen sie erneut Telnet an die virtuelle Telnet-IP-Adresse senden. Dadurch wird die Sitzung deaktiviert. Dies wird in diesem Beispiel veranschaulicht.

Die erste Authentifizierung

```
 109001: Auth start for user '???'
    from 172.18.124.114/32862 to 99.99.99.30/23
 109011: Authen Session Start: user 'cse', Sid 15
 109005: Authentication succeeded for user
    'cse' from 172.18.124.114/32862 to
    99.99.99.30/23 on interface inside
```

Nach der ersten Authentifizierung

```
pixfirewall#show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
user 'cse' at 172.18.124.114, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

Die zweite Authentifizierung

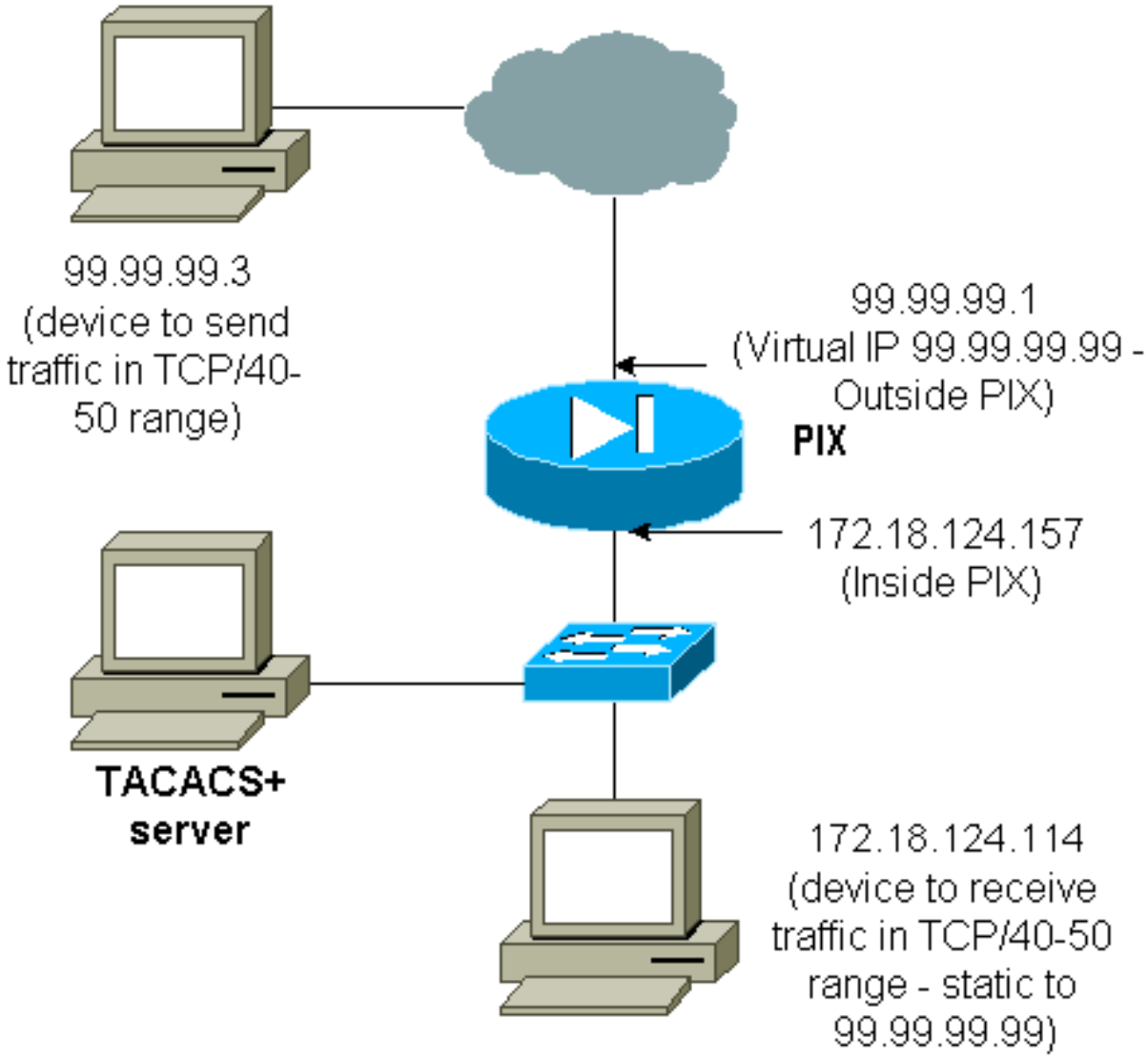
```
pixfirewall# 109001: Auth start for user 'cse'
   from 172.18.124.114/32863 to    99.99.99.30/23
109005: Authentication succeeded for user 'cse'
   from 172.18.124.114/32863 to    99.99.99.30/23
   on interface inside
```

Nach der zweiten Authentifizierung

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

Port-Autorisierung

Netzwerkdiagramm



Die Autorisierung ist für Port-Bereiche zulässig. Wenn auf dem PIX virtuelles Telnet konfiguriert und die Autorisierung für einen Portbereich konfiguriert ist, öffnet der Benutzer das Loch mit virtuellem Telnet. Wenn dann die Autorisierung für einen Port-Bereich aktiviert ist und der Datenverkehr in diesem Bereich auf den PIX trifft, sendet der PIX den Befehl zur Autorisierung an den TACACS+-Server. Dieses Beispiel zeigt die eingehende Autorisierung für einen Port-Bereich.

```
aaa authentication include any outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authorization include tcp/40-50 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
!--- OR the new 5.2 feature allows these three statements !--- to perform the same function as
the previous two statements. !--- Note: The old and new verbiage should not be mixed.

access-list 116 permit tcp any any range 40 50
aaa authentication match 116 outside AuthInbound
aaa authorization match 116 outside AuthInbound
!
!--- plus ! static (inside,outside) 99.99.99.99 172.18.124.114
netmask 255.255.255.255 0 0
conduit permit tcp any any
virtual telnet 99.99.99.99
```

TACACS+-Serverkonfigurationsbeispiel (Freeware):

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

Der Benutzer muss zuerst Telnet mit der virtuellen IP-Adresse 99.99.99.99 verbinden. Wenn ein Benutzer nach der Authentifizierung versucht, den TCP-Datenverkehr im Bereich von 40-50 über PIX auf 99.99.99.99 (172.18.124.114) zu übertragen, wird cmd=tcp/40-50 mit cmd-arg=17 an den TACACS+-Server gesendet. 2.18.124.114, wie hier dargestellt:

```
109001: Auth start for user '???' from 99.99.99.3/11075
    to 172.18.124.114/23
109011: Authen Session Start: user 'cse', Sid 13
109005: Authentication succeeded for user 'cse'
    from 172.18.124.114/23 to 99.99.99.3/11075
    on interface outside
109001: Auth start for user 'cse' from 99.99.99.3/11077
    to 172.18.124.114/49
109011: Authen Session Start: user 'cse', Sid 13
109007: Authorization permitted for user 'cse'
    from 99.99.99.3/11077 to 172.18.124.114/49
    on interface outside
```

AAA-Abrechnung für Datenverkehr außer HTTP, FTP und Telnet

Nachdem Sie sichergestellt haben, dass virtuelles Telnet den TCP/40-50-Datenverkehr zum Host im Netzwerk zulässt, fügen Sie mit diesen Befehlen die entsprechende Abrechnung für diesen Datenverkehr hinzu.

```
aaa accounting include any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
!--- OR the new 5.2 feature allows these !--- two statements to replace the previous statement.
!--- Note: Do not mix the old and new verbiage.

aaa accounting match 116 outside AuthInbound
```

```
access-list 116 permit ip any any
```

Beispiel für TACACS+-Accounting-Datensätze

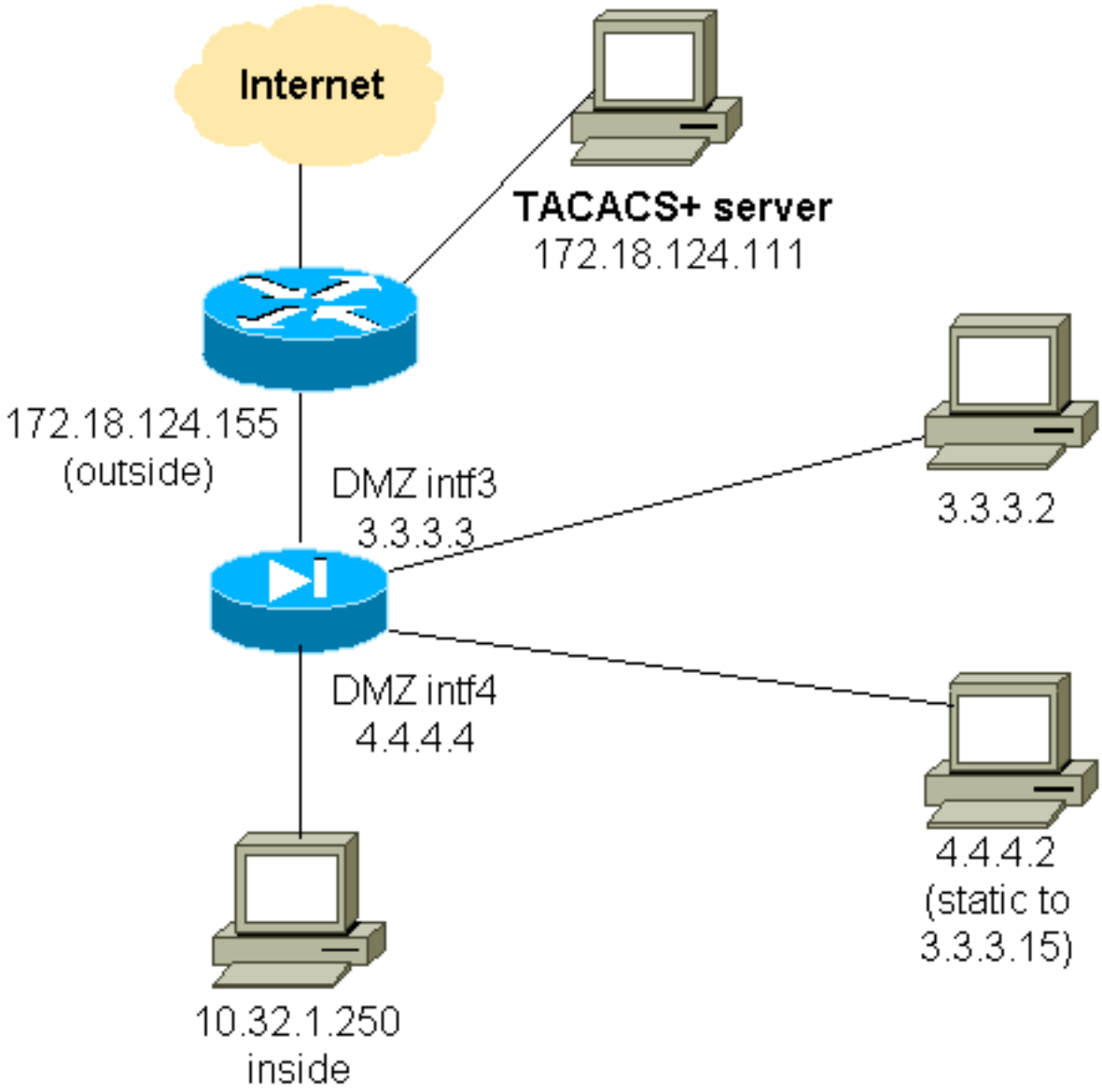
```
Thu Aug 24 08:06:09 2000 172.18.124.157 cse PIX 99.99.99.3
start task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
cmd=tcp/40-50
Thu Aug 24 08:06:17 2000 172.18.124.157 cse PIX 99.99.99.3
stop task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
cmd=tcp/40-50 elapsed_time=8 bytes_in=80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

Authentifizierung auf der DMZ

Um Benutzer zu authentifizieren, die von einer DMZ-Schnittstelle zu einer anderen wechseln, weisen Sie den PIX an, den Datenverkehr für die benannten Schnittstellen zu authentifizieren. Auf dem PIX sieht die Anordnung folgendermaßen aus:

```
least secure
PIX outside (security0) = 172.18.124.155
pix/intf3 (DMZ - security15) = 3.3.3.3 & device 3.3.3.2
pix/intf4 (DMZ - security20) = 4.4.4.4 & device 4.4.4.2 (static to 3.3.3.15)
PIX inside (security100) = 10.32.1.250
most secure
```

Netzwerkdiagramm



Partielle PIX-Konfiguration

Authentifizierung des Telnet-Datenverkehrs zwischen pix/intf3 und pix/intf4, wie hier gezeigt.

Partielle PIX-Konfiguration

```
  nameif ethernet0 outside security0
  nameif ethernet1 inside security100
  (nameif ethernet2 pix/intf2 security10)
  nameif ethernet3 pix/intf3 security15
  nameif ethernet4 pix/intf4 security20
  (nameif ethernet5 pix/intf5 security25)
  interface ethernet0 auto
  interface ethernet1 auto
  (interface ethernet2 auto shutdown)
  interface ethernet3 auto
  interface ethernet4 auto
  (interface ethernet5 auto shutdown)
  ip address outside 172.18.124.155 255.255.255.0
  ip address inside 10.32.1.250 255.255.255.0
  ip address pix/intf3 3.3.3.3 255.255.255.0
  ip address pix/intf4 4.4.4.4 255.255.255.0
  static (pix/intf4,pix/intf3) 3.3.3.15 4.4.4.2 netmask
255.255.255.255 0 0
```

```
  conduit permit tcp host 3.3.3.15 host 3.3.3.2
  aaa-server xway protocol tacacs+
  aaa-server xway (outside) host 172.18.124.111 timeout
5
  aaa authentication include telnet pix/intf4 4.4.4.0
255.255.255.0 3.3.3.0
  255.255.255.0 3.3.3.0 255.255.255.0 xway
  aaa authentication include telnet pix/intf3 4.4.4.0
255.255.255.0 3.3.3.0
  255.255.255.0 3.3.3.0 255.255.255.0 xway
!--- OR the new 5.2 feature allows these four statements
!--- to replace the previous two statements. !--- Note:
Do not mix the old and new verbiage.

  access-list 103 permit tcp 3.3.3.0 255.255.255.0
4.4.4.0 255.255.255.0 eq telnet
  access-list 104 permit tcp 4.4.4.0 255.255.255.0
3.3.3.0 255.255.255.0 eq telnet
  aaa authentication match 103 pix/intf3 xway
  aaa authentication match 104 pix/intf4 xway
```

Informationen, die beim Öffnen eines TAC-Tickets gesammelt werden müssen

Wenn Sie nach den oben beschriebenen Schritten zur Fehlerbehebung weiterhin Hilfe benötigen und ein Ticket beim Cisco TAC erstellen möchten, geben Sie zur Fehlerbehebung für Ihre PIX-Firewall diese Informationen an.

- Problembeschreibung und relevante Topologiedetails
- Fehlerbehebung vor dem Öffnen des Gehäuses
- Ausgabe des Befehls **show tech-support**
- Ausgabe des Befehls **show log**, nachdem Sie mit dem Befehl **logging buffered debugging** ausgeführt haben, oder Konsolenaufzeichnungen, die das Problem veranschaulichen (falls verfügbar)

Hängen Sie die erfassten Daten im unverzippten Textformat (.txt) an Ihren Fall an. Fügen Sie Informationen zu Ihrem Fall hinzu, indem Sie diese mithilfe des Case Query Tool hochladen (nur registrierte Kunden). Wenn Sie nicht auf das Tool für die Fallabfrage zugreifen können, senden Sie die Informationen in einem E-Mail-Anhang an attach@cisco.com mit Ihrer Ticketnummer in der Betreffzeile Ihrer Nachricht.

Zugehörige Informationen

- Cisco PIX Firewall-Software
- Cisco Secure PIX Firewall - Befehlsreferenzen
- Problemhinweise zu Sicherheitsprodukten (einschließlich PIX)
- Anforderungen für Kommentare (RFCs)
- Cisco Secure Access Control Server für Windows

- Cisco Secure Access Control Server für UNIX
- Terminal Access Controller Access Control System (TACACS+)
- RADIUS (Remote Authentication Dial-In User Service)
- Technischer Support und Dokumentation - Cisco Systems