Beispielkonfigurationen für PIX, TACACS+ und RADIUS: 4,2 x

Inhalt

Einführung

Die RADIUS- und TACACS+-Authentifizierung kann für FTP-, Telnet- und HTTP-Verbindungen erfolgen. Die TACACS+-Autorisierung wird unterstützt. Die RADIUS-Autorisierung ist nicht aktiviert.

Die Syntax für die Authentifizierung wurde in PIX Software 4.2.2 leicht geändert. Dieses Dokument verwendet die Syntax für Softwareversionen 4.2.2.

Voraussetzungen

Anforderungen

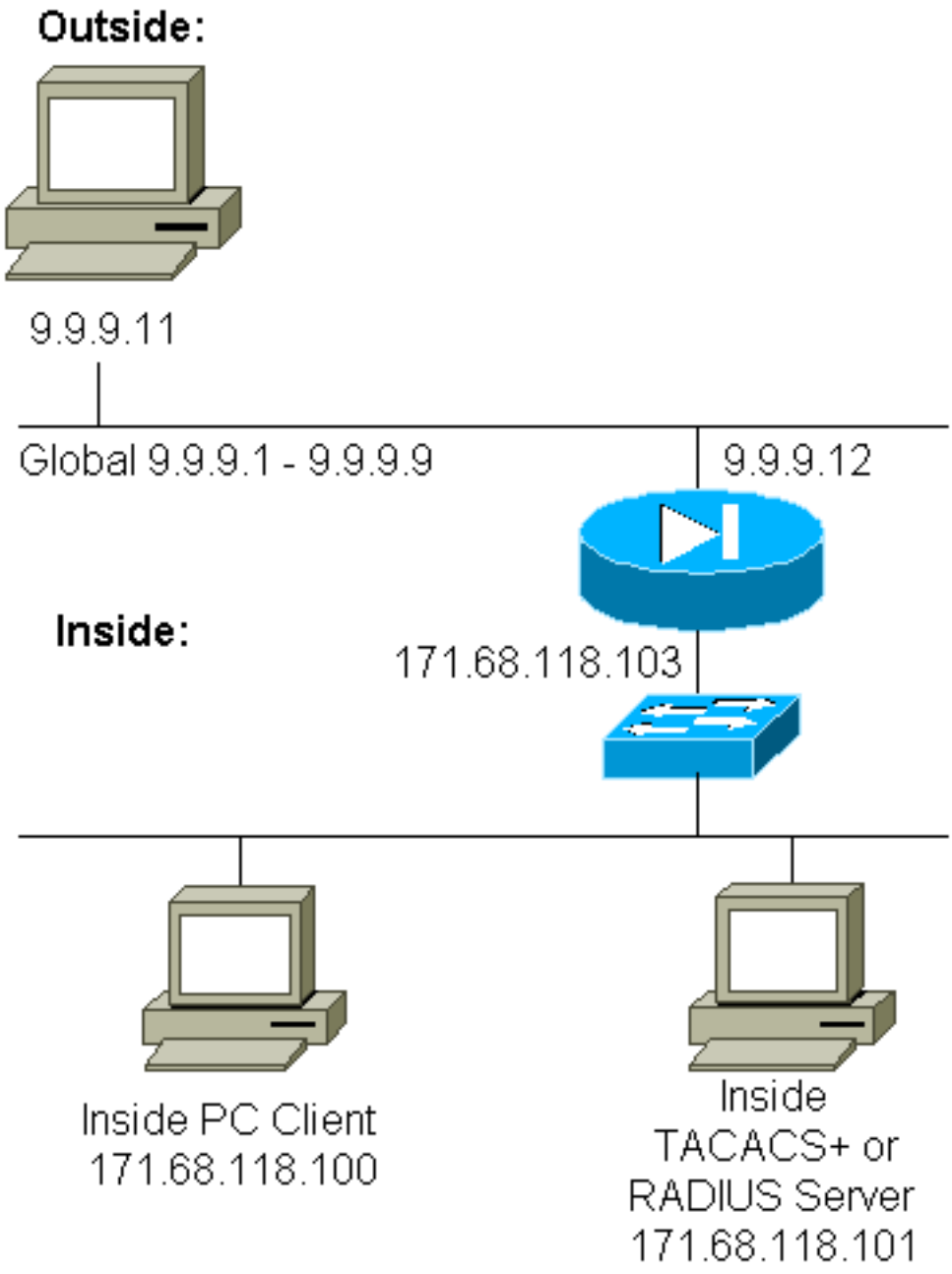
Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



PIX-Konfiguration

```
pix2# write terminal
Building configuration
: Saved
:
PIX Version 4.2(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd OnTrBUG1Tp0edmkr 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 with: 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]
```

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Authentifizierung und Autorisierung

- Die Authentifizierung ist *der* Benutzer.
- Autorisierung ist *das, was* der Benutzer tun kann.
- Die Authentifizierung *ist* ohne Autorisierung gültig.
- Die Autorisierung *ist* ohne Authentifizierung *nicht* gültig.

Angenommen, Sie haben 100 Benutzer im Netzwerk, und nur sechs dieser Benutzer möchten FTP, Telnet oder HTTP außerhalb des Netzwerks ausführen können. Weisen Sie den PIX an, ausgehenden Datenverkehr zu authentifizieren, und geben Sie alle sechs Benutzer-IDs auf dem TACACS+/RADIUS-Sicherheitsserver an. Mit einer einfachen Authentifizierung können diese sechs Benutzer mit Benutzername und Kennwort authentifiziert werden. Anschließend können sie die Authentifizierung beenden. Die anderen vierundneunzig Benutzer können nicht ausgehen. Das PIX fordert Benutzer zur Eingabe von Benutzername/Kennwort auf und übergibt ihren Benutzernamen und ihr Kennwort an den TACACS+/RADIUS-Sicherheitsserver. Je nach Antwort wird die Verbindung außerdem geöffnet oder verweigert. Diese sechs Benutzer können FTP, Telnet oder HTTP verwenden.

Gehen Sie jedoch davon aus, dass einer dieser drei Benutzer, "Terry", nicht vertrauenswürdig ist. Sie möchten Terry FTP erlauben, aber nicht HTTP oder Telnet nach außen. Das bedeutet, Sie müssen die Autorisierung hinzufügen. Das bedeutet, dass Benutzer nicht nur authentifizieren können, sondern auch, was sie tun können. Wenn Sie dem PIX eine Autorisierung hinzufügen, sendet das PIX zunächst Terrys Benutzernamen und Kennwort an den Sicherheitsserver und sendet dann eine Autorisierungsanfrage, die dem Sicherheitsserver mitteilt, welchen "Befehl" Terry zu tun versucht. Wenn der Server korrekt eingerichtet ist, kann Terry "FTP 1.2.3.4" verwenden, aber es wird ihm die Möglichkeit verweigert, "HTTP" oder "Telnet" überall zu verwenden.

Was der Benutzer mit Authentifizierung/Autorisierung auf

Wenn Sie versuchen, von innen nach außen (oder umgekehrt) mit Authentifizierung/Autorisierung auf:

- **Telnet** - Der Benutzer sieht eine Eingabeaufforderung mit dem Benutzernamen, gefolgt von einer 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 den Benutzernamen. Der Benutzer muss "local_username@remote_username" als Benutzernamen und "local_password@remote_password" als Kennwort eingeben. Der PIX sendet den "local_username" und den "local_password" an den lokalen Sicherheitsserver, und wenn die Authentifizierung (und Autorisierung) auf dem PIX/Server erfolgreich ist, werden der "remote_username" und das "remote_password" darüber hinaus an den FTP-Zielserver übergeben.
- **HTTP** - Im Browser wird ein Fenster angezeigt, in dem ein Benutzername und ein 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 synchronisieren sollte, 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. Diese wird dann an den Authentifizierungsserver weitergeleitet. PIX-Syslog und/oder Server-Debug zeigen dieses Phänomen. Wenn Telnet und FTP normal arbeiten, HTTP-Verbindungen jedoch nicht, dann ist dies der Grund.

Für alle Szenarien verwendete Serverkonfigurationen

Wenn in den Konfigurationsbeispielen für den TACACS+-Server nur die Authentifizierung aktiviert ist, funktionieren Benutzer "all", "telnetonly", "httponly" und "ftponly" alle. In den RADIUS-Serverkonfigurationsbeispielen funktioniert "all" (Alle) des Benutzers.

Wenn dem PIX eine Autorisierung hinzugefügt wird, sendet PIX neben dem Senden von Benutzername und Kennwort an den TACACS+-Authentifizierungsserver Befehle (Telnet, HTTP oder FTP) an den TACACS+-Server. Der TACACS+-Server überprüft dann, ob dieser Benutzer für diesen Befehl autorisiert ist.

In einem späteren Beispiel gibt der Benutzer unter 171.68.118.100 den Befehl **telnet 9.9.9.11 aus**. Wenn dies an der PIX-Schnittstelle eingeht, übergibt der PIX den Benutzernamen, das Kennwort und den Befehl zur Verarbeitung an den TACACS+-Server.

Mit der Autorisierung auf kann zusätzlich zur Authentifizierung der Benutzer "telnetonly" Telnet-Operationen über den PIX ausführen. Die Benutzer "httponly" und "ftponly" können jedoch keine Telnet-Vorgänge über den PIX ausführen.

(Auch hier wird aufgrund der Art der Protokollspezifikation keine Autorisierung mit RADIUS unterstützt).

Cisco Secure UNIX TACACS+-Serverkonfiguration

Cisco Secure 2.x

- Benutzerstatistiken werden hier angezeigt.
- Fügen Sie die PIX-IP-Adresse oder den vollqualifizierten Domänennamen und -schlüssel

CSU.cfg hinzu.

```
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 .*
}
}
}
```

Cisco Secure UNIX RADIUS-Serverkonfiguration

Verwenden Sie die erweiterte grafische Benutzeroberfläche (GUI), um die PIX-IP-Adresse und den Schlüssel zur Liste der Netzwerkzugriffsserver (NAS) hinzuzufügen. Der Benutzer stanza wird wie folgt angezeigt:

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

Cisco Secure NT 2.x RADIUS

Der Abschnitt "Beispielkonfigurationen" in der Online- und Webdokumentation zu CiscoSecure 2.1 beschreibt die Einrichtung. Attribut 6 (Servicetyp) lautet Login (Anmeldung) oder Administrative (Verwaltung).

Fügen Sie die IP-Adresse des PIX im Abschnitt "NAS Configuration" (NAS-Konfiguration) mithilfe der GUI hinzu.

EasyACS TACACS+

Die EasyACS-Dokumentation enthält Setup-Informationen.

1. Klicken Sie im Gruppenbereich auf **Shell Exec** (um Exec-Berechtigungen zu gewähren).
2. Um dem PIX die Autorisierung hinzuzufügen, klicken Sie unten in der Gruppeneinrichtung

auf **Nicht übereinstimmende IOS-Befehle verweigern**.
3. Wählen Sie **Add/Edit** für jeden Befehl aus, den Sie zulassen möchten (z. B. Telnet).
4. Wenn Sie Telnet für bestimmte Standorte zulassen möchten, geben Sie die IP(s) im Abschnitt Argument ein. Um Telnet allen Standorten zu ermöglichen, klicken Sie auf **Alle nicht aufgeführten Argumente zulassen**.
5. Klicken Sie auf **Bearbeitungsbefehl beenden**.
6. Führen Sie die Schritte 1 bis 5 für jeden der zulässigen Befehle aus (z. B. Telnet, HTTP und/oder FTP).
7. Fügen Sie die IP-Adresse des PIX im Abschnitt "NAS Configuration" (NAS-Konfiguration) mithilfe der GUI hinzu.

Cisco Secure NT 2.x TACACS+

Die Cisco Secure 2.x-Dokumentation enthält Setup-Informationen.

1. Klicken Sie im Gruppenbereich auf **Shell Exec** (um Exec-Berechtigungen zu gewähren).
2. Um dem PIX die Autorisierung hinzuzufügen, klicken Sie unten in der Gruppeneinrichtung auf **Nicht übereinstimmende IOS-Befehle verweigern**.
3. Aktivieren Sie das Kontrollkästchen **Befehl** unten, und geben Sie den Befehl ein, den Sie zulassen möchten (z. B. Telnet).
4. Wenn Sie Telnet für bestimmte Standorte zulassen möchten, geben Sie die IP im Argumentabschnitt ein (z. B. "permit 1.2.3.4"). Um Telnet allen Standorten zu ermöglichen, klicken Sie auf **Nicht aufgeführte Argumente zulassen**.
5. Klicken Sie auf **Senden**.
6. Führen Sie die Schritte 1 bis 5 für jeden der zulässigen Befehle aus (z. B. Telnet, FTP und/oder HTTP).
7. Fügen Sie die IP-Adresse des PIX im Abschnitt "NAS Configuration" (NAS-Konfiguration) mithilfe der GUI hinzu.

Konfiguration des Livingston RADIUS-Servers

Fügen Sie die PIX-IP-Adresse und den Schlüssel zur Client-Datei hinzu.

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

RADIUS-Serverkonfiguration vermerken

Fügen Sie die PIX-IP-Adresse und den Schlüssel zur Client-Datei hinzu.

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

TACACS+ Freeware Server-Konfiguration

```
# 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 .*
}
}
```

Debugschritte

- Stellen Sie sicher, dass die PIX-Konfigurationen funktionieren, bevor Sie AAA (Authentication, Authorization, Accounting) hinzufügen.Wenn Sie Datenverkehr nicht vor der Einrichtung von AAA weiterleiten können, können Sie dies später nicht mehr tun.
- Aktivieren Sie die Protokollierung in PIX:Der Befehl **zum Debuggen der Protokollierungskonsole** sollte auf einem stark ausgelasteten System nicht verwendet werden.Der Befehl **logging buffered debugging** kann verwendet werden. Die Ausgabe der Befehle **zur Anzeigeprotokollierung** oder **Protokollierung** kann dann an einen Syslog-Server gesendet und geprüft werden.
- Stellen Sie sicher, dass das Debuggen für die TACACS+- oder RADIUS-Server aktiviert ist. Diese Option steht allen Servern zur Verfügung.

Authentifizierungs-Debug-Beispiele aus PIX

PIX Debug - Gute Authentifizierung - RADIUS

Dies ist ein Beispiel für ein PIX-Debuggen mit guter Authentifizierung:

```
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 - Schlechte Authentifizierung (Benutzername oder Kennwort) - RADIUS

Dies ist ein Beispiel für ein PIX-Debuggen mit schlechter Authentifizierung (Benutzername oder Kennwort). Der Benutzer sieht vier Benutzername/Kennwort-Sets. Der "Fehler: Die maximale

Anzahl von Wiederholungen überschritten"-Meldung wird angezeigt.

Hinweis: Wenn es sich um einen FTP-Versuch handelt, ist nur ein Versuch zulässig. Für HTTP sind unbegrenzte Wiederholungen zulässig.

```
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

Dies ist ein Beispiel für ein PIX-Debuggen mit ausgefallenem Server. Der Benutzer sieht den Benutzernamen einmal. Der Server "stürzt" dann und fragt nach einem Kennwort (dreimal).

```
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 - Gute Authentifizierung - TACACS+

Dies ist ein Beispiel für ein PIX-Debuggen mit guter Authentifizierung:

```
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 - Schlechte Authentifizierung (Benutzername oder Kennwort) - TACACS+

Dies ist ein Beispiel für ein PIX-Debuggen mit schlechter Authentifizierung (Benutzername oder Kennwort). Der Benutzer sieht vier Benutzername/Kennwort-Sets. Der "Fehler: Die maximale Anzahl von Wiederholungen überschritten"-Meldung wird angezeigt.

Hinweis: Wenn es sich um einen FTP-Versuch handelt, ist nur ein Versuch zulässig. Für HTTP sind unbegrenzte Wiederholungen zulässig.

```
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+

Dies ist ein Beispiel für ein PIX-Debuggen mit ausgefallenem Server. Der Benutzer sieht den Benutzernamen einmal. Sofort wird die Meldung "Fehler: Es wird die maximal zulässige Anzahl von Versuchen überschritten" angezeigt.

```
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
```

Autorisierung hinzufügen

Da die Autorisierung ohne Authentifizierung nicht gültig ist, ist die Autorisierung für dieselbe Quelle und dasselbe Ziel erforderlich:

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

Wenn alle drei ausgehenden Dienste ursprünglich authentifiziert wurden:

```
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
```

Debug-Beispiele für Authentifizierung und Autorisierung aus PIX

PIX Debug - Gute Authentifizierung und Autorisierung - TACACS+

Dies ist ein Beispiel für ein PIX-Debuggen mit guter Authentifizierung und Autorisierung:

```
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 - Gute Authentifizierung, aber Fehler bei der Autorisierung - TACACS+

Dies ist ein Beispiel für ein PIX-Debuggen mit guter Authentifizierung, aber Fehler bei der Autorisierung:

```
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-Debugging - Fehlerhafte Authentifizierung, Autorisierung nicht versucht - TACACS+

Dies ist ein Beispiel für ein PIX-Debuggen mit Authentifizierung und Autorisierung, aber die Autorisierung wurde nicht versucht, da eine falsche Authentifizierung (Benutzername oder Kennwort) vorliegt. Der Benutzer sieht vier Benutzername/Kennwort-Sets. Der "Fehler: maximale Anzahl von Wiederholungen überschritten." Meldung wird angezeigt

Hinweis: Wenn es sich um einen FTP-Versuch handelt, ist nur ein Versuch zulässig. Für HTTP sind unbegrenzte Wiederholungen zulässig.

```
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 - Authentifizierung/Autorisierung, Server Down - TACACS+

Dies ist ein Beispiel für ein PIX-Debuggen mit Authentifizierung und Autorisierung. Der Server ist ausgefallen. Der Benutzer sieht den Benutzernamen einmal. Sofort wird die Meldung "Fehler: Die maximale Anzahl der Versuche wurde überschritten." wird angezeigt.

```
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 hinzufügen

TACACS+

```
aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0: tacacs+
```

Debug sieht gleich aus, ob die Accounting aktiviert oder deaktiviert ist. Zum Zeitpunkt des Built-Projekts wird jedoch ein "Start"-Accounting-Datensatz gesendet. Zum Zeitpunkt der "Entfernung" wird außerdem ein "Stopp"-Buchführungsdatensatz gesendet:

```
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
```

Die TACACS+-Accounting-Datensätze sehen wie diese aus (diese stammen von CiscoSecure UNIX; Die Datensätze in Cisco Secure Windows können durch Kommas getrennt sein):

```
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
```

Die Felder sind wie folgt aufgeteilt:

```
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

```
aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 radius
```

Debug sieht gleich aus, ob die Accounting aktiviert oder deaktiviert ist. Zum Zeitpunkt des Built-Projekts wird jedoch ein "Start"-Accounting-Datensatz gesendet. Zum Zeitpunkt der "Entfernung" wird außerdem ein "Stopp"-Buchführungsdatensatz gesendet:

```
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-Datensätze sehen wie diese aus (diese stammen von Cisco Secure UNIX; die in Cisco Secure Windows durch Kommata getrennt sind):

```
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
```
Die Felder sind wie folgt aufgeteilt:

```
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. Sitzungen und Anzeigen angemeldeter Benutzer

Einige TACACS- und RADIUS-Server verfügen über die Funktionen "max-session" (max. Sitzung) oder "view login users" (Benutzeranmeldung). 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. eine Sitzung durch den PIX). Dies funktioniert aufgrund der Art der Verbindungen gut für Telnet- und FTP-Verbindungen. Als Beispiel:

Die Telnet-Benutzer von 171.68.118.100 bis 9.9.9.25 über das PIX authentifizieren sich auf dem 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
```
Da der Server einen "Start"-Datensatz, aber keinen "Stopp"-Datensatz gesehen hat (zu diesem Zeitpunkt), zeigt der Server 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 für diesen Benutzer die maximale Anzahl von Sitzungen auf "1" gesetzt ist, wird die Verbindung vom Server abgelehnt.

Der Benutzer geht auf dem Ziel-Host Geschäfte, dann beendet (verbringt dort 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
```
Legt fest, ob uauth 0 (d. h. jedes Mal authentifizieren) oder mehr (einmal und nicht wieder authentifizieren während der Laufzeit), wird für jede Website, auf die zugegriffen wird, eine Kürzung der Buchführungsdaten vorgenommen.

Allerdings funktioniert das HTTP aufgrund der Art des Protokolls anders. Dies ist ein Beispiel:

Der Benutzer durchsucht das PIX von 171.68.118.100 bis 9.9.9.25.

```
(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 eine heruntergeladene Webseite.

Notieren Sie sich die Uhrzeit. Dieser Download dauerte eine Sekunde (es gab weniger als eine Sekunde zwischen dem Start und dem Stopp Record). Ist der Benutzer immer noch auf der Website angemeldet und die Verbindung ist noch offen? Nein.

Funktionieren hier die max. Sitzungen oder die Ansicht der angemeldeten Benutzer? Nein, da die Verbindungszeit in HTTP zu kurz ist. Die Zeit zwischen "Built" und "Teardown" (der Datensatz "start" und "stop") liegt unter einer Sekunde. Es wird keinen "Start"-Datensatz ohne "Stopp"-Datensatz geben, da die Datensätze praktisch im selben Augenblick auftreten. Es wird immer noch "start" und "stop" Datensatz an den Server für jede Transaktion gesendet, unabhängig davon, ob die Authentifizierung auf 0 oder etwas Größeres festgelegt ist. Die maximale Anzahl von Sitzungen und die Ansicht der angemeldeten Benutzer funktionieren jedoch aufgrund der Art der HTTP-Verbindungen nicht.

Verwendung des Befehls "Except"

Wenn in unserem Netzwerk entschieden wird, dass ein ausgehender Benutzer (171.68.118.100) nicht authentifiziert werden muss, können wir Folgendes tun:

```
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+
```

Authentifizierung des PIX selbst

Die vorige Diskussion betrifft die Authentifizierung von Telnet- (und HTTP-, FTP-) Datenverkehr über das PIX. Mit 4.2.2 können auch Telnet-Verbindungen zum PIX authentifiziert werden. Hier definieren wir die IPs von Boxen, die Telnet mit dem PIX verbinden können:

```
telnet 171.68.118.100 255.255.255.255
```

Geben Sie dann das Telnet-Kennwort ein: **passwd ww**.

Fügen Sie den neuen Befehl hinzu, um Benutzer zu authentifizieren Telnetting zu PIX:

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

Wenn Benutzer Telnet an den PIX anschließen, werden sie zur Eingabe des Telnet-Kennworts aufgefordert ("ww"). Der PIX fordert außerdem den TACACS+- oder RADIUS-Benutzernamen und das -Kennwort an.

Ändern der Aufforderung für die Benutzer

Wenn Sie den Befehl hinzufügen: **auth-prompt YOU_ARE_AT_THE_PIX** wird die Sequenz von Benutzern, die den PIX durchlaufen, angezeigt:

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

Bei der Ankunft am Ziel werden die Aufforderungen "Username:" und "Password:" angezeigt. Diese Eingabeaufforderung wirkt sich nur auf Benutzer aus, die den PIX durchlaufen, nicht auf den PIX.

Hinweis: Für den Zugriff auf das PIX gibt es keine getrennte Buchhaltung.

Zugehörige Informationen

- Produkt-Support für die Cisco PIX Firewall
- Cisco Secure PIX Firewall - Befehlsreferenzen
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems